ING Bank Śląski S.A. Information on the processing of personal data

(Privacy Statement of ING Bank Śląski S.A.)

I. Explanation of the names used, legal basis for the information:

We, i.e. the Bank - ING Bank Śląski Spółka Akcyjna with its registered office in Katowice. Detailed information about the Bank, including the Bank's registration in the court register, the Tax Identification Number and the address of the KNF Board, which is the supervisory authority, can be found at the bottom of each page of this statement (known as the footer) and at www.ing.pl.

You, i.e. the Customer - an individual whose personal data the Bank processes for at least one of the purposes indicated in this statement. We have taken the liberty of using a direct phrase to increase the clarity of the text. For the purposes of this statement, a *Customer* is:

- both a natural person who was or is or will become a party to a legal transaction/relation performed with the Bank's participation, regardless of its type, or who submitted applications, forms for services offered by the Bank, as well as their heirs or legatees, or beneficiaries whose data are indicated in the documentation available to the Bank. The group of *Customers* includes persons with whom the legal form of security established in favor of the Bank is attached,

as well as

- attorney, user, legal representative or other representative. A *Customer* is also a natural person representing a legal entity or other entity who was or is a member of the bodies of such an entity, e.g., a member of the management or supervisory board, and a beneficial owner.
- In addition, a *Customer* is also understood as a person whose data is or will be processed in the future for marketing purposes, in particular in connection with the preparation or transmission of commercial information or offers.
- *A Customer* within the meaning of this statement is also a person who uses the Bank's websites or services, as long as the Bank processes his/her personal data. In the case of using social media, the Bank provides separate information on the processing of personal data.

Legal basis

The statement is prepared in accordance with Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016, OJ EU L.2016.119.1 of 4 May 2016, applicable as of 25 May 2018 (hereinafter referred to as the Regulation).

II. Bank - the controller of your personal data, contact details of the Bank and the Data Protection Officer.

ING Bank Śląski S.A. is the controller of your personal data. The Bank has its registered office in Katowice postal code 40-086, ul. Sokolska 34, Poland, website: www.ing.pl, the Bank's email address: info@ing.pl, Hotline no: 32 357 00 69 (for Individuals), 32 357 00 96 (for Entrepreneurs), 32 357 00 24 (for Companies). The Bank conducts operations in accordance with its Articles of Association, including brokerage activities in an organizationally separate Brokerage Office of ING Bank Śląski S.A.

The Bank's Data Protection Officer can be contacted:

- in writing to the Bank's postal address, preferably with the addition reading "Data Protection Officer"

- electronically to the e-mail address: abi@ing.pl.

Other means of contact may be indicated at ing.pl.

III. Supervisory authority for personal data. Right to lodge a complaint with the supervisory authority.

The supervisory authority for personal data in Poland is the President of the Office for Personal Data Protection address ul. Stawki 2, 00-193 Warsaw. You have the right to lodge a complaint with the supervisory authority.

IV. Data sources and categories of data processed.

Data sources

- we obtain data directly from you when you fill out applications or forms, when you enter into contracts or perform other activities, when you contact us or we provide commercial information,
- we obtain data from legal entities or other entities that you represent or that have designated you as a contact person,
- from other available sources, such as, for example: land and mortgage registers, commercial registries, business registries, debtor registries, Credit Information Bureau, business information bureaus, social/internet or traditional media, cookies and comparable technologies (https://www.ing.pl/indywidualni/tabele-i-regulaminy/regulacje/polityka-plikow-cookie), publicly available sources, other ING companies or institutions, state or local government bodies or offices.

Categories of data processed

- We process identification data, e.g.: first and last name, date and place of birth, PESEL number, e-mail address, telephone number, title, nationality and signature specimen, tax identification number , residence/correspondence address, parents' names, mother's family name, ID numbers and series. The data may also include biometric data.
  We check whether the data is consistent with the data provided or received from relevant documents, records or lists, as well as with the device identification data (e.g., phone number, IP, email, mobile device numbers) used by the Customer.
- We process data on marital status and family situation, also on dependents (e.g. children), in a common household, gender, education.
- We process identification data to check and verify identity. We process biometric data when the prerequisite provided by law is met, such as the express consent of a specific person. We process data on marital status or family situation (children's data) for the purpose of performing e.g. loan agreements, mortis causa instructions, or when it is related to a service offered by the Bank or another activity (e.g. social benefits (e.g. 800+).
- We process transactional data. This is data which makes it possible to process a specific transaction or which is related to its identification or processing, such as the bank account number, possible deposits, withdrawals and transfers made from or to the account, the date and place of their execution, transaction identifiers and related information.
- We process financial or service-related data, e.g. information about your financial or asset situation, data on your assets or liabilities, data determining your creditworthiness and reliability, accounting documents, credit history, creditworthiness, tax status, income and other income and/or your financial products at ING, entry in relevant registers, arrears, data

on electronic payment instruments, such as card number, expiration date or card verification code (CVV/CVC), phone number.

We process transactional data and financial data in connection with the provision of services, in order to perform the agreements concluded by the Bank, as well as to comply with applicable laws and regulations (e.g. banking law, commercial law, anti-money laundering and anti-terrorist financing law).

- We also process data on business, professional or social activities. It is data or information about such Customer's activity required or related to a service or product offered by or through the Bank.
- We process personal search data on the websites we administer. This is data such as: the IP address or ID of your mobile device or computer. They are processed in accordance with the Cookie Policy, which is available at https://www.ing.pl/indywidualni/tabele-i-regulaminy/regulacje/polityka-plikow-cookie and this statement, unless individual websites indicate other statements. Data may be processed on the basis of a separate consent or in accordance with the law.
- We process data relating to interests, needs or behavior. This data is data analyzed for the purpose of providing the service on the basis of consent (e.g., to provide profiled commercial information or to complete a survey or to use websites or services), on the basis of legal provisions obliging us to analyze particular behavior, e.g., anti-money laundering act, another legal basis, or laws mandating analysis of transactions to prevent crimes, to implement sanctions imposed by competent authorities or relevant laws.
- We process audio-visual data, e.g. recordings related to the security of property or assets (video surveillance), recording of conversations or video calls or chats conducted primarily with our customers or employees. Video surveillance data is processed on the basis of legitimate interest (which you can find at https://www.ing.pl/indywidualni/tabele-i-regulaminy/monitoring-wizyjny).
- We process location data or other data needed to use the Bank's services and communicate with the Bank, e.g., through a mobile application or when withdrawing cash from an ATM. Location data may be processed on the basis of laws that relate to the monitoring of transactions (the obligation is also performed by the location of the devices with which the transaction is ordered, e.g. we check when a card payment was ordered in different locations, in short time intervals) may result from the terms of performance of a particular service/contract or may be processed on the basis of consent.
- We process personal data related to interactions with ING on social media such as: Meta (Facebook), Instagram, Twitter (Social Network X), Linkedin or YouTube. We monitor public messages, posts, likes and replies directed to and about ING online. Data related to social media interactions are processed on the basis of the Bank's legitimate interest or the Customer's consent (see separate information on this matter at https://www.ing.pl/_fileserver/item/1130538).
- In certain cases, we may process sensitive personal data (special category data). This is a broad group of data that includes personal data relating to health, ethnicity, religious or political beliefs, genetic or biometric data, but the Bank may only process data that is necessary for one of the purposes described in this statement. We process such data on the basis of your separate express consent or where permitted by law for the purposes described below (e.g. on the basis of consent) or where we are required to do so by applicable law.

Furthermore, the Bank may process other personal data delivered by the Client provided that they cannot be classified to any of the groups specified hereinabove and are processed for the purposes specified in this document.

V. Purposes of personal data processing, legal basis for processing.

The Bank processes data for the following purposes:

1. Purpose of performing activities in accordance with the consent given - e.g., for marketing purposes or credit assessment and risk analysis after the expiration of the commitment. As regards minors (above 13 years of age), trade information is transferred for marketing purposes after obtaining consent from a parent or guardian (statutory representative). Personal data may be combined and further processed for marketing purposes when using publicly available websites upon acceptance of relevant declarations/consents or policies.

   Based on your consent, we process your data for marketing purposes, which include transferring, displaying or sending:

   - commercial information, including on electronic or telephonic communication devices that the Bank identifies as yours. These activities may also be performed via systems that transfer this information automatically,
   - by means of traditional mail commercial information,
   - profiled commercial information. This involves combining your data with information about your economic situation, your characteristics or behavior, or your preferences in order to tailor commercial information to your known or anticipated needs or expectations (known as profiling).

   as well as

   - geolocation for marketing purposes of your electronic communication devices to send commercial information.

   Commercial information - is any form of advertising, promotions, contests and games of chance, as well as commercial offers or purchase proposals. It may concern: promotion of the image, services or products of the Bank or other entities whose services or products are offered by the Bank or relate to the Bank's business. Trade information may be profiled or non-profiled. You can opt out of profiled marketing at any time. The Bank may process data for marketing purposes on the basis of the Customer's consent or on the premise of the Bank's legitimate interest, except that if data is processed on the basis of consent and it is withdrawn, the Bank will not process the data for marketing purposes unless the Customer has given a different consent. Consents or mandates are given on the following legal grounds: Regulations, community law (European Union law) or Polish law applicable to banks or acts, secondary legislation specifically concerning a given consent/mandate, including: banking law, act on trading in financial instruments, act on provision of economic information, act on provision of electronic services, telecommunications law;

2. Purpose of processing the application or activities preceding its submission, or related to the execution, performance or termination of the contract and the performance of other activities related to the contract, including pre-contractual activities.

   These are: analysis, risk assessment, other activities in the process of concluding, performing or terminating the agreement.

   This may also include other activities or statements related to the contract, including those related to security for repayment of obligations, or activities or statements related to the representation of an individual (e.g., power of attorney or actions of a parent/guardian, data

derived from records or lists of data of such persons in these entities or entities affiliated by capital or persons, which are collected or provided in connection with the execution or performance of contracts), including activities of the representative himself/herself, as well as activities commissioned by other entities, but related to Customer service. We mean all agreements or activities, also the ones we perform on behalf of other entities or for them.

Activities also include services related to the performance of contracts such as performing a specific service (e.g., consulting and advisory services as provided for in an Internet banking system contract), making payments or investments, providing access to account statements, fixing any product dysfunctions, handling complaints, requests and grievances, contacting for notifications related to a specific contract/legal transaction, e.g., regarding security interests or repayment of liabilities. We may also need an additional consent or launch a specific service or function to perform some services for you, e.g. geolocation of ATMs or bank outlets in the application;

3. Purpose of performing a legal obligation. Such obligations result from the law, including: community law (European Union law) or Polish law applicable to banks, e.g. banking law, act on trading in financial instruments, consumer credit act, act and other regulations on providing payment services.

   These are, in particular, the obligation to maintain the security of the funds stored, or the obligation to transfer and retrieve data to/from information databases related to the assessment of Customers' capacity or creditworthiness, or risk analysis, or related to the processing of beneficial owner data.

   These obligations may also arise from the banking law, competition and consumer protection law or other laws that provide requirements to adapt the services offered to consumers to their characteristics or to propose the adequacy of these services.

   Furthermore, the Bank is required to discharge obligations resulting from tax law, companies and partnerships law as well as regulations concerning trading in financial instruments, accounting and archiving regulations.

   The Bank also acts as an obliged institution, within the meaning of the laws concerning counteracting the acts prohibited by law or imposing obligations to keep transactions secure, by performing obligations of identification and verification or monitoring of economic relations (e.g. they result from regulations concerning counteracting money laundering and terrorism financing or regulations on payment services security).

   The Bank is also required to use statistical methods or models provided for by relevant laws. We take these actions as part of external (towards other entities) or internal reporting obligations.

   Their performance is legally grounded in community law (European Union law) or Polish law concerning banks, including banking supervision law and laws stipulating the duties towards regulators, National Bank of Poland, stock exchanges, accounting and bank management laws, while in terms of management the Bank is required to comply with the recommendations issued by regulators for the banking sector or a given business pursued by the Bank. These obligations may arise from the Commercial Companies Code, Banking Law or the Payment Services Law or the Financial Instruments Trading Law or the Public Offering Law, as well as the Competition and Consumer Protection Law or laws relating to the activity in question, including special laws such as insurance law.

The Bank has the right to process data in order to comply with obligations under the law explained in recommendations or recommendations issued by competent authorities or institutions.

4. The purpose of performing tasks in the public interest - to the extent of the law and the activities undertaken;

5. Purposes performed on the basis of bank's legitimate interests, and such as:
   - ensuring the safety of persons (primarily Customers and employees) and property of the Bank. It also applies to Bank branches monitoring – while observing privacy and dignity of persons,
   - ensuring security of funds and transactions which is not required by law but by principles and policies adopted by the Bank,
   - the exercise or defense of claims or rights of the Bank or the entity the Bank represents; this purpose also includes the Bank's processing of data related to complaints, amicable proceedings, alternative dispute resolution or mediation that may be filed or initiated against the Bank or by the Bank or the entity the Bank represents,
   - relationship management and for marketing purposes, including profiled advertisements for specific Customers or groups of Customers,
   - transfer of data to the archive and archiving of documentation for the relevant period,
   - audits or investigation proceedings,
   - implementing business control mechanisms, management control, management analysis and economic data analysis, and ensuring the effective and efficient execution of internal business processes, including when these mechanisms or processes are changed as a result of the implementation of guidelines, recommendations, recommendations of supervisory authorities and laws that do not directly impose a legal obligation on the Bank;
   - other statistical or historical research, or scientific research,
   - business, economic or legal advice that is provided to the Bank,
   - maintaining, displaying websites or communicating through these websites. To do so, we deploy identification data such as IP number, device numbers or other data. Data are deployed in scope of and based on your consent or applicable laws, including telecommunication law or community law. These laws determine if and when data processing requires consent. They also describe how such consent is granted or revoked,
   - developing and improving our products, e.g. by obtaining your feedback on our products and services; to the extent not requiring consent under applicable laws

VI. Transfer of data to other entities.

Within the meaning of this statement
"*transfer of data*" may mean that the entity to which the data is made available will become the new controller, or will remain only the entity to which the Bank entrusted the personal data under the agreement, or the Bank's counterparty, entrusted the data to a subcontractor, under a relevant agreement with the Bank. We may transfer personal data to entities, institutions or authorities:

- which are authorized by law; these are, for example, judicial institutions, authorities established for the prosecution of crimes, supervisory authorities.
- which are other banks, credit or payment institutions or other competent institutions, in cases provided by law,

- to whom the transfer of data is necessary for the performance of a specific activity, e.g. a payment transaction or other service or contractual activity,
- that may obtain data based on your consent or mandate, or under a concluded agreement,
- that maintain databases for the purpose of credit capacity assessment or risk analysis. Currently, such entities include, for example, Biuro Informacji Kredytowej S.A. and the Polish Bank Association,
- clearing houses or other settlement or clearing entities, payment institutions or schemes, or entities represented by them. Entities (institutions) relevant for a recipient of a given transaction, to which we transfer data, may operate in Poland, countries of the European Economic Area or outside them. A given transaction type may require an entity operating in Poland, in the European Economic Area or outside it. Organizations operating outside Poland include: Society for the Worldwide Interbank Financial Telecommunication (SWIFT) with its registered office in Belgium. As regards card transactions, or transactions performed with other payment instruments, which are accepted by payment organizations – we transfer data to the card organization whose logo is on the card or the other payment instrument (e.g. Visa or MasterCard). These organizations operate in the European Economic Area, the UK and the US,

In addition, data may be transferred to consultants and service providers for the purpose of:

- establishing, exercising or protecting claims;
- cooperating with service providers or activities at our request. We carefully select such companies and enter into agreements with them. We remain the entity responsible for your personal data. Service providers provide us with support for, among other things, activities such as, for example, designing, developing, operating and maintaining online tools and applications, websites or social media, handling customer communications, printing materials, designing or testing services/products, archiving documentation, other support, consulting, or other specialized services provided by advisors, brokering services offered by the Bank;
- cooperating with research institutions, companies, universities that conduct research and use data for R&D purposes.

If it is possible given the purpose of the transfer, including entrusting of data, data will be shared at the aggregate level to ensure anonymity of, for example, the results of a survey or other development activities.

The Bank may transfer data to other entities as part of entrusting of processing while still retaining the function of their controller, or transfer data to other entities as separate controllers. If the recipient of the data, in accordance with the separately indicated legal grounds, is ING Bank NV, with its registered office in Amsterdam, the Kingdom of the Netherlands (ING Bank NV), then the information about the processing of the data by ING Bank NV, referred to as the Privacy Statement for Clients is posted on the Bank's website www: ing.pl/ochrona danych osobowych.

VII. Transfers of data outside the European Economic Area.

Note on safeguards

The Bank may transfer data outside the European Economic Area (EEA) to countries for which the European Commission has determined an adequate level of protection. In addition, where data is transferred outside the European Economic Area (EEA) to countries for which there is no decision of the European Commission stating an adequate degree of protection, the Bank shall apply appropriate safeguards in the form of:

- standard contractual clauses (standard data protection clauses) adopted by the European Commission or
- with respect to ING Group entities - binding corporate rules (Binding Corporate Rules).

In connection with the transfer of data outside the EEA, you may request information about the relevant aforementioned safeguards in this regard, obtain a copy of these safeguards or information about where they are available by contacting the Bank - contact details are described in Section 2 of this statement. In addition, the Bank may transfer personal data to third countries (outside the EEA) that do not meet the appropriate safeguards listed above only in cases provided by law, e.g., in order to perform financial operations, processing is necessary for the performance of the contract (e.g., foreign transfer at the request of the Customer) or when you give your consent or the transfer is necessary for the establishment, exercise or defense of claims.

VIII. Know your rights towards the Bank.

You have the right to:

- request from the Bank access to personal data concerning you and
- the right to rectify them when they are inconsistent with the actual state of affairs, and moreover
- in cases provided by law to request erasure of data,
- in cases provided by law to request restriction of data processing,
- object to the processing of data in cases provided for by law. The objection will be considered by the Bank, except that if the objection relates to the processing of data based on the premise of legitimate interest we examine whether there are overriding legitimate grounds that may exceptionally justify the processing of data. The objection may concern a specific purpose of data processing. Objections to data processing for marketing purposes are always taken into account by the Bank, except that if at the same time you maintain other consents or consent to data processing for marketing purposes or in the course of processing your objection or later give such consents we will ask you about your decision.
- Withdraw consent because you give all consents voluntarily. You may withdraw all or some consents to personal data processing at any time. The withdrawal mode is specified for a given process. A data processing consent may be necessary for a given activity. The withdrawal of a consent does not impact the Bank's right to process data for the purpose stated therein before its withdrawal. It is also possible that the Bank will be legally authorized to process data on another legitimate basis or for another purpose.
- In addition, you have the right to data portability or to obtain a copy of the data, with the proviso that this right must not adversely affect the rights and freedoms of others, including trade secrets or intellectual property, to the extent of the request to send directly to another controller, this right will be exercised to the extent technically possible. The first copy of data is free of charge. To transfer data under other provisions, e.g. banking law, it may be necessary to obtain a consent from the Client or another person or to meet other conditions as required thereunder. The right of data portability applies to data processed by automated means.

Requests concerning exercise of rights may be filed by the Client electronically as described in the online banking system or in writing. Submission of such requests by telephone will be permitted, provided that the Bank, for the execution of a given right, makes such a process available, taking into account the requirements for verification of the Customer's identity. The Bank may request that information or activities concerned be clarified. By performing the request for data transfer or obtaining their copy, the Bank transfers them and communicates the electronic format or carrier

used. The Client having access to the Bank's online banking system will also have access to their data in that system.

Whether the provision of data is a statutory or contractual requirement

Personal data must be provided to conclude an agreement. In addition, provision of data is also necessary for the Bank to perform transactions or accept documents (e.g., granting a power of attorney, giving mortis causa instructions) or to perform other transactions. The provisions of law may require the provision of data for the purpose described therein (e.g., the Anti-Money Laundering and Terrorist Financing Law requires identification and verification of identity). Should the Client not provide the data required by the agreement or another document used by the Bank under its procedures or law, the Bank will not enter into the agreement with them or will not perform a transaction or activity.

IX. Automated decision-making and profiling.

Terms:

In this statement, we use the terms "automated data processing" and "profiling" as they appear in the GDPR Automated processing involves a decision-making process using technological means without significant human involvement that may involve legal consequences or similarly materially affect you (we refer to it as an automated decision). The Bank may profile your personal data. This means that the Bank processes your personal data in an automated manner and uses it to evaluate certain personal factors, in particular to analyze or forecast aspects of your work performance, economic situation, personal preferences, interests, reliability, behavior, location or movement.

Decisions based on automated data processing, including profiling

The Bank may make decisions based solely on automated processing of personal data, including profiling, which may involve legal consequences or similarly materially affect you. These decisions are based on relevant information that depends on the type of activity. They may be undertaken for preparation, processing of applications or provision of:

- Services for loan processes - relevant information that affects the automated decision, including using profiling technology, is information that affects your credibility and creditworthiness and credit risk analysis; we assess your ability to meet your financial obligations to us and to avoid offering you a loan that is unsuitable for you. Risk is assessed in points (scoring). The automated decision takes into account the current and projected financial situation. We process data by accessing information from external databases to obtain relevant financial information (financial statements, turnover/insolvency, payment history). If you have already cooperated with us we combine external financial information with your internal payment history (taking into account the applicable retention period). If the analysis on a credit product that applies to you (including in connection with a projected security) shows that the risk is too high, a decision based on automated data processing, including profiling, will be negative.
- The result of a credit analysis (scoring) may also be necessary for the preparation of a marketing offer, but then it occurs in connection with the consent to provide commercial information. If we believe your scoring does not meet the minimum requirements we will not provide you with an offer/proposal or commercial information.
- Services for the processes of providing deposit services, e.g., account maintenance or deposit services, investment services or electronic services (Internet banking system) - relevant information is, in the Bank's possession, information about the financial or asset situation

that may affect the terms of the activity or service or the content of the information or consultation provided.

- Settlement or transaction services in order to perform activities necessary to enter into a contract or perform a transaction. We analyze the circumstances of the transactions such as the NIP, unusual place of the transaction order, unusual types of orders, unusual (usually too high) amounts. The effect of the decision may be the suspension or refusal of the transaction, of which you will be informed as the Customer/authorized person, in accordance with the relevant agreement.
- Obligations regarding statistical methods and models; in accordance with the law, the Bank is required to develop and implement statistical methods and models; this includes credit methods and models to calculate counterparty risk and exposure. This allows ING to determine our risk and the range of relevant capital or financial ratios we are required to maintain. Methods and models may not process personal data, but their creation may require personal data since they must be reliable.
- Analysis related to the performance of regulatory obligations, including the performance of obligations under anti-money laundering and counter-terrorist financing regulations. The Bank is required to prevent the use of its activities for purposes related to this crime and to apply financial security measures. The measures are those described in the Anti-Money Laundering and Counter-Financing of Terrorism Act. Accordingly, we pay special attention to unusual transactions and to transactions that, by their nature, result in a relatively high risk of fraud, money laundering or terrorist financing. If there is a suspicion that a transaction is related to money laundering or terrorist financing, we are required to take appropriate action as prescribed by law, which may include refusal to execute the transaction or reporting it to the competent authorities.

  Examples of factors that we take into account as potentially indicating an increased risk of fraud or money laundering and terrorist financing: changes in a person's standard payment and expense behavior, for example, transferring or crediting unexpectedly large amounts; two PIN payments made by a single person in two significantly distant locations at the same time.

The right to express your view, appeal against an automated decision, including profiling

You have the right to express your view and challenge a decision based solely on automated data processing, including profiling, which may involve legal consequences or similarly materially affect your situation. Challenging a decision will mean appealing it. You can file an appeal just as you would a complaint in a given case. Such an appeal will be considered by a Bank employee. Upon your request, the Bank will provide applicable explanations about the rules of decision-making and the consequences of profiling while maintaining legally protected secrecy (e.g. bank or regulatory secrets or company secrets). If the law (e.g., banking law) so provides, the Bank will, based on the relevant application and in accordance with a separate instruction, prepare an explanation of its assessment of the applicant's creditworthiness.

X. How long will the Bank process the data?

1. The data processing period depends on the purpose wherefor the data were collected and are processed. It also depends on the laws as well as your consents and declarations. The basic period of data processing - for the time necessary to process the application, prepare for the performance of the activity in question does not exceed the archiving period of documentation,

which is 6 (six) years, except that this period ends on the last day of the calendar year, unless the law provides for a different period.

2. Notwithstanding the principles described in point 1, specific processing periods are related to:
   - application for a loan process - if the agreement has not been successfully executed, the archiving period for the application for this transaction is 1 year from the date of the application, unless the law for such archival data provides for a different period for a specific purpose of processing, or in the subsequent period when the Bank is processing your request regarding this application and arising from the law;
   - our calculations of financial ratios and capitals, including the statistical methods set for the Bank (generally referred to as methods and models). In keeping with the banking law, the period of information processing under methods and models is 12 (twelve) years form the liability expiration date;
   - if there is a dispute, lawsuit or other proceedings (especially criminal proceedings) in progress, the archiving period will be calculated from the date of the final conclusion of the dispute, and in the case of a number of proceedings, from the final conclusion of the last one.
   - court decision - data may be processed during the period of limitation of claims (i.e. the period when claims can be effectively pursued in court) The general limitation period is 6 years from the date of the final and non-appealable decision, except that individual claims may be subject to special provisions indicating other limitation periods;
   - Customer consent – for the period stated in the consent document or in any case until such consent is revoked;
   - obtaining data from databases maintained by other entities or data provided by other entities, such as Biuro Informacji Kredytowej S.A. (BIK SA), to assess capacity and analyze credit risk. The Bank processes the inquiry regarding your person directed to BIK SA, which is submitted for the purpose of obtaining a credit report. We process this request for a period of six months after it is sent. The report is used for capacity assessment and credit risk analysis and is processed for archival purposes for 3 years.

The said periods do not add up. The data may be processed separately for individual purposes and on different legal grounds; e.g. a given data processing consent for marketing purposes can be revoked, but this does not deprive the Bank of the right to process data for another purpose or under different legal grounds.

XI. Final Provisions.

This Statement supersedes ING Customer Privacy Policy (v.2.1) with respect to the processing of data of persons who use our websites or online services, insofar as the Bank processes your personal data as a result of such use.

For more information or to exercise the rights described in this statement, or if you suspect a breach of your data protection, please contact us using the contact information provided above in this statement or at ing.pl

We reserve the right to make changes to this Statement. Changes may result from provisions of law and/or reflect changes in the Bank's processing of personal data. This version was created on 20/03/2024.