

Erste Bank a.d. Novi Sad, Industrijska 3J, TIN: 101626723, REG. NO.: 08063818 (hereinafter: Bank) is, in accordance with the business activity performed, **personal data controller**.

As the controller of personal data of its clients and other persons whose data are necessary to the Bank for the execution of its business obligations, the Bank is responsible for the protection of such data, **in accordance with the Personal Data Protection Law ("Official Gazette of RS", no. 87/2018), applicable from 21 August 2019.**

For any issues and for exercising your rights in connection with processing of your personal data, please contact the Bank through all regular communication channels (visit to branch, calling call center, etc.) or directly contact **Personal Data Protection Expert by e-mail address** dpo@erstebank.rs.

Correct Understanding of Key Terms Is Important

Personal data mean any data relating to a private individual whose identity is, directly or indirectly, determined or determinable, in particular, based on identity designation, such as name and identification number, as well as based on data on location, identifier in electronic communication networks, or one or several features of his/her physical, physiological, genetic, mental, economic, cultural, and social identity.

Personal data processing is any automated or non-automated action or a set of actions with personal data or their sets, such as collection, recording, classification, restriction, deletion, or destruction, etc.

Profiling is any form of automated processing used to assess specific personality feature, in particular, aimed at the analysis or forecasting work performance of private individual, his/her economic position, health status, personal affiliations, interests, reliability, behaviour, location, or movement.

Controller is a private individual, legal entity, or public authority which, individually or jointly with others, sets out processing purpose and method.

Processor is a private individual, legal entity, or public authority processing personal data on behalf of controller.

Which Data Are Collected and Processed by the Bank?

In its operation, personal data are processed by the Bank for the purpose of entering into and executing agreement with client, as well as for the purpose of meeting obligations set out in law and other regulations. Implementation of business relation with the Bank is not possible unless obligatory data relating to particular business are collected and processed.

The first group of data are those the **Bank must process based on various regulations** governing its operation (fulfilment of statutory obligation of the Bank). Those are identification data from valid ID, as well as other data which the Bank is obligated to collect in accordance with the Law on the Prevention of Money Laundering and Terrorism Finance and other applicable regulations, as follows: name and surname, address of domicile or place of stay, personal identification number, date, place, and state of birth, nationality(ies), name and number of ID, including the name and state of issuer thereof, document validity period, as well as validity of residence permit, data relating to non-RS tax domicile, and other data, in accordance with the above-mentioned Law. If you perform business activity (entrepreneurship or self-employed activity), basic data collected by the Bank are data from competent register, as follows: name, address of head office, and registration number.

Other data group processed by the Bank are **data the processing of which is necessary for the purpose of the execution of agreement** with data subject or to take actions upon request of data subject, prior to agreement execution. In specific case, these data depend on service/product agreed and/or used, whereby strict care is taken by the Bank to be in compliance with the "data minimum" principle (only those personal data necessary for respective processing purpose are processed).

For products and services with credit exposure towards the Bank, data for credit risk management by the Bank are necessary, in particular, data on client's property, household members, income and employment, and if you perform self-employed activity, they also include status data, financial data on business, and similar data.

Other data necessary for agreement execution may also be contact data, as necessary for the implementation of Bank service or product (e.g. e-mail address for netbanking service or mobile telephone number for the service of sending SMS on balance/turnover under account).

Contact data are voluntarily provided data, used for notification by the Bank, in the fastest and simplest manner, on facts and events significant for respective product or service you have shown interest in or which is used by you, and for providing other useful information/documentation by the Bank upon your request unless otherwise agreed or prescribed as the statutory obligation of the Bank. Such data include: address if it differs from the address of domicile or place of stay provided by you based on the law, telephone number, mobile telephone number, e-mail address. If you perform self-employed activity, such data include: address if it differs from the address of domicile, contact person name and surname, number of telephone, mobile telephone, fax, and/or e-mail address.

Grounds for Personal Data Collection and Processing

1. Business relation implementation and fulfilment of obligations set out in regulations.

Data are collected by the Bank directly from client when contracting or showing interest in services and products, using Bank products and services (for example: when using payment transaction service), as well as in any communication of client with the Bank (for example: call to contact center).

For the the purpose of implementing business relation and exercising the rights and obligations of the Bank set out in regulations, data are also collected by the Bank from publicly available registers, such as register of Business Registers Agency, Single Account Register, Credit Bureau, etc.

2. Personal consent to data processing

Based on consent granted, data included in statement on agreement are processed by the Bank solely for the purpose or purposes for which such consent has been granted. Consent for personal data processing for one or several specified purposes is completely voluntarily granted, therefore, consent granting and revocation do not impact agreement relating to use of the Bank products or services or realisation of already agreed products and services.

Data processing based on personal consent impacts continuing quality improvement of the Bank products and services, in particular, quality of managing your personal financial requirements.

Acceptance of data processing may be given for one or several specified processing purposes, such as:

- Creation of specific offers/recommendations of products, services, and options of their use (personalised marketing) in order for you, as the client, to efficiently manage your finance. For the above-mentioned purpose, data are processed by the Bank based on product and service use (for example: data on account balance, card use, data on visits to the Bank branches, etc.). The above-mentioned data processing may include creation of your profile on the grounds of the analysis of your personal interests, behaviour, and location. Such profiling is used to forecast your needs in order for the Bank to respond to such needs in a timely manner through relevant offer of products, services, or by giving recommendations.
- Temporary information on products and services, benefits, prize games, news, and changes in the operation of the Bank, Erste Group members, and business partners with which you may agree cooperation through the Bank (direct marketing) for the purpose of the availability of useful information on the Bank operation, products, and services which may be of interest to you.
- Improvement of the Bank products and services based on your requirements and expectations, based on results of interim surveys about your satisfaction and experience in connection with the use of the Bank products and services.

At any time, you may **withdraw (recall) your consent of data processing**, after which your data will not be processed by the Bank for the purpose approved based on your consent.

Consent may be withdrawn in the manner in which it has been granted, in writing, by mail, electronically to the address dpo@erstebank.rs or directly at the Bank teller desk. Also, you may withdraw your consent only partially, e.g. you may ask that marketing material is sent only through particular communication channel.

3. Legitimate interest of the Controller in the processing of personal data

For the realization of the Bank's legitimate interest, the processing of personal data may also be carried out for the purpose of:

- Review and analyze data in order to optimize customer needs and offers, as well as to improve the services offered by the Bank;
- Implementing the most adequate and efficient business management and enabling further development of services and products;
- Enabling IT security and IT operations of the Bank;
- Further development of the functionality of our services, such as applications;
- Ensuring the protection of clients and employees, as well as for securing the Bank's assets and for the prevention and investigation of abuses;
- Undertaking activities (including data assessment, e.g. payment transactions) to monitor and prevent fraudulent transactions, prevent money laundering and terrorist financing and criminal offences;
- Video surveillance for the purpose of gathering evidence in the case of a criminal offence or as evidence of the execution of a transaction (such as ATMs and bank premises that are publicly available) – in particular with a view to protecting clients and employees.

Automated Decision Making and Profiling

Regarding its business relation with client, automated, individual decision-making resulting in adverse legal consequences to the client is not used by the Bank.

For clients using products and services with credit exposure, the Bank has the statutory obligation in accordance with the Bank Law and relevant by-laws to calculate credit rating. Credit rating is determined by comparing statistical models on the grounds of available data, among all, data collected from client, data on products and services used by client, as well as whether liabilities are settled at maturity.

Data of Proxy Holders, Legal Representatives, and Legal Entity Beneficial Owners

Identification data from valid ID and other basic data must be directly collected and processed by the Bank, in accordance with the Law on the Prevention of Money Laundering and Terrorism Finance, for legal representative of minor client/person under guardianship, legal entity's legal representative; and legal entity's beneficial owner, and for person performing self-employed activity, as follows: name and surname, address of domicile and/or place of stay, personal identification number, date, place and state of birth, ID name and number, including the name and state of issuer, nationality(ies), and other data prescribed in this Law.

Without above-mentioned data, the Bank is not able to implement business relation through proxy holder or legal representative, or business relation with legal entity or a person performing self-employed activity.

Personal data processing and protection are based on the following principles:

- Principle of legality, fairness, and transparency
- Principle of restriction relating to processing purpose
- Principle of data minimising (it is permitted to process only those data which are obviously necessary and appropriate for achieving statutory processing purpose);
- Principle of accuracy (also includes obligation of updating, correction, and deletion of incorrect data)
- Principle of restricted retention (retention only within the term necessary for the realisation of processing purpose)
- Principle of integrity and confidentiality (relevant protection, IT; technical, organisational, and human resources measures).

Who Are Data Provided to by the Bank?

Particular data processing is performed by the Bank using providers' services, applying relevant technical and organisational personal data protection measures, e.g. providers of IT services, archiving, printing and sending letters to clients, card transaction processing service, card and PIN making (personalisation), etc.

Service providers of the Bank as processing controller have the capacity of processors in relation to personal data, therefore, care is taken by the Bank that such service providers are always from the Republic of Serbia, EU, or the states which are the members of the Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, pursuant to the Personal Data Protection Law.

The Bank is entitled to forward personal data relating to a person, as well as data on his/her related persons, documentation relating to person, as well as other data to:

- Members of its bodies, its shareholders, Erste Group members the updated list of which may be found on the following web page <https://www.erstegroup.com/en/about-us>
- Bank's external auditor,
- Serbian Bank Association Credit Bureau,
- National Bank of Serbia,
- Other public authorities and persons who, due to the nature of the work they perform, must have access to such data, in accordance with the Bank Law.
- Third parties with which the Bank has entered into Agreement setting out treatment of confidential data, solely in accordance with the above-mentioned principles.

Data Processing Security

A series of technical, human resources, and organisational protection measures are performed by the Bank to ensure relevant level of security of processing your data, in accordance with the Personal Data Protection Law.

Personal Data Retention Term

Data collected for the purpose of exercising the rights and obligations from business relation will be processed by the Bank as long as the business relation of the Bank and respective data subject lasts, save in cases when the Bank is obligated to retain data for a limited period after the termination of business relation with data subject, based on the law, consent by data subject, and legitimate interest of the Bank (e.g. in the event of any dispute of respective data subject and the Bank).

Personal data processed solely based on consent by data subject are processed only within the period necessary for the fulfilment of processing purpose for which consent has been granted, or until the revocation of consent by data subject.

Rights of Data Subjects in Connection with Personal Data Processing?

Data subject is **entitled to access** personal data processed by the Bank.

In the cases provided for in the Personal Data Protection Law, data subject is **entitled to request data correction, updating, deletion**, as well as **processing** restriction. Under the conditions stipulated in the Personal Data Protection Law, data subject is **entitled to personal data transferability** i.e. to receive from the Bank any data which have been provided to the Bank by data subject, for the purpose of transfer to other controller, direct transfer of data subject's data by the Bank to other controller if it is technically feasible and, based on the assessment by the Bank, necessary personal data transfer security standard has been ensured.

If deemed reasonable in terms of particular situation, data subject whose data are processed is entitled to, at any time, provide the Bank, as the controller, with **complaint regarding processing** of his/her personal data, in accordance with the Personal Data Protection Law, also including profiling based on such Law.

Request for exercising his/her rights are filed, by client and/or person whose data are processed, to the Bank in writing, by mail, electronically to dpo@erstebank.rs or zalbe.stanovnistvo@erstebank.rs or directly at the Bank teller desk by completing particular form for respective request.

The Bank must provide the client and/or person whose data are processed with information based on his/her request, no later than 30 days from the date of request receipt. Such deadline may be prolonged by further 60 days, as necessary.

If the Bank fails to act upon request of person whose data are processed, it must, without any delay, notify such person on reasons of such failure within the term stipulated in the law and instruct such person **on his/her right to file complaint to the Commissioner** or to file claim to respective court.