

GENERAL INFORMATION ON THE PROCESSING OF PERSONAL DATA (CLIENTS)

NLB Banka a.d. Banja Luka (hereinafter: **the Bank**) continuously works on improving its banking services in order to better tailor them to clients' needs and expectations. In that process, certain personal data that are collected and processed enable the provision of more relevant information, more efficient communication, and a higher-quality customer experience.

The Bank, as the controller, processes personal data relating to the Bank's clients who are natural persons and other persons (e.g., authorized representatives, agents of clients, prospective clients, etc.) whose data are processed in the course of providing banking products and services. The processing of personal data is carried out in accordance with the Law on the Protection of Personal Data ("Official Gazette of Bosnia and Herzegovina", No. 12/2025, hereinafter: **the Law**) and other regulations governing matters related to the processing of personal data.

The privacy of clients and other persons is of utmost importance to the Bank. The Bank applies the highest standards of personal data protection, ensuring confidentiality and integrity. Protection measures include, but are not limited to, technical, organizational, legal, and procedural safeguards in accordance with applicable regulations.

The Bank's employees are obliged to respect the confidentiality of clients' data, and data security is also ensured through the Bank's internal acts regulating the protection of confidential information and personal data.

In order to ensure transparent processing of personal data and in line with the principle of transparency, the Bank provides general information regarding the processing of personal data, personal data protection, and the rights of data subjects.

1. BASIC DEFINITIONS

Personal data - any information relating to an identified or identifiable natural person.

Data subject - a natural person whose identity is identified or can be identified, directly or indirectly, in particular by reference to an identifier such as a name, identification number, location data, online identifier, or one or more factors specific to the physical, physiological, genetic, mental, economic, cultural, or social identity of that person;

Processing of personal data - any operation or set of operations performed on personal data or sets of personal data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure, or destruction (hereinafter: **processing**).

Controller - a natural or legal person, public authority, or competent body which alone or jointly

with others determines the purposes and means of the processing of personal data.

Processor - a natural or legal person or public authority that processes personal data on behalf of the controller.

2. INFORMATION ON THE BANK AS CONTROLLER AND CONTACT DETAILS OF THE DATA PROTECTION OFFICER

NLB Banka a.d. Banja Luka
Milana Tepića 4
78 000 Banjaluka
www.nlb-rs.ba
nlbinfo@nlb-rs.ba

The bank has internally established a position and appointed a **personal data protection officer (DPO)**.

The Bank will consider your inquiries regarding the processing of personal data and enable you to exercise your rights as prescribed by the Law. For this purpose, you may contact us as follows:

- by email: dpo@nlb-rs.ba;
- by post to the Bank's registered office: Milana Tepića 4, 78000 Banja Luka, Republika Srpska/BiH– marked "for the DPO";
- by telephone: [0800 50510](tel:080050510).

authorities, handling complaints, applying tax regulations, etc. Consent of the data subject is not required for processing that is necessary for compliance with the law and the Bank's statutory obligations.

3. LEGAL BASIS AND PURPOSE OF DATA PROCESSING

The legal bases for data processing are prescribed by the Law, and the Bank is obliged to determine, for each processing purpose, the legal basis under which such processing is carried out.

The purpose for which the Bank processes personal data depends on the type of product and services for which the data subjects apply or which have been contracted. Such data are processed to fulfil the purpose for which they are collected.

Accordingly, the legal bases and purposes of processing under which the Bank processes personal data are set out below:

a) Performance of a contract or pre-contractual obligations

Processing is necessary for the conclusion and performance of a contract on the use of the Bank's products and/or services (e.g., opening an account, activation and use of payment cards, approval of loans, deposits, processing payment orders, deposits and withdrawals and standing orders, use of the Bank's electronic services, sending mandatory notifications, collection of overdue receivables) or for the Bank to take certain steps prior to concluding a contract (e.g., processing requests to establish a business relationship with the Bank, preparing a loan offer, etc.). If a data subject refuses to provide the data necessary for this purpose, the Bank will not be able to conclude the contract or provide the requested service.

b) Compliance with the Bank's legal obligations as controller

The Bank processes personal data for the purpose of fulfilling obligations prescribed by laws and by-laws binding on the Bank (e.g., regulations governing banking operations, prevention of money laundering and terrorist financing, domestic payment operations, foreign exchange operations, risk management), as well as for the purpose of meeting the requirements of competent public

c) Legitimate interests of the Bank or a third party

In certain cases, processing is necessary to pursue the legitimate interests of the Bank or a third party, taking into account that the Bank's interests do not override the interests, rights, or freedoms of the person whose data are processed. The Bank relies on legitimate interest, for example, in the following situations, for the purpose of:

- communicating with clients to provide information, technical support, security notifications, and to improve the customer experience;
- measuring client satisfaction with the Bank and its products and services, including satisfaction after a service is concluded or a product is used, in order to improve the products and services offered by the Bank;
- planning, monitoring, and analyzing the implementation of sales activities of banking products, in order to improve sales, optimize processes, and make business decisions;
- monitoring and maintaining security in the Bank's premises in order to manage visitor movement within Bank facilities (or official visits and other bases in the Head Office and Branch 1 Banja Luka), including persons providing services to the Bank on various grounds, and to prevent unauthorized movement and possible criminal offences;
- receiving, recording, and reviewing donation requests, as well as deciding on and implementing the granting of donations by the Bank;
- processing data for the purpose of client segmentation, with the aim of offering products and services that better match the needs and preferences of specific client categories, etc.

Consent is not required for processing based on legitimate interest, but the data subject has the right to submit a request to exercise their rights at any time in the manner described in Section 11 of these General Information.

d) Consent of the data subject to data processing

For one or more specifically defined purposes, the Bank processes data based on the data subject's explicit consent. In such situations, the purpose of processing will be presented to the data subjects at the time consent is obtained, including:

- processing for the purpose of organizing and conducting a prize competition, including identification and contacting of winners, awarding and delivering prizes;
- processing for the purpose of direct marketing, including profiling to create and deliver personalized offers and information about products, services, and benefits tailored to your interests and needs.

Refusal to give consent does not affect the performance of a contract concluded with the Bank, compliance with the Bank's statutory obligations, nor processing based on the legitimate interests of the Bank or a third party, except where the law prescribes consent as a necessary condition for the performance of certain obligations.

Consent may be withdrawn at any time by submitting a request to withdraw consent in accordance with Section 11 of these General Information.

e) Personal data processed by the Bank in the role of processor

In addition to acting as a controller, the Bank also processes certain personal data as a processor based on contracts under which third parties have entrusted the Bank with specific personal data processing activities (e.g., as an insurance agent, etc.). In such cases, the Bank processes data solely on the order and instructions received from the controller, in accordance with the Law.

4. CATEGORIES OF DATA PROCESSED

Basic personal and identification data from identity and other documents: first and last name, father's name, marital status, date, place and country of birth, gender, unique personal identification number (JMBG), identification document data, residency indicator, etc. For certain products and services, identification data

are also collected from co-debtors, guarantors, pledgors, legal representatives, authorized representatives, etc.

Contact data: address, landline and/or mobile phone number, email address, etc.

Financial data: account number, IBAN, account status, contract number, expected monthly inflow/outflow, monthly income, additional income, data on liabilities from the Credit Registry (CRK) (amount, due obligations, start and end date, risk level, bank name, account/party number), savings data (amount, date of term placement, term period, account/party number), card number and status, card usage data (transaction date and time, amount, currency, authorization status), data on limits and changes in card status, digital wallet data (status, device type), data for U.S. clients.

Other types of data: education level, occupation, professional title, politically exposed person status (PEP), purpose of opening an account, data from FATCA/CRS questionnaires, as well as other data arising from the provision of banking products and services and required for such services.

5. METHOD OF COLLECTING PERSONAL DATA

The Bank collects data directly from the data subject and indirectly from competent institutions or other sources (e.g., public registers, publicly available information, etc.).

6. ACCESS TO PERSONAL DATA

Access to personal data processed by the Bank is granted to:

- a) Within the Bank** – employees who, given the nature of their work and the scope of work of the organizational unit, must have access to such data for the purpose of fulfilling contractual and legal obligations, as well as pursuing the legitimate interests of the Bank and third parties, and members of the Bank's management and supervisory bodies;
- b) NLB d.d. Ljubljana as the Parent Bank of the banking group and its supervisory bodies** – to whom the Bank provides personal data for the purpose of performing the Bank's regular operations, fulfilling obligations under contracts with clients, fulfilling legal

obligations, fulfilling other contractual obligations and implementing contracts, and pursuing the legitimate interests of the Bank, etc.;

c) State/entity authorities and institutions – (e.g., CBBiH, ABRs, IRBRs, Tax Administration, courts, etc.) to whom data are provided in order to fulfil legal obligations, for the purposes of conducting court proceedings, etc., and other legal entities where required by law;

d) Service providers to the Bank/processors to whom certain Bank activities have been outsourced or who provide services necessary for the performance of, or related to, the contractual relationship between the data subject and the Bank, as well as for fulfilling legal obligations or pursuing the lawful legitimate interests of the Bank. The Bank has concluded appropriate cooperation agreements with such entities that also regulate data processing in accordance with applicable regulations. Examples include insurance companies, law firms, and service providers for IT system maintenance, security of persons and property, receivables collection services, SWIFT services, and similar. These service providers/processors and their subcontractors are obliged to apply an adequate level of technical and organizational protection measures, bearing in mind that personal data constitute banking secrecy, and to act on behalf of the Bank solely in accordance with its instructions. The Bank provides access only to processors that guarantee personal data protection to the same extent as if the Bank processed the data itself.

7. TRANSFER OF PERSONAL DATA TO ANOTHER COUNTRY OR INTERNATIONAL ORGANISATION

The Bank processes personal data within the territory of Bosnia and Herzegovina. Transfers to other countries or international organizations are carried out where necessary for the performance of a contract or client instructions (e.g., the use of debit and credit cards involving international card organizations), for compliance with the Bank's legal obligations, or for pursuing the lawful legitimate interests of the Bank. Such transfers are carried out to processors and sub-processors

acting on behalf of the Bank and with whom agreements are concluded regulating data processing in accordance with applicable regulations, or to third parties (the Parent Bank, NLB d.d. Ljubljana). Transfers are made to EU Member States that ensure an adequate level of personal data protection, as well as to countries in the region – the Republic of Serbia and the Republic of North Macedonia – which are signatories to Convention 108+ (Protocol CETS 223) and for which it has been determined that they ensure an adequate level of protection, with the application of all appropriate technical and organizational protection measures.

8. AUTOMATED DECISION-MAKING, INCLUDING PROFILING

In some cases, the Bank applies automated decision-making, including profiling, for the purpose of assessing the performance of a contract between the data subject and the Bank, for example when approving an overdraft, a credit card, or a cash loan, and in accordance with the Law on the Prevention of Money Laundering and Terrorist Financing, when developing risk analysis models for money laundering.

In the case of automated decision-making, the data subject has the right not to be subject to a decision based solely on automated processing, i.e., has the right to request human intervention by the Bank in order to express their point of view and contest the decision.

9. PERSONAL DATA SECURITY

The Bank has established high-level information security management, which entails applying best practices derived from internationally recognized standards such as ISO/IEC 27001, ISO/IEC 27002, CIS, and others. In addition, the Bank treats all personal data as business and banking secrets and applies all reasonable and available technical and organizational protection measures in accordance with the law and internal acts.

10. DATA RETENTION PERIOD

The retention period depends on the legal basis and the processing purpose for each category of data. The Bank processes personal data collected for the purpose of exercising rights and obligations arising from a contractual relationship until that

relationship ends, and after termination, within the time limits prescribed by law, most commonly ten years (e.g., under the Law on the Prevention of Money Laundering and Terrorist Financing and the Law on Banks, etc.), on the basis of the data subject's consent (e.g., until consent is withdrawn), or for pursuing the lawful legitimate interests of the Bank, where a separate retention period is defined for each legitimate interest, necessary to fulfil the processing purpose.

11. RIGHTS OF DATA SUBJECTS

a) Right of access

The data subject has the right to obtain confirmation from the Bank as to whether their personal data are being processed and, if so, access to the personal data and information about the processing. Upon request, the Bank will provide a copy of the personal data being processed. If the request is submitted electronically and unless otherwise requested, the Bank will provide the information in electronic form.

b) Right to rectification

The data subject has the right to request the correction of inaccurate personal data or the completion of incomplete data.

c) Right to erasure

The data subject has the right to request the erasure of their personal data if the conditions prescribed by the Law are met (e.g., the purpose for which the data were collected has been fulfilled, consent has been withdrawn and there is no legal basis for processing). The Bank cannot erase personal data if processing is required by law, if processing is mandatory for reasons of public interest (e.g., acting upon an order of a public authority), or if processing is necessary for the establishment, exercise, or defense of legal claims.

d) Right to restriction of processing

The data subject has the right to request from the Bank the restriction of the processing of his personal data in cases prescribed by the Law (e.g. if the accuracy of the personal data or the legality of the processing is justifiably contested, if the personal data are no longer necessary for the purpose of the processing, if an objection to the processing has been submitted, and an assessment is underway as to whether the legal basis for the processing by the Bank outweighs the

interests of the person who submitted the request).

e) Right to data portability

The data subject has the right to receive personal data in a structured, commonly used, and machine-readable format and to transmit those data to another controller without hindrance, provided that: (a) processing is based on consent or is necessary for the performance of a contract, and (b) processing is carried out by automated means. This right also includes the possibility to request that the Bank transmit the personal data directly to another controller where technically feasible.

f) Right to object

At any time, the data subject has the right to object to the Bank's processing of personal data based on legitimate interest or necessary for the performance of tasks in the public interest. After submitting the objection, the Bank will suspend further processing of such data, unless there are compelling legitimate grounds for the processing which override the interests or freedoms of the data subject or if the processing is carried out for the purpose of initiating, filing or defending legal claims (e.g. filing a lawsuit, counterclaim, etc.).

Where personal data are processed for direct marketing purposes, the data subject has the right to object at any time to the processing of personal data concerning them for such marketing, including profiling to the extent it is related to direct marketing.

g) Right to challenge a decision made in an automated decision-making process, including profiling

If the data subject considers that their rights have been infringed by a decision made in an automated decision-making process, they have the right to challenge such a decision, express their view, and request that the decision be reviewed with the involvement of an authorized Bank employee.

h) Right to lodge a complaint with the Personal Data Protection Agency of BiH

The data subject has the right to lodge a complaint with the Personal Data Protection Agency if they believe that the processing of their personal data is carried out contrary to the provisions of the Law on the Protection of Personal Data.

The data subject has the right to an effective legal remedy against the Bank as the data controller, i.e. the right to judicial protection, if they consider that their rights under the Law on the Protection of Personal Data have been infringed as a result of the processing of personal data, without prejudice to any other administrative or out-of-court remedy, in accordance with Article 110 of the Law on the Protection of Personal Data.

i) Exercising rights

To exercise their rights, data subjects may contact the Bank by completing and submitting a Request for the Exercise of Rights in accordance with the instructions provided therein. The request form can be obtained at any Bank branch or on the Bank's website.

The Bank will inform you of the actions taken without undue delay and no later than 30 days from receipt of the request. This period may be extended by a further 60 days if necessary, taking into account the complexity and number of requests, of which the Bank will notify you within 30 days, stating the reasons for the delay.

Measures taken by the Bank in relation to the exercise of rights are free of charge. Only in the case of manifestly unfounded or excessive requests, in particular if they are repetitive, may the Bank charge a reasonable administrative fee or refuse to act on the request.

FINAL PROVISIONS

The Bank reserves the right to amend and update these General Information. The updated version will always be published on the Bank's website, where data subjects may review and be informed of the updated content of the General Information, and they will always be available at a branch upon the data subject's request.

The transitional period for the full application of the rights defined in Section 11 of these General Information is two years from the date of entry into force of the Law on the Protection of Personal Data, i.e., until 08 March 2027.