NOTICE ON THE PROCESSING OF PERSONAL DATA

NLB banka AD Beograd (hereinafter: **the Bank**), as a controller, processes personal data of clients, proxies and legal representatives of clients, beneficial owners of legal entities, potential clients and other persons whose data the Bank processes within the scope of providing its products and services in in accordance with the Law on Personal Data Protection ("Official Gazette of RS", No. 87/2018 - hereinafter: **the Law**) and other regulations governing issues related to the processing of personal data. In order to transparently process personal data, the Bank hereby provides basic information regarding the processing of personal data, the protection of personal data and the rights of individuals regarding processing.

1. BASIC TERMS

Personal data - any data relating to a natural person whose identity is determined or determinable, directly or indirectly, especially based on an identity marker, such as name and identification number, location data, identifiers in electronic communication networks or one, i.e. more features of his physical, physiological, genetic, mental, economic, cultural and social identity.

Processing of personal data - any action or set of actions performed automatically or non-automated with personal data or their sets, such as collection, recording, sorting, grouping, i.e. structuring, storing, adapting or changing, revealing, viewing, using, disclosure by transmission, i.e. delivery, duplication, dissemination or otherwise making available, comparison, restriction, deletion or destruction (hereinafter: **processing**).

Data subject - natural person whose personal data is processed within the scope of the provision of products and services by the Bank.

Controller - natural or legal person, i.e. the authority that independently or together with others determines the purpose and method of processing.

Processor - natural or legal person, i.e. the authority that processes personal data on behalf of the controller.

2. INFORMATION ABOUT THE BANK AS THE CONTROLLER AND CONTACT INFORMATION OF THE PERSON IN CHARGE FOR THE PROTECTION OF PERSONAL DATA

NLB banka AD Beograd
Bulevar Mihajla Pupina 165 V
11070 Novi Beograd
Company Reg. No.: 07737068
www.nlb.rs

The Bank has appointed a **Data protection officer** whom you can contact in connection with all issues related to the processing of personal data, as well as in connection with the exercise of your rights prescribed by this Law, in one of the following ways:

- by sending an e-mail to the address: dpo@nlb.rs;
- by sending a letter to the address of the Bank's headquarters: NLB banka AD Beograd, Bulevar Mihajla Pupina 165V, 11070 Novi Beograd – with the indication „for attn. of Data Protection Officer";
- by handing over the letter at the Bank's branches, with the indication "for attn. of Data Protection Officer".

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 the legal basis for each processing purpose.

The purpose for which the Bank processes data depends on the type of products and services for which the Data subjects apply or are contracted. These data are processed to fulfill the purpose for which they are collected.

In accordance with this, below are stated the legal bases and processing purposes on the basis of which the Bank processes personal data:

a) Execution of the concluded contract or undertaking of previous actions in order to conclude the contract

Data processing is necessary for the conclusion and execution of a contract on the use of the Bank's products and/or services (e.g. account opening, activation and use of payment cards, use of the Bank's electronic services, authorization of persons through a record of deposited signatures, sending prescribed notifications, collection of outstanding claims) or in order for the Bank to take certain actions before the conclusion of the contract (e.g. processing requests for establishing a business relationship with the Bank, preparing a loan offer, etc.). If the Data subject refuses to provide the data required for this purpose, the Bank will not be able to conclude the contract or provide the requested service.

b) Compliance with the Bank's obligations prescribed by the Law

The Bank processes personal data for the purpose of fulfilling the obligations prescribed by the laws to which the Bank is liable, e.g. regulations governing the operation of banks, prevention of money laundering and financing of terrorism, provision of payment and financial services, risk management, as well as for the purpose of meeting the requirements of competent state authorities, preventing fraud and abuse, resolving complaints, applying FATCA and other tax regulations, etc. The consent of the Data subject is not required for the processing of data, which is necessary

for compliance with the Law and the fulfillment of the prescribed obligations of the Bank.

c) Realization of legitimate interest of the Bank or a third party

In certain cases, processing is necessary in order to achieve the legitimate interests of the Bank or a third party, while considering that the interests of the Bank do not prevail over the interests or rights and freedoms of the person whose data it processes. The Bank bases data processing on legitimate interest, e.g. in the following situations:

- monitoring and maintaining security at the Bank's business premises (e.g. video surveillance of those premises, ATMs, visitor records);

- monitoring and preserving the security of the Bank's IT system and operations, including the security of the services offered to clients;

- prevention and investigation of fraud, abuse and other criminal acts that may harm the Bank, its clients and/or third parties;

- assessment of the risks that the Bank is obliged to monitor (e.g. the Bank's exposure to risk in relation to a group of related parties);

- initiation and conduct of legal proceedings before state authorities in order to realize the rights and interests of the Bank or other persons;

- recording of telephone conversations, for the purpose of records of submitted requests, implementation of controls and adequate processing of all requests of Data subjects;

- providing answers to questions, comments and suggestions addressed to the Bank through all communication channels;

- researching the satisfaction, experience and needs of clients of a particular product and service within the framework of the improvement and development of the Bank's products and services;

- data processing for the purpose of determining preferences and segmentation of clients with the aim of offering products and services that better suit the needs and wishes of certain categories of clients;

- exchange of data with members of the Banking Group and their supervisory bodies, etc.

Data processing on the basis of legitimate interest does not require the consent of the Data subject, but the Data subject has the right to submit a request to exercise his rights at any time in the manner described in Point 11 of this Notice.

d) Consent to data processing

For one or more specially determined purposes, the Bank processes data based on the given consent/expressed consent of the Data subject. In these situations, the purpose of the processing will be presented to the Data subjects when obtaining consent (e.g. promotion of banking products).

Within the mBank application, consent is requested for the following purposes:
- making phone calls - for the purpose of calling the Bank's customer center;

- taking photos and videos - access to the camera is necessary for the purpose of payment via IPS2, i.e. by scanning the QR code, as well as for the purpose of setting the profile picture;

- access to the location of the device - access to the location is necessary for the purpose of displaying the nearest branches and ATMs.

Refusal of providing consent to processing does not affect the performance of the contract concluded with the Bank, the management of its prescribed obligations, nor processing based on the legitimate interest of the Bank or a third party, except in cases where the laws prescribe that consent is a necessary condition for the performance of certain obligations.

Consent can be revoked at any time, in the same way as it was given - by submitting a request for revocation of consent at a Bank branch, by changing parameters in the eBank settings, by changing the settings in the mobile device (Settings - Application - Permissions) or by sending a request to the Data Protection Officer.

e) Personal data processed by the Bank as a processor

In addition to be a controller of the processing, the Bank also processes certain personal data as a processor based on the contract by which third parties entrusted it with certain personal data processing tasks (e.g. as an insurance agent, in the promotion and provision of services of investment companies, money transfer via Western Union, etc.). In those cases, the Bank processes data exclusively according to the order and instructions received from the data controller in accordance with the Law.

4. CATEGORIES OF DATA PROCESSED

Basic personal and identification data from personal and other documents: name and surname, date and place of birth, gender, picture, Unique Personal Id. No., residence and/or address registration, information on the type and number of identification document, citizenship, as well as others. For certain products and services, identification data is also collected from joint debtors, guarantors, pledged debtors, legal representatives, proxies, etc.

Contact information: mailing address, landline and/or mobile phone number, e-mail address, etc.

Data on the bank's products: data from the payment order, data on the receiver of the payment, intermediaries in the transfer of payment orders, data on the amount, purpose

and reference of payment, data on the use of credit and debit payment cards, data on indebtedness and outstanding interest due, savings transactions and transactions with securities, etc.

Other types of data: data on creditworthiness, regularity of repayment and other data required for processing credit requests (e.g. type and amount of income, loans in repayment, marital status, number of household members, data on spouse, related parties, number of dependents, professional qualification, employment status, level of income, expenses, tenant status, ownership of real estate, etc.), audio recordings of telephone conversations, data relevant to promotions of banking products, investigation of possible abuses, data generated by users (photos and messages entered in the Bank's applications), technical data that are a prerequisite for the use of services via means of remote communication (e.g. data on the sort and type of mobile device or computer, name and version of the mobile application, location), etc.

5. METHOD OF COLLECTION OF PERSONAL DATA

The Bank collects data directly from the Data subject, from third parties or from publicly available sources (e.g. to assess the Bank's risk exposure when deciding on a request for placement approval).

6. ACCESS TO PERSONAL DATA

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

a) **Within the Bank** - employees within the Bank who, in accordance with the nature of their work, must have access to such data in order to fulfill contractual and legal obligations, as well as to realize the legitimate interests of the Bank and third parties, members of the Bank's bodies;

b) **Members of the Banking Group and their supervisory bodies** - to whom the Bank provides data on the Data subjects based on regulations, when it is necessary for the implementation of the contractual relationship with the Bank or when there is a legitimate interest of the Bank.

c) **Competent authorities and organizations** - e.g. The National Bank of Serbia, the Pension and Disability Insurance Fund, the Securities Commission, the Loan and Payment cards Abuse Prevention Forum at the Chamber of Commerce and Industry of Serbia, judicial, administrative and tax authorities of the Republic of Serbia, public enforcement officers, external auditors, etc.;

d) **Public information systems** - e.g. The unique register of accounts of natural or legal persons with the National Bank of Serbia and information systems managed by the Association of Serbian Banks (e.g. Credit Bureau), Serbian Business Registers Agency, Real Estate Cadaster Office;

e) **Third parties** with whom the Bank has concluded an appropriate contract on business cooperation which is necessary for the implementation or is related to the contractual relationship between the Data subjects and the Bank (e.g. persons who provide postal, courier, telecommunication services, services regarding the use of cards, insurance companies, law offices, appraisers, debt collection agencies, IT system maintenance, persons participating in the approval and collection of subsidized loans, correspondent and/or custodian banks, etc.).

7. TRANSFER OF PERSONAL DATA TO ANOTHER COUNTRY OR AN INTERNATIONAL ORGANIZATION

The Bank processes personal data in the Republic of Serbia. The transfer of data from Serbia to other countries is carried out only if it is necessary for the execution of contracts and/or orders (e.g. the use of debit and credit cards may lead to the necessary involvement of international card organizations, due to which data is processed in other countries).

The Bank transfers personal data to another country or to an international organization if it has been determined that the other country or international organization provides an appropriate level of personal data protection based on signed agreements governing data processing.

The transfer of data to a state or an international organization that does not meet the stated conditions is carried out only with the express consent of the Data subject or with the undertaking of other security measures prescribed by the Law.

8. METHOD OF PERSONAL DATA PROCESSING

The Bank processes personal data manually and electronically, in a way that ensures security and confidentiality.

When processing certain credit requests, the Bank carries out automated or semi-automated data processing, including profiling. In such cases, the Bank provides an additional check of the processing results performed by an authorized employee of the Bank in the event of an unfavorable outcome for the person who applied for the loan.

For clients who use products and services with credit exposure, the Bank has a legal obligation, in accordance with the Law on Banks and relevant by-laws, to calculate a credit rating. The credit score is determined by comparing statistical models based on available data, among other things, data collected from the client, data on products and

services used by the client, as well as regularity in meeting obligations.

9. SECURITY OF PERSONAL DATA

The bank has defined information security management at a high level, which implies the implementation of the most modern technical tools as well as the implementation of the ISO/IEC 27001:2013 Standard. Also, the Bank treats all data as a business and banking secret, with the application of all available technical and organizational protection measures, in accordance with the Law and internal acts.

10. STORAGE PERIOD OF PERSONAL DATA

The Bank processes personal data collected for the purpose of exercising rights and obligations from the contractual relationship until the end of that relationship, except in cases where the Bank is obliged to keep the data even after the termination of the contracted cooperation, and on the basis of the Law (e.g. certain documentation should be stored for 10 years from the termination of the contractual relationship in accordance with the Law on Prevention of Money Laundering and Financing of Terrorism), consent of the Data subject (e.g. data processed for the purpose of promoting banking products is stored for 10 years, i.e. until withdrawal of the consent) or for the purpose of realizing their legitimate interest. In cases where the request for placement approval is rejected, the data is stored for the period in which an objection can be filed with the National Bank of Serbia (3 years).

11. THE RIGHTS OF THE DATA SUBJECTS

a) The right of access

The right of access implies that the Data subject can receive from the Bank information on whether their personal data is being processed and, if this is the case, permission to access their personal data and obtain information about the processing. Upon request, the Bank will provide a copy of the personal data it processes. If the request is submitted electronically and unless otherwise requested, the Bank will submit the information in electronic form.

b) The right to correct, supplement and delete data

At the request of the Data subject, the Bank will correct inaccurate personal data or supplement incomplete data.

At the request of the Data subject, the Bank will delete their personal data if the conditions prescribed by the Law are met (e.g. if the purpose for which they were collected is fulfilled, if consent for processing is withdrawn but there is no legal basis for processing). The Bank cannot delete personal data: if the obligation to process them is prescribed by the Law or if the processing is mandatory for reasons of protection of public interest (e.g. acting on the order of a state authority) or it is necessary for initiating, submitting or defending a legal claim (e.g. filing a lawsuit, etc.).

c) The right to restriction of processing

At the request of the Data subject, the Bank will limit the processing of their 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 needed to achieve the purpose of the processing, if it has been submitted complaint to the processing, and an assessment is underway as to whether the legal basis for the processing by the Bank prevails over the interests of the person who submitted the request).

d) The right to data transferability

At the request of the Data subject, the Bank will deliver personal data in a structured, commonly used and electronically readable form (e.g. on a computer) and enable him to transfer them to another controller without interference from the Bank if the following conditions are met: (a) the processing is based on consent or it is necessary for the performance of the contract and (b) the processing is automated. This right also includes the possibility to demand that the Bank directly transfer personal data to another operator if this is technically feasible.

e) The right to complain

At any time, the Data subject can submit a complaint to the Bank about the processing of personal data based on a legitimate interest or the one which is necessary for the purpose of performing tasks in the public interest or exercising the Bank's powers prescribed by Law. After submitting a complaint, the Bank will suspend further processing of such data, unless there is a legitimate basis for processing that prevails over the interests or freedoms of the Data subject, or if the processing is carried out for the purpose of initiating, submitting or defending against a legal claim (e.g. filing a lawsuit, counterclaims and the like).

A person who has given consent to the processing of data for the purpose of promoting banking products has the right to complain at any time to the processing of his personal data that is processed for the purposes of direct advertising, including profiling, to the extent that it is related to direct advertising.

f) The right to dispute a decision made in an automated decision-making process, including profiling

If Data subject believes that their rights have been violated by a decision made in the automated decision-making process, the Data subject has the right to dispute such decision, to express their position and to request that the decision be reviewed with the participation of an authorized employee of the Bank.

g) The right to complain to the Commissioner for Personal Data Protection

The Data subject has the right to file a complaint with the Commissioner for information of public importance and personal data protection, if he believes that the processing of his personal data is carried out contrary to the provisions of the Law or other valid regulations.

h) Exercise of rights

In order to exercise their rights in connection with the processing of personal data, individuals can contact the Bank by filling out and submitting a Request for the exercise of rights in accordance with the instructions in the Request itself. The Request for exercising the right can be taken over at any branch of the Bank or downloaded from the Bank's website.

The measures taken by the Bank in connection with the exercise of personal rights are free of charge. Only in the case of unfounded or excessive requests, and especially if they are frequently repeated, the Bank may charge compensation for the necessary administrative costs of providing information, that is, acting on the request or refusing to act on the request.

FINAL PROVISIONS

The Bank reserves the right to amend and update this Notice on Personal Data Processing. The updated version of this Notice will always be published on the Bank's website, where the Data subject will be able to inform themselves with the updated content of the Notice.