Ljubljana, 9 October 2023

NLB d.d.
Trg republike 2
SI-1520 Ljubljana
Slovenia
SWIFT: LJBASI2X
www.nlb.si

NLB AML/CFT and Sanctions Policy Statement and Important General Information

Dear Business Partners,

To comply with all EU Regulations, U.S. Patriot Act requirements as well as in line with NLB business practice to keep its business partners informed on the major changes in NLB d.d. and on other relevant changes in Slovenian legislation (*Prevention of Money Laundering and Terrorist Financing Act*) and on money laundering and terrorist financing prevention policies in Nova Ljubljanska banka d.d. (NLB d.d.) we are providing the updated NLB d.d. AML & KYC policy related document that supersedes any documents on the subject issued by now.

1. Overview

Nova Ljubljanska banka d.d., Ljubljana (NLB d.d.) (hereinafter: the “Bank” or “NLB”) is a universal institution combining the functions of a commercial, investment and savings bank. Under the licensed authority of the central bank, Banka Slovenije (the Bank of Slovenia), and in accordance with the existing regulations the Bank’s Group provides a complete range of domestic and international banking and parabanking services to corporate and individual clients.

The Bank traces its origins back to the 19th century when the City Savings Bank in Ljubljana was founded in 1889. Under its present charter, the Bank was established by a legislative act of the National Assembly of the Republic of Slovenia on 27 July 1994, commencing operations on 28 July 1994.

NLB d.d.'s shares have been listed on the London and Ljubljana Stock Exchanges on 19 November 2018. The details are available on the NLB web pages:

https://www.nlb.si/investor-relations
https://www.nlb.si/shares
The ***ownership structure*** is being regularly updated and made available on NLB
https://www.nlb.si/shares

Current International Ratings: https://www.nlb.si/ratings

NLB Management Board and ***Supervisory Board*** members are presented at:
https://www.nlb.si/management-and-supervisory-board

For the complete list of ***NLB Group member banks*** and ***associated companies*** please refer to our website at http://www.nlbgroup.si/profile.

Nova Ljubljanska banka d.d., Ljubljana, Trg republike 2, Ljubljana, Slovenia, entered into the Court Register of District Court in Ljubljana under ID No. 5860571.
Share capital of the company is EUR 200,000,000.00.
Tax Number 91132550.

2. Prevention of Money Laundering and Financing of Terrorism Issue

Financial crime linked to money laundering remains a current issue, while the risk of various forms of financial terrorism has risen in recent years. Effectively combating this problem transgresses national boundaries and is becoming an increasingly global challenge. Nova Ljubljanska banka d.d. is committed to combating financial crime and ensuring that accounts held at our bank are not misused for the purpose of money laundering or terrorism financing. As such, adherence with applicable laws and regulations regarding Anti-Money Laundering (AML) and Countering the Financing of Terrorism (CFT) and Sanctions is mandatory and fundamental to our program.

The Republic of Slovenia became a member of the European Union (EU) on 1 May 2004 and upon its accession to the EU takes part in the creation of EU policies and legislation. Pursuant to European legislation, the National Assembly of the Republic of Slovenia in 2007 adopted the new Law on the Prevention of Money Laundering and Terrorist Financing (hereinafter: the ZPPDFT) which has replaced the previous Law on Prevention of Money Laundering and harmonized national law with the provisions of revised anti-money laundering legal instruments as well as brought Slovenian legislation in line with the new standards on countering of the financing of terrorism. The ZPPDFT was in line with international documents relating to the prevention of money laundering (Directive of European Community; Convention on Laundering, Search, Seizure and Confiscation of the Proceeds from Crime; Financial Action Task Force on Money Laundering and others) and implemented some additional obligations and differentiated customers and their treatment according to the certain risk factors regarding the money laundering and financing of terrorism. Within our bank, the Law has been carried out in accordance with the Instructions for the Implementation of the Law on the Prevention of Money Laundering and Financing of Terrorism containing detailed determination of our obligations regarding the implementation of the Law.
Most important Bank's obligations imposed by the Law are:

- Nomination of the authorized person for prevention of money laundering and financing of terrorism;
- Customer due diligence that includes the implementation of the following measures: determining and verifying a customer's identity, determining a customer's beneficial owner, collecting legally required data and the regular diligent monitoring of a customer's business activities. According to the potential risks involved, all business relationships, regardless whether corporate or private persons, have to be examined (know your customer proceedings) through either standard, simplified or enhanced due diligence proceedings depending on the nature of their business and type of transaction(s) to be concluded:
  - Enhanced due diligence is mandatory when entering into a correspondent banking relationship with a correspondent bank or similar credit institution situated in a third country, prior any business relationship is established with politically exposed persons and customers from high-risk countries, in case a person wishing to open an account is not present in person at the opening and whenever a customer is identified as high-risk.
  - Simplified due diligence may be used only in assessment of banks and financial institutions headquartered in countries with strict anti-money laundering and anti-terrorist financing legislation, Republic of Slovenia – i.e. the government, ministries, municipalities, corporate listed on the Stock Exchange and in certain transactions with very limited risks involved (the full list is determined, published and updated by the Ministry of Finance of the Republic of Slovenia)
  - Standard due diligence is mandatory prior any type of business relationship is established (except above mentioned) and when executing transactions of EUR 15,000 or more.
- Establishing and maintaining a Risk Based Approach (RBA) towards assessing and managing the money laundering and terrorist financing risks: the bank is obliged to carry out a risk analysis to assess the risks associated with an individual group of customers, business relationships, products and services in terms of possible abuse for the purpose of money laundering or terrorist financing, and to implement appropriate measures on this basis.
- Establishing and maintaining risk based systems and procedures to monitor ongoing customer activity;
- Detection and reporting of suspicious transactions: suspicious transactions are detected by the help of indicators of such transactions prepared by the Slovene bank Association and utilized by the banks located in Slovenia. Of great assistance for the detection of such transactions are also seminars for

the bank staff where local and foreign experts raise the level of awareness of this urgent global issue among the employees and make them acquainted with individual simple as well as sophisticated cases of money laundering.
- Reporting of the requested data and presentation of the requested documentation to the Office for Money Laundering Prevention of the Republic of Slovenia;
- Keeping the records of data on customers for 10 years from the cessation of business relationship or completed transaction;
- Permanent training of employees and internal supervision,

- Performance of the measures for detecting and prevention of money laundering and financing of terrorism in the Bank's branches and in wholly-owned subsidiaries in third countries (excluding EU and other countries with adequate anti-money laundering legislation);
- Independent verification of the compliance and effectiveness of the system for the prevention of money laundering and terrorist financing.

To ensure the comprehensive and systematic implementation of all prescribed requirements related to the prevention of money laundering and terrorist financing, the bank developed the AML program that includes the following elements:
- Organizational and personnel conditions, which include: the management board, the authorized person and his deputies, and coordinators for the prevention of money laundering and terrorist financing by individual business lines;
- A system of internal controls which includes policies and procedures defined by the bank to ensure compliance with legal requirements related to the prevention of money laundering and terrorist financing, and thus improve the management of relevant risks;
- Education and training which is one of the key factors in an effective system for the prevention of money laundering and terrorist financing is the adequate education and training of all employees;
- Independent verification: the internal audit department performs the independent verification of system for the prevention of money laundering and terrorist financing.

According to the EU Fourth Anti-Money Laundering Directive[1], which entered into force in June 2015, the Member States were obliged to bring into force the legislation necessary to comply with this Directive by June 2017. The Parliament of the Republic of Slovenia in 2016 adopted the new Act on Prevention of Money Laundering and Terrorist Financing (hereinafter: the ZPPDFT-1), thus transposing the requirements set out into the aforementioned directive into Slovenian law. Beside this, the ZPPDFT-1 has also been focused on the adjustment of Slovenian legislation with the international standards from this field, especially with the new FATF (Financial Action Task Force) recommendations from 2012 that all the countries should take into consideration at performing measures of detection and prevention of money laundering and terrorist financing and as a novelty, also financing of weapons for mass destruction.
The key novelties of ZPPDFT-1 are:
- establishment of the Register of Beneficial Owners, to ensure transparency of ownership structures of business subjects;
- competence of Office for money laundering prevention (OMLP) to perform on-site inspections at obliged entities in order to improve the supervision system and sanctioning;
- enforcement of RBA to increase the effectiveness of performing of measures at the level of obliged entities, state and European level;
- introduction of the wider definition of PEPs (politically exposed persons), which (beside foreign PEPs) includes also the domestic ones;
- reduction of the amount of cash transactions which have to be reported to OMLP to 15.000 EUR, that would have preventive and deterrent effect and would also present higher barrier for performing illegal activities;
- possibility of determination and verification of the identity of customer, who is a natural person, without his/her personal presence by the use of video electronic identification;

[1]Directive (EU) 2015/849 of the European parliament and of the Council on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing

- extension of the possibilities of use of electronic identification means (before: qualified digital certificate) at determination and verification of the identity of customer also to the legal representatives of companies and authorized persons of all customers;
- extension of set of obliged entities for performing measures of detection and prevention of money laundering and terrorist financing.

Law authorizes the Office for Money Laundering Prevention to perform duties relating the prevention and detection of money laundering and terrorist financing, and other duties as stipulated by the ZPPDFT-1. The Office is a founding member of the EGMONT international group, which unifies similar institutions (the so-called Financial Intelligence Units), which are engaged, throughout the world, in the prevention and detection of money laundering and financing of terrorism.

NLB already complies with all the required changes. According to the Law requirements, NLB however re-evaluate on a regular basis all its business relationships from the perspective of anti-money laundering or preventing of terrorist financing to make sure that all the risks addressed by the Law are covered in line with the legal requirements.

Money laundering detection and prevention policies set for NLB apply for the whole NLB network, provided that the bank's branches abroad are also subject to respective laws and regulations in force in a particular foreign country. Based on the abovementioned EU Fourth AML Directive the ZPPDFT-1 requires obliged entities that are part of a group to implement group-wide policies and procedures, including data protection policies and policies and procedures for sharing information within the group for AML/CFT purposes. Those policies and procedures must be implemented effectively at the level of branches and majority-owned subsidiaries in Member States and third countries. ZPPDFT-1 also requires that, where a third country's law does not permit the implementation of the policies and procedures, obliged entities ensure that branches and majority-owned subsidiaries in that third country apply additional measures to effectively handle the risk of money laundering or terrorist financing, and inform the competent authorities of the Republic of Slovenia. If the additional measures are not sufficient, the competent authorities shall exercise additional supervisory actions, including requiring that the group does not establish or that it terminates business relationships, and does not undertake transactions and, where necessary, requesting the group to close down its operations in the third country.

3. NLB AML/CFT and Sanction Policy Mainframe

Customer due diligence:

Customer due diligence is a key element of the system for detecting and preventing money laundering and terrorist financing. Through customer due diligence, the bank reliably determines and verifies a customer's identity and establishes the purpose of a transaction and the expected nature of a business relationship, in order to mitigate the risk of doing business with an unknown customer who might try to use the bank for money laundering or terrorist financing.

Customer due diligence includes the implementation of the following measures:

- determining and verifying a customer's identity,
- determining a customer's beneficial owner,
- collecting legally required data and
- regular diligent monitoring of customers business activities.

The bank carries out customer due diligence when establishing a business relationship, when executing transactions of EUR 15,000 or more, when executing transactions by an occasional customer, when there are doubts regarding the veracity or adequacy of previously obtained data, and whenever there is a suspicion of money laundering or terrorist financing relating to a transaction or customer.

The bank carries out enhanced due diligence for customer that represent high risk. In this regard, the bank provides for additional controls to ensure the appropriate management of the increased risks associated with such a customer in the following cases:

- entering into a correspondent banking relationship with a respondent bank or similar credit institution situated in a third country;

- entering into a business relationship or carrying out a transaction exceeding EUR 15,000 with a customer who is a politically exposed person;
- when the customer or transaction are linked to a high-risk third country;
- when executing transactions of EUR 1,000 or more (non-customers);
- where the bank assesses that a customer, business relationship, transaction, product, service, country or geographic area represent increased risk for money laundering or terrorist financing;
- if the bank assesses that there is a high risk of money laundering or terrorist financing due to the nature of the business relationship, form or manner of executing the transaction, business profile of the customer, or other circumstances relating to the customer.

The bank also carries out additional activities related to the identification of politically exposed persons, a customer's risk assessment and verification of the possible inclusion of a customer on the lists of persons (natural and legal persons and other entities) against whom the international organisations issued restrictive measures.
The bank also defines a customer's risk profile in the scope of customer due diligence, conducted during the establishment of a business relationship. A customer's initial risk profile is based on static criteria that relate to the customer's status and the geographical regions where the customer has its registered office or address.

Limitations when establishing a business relationship with a customer:
The bank does not allow:

- opening, issuing or keeping anonymous accounts, passbooks or bearer passbooks, or other products enabling, directly or indirectly, the concealment of the customer's identity.
- entering into or continue a correspondent banking relationship with a respondent bank that operates or may operate as a shell bank, or other similar credit or financial institution known to allow shell banks to use its accounts.
- entering in a business relationship or perform a transaction amounting to EUR 15,000 or more (regardless of whether the transaction is carried out in a single operation or in several operations which are evidently related), if the customer proves the ownership of a legal entity or a similar entity under foreign law based on the bearer shares that cannot be tracked through the central clearing and depository company or a similar register or trading account or if it cannot be established on the basis of other business documentation.

Risk based approach:
We risk rank all our clients based on our prepared risk analysis and establishment a risk assessment for individual groups or customers, business relationships, products or transactions with respect to their potential misuse for money laundering or terrorist financing. The risk analysis is drawn up in accordance with guidelines issued by and within the powers of our supervisory body, The Bank of Slovenia.
The risk assessment is a dynamic process, as risks change over time due to various external influences (e.g. the introduction of new techniques and methods of money laundering and terrorist financing), internal influences (e.g. the introduction of new products and expansion to new markets) and legislative changes. Therefore, the bank regularly updates the risk analysis.

Regular diligent monitoring of a customer's business activities:
The bank defined appropriate procedures for the regular diligent monitoring of a customer's business activities in its internal acts, policies and work instructions.
We monitor business activities undertaken by the customers through the bank with due diligence and thus ensure knowledge of the customers, including the origin of assets used in business operations. Monitoring includes verification of the customer's business operations compliance with the purpose and intended nature of the business relationship, monitoring and verification of the customer's business operations compliance with his regular scope of business and verification and updating obtained documents and data on the customer.

Given the number of customers and the scope and complexity of banking services, the bank introduced appropriate IT support. In the automated transaction monitoring system the check is based on scenarios

defined in the research system. Following upon the analysis of the alerts, the cases are rated and measures are taken and documented. The parameters and thresholds of the system are: different thresholds within scenarios, behavioural trends, relationships (persons, transactions, partners, etc.), countries, change in ratio, in customer's profile, difference regarding to the anticipated purpose of business. Automated procedures benefit when identifying unusual transactions and are of key importance for providing an analysis of all unusual cases, in terms of identifying grounds to suspect money laundering or terrorist financing.

Reporting to the Office for Money Laundering Prevention (OMLP):
The bank defined procedures for the timely and accurate reporting of data regarding transactions executed in its internal acts, policies and work instructions. The bank provides the OMLP with data on every cash transaction that exceeds EUR 15,000, taking into account the rules on the method of forwarding information to the OMLP and the rules laying down conditions under which there is no obligation to report cash transaction data for certain customers. The bank also reports transactions exceeding EUR 15,000 EUR to high-risk countries or to customers who have permanent or temporary address in these countries.

Pursuant to the ZPPDFT-1, the bank forwards the prescribed data to the OMLP, whenever there are grounds to suspect money laundering or terrorist financing in relation to a transaction or customer.
We also defined procedures for the consistent implementation of additional measures, which a bank must implement at the request of the OMLP.

Protection and retention of data and records management:
The bank is obliged to protect as a trade secret all data obtained and managed on the basis of the ZPPDFT-1. The obligation to protect the secrecy of data applies to all employees and other persons with access to these data.
The bank ensures the appropriate retention of all data and related documents obtained in the process of customer due diligence for 10 years following the termination of a business relationship or the execution of a transaction.

Training in the area of money laundering and terrorist financing prevention:
The bank provides regular professional training and education to all employees carrying out tasks for the prevention and detection of money laundering and terrorist financing.
The professional training and education refers to learning about the provisions of the ZPPDFT-1 and the implementing regulations issued on its basis and internal acts, the specialised literature on money laundering and terrorist financing prevention and detection, the lists of indicators for recognising customers and transactions in relation to which there are reasons to suspect money laundering or terrorist financing, including appropriate requests concerning data protection.
The trainings depend on type of employees and the content: new employees (elementary or basic training), other employees (knowledge refreshment, special trainings for management, thematic trainings like KYC, beneficial owner, suspicious transactions, sanctions screening), trainings for AML/CFT staff.
Similar approach is in place in NLB Group Members (based on NLB d.d. Standards Compliance and Integrity).

Correspondent banking services
We apply the customer due diligence measures on institutions to which we offer correspondent banking services and all new correspondent relationships are approved by a senior manager. The due diligence process depends on a country risk and other factors. Whenever a foreign bank has a registered office in a third country, the bank is required by law to conduct enhanced customer due diligence. In the process of due diligence, we obtain sufficient information to gain an understanding of our correspondents' AML/CFT measures, regulatory history and reputation. We perform regular diligent monitoring of business activities and carefully monitor the transactions. We established effective controls on a permanent basis to detect any activities suspected of money laundering or terrorist financing or applicable Sanctions' violation.

Compliance with the requirements laid down in Regulation (EC) No. 845/2015 of the European Parliament and of the Council on information on the payer accompanying transfers of funds:

The traceability of transfers of funds is an important and valuable tool in the detection and prevention of money laundering and terrorist financing, as well as in the implementation of restrictive measures. The EU Regulation on information accompanying transfers of funds[2] lays down rules on the information on payers and payees, accompanying transfers of funds, in any currency, for the purposes of preventing, detecting and investigating money laundering and terrorist financing, where at least one of the payment service providers involved in the transfer of funds is established in the Union. This Regulation represents a preventive measure in the area of preventing money laundering and terrorist financing and the bank established and implemented appropriate internal acts and work instructions regarding compliance with the requirements laid down in the regulation.

Implementation of restrictive measures and sanctions screening:

The Act Regulating Restrictive Measures Introduced or Implemented by the Republic of Slovenia in Accordance with Legal Acts and Decisions Adopted by International Organisations (ZOUPAMO; Official Gazette of the RS, no. 127/2006), systemically regulates the area of restrictive measures in Slovenia. The aforementioned act prohibits banks from establishing or continuing a business relationship with a person included on the list of persons (natural and legal persons and other entities), against whom United Nations Security Council or European Union restrictive measures are in effect or have been issued. Those measures comprise the freezing of funds and economic resources of certain natural and legal persons, entities and bodies. Certain EU Regulations apply additional restrictive measures – embargoes that comprise, in particular, additional restrictions on trade, investment, supply of arms and military equipment, export of certain dual-use goods and technology, access to the capital market for financial institutions, etc. The bank and its customers are legally bound to adhere to sanctions and embargoes therefore the bank has to ensure by internal procedures/measures and guidelines that all embargo and sanction requirements are fulfilled.

In addition to the local legislation in the area of restrictive measures, the NLB Group also complies with the legislative requirements of the international community (United Nations), the EU, the USA. Based on this commitment, each NLB Group member must implement the following sources of data/groups of sanction lists:

a) UN (United Nations Security Council),
b) EU (European Union or Council of Europe),
c) OFAC (United States Treasury's Office of Foreign Assets Control & Other US Sanction Lists),
d) FINCEN (United States – Financial Crimes Enforcement Network),
e) HMT (United Kingdom – HM Treasury),
f) SOR (Ownership of Sanctioned Entities and Persons),
g) INTERNAL.

The bank conducts a stricter sanctions approach than the current EU/UN sanctions regime. In accordance with the existing adopted documents, the NLB Group does not establish business relationships or perform transactions with the following countries and areas:

- Iran,
- North Korea,
- Afghanistan,
- Syria,
- Sudan, South Sudan,
- Myanmar (Burma),
- Cuba (USD),
- the Crimean peninsula and Sevastopol.
- Donetsk, Lugansk, Kherson and Zaporizhia regions

In accordance with the rules adopted, the NLB Group does not enter into contractual relationships or perform transactions with entities operating in the branch of production and/or sale of mass destruction weapons, substances and equipment.

[2] No 847/2015 entered into force on 26 June 2017 and at the same time repealed the previous Regulation No 1781/2006.

The Policy on the implementation of restrictive measures defines the contents and scope of activities of control implementation, delineates the responsibilities and ownership of risks of individual organisational units in relation to the performance of the tasks concerning these contents, defines the technological support for the implementation of controls, defines the minimum standard for testing the adequateness of the control system (application and process), and defines the method of supervising the performance of the tasks with the contents and scope.
Work process:
The three-level system of controls (three-level system of defence against the attacks of financial crime) of international restrictive measures distinguishes between three groups or levels:

I. Level: the Bank's business lines providing services for clients (Service conclusion processes – front office who deal with customers, Payment systems, Settlement and Financial market services, Investment banking services and Custody services, Card operations). The function of the Bank's business lines and other organizational units who perform the control activities is to implement operational controls when a business event happens. They own risks and manage risks at the operational and implementation level and are responsible for an appropriate performance of tasks.
II. Level: Compliance – the MLTFP function. In line with its function and pursuant to the legislation, it prepares the strategy of risk management and the framework of acceptable risks, prepares the policy and gives guidelines, carries out training, performs supervision of the appropriateness of the system, and proposes measures for the improvement of the system. In case of a "real" hit, it shall inform the relevant external supervisory authorities and give instructions to the business lines of the bank on further activities.
III. Level: The internal audit carries out independent audit of the established system and issues recommendations on the improvement of the system.

Should you need any further details regarding the above (e.g. latest audited financial statements, etc.) please refer to our website www.nlb.si/en or visit SWIFT KYC Registry and/or “BankersAlmanac – Due diligence module”.

For full contents of the AML Law please access at:
http://uppd.arhiv-spletisc.gov.si/en/legislation_and_documents/index.html

Should you need any further details regarding the above please refer to our website www.nlb.si/en or contact Nova Ljubljanska banka d.d., Ljubljana.

Yours sincerely,

Tadej Nardin

Digitally signed by Tadej Nardin
Date: 2023.10.09 16:22:53 +02'00'

Tadej Nardin
AML Officer

Digitalno podpisal URŠULA KOVAČIČ KOŠAK
11. 10. 2023 12:47:24

Uršula Kovačič Košak
Executive Assistant to the Management Board