Евразийский Банк

for wide use

THE KNOW YOUR CUSTOMER POLICY

POLICY

The Know Your Customer Policy (hereinafter – the Policy) was developed in compliance with the Law of the Republic of Kazakhstan "Concerning the Counteraction of the Legitimation (Laundering) of Proceeds of Crime and the Financing of Terrorism" (hereinafter – the AML/FT Law), the Rules of Formation of Risk Management and Internal Control Systems at Second-Tier Banks, approved by Order of the Management Board of the National Bank of the Republic of Kazakhstan dated 12 November 2019 No. 188 (hereinafter – Regulation No.188), the Internal Normative Regulation Policy, the Instructions on Internal Normative Documents Management , within the framework of the recommendations of the Know Your Customer Basel Committee, the Financial Action Task Force on money laundering (FATF).

Section 1. THE GENERAL PROVISIONS

1. The Policy was developed with the aim of determining the main principles and directions in execution of the AML/FT Law requirements and is aimed at prevention of transactions with money and (or) other property, performed by the customer through the Bank for criminal purposes and non-admittance of risk of involvement of the Bank into transactions of the customer, related to legalization (laundering) of proceeds of crime and the financing of terrorism.

2. In the Policy there are used the main notions, stipulated in the legislation of the Republic of Kazakhstan (hereinafter – the RoK), as well as the following notions, abbreviations and conventional notations:

1) **the Bank** – Eurasian Bank JSC and its Branches;

2) **the beneficiary owner** – an individual, who directly or indirectly owns more than twenty-five per cent of participation interests in the chartered capital or of placed (exclusive of the privileged and redeemed by the company) shares of the customer legal entity, as well as an individual, exercising control over the customer in a different manner, or in the interests of which the customer preforms transactions with money and (or) other property;

3) **The Financial Action Task Force on money laundering (FATF)** is the intergovernmental organization, developing the recommendations in the area of combatting money laundering and the financing of terrorism;

4) **business relationship** is a relationship of providing by the Bank to the customer of services (products), related to financial activities and financial services;

5) **the customer file** is the customer information, obtained within the framework of due diligence of the customer, his/her representative, the beneficiary owner with the aim of identification and registration of the customer information and data in hard copy and/or in e-format;

6) **foreign public official** (hereinafter – FPO) is a person, appointed or elected, holding any position in the legislative, executive, administrative, judicial body or military forces of a foreign state, and/or

any person, performing any public function for a foreign state, and/or

any person, occupying a position in management of companies, founded on the basis on treaties having the international treaty status;

7) **an authority of a foreign state** is a body of a foreign state, performing in compliance with its legislation the collection, processing, analysis and use of information about transactions with money and (or) other property;

8) **due diligence** consists of actions, performed in the aims of collection of data, information and documents in relation to the customer, his representative and beneficiary owner, including on transactions with money and/or other property;

9) **risk management of legalization (laundering) of illegally obtained money and the financing of terrorism** (hereinafter – ML/FT) is an amount of actions taken by the Bank on identification, assessment, monitoring the ML/FT risks, and also their minimization (in relation to products/services, customers, and also transactions performed by customers);

10) **the ABFM list** is a list of organizations and persons, related to the financing of terrorism and extremism, formed by the authorized body for financial monitoring;

11) **AML/FT** – counteraction of the legitimation (laundering) of proceeds of crime and the financing of terrorism;

12) **a suspicious transaction with money and (or) other property** is a transaction of the customer (including an attempt of performing such a transaction, a transaction being in the course of performing or a

transaction already performed), in relation to which there appear suspicions on that money and (or) other property, used for performing it, are proceeds of crime, or a transaction itself is aimed at legitimation (laundering) of proceeds of crime and the financing of terrorism or any criminal activities;

13) **the customer relations subdivision employee** is an employee of a structural subdivision of the Bank, of Bank Branch, whose function is, including setting business relationship with customers, concluding deals with customers, conducting customers' conversion transactions, concluding deals on behalf of the Bank at the customers' expense, additionally, cashiers and currency controllers;

14) **Compliance subdivision employee** is the Bank's Compliance and Internal Control Service employee, whose functions include the AML/FT issues pursuant to The Rules of internal control within the aims of counter-acting legalization (laundering) of proceeds of crime and the financing of terrorism (hereinafter – the Rules of internal control), The Regulations on the Compliance and Internal Control Service, the job description;

15) **the sanction directories (lists)** are the directories (lists) of organizations and persons, in relation to which by competent bodies of foreign states, the UN Security Council there have been introduced the sanctions (resolutions), and other directories (lists), pursuant to the Rules of internal control;

16) **the authorized body for financial monitoring** is a state body, performing financial monitoring and taking other actions on counteraction of the legitimization (laundering) of proceeds of crime, the financing of terrorism, the financing of proliferation of weapons of mass destruction in accordance with the AML/FT Law;

17) **the authorized internal control employee within the AML/FT aims** is the head of a structural subdivision of the head office of the Bank, Managing/Executive Director – Branch Director or any other Bank employee who, in compliance with an order (instruction) by the Bank, assumed responsibility for provision and control over implementation in the Bank of relevant actions in compliance with the RoK legislation and the internal normative documents of the Bank on the issues of the counteraction of the legitimation (laundering) of proceeds of crime and the financing of terrorism.

3. Other specific terms and contractions, sued in the Policy text, are used in the meaning, assigned in other internal normative documents of the Bank (hereinafter – the INDs of the Bank), and at their absence in the INDs of the Bank - in the meaning, assigned in the RoK legislation or accepted in the international banking practice.

Section 2. THE SPECIAL PROVISIONS
Chapter 1. The main tasks

4. In the aims of effective AML/FT implementation, the Bank in its activities shall be guided by the following Know Your Customer main tasks:

1) performing due diligence (identification) of the customer, his/her representative, the beneficiary owner prior to setting business relationship with him/her;

2) excluded;

3) prohibition on opening banking accounts in the name of anonymous owners, that is without submittal by a person opening a bank account of documents required for the customer's due diligence;

4) prohibition on accepting a transaction for execution from/for anonymous owners;

5) right for refusal in rendition/provision of banking services to the customer, his/her representative on the condition that such a right of the Bank is stipulated in an agreement concluded with such a customer, in the following cases:

– availability of information on the customer, his/her representative, the beneficiary owner in the ABFM list and in the sanction directories (lists);

– if one party/ participant of a transaction/deal or transaction obligation is a person, registered/being in a country with significant risks of money laundering and the financing of terrorism, determined by an international organization, a competent body of a foreign state or the authorized body, or if such a person participates in execution of such transaction/deal;

– assigning the customer a "critical" risk level;

– in other cases stipulated by the INDs of the Bank, and also if refusal is stipulated and/or permitted by the RoK legislation or an agreement, concluded between the Bank and the customer;

6) prohibition on setting relationship with banks that do not take appropriate actions for prevention of the legitimation (laundering) of proceeds of crime and the financing of terrorism, or do not have factual presence in states where they are registered;

7) taking required actions for revision of personal identity/authenticity of the customer, his/her representative, the beneficiary owner, based on submitted documents and non-performance of transactions prior to identification of personal identity of the customer, his/her representative, the beneficiary owner;

8) finding out the assumed purpose of the customer's contact with the Bank and further nature of business relationship;

9) conducting monitoring of the customer's activities regarding correspondence of the purposes stated by the customer;

10) taking appropriate actions for identification in the customer's activities of transactions subject to financial monitoring, including suspicious transactions with money and/or other property;

11) informing the authorized body on transactions subject to financial monitoring, including suspicious transactions with money and/or other property;

12) taking additional actions regarding customers with high and/or critical risk level;

13) performing registration of data and information on the customer, his/her representative, the beneficiary owner;

14) provision of storage of required documents and information within the term set by the RoK legislation and the INDs of the Bank;

15) review and updating the information on the customer, his/her representative, the beneficiary owner taking into account the risk-oriented approach;

16) prohibition on informing the customer, his/her representative on actions taken in the Bank in the AML/FT aims;

17) organizing required training of the Bank employees on implementing by them in current work of the provisions of the Policy and other INDs of the Bank, regulating the actions taken by the Bank for implementation of the AML/FT Law requirements.

5. To perform the set Policy tasks, employees of customer relations subdivision shall be guided by the Rules of internal control.

Chapter 2. The main requirements of due diligence of the customer, his/her representative, the beneficiary owner.

6. In the aims of due diligence of the customer, his/her representative, the beneficiary owner the following actions are performed:

1) registration of information required for identification of the customer, his/her representative;

2) identification of the beneficiary owner and registration of information required for his identification;

3) identification of the assumed purpose and the nature of business relationship;

4) performing on a regular basis of revision of business relationship and studying of transactions conducted by the customer through the Bank, including if required getting and registration of information on sources of financing the transactions conducted;

5) revision of authenticity of information required for identification of the customer (his/her/its representative), the beneficiary owner and updating of information on the customer, his/her/its representative and the beneficiary owner.

7. Due diligence of the customer, his/her representative, the beneficiary owner is performed by an employee of customer relations subdivision based on documents and information submitted by the customer himself (herself) or his/her representative to the Bank. The list of documents and information, required for due diligence of the customer, his/her representative, the beneficiary owner is determined by the RoK legislation and the INDs of the Bank.

8. Identification of the beneficiary owner is performed based on information and (or) documents, submitted by the customer. In case if the beneficiary owner of the customer, a legal entity, is not identified, a single executive body or a head of collegial executive body of the customer can be recognized as the beneficiary owner.

9. The Bank details in documents should comply with RoK legislation requirements (availability of all required signatures, dates, seals, stamps if required by the RoK legislation). Documents are accepted at absence of erasures, typeovers, writeovers and should not cause doubts in credibility of a submitted document.

10. All the documents, submitted by the customer or his/her representative for due diligence should be valid as of date of their submittal. Documents with expired validity date are not accepted for review and are not used for due diligence.

11. When conducting due diligence of the customer the Bank documentarily registers information on him on the basis of submitted at the customer's (his/her representative's) discretion of originals or notarized copies of documents, or copies of documents with apostille or in a legalized order established by international treaties, ratified by the RoK.

12. If it is required to obtain additional information in the aims of studying its customers, the Bank can use documents and information, obtained from other sources, available to the Bank on a legal basis and authenticity of which do not cause doubts (bodies of state authority and management, legal and judicial bodies, official reference books and other sources).

13. Documents and information, obtained by the results of due diligence of the customer, including the customer file, account details, and correspondence with him should be stored for not less than five years from the date of termination of business relationship with the customer. Documents and information on transactions with money and (or) other property, subject to financial monitoring, and suspicious transactions with money and (or) other property, and also results of studying all complex, unusually large and other unusual transactions should be kept for not less than five years from the date of conducting a transaction.

The documents and information specified in this paragraph shall contain information that is stipulated by the Rules of internal control.

14. Data and information on the customer, his/her representative, the beneficiary owner are registered in the customer file by a customer relations subdivision employee, including by way of filling in (formalization) of the customer card.

15. The form and requirement on formalization of the customer card are determined by the Rules of internal control.

16. At conducting by the customer of a transaction (deal) with money and (or) other property, a customer relations subdivision employee should perform revision regarding correspondence of the information on the customer, his/her representative, the beneficiary owner with the ABFM list and the sanction directories (lists). Revision is performed using the Bank's software complex, in the automated mode, or in cases of absence of required software by way of manual reconciliation.

17. A customer relations subdivision employee cannot perform due diligence of the customer, his/her representative, the beneficiary owner, if such has already been identified by the Bank and a customer relations subdivision employee was provided with a current permanent access to the information on this customer, his/her representative, the beneficiary owner, contained in the customer file.

18. A customer relations subdivision employee should conduct a repeated due diligence of the customer, his/her representative, the beneficiary owner, if he gets doubts in credibility of data, obtained earlier in the result of implementation of actions on their identification. At that a customer relations subdivision employee can employ a security subdivision for conducting due diligence of the customer, regarding authenticity and timeliness of submitted documents and information.

19. In case it is impossible to take actions, stipulated in sub-paragraphs 1), 2) and 3) of paragraph 6 of the Policy, business relationship with the customer are not established.

In case it is impossible to take actions, stipulated in sub-paragraphs 1), 2), 3) and 5) of paragraph 6 of the Policy, transactions with money and (or) other property are not conducted.

Chapter 3. The main requirements of due diligence of a foreign public official

20. In compliance with the recommendations of international organizations and foreign authorities– The Financial Action Task Force (on Money Laundering) (FATF) the following foreign nationals can be referred to the FPOs category:

1) Persons, who assumed or have previously assumed (from the date of quitting the office less than one year passed) execution of important state functions, and notably:

– heads of states (including reigning royal dynasties) or governments;

– ministers, their deputies and assistants;
– higher government officials;
– public officials of judicial bodies of the last instance authority (the Supreme, the Constitutional Court), whose decisions are not appealed;
– state prosecutor and his deputies;
– higher military officials;
– heads and members of the Boards of Directors of the National Banks;
– ambassadors;
– heads of state corporations;
– members of Parliament or other legislative body;

2) persons, lodged with public confidence, in particular:

– heads, deputy heads of international organizations (the United Nations Organization (UNO), the Organization of Economic Cooperation and Development (OECD), Organization of the Petroleum Exporting Countries (OPEC), the Olympic Committee, the World Bank and others), the European Parliament members;
– heads and members of international judicial organizations (European Court of Human Rights, the Hague Tribunal and others);

3) other persons, appointed or elected, holding any office in a legislative, executive, administrative, judicial body or military forces of a foreign state, any persons, performing any public function for a foreign state, as well as persons occupying a position in management of organizations founded on the basis of treaties with international treaty status.

21. Identification of FPOs is performed by customer relations subdivision employees prior to establishment of business relationship with the customer, based on documents and information, obtained at identification. Repeated (control) revision is performed at registration of the customer data and information in the customer file in the automated mode using the commercial list of foreign public officials and persons associated with them, developed and supported by the Factiva informational-analytical service.

22. For FPOs identification customer relations subdivision employees can use the following information sources:

1) documents and information, obtained at the customer due diligence. Information on the customer status can be obtained from an identity document, or a document confirming the right to reside in the RoK territory. If the data on the occupied position are given by the customer himself/herself, a customer relations subdivision employee can request from the customer the documents, certifying the status of FPO, with further copying of the document and its storage in the customer file;

2) data, obtained in the result of one's own investigation of public access sources, periodic publications, including using the Internet.

23. Establishment (continuation) of business relationship with FPOs is performed upon permission of the managing employee of the Bank for establishment (continuation) of business relationship with such a customer.

Chapter 4. Management of risk of the legitimation (laundering) of proceeds of crime and the financing of terrorism

24. The procedure of organization of ML/FT risk management by the structural subdivisions of the Bank regarding AML/FT is determined by the Rules of internal control, the INDs of the Bank, regulating activities of customer relations subdivisions, the Regulations on customer relations subdivisions and the Regulations on the compliance subdivision.

25. The main task of ML/FT risk management is classification of customers and sectors of the Bank activities (products and (or) services, rendered to customers) by risks levels for focusing attempts on sectors exposed to the highest risks level. In the aims of ML/FT risk management the Bank employees should perform the following procedures:

1) risk identification, including detection and assessment of risk level;
2) measures on prevention of risk realization (minimization).

26. Assessment of customer risk level can be performed by customer relations subdivision employees at the identification stage when setting business relations and is the result of analysis of the documents, information and data on the customer and his/her activities available at the Bank. Subsequently,

based on the data, received in the result of investigation of the customers, including on their transactions, and as far as the customer information is updated, ML/FT risk level can be changed (reconsidered) both in the automated mode by relevant software, and by the compliance subdivision employees by the results of monitoring of transactions (business relationship) and as far as the information about the customer (his/her/its representative) and the beneficiary owner is updated.

27. In the aims of ML/FT risk management, a customer relations subdivision employee should duly perform procedures on identification and registration of customer data in the customer file pursuant to the Rules of internal control.

28. Assessment of ML/FT risk level is performed in relation to all customers, including customers, conducting transactions without opening a bank account. Customers, in relation to whom the procedure of registration within the framework of identification and due diligence is not performed, assessment of risk level is not performed.

29. ML/FT risk level is grouped as "low", "medium", 'high" and "critical". Depending upon the ML/FT risk level, the appropriate client due diligence procedures shall apply pursuant to the Rules of internal control.

30. The structure of the ML/FT risk levels assessment includes the following types (categories) of risks level:

1) risk by customer type;
2) service (product) risk and/or method of its provision;
3) country (geographical) risk.

31. Compliant with Regulation No. 188 and the INDs of the Bank, the compliance subdivision performs preparation and submits the appropriate reporting in the AML/FT field to the Management Board, Committee at the Board of Directors, the Board of Directors of the Bank.

SECTION 3. THE CONLUDING PROVISIONS

32. An authorized employee on the issues of internal control in the AML/FT aims bears responsibility for timely, full and quality performance of tasks and aims of a structural subdivision, determined in the Policy, INDs and other documents of the Bank, regulating procedures in the AML/FT area.

33. Responsibility for conducting due diligence of the customer, his/her representative, the beneficiary owner is assumed by the structural subdivisions of the Bank, establishing business relationship with the customer, including acting as initiators of conclusion of agreements with respondent banks and other financial organizations within their authorities.

34. All the Bank employees bear responsibility for observance of the confidentiality mode and non-disclosure to the third parties of information on procedures, performed by the Bank in the AML/FT aims and confidential information, obtained in the result of application of the Policy.

35. The Policy comes into force on the following business day after introduction into the INDs DB of the Bank are obligatory for application and guidance by all Bank employees.

36. Issues, not regulated by the Policy, are solved in compliance with the RoK legislation and the INDs of the Bank.

37. Changes and amendments are introduced into the Policy as required, in compliance with the normative legal acts of the RoK and the INDs of the Bank.