SANCTIONS POLICY

CONTENT

Policy Summary Profile 2
1. Introduction 3
2. Objective 3
3. Scope 3
4. References 3
5. Responsibility 4
6. Effective Date and Amendments 4
7. Definitions and Abbreviations 4
8. Policy Statement 6
9. Senior Management and Financial Crime Compliance Division Responsibilities 6
10. Individual Employee Responsibility 7
11. Transparency 8
12. Sanctions Risk Assessment and Management 8
13. Sanctions Breaches 8
14. Training 9
15. Record Retention 9
16. Audit 10

Responsible	Approval	Enforcement Approval	Confidentiality
Internal Control and Compliance Department	Board of Directors	HR	Inhouse

SANCTIONS POLICY

Policy Summary Profile

Policy Name	Sanctions Policy
Function/Division	Enpara Bank A.Ş Financial Crimes Compliance Unit
Date Created	20/09/2024
Next Review Date	20/09/2025
Last Updated Date	10/09/2026
Last Review Date	10/09/2026
Version	2.0

SANCTIONS POLICY

1. Introduction

Enpara Bank (hereinafter referred to as "the Bank") has created this policy as part of Bank's Sanctions Compliance Program. In this context, the Bank adopts the Sanctions Policy (hereinafter referred to as the "Policy") that is subject to the Policy on AML/CFT.

2. Objective

The objectives of the Policy are the following:

- To demonstrate Bank's commitment to sanctions compliance,
- To articulate Bank's sanctions compliance program, which commensurate with Bank sanctions risk profile,
- To identify higher-risk areas of Bank's operations,
- To establish proper controls for customers and transaction screening,
- To document the requirement to report potential sanctions breaches to competent authorities,
- To articulate the role of independent testing in Bank's sanctions compliance program,
- To identify the responsibilities of Bank's Sanctions Compliance Officer,
- To describe how Bank, organization-wide, will maintain an up-to-date sanctions compliance program and respond to legal and regulatory changes,
- To ensure that Bank maintains effective controls to prevent and mitigate against potential sanctions breaches,
- To describe the process by which Bank will conduct,
- To protect Bank reputation from being involved or conducting business with or on behalf of any sanctioned country, organizations, activities, individuals and entities,
- To prevent Bank from financial risks associated to penalties linked to any breach of any sanctions program that might be applicable,
- To enhance the integrity of Bank in the financial markets, with respect to its shareholders, employees, customers and stakeholders.

3. Scope

This policy sets up the minimum requirements and guidelines, to mitigate potential Financial Crime Compliance and reputational risks associated to sanctions legislations and the risk of engaging in business relationships and transactions with sanctioned targets (individuals and entities).

All Bank employees must understand and comply with the Sanctions Policy.

4. References

The Bank will adhere to all the sanctions programs applicable to its operations in all jurisdictions where it conducts its businesses. This policy combines sanctions regulatory requirements and guidance, as well as financial industry best practices and market trends to

SANCTIONS POLICY

ensure compliance with sanctions programs imposed by, but not limited to, the following authorities and countries:

- Türkiye (any relevant official authority)
- Qatar (any relevant authorities)
- United States (OFAC)
- United Nations (UN)
- European Union (EU)
- United Kingdom (HMT)

This policy has been prepared in accordance with national and international legislation and QNB Group's obligations regarding sanctions regulations, and in case of any non-compliance, more stringent measures will apply.

5. Responsibility

The Internal Control and Compliance Department is responsible for the development, implementation, and, where necessary, periodic review and update of this Policy.

6. Effective Date and Amendments

Adequacy and effectiveness of this policy must be reviewed annually or whenever necessary. This Policy is issued in accordance with national and international regulations and obligations of QNB Group regarding sanctions and in case of compliance, more severe measures will apply.

This Policy and any amendments thereto shall enter into force upon approval by the Board of Directors, following the review and recommendation of the Audit Committee.

7. Definitions and Abbreviations

Sanctions: Refer to the totality of economic and legal measures, including the freezing of assets, prohibition of providing funds or financial services, and commercial restrictions, imposed by authorized international bodies such as the United Nations Security Council (UNSC), the European Union (EU), and the U.S. Office of Foreign Assets Control (OFAC) against specific countries, regimes, and natural or legal persons, with the objective of maintaining international peace and security, and preventing money laundering, the financing of terrorism, and the proliferation of weapons of mass destruction.

Fund: It refers to bank loans, bank and traveler's cheque, remittance, securities, stocks, collateral, bonds, bills, policies, letters of credit and similar securities, the value of which can be represented by money or money itself in any kind of form and all kinds of goods, rights, receivables movable or immovable, tangible or non-tangible and all kinds of documents, including electronic or digital, that confirm and represent property rights or interest on such goods, rights, receivables.

Asset: Asset is defined as funds and income partially or fully owned or possessed by, or directly or indirectly controlled by, a real or legal entity, and the benefits and value derived from

them or their conversion, funds and income partially or fully owned or possessed by a real or legal entity acting on behalf or account of them, and the benefits and value derived from them or their conversion to each other.

Asset freeze: Asset freeze refers to removal or restriction of the power of disposition on the assets in order to prevent the destruction, consumption, conversion, transfer, relocation and assignment of assets and other saving transactions (within the framework of exceptions).

Laundering Crime: Laundering crime is regulated under article 282 of the Turkish Criminal Law no.5237 dated September 26, 2004. This crime is generally defined as all kinds of transactions aimed at hiding the illegal sources of revenues obtained through predicate crimes and to make such revenues appear as if they were obtained from legal sources.

Terrorism Financing Crime: It refers to providing or collecting funds for a terrorist or terrorist organizations for the purpose of being used wholly or partially to perform the acts regulated as a crime as per article 3 of the Law no. 6415 on the Prevention of the Financing of Terrorism, or to do so knowingly and willingly, even without being linked to a specific act.

Financing the Proliferation of WMD: It is the violation of Law No. 7262 on the Suppression of the Financing of the Proliferation of Weapons of Mass Destruction and United Nations Security Council (UNSC) sanction decisions aimed at prevention of financing the proliferation of WMD.

Money Laundering/ Financing of Terrorism/ Financing of Proliferation of Weapons of Mass Destruction: ML/FT/FPWMD

Compliance Officer: The compliance officer is employed and authorized as required to ensure compliance with the obligations stated in the Law No. 5549 on Prevention of Laundering Proceeds of Crime and in the legislation implemented as per the Law.

Compliance Unit: This unit reports to the Compliance Officer and consists of the personnel assigned to carry out the compliance program. **(Financial Crime Compliance Division)**

Board of Directors: It is the decision-making body with the highest level of executive authority within the institution (BoD).

Senior Executive: According to the Regulation on Corporate Governance Principles of Banks, it refers to the bank's general manager, executive vice presidents (EVPs), managers of units within the scope of internal systems, and—even if employed under different titles—managers of units other than advisory units, who hold positions equivalent to or higher than an executive vice president (EVP) in terms of their authorities and duties.

Senior Management: According to the Regulation on Corporate Governance Principles of Banks, it refers to the Board of Directors and senior executives of the bank.

Audit Committee: According to Article 24 of the Banking Law No. 5411, refers to the committee consisting of at least two non-executive members of the board of directors, established to assist the board of directors in its audit and supervision activities.

SANCTIONS POLICY

QNB Financial Group: QNB Financial Group is comprised of QNB Bank, which is the parent financial institution, along with its subsidiaries and affiliates and the financial institutions located in Türkiye that are affiliated to or controlled by QNB Group, based on the financial group definition.

Customer Due Diligence (CDD): It refers to fulfilling the liabilities regarding identity authentication and verification and taking the measures for this purpose (confirming the authentication as required, determining whether the customer is acting on his/her own behalf or on behalf of another person, identifying the UBO, collecting information about the purpose and nature of the business relationship, etc.).

8. Policy Statement

The Bank is committed to full compliance with sanctions laws and regulations in the jurisdictions in which it operates.

The Bank must prevent the opening or maintenance of relationships or the execution of transactions for, on behalf of, or for the benefit of, a sanctioned individual, entity, country or organization in violation of the sanction laws and regulations.

This policy establishes the minimum standards for:

- Screening of customers and connected parties' names
- Screening of transactions processed through the Bank
- Screening of Bank employees and service providers
- Assessment and response for potential true matches
- Maintenance of sanctions lists used for screening
- Management of sanctions regulatory licenses
- Provision of Sanctions Regulatory Reports
- Staff awareness and training
- Production and reporting of Sanctions management information
- Sanctions Risk Assessment framework

9. Senior Management and Financial Crime Compliance Division Responsibilities

Board of Directors and Executive Management are accountable and committed to full compliance of all sanction laws and regulations applicable to Bank business and operations.

Executive Management is responsible for ensuring that sufficient and effective resources, systems and processes operating across Bank are available to support Financial Crime Compliance Division to mitigate the sanctions risk across the Bank allowed by the local laws and regulations.

Senior management has the following responsibilities:

- Ensure that Financial Crime Compliance Division has sufficient authority and autonomy to deploy Bank Sanctions Policy and Procedures,

SANCTIONS POLICY

- Oversee the implementation of the Sanctions Policy and applicable sanctions controls across business departments and operational areas,
- Ensure the existence of direct reporting lines between the Sanctions Compliance Program functions and senior management, including the appropriate forum for discussion and report of sanctions matters,
- Demonstrate recognition of the seriousness of potential sanctions breaches of the relevant sanctions laws and regulations administered by the relevant sanction authorities, or malfunctions, deficiencies, or failures by the Bank and staff to comply with the Sanctions Compliance Program, and implement necessary measures to reduce the occurrence of potential sanctions breaches and represent systemic solutions whenever possible.

Financial Crime Compliance Division is responsible for implementing, developing and reviewing this Policy approved by the BoD and the BoD is ultimately responsible for ensuring the fulfillment of the obligations to which the Bank is subject within the scope of the relevant regulations. The Chief Internal Control and Compliance Officer is responsible for the Bank's risk assessments regarding of policies and procedures regarding this issue in accordance with sanction regulations and QNB Group Policies.

Financial Crime Compliance Division has the following responsibilities:

- To ensure that this policy is update and aligned with the relevant sanction developments affecting Bank.
- To provide consistent and effective sanctions advisory to the different areas of the Bank.
- To oversee, review and assess the financial crime compliance risk of sanctions across the different Bank business and operational areas.
- To produce and deliver sanctions trainings and awareness to Bank employees to leverage staff capabilities regarding to sanctions risk and how to mitigate it.

10. Individual Employee Responsibility

This policy applies to all Bank employees and to support this policy, all employees are required to:

- Comply with this policy, applicable sanctions laws, regulations, and supporting control procedures,
- Report to Financial Crime Compliance Division any customer activity involving sanctioned countries, individuals and entities, as well any notice of internal support to, or customer intention to circumvent or evade sanctions,
- Not give any advice to customers that can instruct how to structure a transaction or a customer CDD to evade Bank sanctions controls,
- Employees that fail to comply, negligee or deliberated ignore this policy may be subject to administrative disciplinary actions. Employees responsible for breaches on sanctions laws and regulations may also be subject to criminal prosecution.

SANCTIONS POLICY

11. Transparency

Bank employees cannot change, delete or hide the instructions, documents and/or information contained in the data of the parties to the transaction, in order to avoid sanctions or to prevent the detection or emergence of an issue related to sanctions. Requests from the other party to delete or hide the relevant names, addresses or other information included in the transaction records or documents related to the transaction and sanction lists, should be rejected and these requests should be immediately forwarded to the Financial Crime Compliance Division.

Any deviation or non-compliance to the requirements of this policy must be reported to Financial Crime Compliance Division, which will assess the risk(s) and advice on the implementation of alternative controls to mitigate the inherent risk(s) of sanctions.

12. Sanctions Risk Assessment and Management

Following a risk-based approach methodology, on an annual basis, Financial Crime Compliance Division will perform a Sanctions Risk Assessment, which consists of the following:

- Identify, review and assess the inherent risk of sanctions that Bank is exposed to,
- Map all systems, process and procedures in place to control and mitigate the sanctions risk,
- Evaluate the efficiency and effectiveness of the existing controls in place,
- Recommend remediation action plans for the identified control deficiencies.

Sanctions risk assessment is subject to reviews caused by Bank organizational changes, as well for external events, such as but not limited to new or material amendments in sanctions laws and regulations.

Bank sanctions screening program uses a centralized sanctions screening tool for matching names and accounts based on the Bank's particular risks.

13. Sanctions Breaches

Any failure to follow Bank Sanctions controls is considered a breach. Breach can be considered a policy breach or a potential regulatory breach. Policy breach is when Bank standard controls to mitigate the risk of sanctions is not followed, increasing the risk of Bank failing to comply with the sanctions laws and regulations, which is considered a potential regulatory breach.

Potential Sanctions breaches are identified by automated sanctions screening processes for customers and transactions, by the investigation of downstream rejected payments, internal escalations, whistleblowing, etc. Root cause analysis, as well investigation surrounding all potential sanctions breaches is performed. As part of remediation actions, customers can be notified about the potential sanctions breach and reminded about Bank Sanctions Policy. In certain cases, relationship termination and or the curtailment of certain services and products (ring fence) can be considered.

SANCTIONS POLICY

All potential breaches (policy or regulatory), must be communicated to Financial Crime Compliance Division, which will review and advice on the necessary actions for remediation and report to the competent authorities (if applicable).

14. Training

The Bank's sanctions training program is tailored to the Bank's risk profile and all appropriated employees and stakeholders.
Sanctions training program provides adequate information and instruction to employees and, as appropriated, stakeholders (for example: Business partners and counterparties) in order to support Bank's sanctions compliance efforts.

In order to enhance the culture of compliance across Bank business operations, sanctions training should be delivered to all Bank staff in an annual basis and upon requirement. The Bank carries out training activities by organizing seminars and panels, establishing working groups, using audio-visual materials and providing computer aided training programs. All employees are included in the scope of such training programs (except drivers, executive and platform assistants, technical personnel, security guards, etc.)

Sanctions training should consider at least the following aspects:

- Sanctions compliance responsibilities is communicated for each employee,
- Training content is tailored and appropriate for the different staff roles and exposure to sanctions risk,
- Training is accessible and routinely delivered,
- Refreshed/Recycled training content is produced to ensure that knowledge remains current and up-to-date,
- Staff are tested, as appropriate, to ensure that they have understood the training.

Following sanctions matters should be included in the training as a minimum:

- Definition of sanctions
- Applicable regulatory sanctions requirements
- Sanctions Authorities (Local and Global)
- List of prohibited countries and key sanctions programs
- Examples of sanctions breaches and evasion attempts
- Consequences of non-compliance with sanctions policies and regulations
- Bank key sanctions controls

15. Record Retention

The Bank should keep the records related to customer accounts and transactions for at least 10 years pursuant to the Banking Law and relevant regulations.

The key sanctions records are the following:

- Specific License authorizing a transaction/account,

SANCTIONS POLICY

- Sanctions Regulatory reports,
- Sanctions trainings attendance lists and content,
- Automated screening alerts for customers and transactions,
- Potential Sanctions Breaches reports.

16. Audit

Internal Audit Department regularly carries out audits to evaluate adequacy and effectiveness of measures taken by the Bank to assess, monitor and manage national and international sanction risks.

The Bank should ensure that, upon becoming aware of a confirmed adverse test result or audit finding related to its sanctions compliance program, whether detected internally or by an external party, it takes prompt and effective action, to the extent possible, to identify and implement compensating controls until the cause of the weakness can be identified and remediated.