


| | | | |
|---|--|--|---|
| Version | 3.0 | Document category | Policy |
| Drafted by | Compliance Unit | Date of drafting | 01/2/12/2023 |
| Reviewed By | Corporate Secretary, Legal and Risk Management Department | Date of revision First approval | 07/12/2023 12/06/2017 |
| Approved by | Supervisory Board | Resolution, Minutes Number and Date | Resolution #2.1, Minutes #06 Dated:26.02.2024 |
| Person responsible for the fulfillment | | Compliance Unit | |
| Addresses | | Everyone | |
| Reference # and name the document | CMP_PL_01_Compliance Policy | Chairman of the Supervisory Board Rovshan Allahverdiyev |  |

Compliance Policy

JSC PASHA Bank Georgia

TABLE OF CONTENTS

| | | |
|------|--|---|
| 1. | PURPOSE | 3 |
| 2. | TERMS AND ABBREVIATIONS..... | 3 |
| 2.1. | Abbreviations | 3 |
| 3. | ROLES AND RESPONSIBILITIES | 3 |
| 3.1. | The roles and responsibilities of the Supervisory Board are to: | 3 |
| 3.2. | The roles and responsibilities of the Board of Directors are to: | 3 |
| 3.3. | The roles and responsibilities of Compliance Unit are to: | 3 |
| 3.4. | The roles and responsibilities of employees are to: | 3 |
| 3.5. | The roles and responsibilities of the DPO are to: | 4 |
| 4. | COMPLIANCE PRINCIPLES | 4 |
| 4.1. | Engage in and promote business and professional ethical conduct | 4 |
| 4.2. | Comply with laws, regulations, rules and professional standards | 4 |
| 4.3. | Avoid any conflicts of interest | 5 |
| 4.4. | Protect confidentiality | 5 |
| 4.5. | Protect the customer's best interests | 5 |
| 5. | COMPLIANCE RISKS | 5 |
| 6. | PERSONAL DATA PROTECTION OFFICER (DPO)..... | 6 |
| 7. | REPORTING..... | 6 |
| 8. | FINAL PROVISIONS | 7 |

1. Purpose

The purpose of the Compliance Policy (the “Policy”) is to provide guidance to the governing bodies and to all employees of JSC PASHA Bank Georgia (the “Bank”) and is intended to communicate general concepts, principles, directions and requirements of compliance function.

2. Terms and Abbreviations

2.1. Abbreviations

The following abbreviations are used in the Policy:

DPO - Personal data protection officer

3. Roles and Responsibilities

3.1. The roles and responsibilities of the Supervisory Board are to:

- Approve the Compliance Policy;
- Review reports of Compliance Unit;
- Oversee the implementation of the Policy.

3.2. The roles and responsibilities of the Board of Directors are to:

- Ensure that the Policy is adhered to;
- Review reports of Compliance Unit;
- React promptly and effectively to the arisen compliance issues.

3.3. The roles and responsibilities of Compliance Unit are to:

- Ensure compliance with all relevant laws, regulations, rules and professional standards and inform relevant Departments/Units regarding the changes;
- Assist senior management in the management and control of regulatory compliance risks;
- Ensure proper handling of customer complaints which refers to the issue of Personal Data;
- Identify and assess the regulatory compliance risks;
- Report to relevant regulatory body;
- Report to the Supervisory Board and the Board of Directors;
- Inform and train employees on compliance and personal data issues.

3.4. The roles and responsibilities of employees are to:

- Ensure compliance with all relevant laws, regulations, rules and professional standards;

- Report immediately to Compliance Unit on violations of relevant laws, regulations, rules and professional standards.

3.5. The roles and responsibilities of the DPO are to:

- To inform the Bank and their employees on issues related to personal data protection, including the adoption or change of regulatory legal norms, providing them with consultation and methodical assistance.
- Participation in the development of the internal regulations related to personal data processing and the impact assessment document on data protection, as well as the monitoring of the implementation of the requirements set by the Georgian legislation and internal organizational documents by the Bank.
- Receiving consultations from the Personal Data Protection Service, submitting information and documents at its request, and coordinating and monitoring the execution of its tasks and recommendations.
- Analysis of received statements and complaints regarding personal data processing and issuing relevant recommendations. In the case of the data subject's request, to provide him with information about data processing processes and his rights;
- Raising the awareness of employees in order to raise the standards of personal data processing in the bank.

4. Compliance Principles

4.1. Engage in and promote business and professional ethical conduct

The Bank shall not seek advantage through illegal or unethical business practices. Indeed, all employees are expected to exhibit the Bank's shared value of integrity. The Board of Directors of the Bank have ultimate responsibility for setting the direction and tone of the Bank's policies and practices in line with this shared value of integrity.

Employees shall carry out their responsibilities honestly, in good faith and with integrity, as well as behave with due care, competence, prudence and diligence, exercising their best independent judgment at all times.

4.2. Comply with laws, regulations, rules and professional standards

Employees act in accordance with the written policies and procedure of the Bank in order to ensure full compliance with laws, regulations, rules and professional standards helping to maintain the Bank's reputation.

The Bank commits to keep the employees up to date on applicable laws and regulations.

Any violation of laws, regulations, rules and professional standards are to be reported immediately to the Compliance Department.

4.3. Avoid any conflicts of interest

Employees shall conduct their business affairs in a manner that ensures their private or personal interests do not interfere with the interests of the Bank or its shareholders including conflicts relative to personal, financial, or other gain. The Board of Directors ensures that a strict segregation of functions is respected and that the necessary measures are taken to safeguard the separation between own account transactions and those for third parties.

4.4. Protect confidentiality

Employees maintain the confidentiality of all information entrusted to them, except when disclosure is authorized or required by law. Strictly confidential, confidential or proprietary information of the Bank includes any non-public information the disclosure of which would be detrimental to the Bank or its shareholders or useful to its competitors.

Employees who leave the Bank are under the ongoing obligation to keep such information confidential.

4.5. Protect the customer's best interests

Employees provide their services to meet the customers' best interests. The Bank always owes its customers a duty of care, honesty and trust. Employees shall be free of any influence, interest or relationship in respect of the customers' affairs, which impairs or risks to impair their professional judgment and objectivity.

The Bank shall handle any customer complaint in an appropriate manner, process them timely and document replies accordingly.

5. Compliance Risks

The Compliance Policy is constituted of all measures, actions and options decided in order to limit risks to an acceptable level in pursue of the Bank's global objectives.

The main Compliance risks are identified as follows:

- **Risk of breach of ethical rules**

This refers to the risk of breach of ethical rules by the Bank or its employees.

- **Legal and regulatory risks**

This refers to the risk of non-compliance with applicable laws, regulations, and professional standards. This entails:

- Litigation risk: risk linked to the outcome of legal action;
- Contract/transaction risk: risk linked to misinterpretation or non-application of legal rules relevant to a contract or a transaction;
- Legislative risk: risk linked to changes in law and regulations.

- **Risk of sanctions**

This consists of:

- Risk of judiciary, administrative or disciplinary sanctions, as a result of non-compliance with laws, regulations, rules, norms and/or contractual agreements.

- **Reputation risk**

This refers to:

- Risk of damage due to the Bank's diminished worthiness and impaired reputation, resulting from true or false adverse publicity, failures in business practices and failures to comply with current laws and regulations.

- **Certain aspects of operational risks originating from or resulting in, one of the above risk.**

6. Personal Data Protection Officer (DPO)

In accordance with the Georgian Law "On Personal Data Protection", DPO must be appointed in the Bank.

Bank must ensure the proper involvement of the DPO in the process of making important decisions regarding data processing, provide him/her with appropriate resources, and also ensure his/her independence in the implementation of activities.

DPO must be independent in the decision making process and should be accountable to the management of the Bank.

7. Reporting

Compliance report is produced on a quarterly/semi-annual basis by Compliance Unit in which key risks, major developments and compliance incidents are brought to attention.

8. Final Provisions

This Policy is effective upon its approval by the Supervisory Board.

The responsibility to review the document for updates is vested upon Compliance Unit.

The Supervisory Board may amend this Policy, from time to time, upon recommendations from any member of the Supervisory Board, Board of Directors and/or Compliance Unit.

Chairman of the
Supervisory Board
of PASHA Bank
Georgia

Prokhor Allahverdiyev


8 pages