GROUP COMPLIANCE POLICY

Purpose

This Group Compliance Policy (the Compliance Policy) lays out the compliance and management principles and standards of compliance risks in Payjeezy (the Group).

The objective of this Compliance policy is to guarantee that compliance risks are well-identified, and adequately mitigated. The Group aims to reduce compliance risks with regard to the nature, scale and complexity of the business. This is aligned with the strategy of the Group, which sets the vision of the Group to be recognized as the most trusted financial partner, and is deeply linked to fair treatment of customers and conducting high integrity business.

This Compliance Policy is designed to meet the requirements of US Bank Security Act and additional applicable legislation. It is also acted in respect to all Financial Crimes Enforcement Network FinCen requirements as to Bank Secrecy Act (BSA), Anti-Money Laundering (AML) and KYC (Know Your Customer) laws.

Scope and application

This Compliance Policy applies to all staff, all roles, all divisions within the Company, and all controlled legal entities once adopted by Senior Management.

Definitions

Compliance is defined as compliance with laws, including the spirit of law, regulations, generally accepted practices, standards, and codes of conduct of the financial industry.

Compliance risk is defined in this Compliance Policy as the risk of legal or regulatory sanctions, material financial loss or loss of reputation that may result from the Group's failure to comply with laws, including the spirit of law, regulations, generally accepted practices, standards, and codes of conduct applicable to Group activities.

Governance

The Board of Directors is responsible for the Group's overall governance and regulatory risk management. The Board of Directors and the Executive Board must ensure that enough internal policies and structures are in place to provide effective and efficient support. Identifying compliance risks, their assessment and appropriate risk management are elements to be considered in any process and form the basis for a risk-based approach when appropriate and applicable countermeasures are established to mitigate the risk.

The Group has established three lines of defense and control governance model to ensure appropriate risk management:

- Business units and group functions represent the first line of defense and are primarily responsible for identifying, managing and mitigating the Group's compliance risks through adequate controls.
- Group Compliance is an independent risk control function led by Group Compliance Head and constitutes the second line of defense of compliance risk. Group Compliance is responsible for independent monitoring of the Compliance Risks of the Company, through risk assessment, tracking, consulting work and external reporting to senior management. Moreover, Group Compliance functions as the Group Data Protection Officer (DPO) and the Designated Group Conflicts Officer (DGCO).
- The Internal Audit Group is the 3rd line of defense and is responsible for auditing the 1st and 2nd line of defense in terms of validating that a robust framework is in place, being adequately implemented and evaluating the effectiveness of internal controls.

Compliance risk and risk tolerance

Compliance risks exists as an inherent part of doing business. Accordingly, compliance risk management in the Group is considered to be of key importance. Identifying compliance risks, their evaluation and effective risk management are elements that must be considered in any system and form the basis for a risk-based approach when determining necessary and relevant countermeasures to mitigate the risk; including the escalation of problem cases according to the Escalation Policy of the Group. Monitoring complaints handling processes in the Group and using complaints as a relevant source of information for compliance reporting is one of the elements for the basis of risk based approach.

Group Compliance must oversee the development and periodic review of the product governance arrangements. In this regard, information about products that are manufactured and distributed by the Group, including their distribution strategies, shall be systematically included in the compliance reports to the management body and made available to National Competent Authorities on request. The relevant Product Committee must assist Group Compliance by providing information about all products when they are developed or reviewed. To the extent required by applicable legislation, subsidiaries must allocate necessary resources to monitor relevant product governance arrangements.

Compliance with the laws on data protection is enabled by the terms of this Compliance Policy and implements them. Group Compliance will supervise compliance with the General Data Protection Regulation (GDPR) and relevant national data protection laws in its capacity as DPO.

The Group does not tolerate infringements of applicable laws, including the spirit of law, regulations, generally accepted practices and standards and codes of conduct applicable to the activities of the Group, substantial fines or other significant enforcement actions.

Compliance Framework

The Group's Compliance framework and strategy is distributed across three security sides. The Compliance Policy outlines the criteria of compliance risk mitigation to provide a comprehensive overview of the compliance framework of the Company. Other governing documents within, but not limited to, financial crime, conflicts of interest, market abuse, data protection, whistleblowing and code of conduct should be considered. As the control function, Group Compliance is responsible for designing, implementing and maintaining a group wide framework for compliance risk identification, assessment, monitoring and reporting. Group compliance follows a risk-based approach to identify, and prioritize the monitoring activities. In addition, Group Compliance is responsible for providing advice to business units and group functions related to compliance risk management and mitigation.

Reporting

Group Compliance must provide to the Executive Board, to the Audit Committee and to the Board of Directors a semi-annual compliance report. As a minimum, the compliance report must include findings of non-compliance.

Review

Group Compliance manages and updates the policy and the Board of Directors approves it. At least annually, the policy needs to be reviewed and updated. Any policy changes must be endorsed and approved by the Board of Directors by the Audit Committee.