GROUP COMPLIANCE POLICY

Purpose

This Group Compliance Policy (the Compliance Policy) outlines Synergy Pay Solutions (the Group) compliance and management concepts and standards for compliance risks.

The purpose of this Compliance policy is to ensure that compliance risks are appropriately identified and addressed. The Group attempts to mitigate compliance risks in relation to the business's nature, size, and complexity. This is consistent with the Group's strategy, which establishes the Group's aim of becoming the most trusted financial partner and is intrinsically related to treating clients fairly and conducting business with the utmost honesty.

This Compliance Policy is intended to comply with the requirements of the US Bank Security Act and other applicable laws. In addition, it adheres to all standards of the Financial Crimes Enforcement Network (FinCen) regarding the Bank Secrecy Act (BSA), Anti-Money Laundering (AML), and Know Your Customer (KYC) regulations.

Scope and application

Once adopted by the Senior Management, this Compliance Policy applies to all employees, all divisions of the company, and all controlled legal entities.

Exceptions to the general applicability of the Compliance Policy may be considered and approved by the subsidiary's senior management if the Compliance Policy contradicts with local standards. Any departures from the Compliance Policy that are material must be reported to the Board of Directors of Join2gether, the administrator of the Information Management Policy, and Group Compliance.

Definitions

Compliance is described as the observance of laws, including their spirit, regulations, generally recognized procedures, codes of behavior, and other financial industry-specific standards.

In this Compliance Policy, compliance risk is defined as the risk of legal or regulatory sanctions, material financial loss, or loss of reputation that may arise from the Group's failure to observe the laws, including the spirit of the law, rules and regulations, generally recognized practices, standards, and codes of conduct relevant to Group activities.

Governance

The Board of Directors is responsible for the governance and regulatory risk management of the Group as a whole. The Board of Directors and Executive Board must ensure that there are sufficient internal policies and processes in place to provide effective and efficient support.

Identifying compliance risks, assessing them, and managing them appropriately are factors to be considered in any process and serve as the foundation for a risk-based strategy where applicable and acceptable countermeasures are devised to minimize the risk.

The Group has built three defensive lines and a control governance approach to ensure proper risk management:

- The first line of defense represented by the business units and group functions are largely responsible for identifying, managing, and reducing the Group's compliance risks via effective controls.
- The second line of defense against compliance risk is composed of an independent risk control group which role is overseen by the Head of Group Compliance. Group Compliance is accountable for the independent monitoring of the Company's Compliance Risks via risk assessment, tracking, consultation, and external reporting to senior management. Group Compliance additionally serves as the Group Data Protection Officer (DPO) and the Designated Group Conflicts Officer (DGCO).
- The third line of defense consisting the Internal Audit Group is responsible for inspecting the first and second lines of defense in terms of assuring that a robust framework is in place, is being executed appropriately, and assessing the effectiveness of internal controls.

Compliance risk and risk tolerance

Compliance hazards are inherent to conducting business. Consequently, compliance risk management in the Group is regarded as being of paramount importance. Identifying compliance risks, evaluating them, and managing them effectively 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 in accordance with the Group's Escalation Policy. One of the cornerstones of a risk-based strategy is the monitoring of complaints handling processes within the Group and the use of complaints as a relevant information source for compliance reporting.

Group Compliance must oversee the creation and occasional assessment of product governance structures. In this regard, information about products manufactured and marketed by the Group, as well as their distribution strategies, will be routinely included in the compliance reports to the management body and made accessible upon request to National Competent Authorities. The relevant Product Committee must provide Group Compliance with information regarding all products when they are developed or reviewed.

The terms of this Compliance Policy facilitate and enforce compliance with the laws governing data protection. In its function as DPO, Group Compliance will oversee compliance with the General Data Protection Regulation (GDPR) and applicable national data protection regulations.

The Group does not tolerate violations of applicable laws, including the spirit of the law, regulations, generally recognized norms and standards, and codes of conduct that apply to the Group's activities, nor does it tolerate hefty penalties or other significant enforcement actions.

Compliance Framework

The Compliance structure and strategy of the Group are dispersed among three security sides. The Compliance Policy establishes the criteria for mitigating compliance risk and provides a complete overview of the Company's compliance system. Other governing papers should be reviewed, including but not limited to financial crime, conflicts of interest, market abuse, data protection, whistleblowing, and codes of conduct.

As the control function, Group Compliance is responsible for establishing, implementing, and maintaining a framework for the identification, assessment, monitoring, and reporting of compliance risks across the entire group. To identify and prioritize monitoring tasks, group compliance employs a risk-based methodology.

In addition, Group Compliance is responsible for advising business units and group functions on the management and reduction of compliance risks.

Reporting

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

The Head of Group Compliance reports to the Chief Financial Officer on a daily basis, with escalation lines to the Executive Board and the CEO of the Executive Board. If escalation is required outside of the Group compliance reporting period, the Head of Group Compliance will escalate through the relevant channels. The Head of Group Compliance has the authority and responsibility to escalate to the Audit Committee any material or systemic violations.

Review

The policy is managed and updated by Group Compliance, and it is approved by the Board of Directors. The policy has to be reviewed and revised at least annually.