SONATA FINANCE PRIVATE LIMITED

Compliance Management Policy

Version	Date of Approval / Review
V.1	10/08/2023

1. Background

Sonata Finance Private Limited ("Sonata" or "the Company") is committed to conducting its business activities lawfully and in a manner that is consistent with its compliance obligations. As part of the overall structure for Corporate Governance, Compliance Function serves a critical role. The Policy on Compliance Management has been framed in accordance with the requirements of RBI Circular on bearing number RBI/2022-23/24 Ref.No.DoS.CO.PPG./SEC.01/11.01.005/2022-23 dated April 11, 2022, on "Compliance Function and Role of Chief Compliance Officer (CCO) – NBFCs" to establish an independent Compliance function and in Sonata and to define its role and responsibilities.

2. Objectives

The purpose of the Policy on Compliance Management is to establish the overarching principles and commitment of the company with respect to achieving compliance by:

- identifying a clear compliance framework within which Sonata operates;
- promoting a consistent, rigorous and comprehensive approach to compliance throughout the organisation;
- developing and maintaining practices that facilitate and monitor compliance within the company;
- to ensure standards of good corporate governance, ethics and community expectations; and
- engendering a culture of compliance where every person within the company accepts personal responsibility for compliance and acts ethically and with integrity.

3. Creating the Culture of Compliance

Strong compliance culture is a pre-requisite for an effective compliance function. It is very important for the company to demonstrate a good Compliance Culture to maintain the reputation and win the trust of customers, investors and regulators. Such culture is essential element in the safe and sound functioning of the company and if not followed effectively may adversely affect the company's risk profile. Sonata ensures the compliance with core elements of this function viz. the laws, rules, regulations, and various codes of conducts and also to be in adherence with fair practice codes, managing conflict of interest and treating customers fairly to assist build a true Compliance Culture. The company shall promote awareness of compliance obligations and ethical values to maintain an appropriate compliance culture throughout its businesses. Compliance shall not be seen as an activity of the Compliance Department alone but as a culture that shall pervade across the company. It is however, reiterated that compliance is a shared responsibility of the business units and the compliance function. Therefore, adherence to applicable statutory provisions and regulations needs to be the responsibility of each staff member of the company and it is the work of the compliance function to ensure the same.

4. Structure of Compliance Function

The compliance function is an integral part of effective governance along with the internal control and risk management processes. The structural set up of the compliance function shall be consistent with the organisational needs. The Compliance function shall be headed by a Chief Compliance Officer (CCO) and shall consist of such number of professionals other than the CCO, as may be required to effectively manage the compliance obligations of the company. The Function shall include staff with basic qualifications and practical experience in business lines / audit & inspection functions, who are knowledgeable in legal cross-regulation, policy and products. The Compliance responsibilities pertaining to the specific area of work shall be exercised by staff of the respective departments, viz. Operations, Accounts, IT, HR etc. The departments concerned shall hold the prime responsibility to ensure the adherence to the statutory provisions and regulations applicable to their role in the company. However, the Compliance Function would need to ensure overall oversight.

5. Appointment and Functions of Chief Compliance Officer (CCO)

5.1 The appointment of CCO shall be recommended by the Remuneration & Nomination committee based on the credentials of the candidate and the final approval for the appointment shall be made by the Board of Directors of the company. The CCO shall be a senior executive of the company with a position not below three levels from the CEO. The Committee shall, while making the appointment, examine the 'Fit and Proper' criteria based on the requirements spelt out in this Policy.

5.2 CCO shall possess the following:

- Should be a Qualified Company Secretary having membership of the Institute of Company Secretaries of India (ICSI).
- Shall have a minimum experience of 15 years in Compliance management and NBFC sector.
- Good understanding of the industry and risk management practices, knowledge of regulations, legal requirements, and have sensitivity to Supervisory expectations
- Should have the ability to exercise judgment independently
- Should have a clean track record and unquestionable integrity

5.3 Intimation to RBI: A prior intimation to the Senior Supervisory Manager, Department of Supervision, Reserve Bank of India, shall be provided before appointment, premature transfer, resignation, early retirement or removal of the CCO. Such information shall be supported by a detailed profile of the candidate along with the 'Fit and Proper' certification by the MD & CEO of the NBFC, confirming that the person meets the prescribed supervisory requirements and rationale for changes, if any.

5.4 Reporting of Chief Compliance Officer: The reporting of the CCO shall be to the Managing Director of the company. Further the CCO shall also report directly to the Board of Directors and Committee's thereof and shall have the authority to interact with the regulators/supervisors.

6. Role of Chief Compliance Officer

6.1 Implementation of the compliance policy and identification and monitoring of the compliance risk through all the levels of the organisation.

6.2 Ensuring the appropriate remedial action if breaches are identified. The disciplinary action on such breaches shall however remain within the scope of the management.

6.3 Ensure that compliance function of the organisation identifies & compiles list of compliance failure and the concerned departments to take steps to mitigate re-occurrence of such failures.

6.4 Submit to the Board/ Audit Committee, on quarterly basis, the status of compliance with the regulatory requirements of different departments and to assist board/ committee members to make an informed judgment on whether the company is managing its compliance risk effectively

6.5 To act as a Nodal point of contact between the company and the Reserve Bank of India and to be a participant to the structured or other regular discussions with RBI.

6.6 Ensuring the timely response/ interactions thereof to the RBI inspection reports through the Compliance Function

6.7 Ensure that the policies, as are applicable upon the company through various regulatory directions are framed and approved by the Board of Directors and the same are reviewed annually is framed and approved by the Board of Directors**.**

6.8 Ensuring submission of the prescribed quarterly Compliance Certificate by the relevant departmental heads and to make efforts that the departments rectify the irregularities pointed out in these Compliance Certificate.

6.9 Leading the compliance function within the organisation and ensuring the fulfilment of the role of the compliance as per the responsibilities delegated to the compliance function.

7. Responsibilities of Compliance Function

7.1 Assist the Board and the Senior Management in supervising the implementation of Compliance Policy, including other policies of the company including the internal code of conduct.

7.2 Assess and identify potential compliance risk within the company, develop proposals for dealing with and avoiding compliance risks.

7.3 The Chief Compliance Officer (CCO) shall be a member of the 'new product' committee/s. All new products shall be subjected to intensive monitoring for at least the first six months of introduction to ensure that the indicative parameters of Compliance risk are adequately monitored.

7.4 Monitoring and testing the effectiveness of the compliance being done by the respective departments within the organisation and suggesting any updates. Circulation to the Senior Management/ Board of instances of Compliance failures, if any alongwith the preventive actions and fixation of the staff accountability for the breach of compliance.

7.5 Ensuring compliance of regulatory/ supervisory directions given by regulators including the Ministry of Corporate Affairs (MCA), Securities and Exchange Board of India (SEBI) and Reserve Bank of India (RBI) and Self-Regulatory Organisations (SROs), in both letter and spirit in a time-bound and sustainable manner. The compliance function shall put in place an effective Compliance Program where all Risk Mitigation Plan (RMP) / Monitorable Action Plan (MAP) points are complied with within the timelines prescribed.

7.6 Attend to compliance with directions from regulators and ensure that discomfort conveyed to the company on any issue by the regulators, and action taken by any other authorities/law enforcement agencies, shall be brought to the notice of RBI.

7.7 Serving as the reference point for the staff from the operational department for seeking clarifications/interpretation of various regulatory and statutory guidelines.

The company shall continue to have a dedicated risk management function headed by the Chief Risk Officer (CRO) which reports to the Board level risk management committee (RMC). The risk management function includes identification, assessment, reporting and avoidance/mitigation of organisational risk including regulatory and compliance risk, in accordance with the risk management policy of the company. The various risks faced by the organisation are identified and assessed and classified into low, medium or high-risk category on the basis of likelihood and impact. Detailed risk reports are presented to the RMC on a quarterly basis and appropriate action to address the key risk areas is taken as per the instructions of the committee. The risk management committee shall continue to carry out the risk assessment of various risks including the legal and compliance risk in accordance with the regulatory requirements.

8. Identification & Monitoring Mechanism:

The independence of the Compliance Function hinges on the extent of information and access granted to it in relation to the services, activities, and transactions undertaken by the regulated entity. In order to perform its duties and take its decisions independently, the Compliance team shall be granted access to all the relevant and pertinent information maintained by other departments, which is necessary for them to discharge their functions

effectively. The CCO and Compliance Function shall have the authority to communicate with any staff member and have access to all records or files that are necessary to enable her / him to carry out entrusted responsibilities in respect of Compliance issues.

The identification of the gaps in compliance of the regulatory requirements shall be made through the process of submission of periodical reports by the departmental heads of the departments which are directly involved in complying with the applicable statutory provisions relevant to the department concerned. Such reports shall be tested/verified by the compliance function and a summary report shall be placed before the Senior management alongwith the discrepancies/ non-compliance if any reported.

In order to ensure the compliance with the regulatory framework, the compliance function shall, on quarterly basis, list and place before the Board/ Committee all major regulatory guidelines issued and shall implement the directions of the board within the company.

As a measure to manage the compliance gaps, the relevant discussions /observations of the Senior Management shall serve as a feedback mechanism for the department to review the control mechanisms and take remedial measures to avoid recurrence of such failures/ breaches.

9. Authority of the Board of Directors / Committee's:

9.1 The Board of Directors retains the ultimate authority for legal and regulatory compliance and overseeing, reviewing and ensuring the effectiveness of Sonata's compliance systems. The board of directors has a fiduciary authority to oversee that the business is run in a profitable way within the bounds of the law. The Board/ Audit Committee shall remain empowered to the following functions:

- Review the Company's Internal financial controls and risk management policies/systems.
- Review the status of compliance on a periodic basis, on the basis of quarterly compliance reports submitted by the management, covering compliance with all laws and regulations applicable to the company.
- Review the Audit reports of internal and external auditors and audits/ inspections carried out by regulatory authorities and monitor the compliance of the observations highlighted in the audit and inspection reports
- Review the effectiveness of the company's Legal Compliance System for monitoring and managing compliance with relevant laws and to give instructions on breaches of key compliance requirements, if any, and remedial measures to prevent the instances of non-compliance

9.2 The compliance risk shall be reviewed on a quarterly basis wherein the compliance during the quarter shall be analysed the reason for any non-compliance or delay in compliance shall be discussed at the committee/Board level.

10. Independence and Authority

Independence is one of the fundamental principles of compliance and any regulated entity shall strive to establish and implement measures and controls in order to ensure that the duties performed, and the decisions taken, by the Compliance Function are carried out on an independently not only from the senior management, but even from all units within the regulated entity. Further there shall be no dual hatting ie. the compliance head shall not be given any responsibility which brings elements of conflict of interest, especially any role relating to the business. The CCO shall not be a member of any committee which conflicts his role as compliance head including the purchase committee/ sanction committee.

11. Compliance Risk Assessment

11.1 "Compliance risk" is the risk of legal or regulatory sanctions, financial loss, or loss to reputation an organization may suffer as a result of its failure to comply with laws, regulations, rules, related self-regulatory organisation standards, and codes of conduct applicable to its activities. Compliance risk management is the process of the identification of the risks that a business can face in relation to its legal compliance, and developing internal policies and procedures to better manage the risks associated with non-compliance. The importance of compliance risk assessment lies in analyzing the compliance risks and taking precautionary steps to avoid and control such risks.

11.2 The Risk Management department shall in co-ordination with the Compliance department, carry out the Compliance risk assessment in order to identify and assess major Compliance risks faced by the company and prepare a plan to manage the risks. The review shall ensure coverage of the following aspects:

i) Compliance failures, if any, and consequential losses and regulatory action, as also steps taken to avoid recurrence of the same;

ii) Compliance with fair practices codes and adherence to standards set by self-regulatory bodies and accounting standards; and

iii) Progress in the rectification of significant deficiencies and implementation of recommendations pointed out in various audits and regulatory inspection reports.

12. Reporting Requirements

12.1 Reporting to RBI: The company shall give prior intimation of appointment, premature transfer, resignation, early retirement or removal of the CCO to RBI in accordance with section 5.3 of this policy.

12.2 Reporting to the Board: Compliance should be a regularly scheduled agenda item at board meetings. Quarterly reports on compliance with statutory requirements shall be submitted to the Board, Audit Committee and Risk Management Committee.

12.3 Compliance Risk Review: The internal audit shall cover the compliance function/risk in the internal audit reports. Further the CCO shall be kept informed of audit findings related to Compliance, which shall serve as a feedback mechanism for assessing the areas of Compliance failures.

//**//**//