Code of Conduct for RegTech

JUN 2025

Fintech Association for Consumer Empowerment (FACE)
RBI-recognised Self-regulatory Organisation in the FinTech Sector (SRO-FT)

Version Control: Version 1.1 was published on 30 Jun 2025, with the Board's approval received via email circulation[1].

The guidelines in blue font are non-mandatory but good to do.

[1] Email for approval sent on 19 Jun 2025.

Table of contents

Acknowledgements

We sincerely thank the RegTech companies within the FACE membership for their initiative in formulating the RegTech Code of Conduct (Code), the first of its kind in India. We also thank the larger FinTech community in FACE for providing input to the Code from a broader perspective and improving it.

In preparing this document, we extensively researched the public literature available on RegTech and borrowed the good practices.

Regulatory Technology (RegTech) refers to using innovative technologies, such as artificial intelligence, machine learning, big data analytics, natural language processing, and blockchain, to streamline, automate, and enhance compliance with regulatory requirements. While it originated within the BFSI sector, RegTech increasingly caters to a broader range of industries, including healthcare, energy, telcom, pharma, gaming, real estate, etc.

By delivering real-time monitoring, automated reporting, and risk assessment tools, RegTech enables companies across industries to navigate increasingly complex regulatory landscapes, reduce compliance costs, and enhance transparency.

Introduction

Context

In the rapidly evolving regulatory landscape of the BFSI sector, Regulatory Technology (RegTech) plays a crucial role in ensuring compliance, and India has witnessed the emergence of several RegTech companies catering to the BFSI sector and beyond.

The RegTech companies are vital to compliance, so promoting and protecting their good practices and integrity is essential. In the past, the industry has also experienced suboptimal solutions, which bring risks to the clients it caters to. Currently, no specific regulations exist for RegTech products/services or companies. RegTech operates based on contractual terms with regulated entities (REs) and other FinTechs and adheres to applicable guidelines, including KYC, AML, and data protection. While various good practices have emerged, the absence of specific regulations calls for universal self-regulatory standards.

RegTech companies at FACE agree to adopt a self-regulatory Code to address this. It builds on existing regulatory norms and aims to improve individual and collective practices, thereby fostering stakeholder trust and improving the company's client experience, market outreach, and brand reputation. The Code reflects stakeholders' rights and guarantees FACE members' voluntary commitment to safeguarding customers/companies using RegTech solutions.

Coverage

All FACE members offering RegTech products or services must adhere to this Code and implement it within six months of its publication. Equally, we welcome industry stakeholders[2] to adapt the Code. For any suggestions or clarifications, please email sro@faceofindia.org.

The Code does not substitute or override rights under various regulations and laws, which take precedence in the event of conflict. The Code does not cover other obligations companies may have, including multiple laws/regulations related to governance, reporting, human resources, technology, foreign investment, taxation, and corporate social responsibility.

The Code is subject to periodic updates by the FACE Board, incorporating feedback from members and stakeholders, to align with evolving regulations, market trends, and technologies, ensuring the Code maintains stewardship of responsible RegTech. Members will be notified of any changes in the Code with timelines for adherence. The Code can be reviewed anytime in exceptional circumstances, such as changes in applicable laws or regulatory mandates.

[2] FACE has published this Code of Conduct, and we welcome the industry to refer to and adopt with adequate attribution to FACE

Code of Conduct

Engagement with government/regulatory authorities

1. Monitor and adhere to all regulations that directly or indirectly apply to the companies regulated by financial sector regulators[3] and government authorities. Please refer to Annexure 1 for relevant regulations[4] . Regularly update internal policies and procedures to ensure compliance with these regulations.
2. Be part of the FinTech repository and contribute accurate and timely information.
3. Engage with regulatory and government authorities to ensure alignment with compliance and risk management expectations, and provide complete, accurate, and timely information as required.
4. Contribute to regulatory and industry consultations/sandboxes/standards.
5. Cooperate with regulators and government authorities during inspections by allowing access to IT infrastructure, applications, data, documents, and other necessary information given to, stored or processed by the company and/or its sub-contractors as applicable to the scope of the investigation.

Responsible innovation

6. Understand the client's[5] compliance needs to provide suitable and professional services.
7. Validate models[6] as per the robust, documented internal processes to mitigate biases and ensure reliable, fair, and robust outcomes across diverse use cases. Implement AI models that are explainable, contestable, protect human agency, and are accountable with periodic reviews and impact assessments after deployment.
8. Conduct thorough risk assessments of solutions before implementation, ensuring alignment with industry best practices and regulatory expectations.
9. Disclose key performance indicators and limitations of the RegTech solutions to the client.

Data Privacy & Security

10. Secure sensitive data with encryption, access controls, and regular audits.
11. Support and ensure your clients take explicit consent[7] for data collection, processing, and sharing, as mandated under applicable data protection laws.

---

[3] RBI, SEBI, IRDAI, PFRDA
[4] Non-exhaustive
[5] Client is a Regulated Entity (RE) or other FinTech to whom RegTech provides its products and services.
[6] Models refer to computational or statistical algorithms, often powered by machine learning or AI, that are designed to analyse data, make predictions, automate decisions, or detect patterns. These models are used in credit scoring, fraud detection, risk assessment, regulatory compliance, and more.
[7] Consent is defined as any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her.

12. Develop clear, concise internal policies that comply with India's data protection laws, sectoral regulations, focusing on obtaining user consent, managing data retention, and handling sensitive personal data.
13. Get relevant certifications. Please refer to Annexure 2 for relevant certifications.
14. Maintain customer and client data confidentiality if serving multiple clients and sharing data with service providers. Ensure compliance with data localisation and data protection guidelines, as applicable.
15. Establish a clear process for reporting and resolving security incidents, data breaches, misuse, or system failures. Conduct third-party audits of security systems.

Partnerships

16. Conduct due diligence on partnerships, both upstream[8] and downstream.
17. Thoroughly assess the service provider, including, but not limited to, financial stability, infrastructure, IT & cybersecurity, reputation, and compliance history. It should also include the ability to handle scale-up, past performance with similar businesses, a business continuity and disaster recovery plan, and previous security breaches.
18. Execute a legally binding agreement with the parties in the value chain covering development, management or operation of APIS/solutions/services, not compromising the integrity, confidentiality, or compliance of the Reg-Tech services. Outline parties' roles, responsibilities, and expectations with details on activities, service levels, data handling, security protocols, and compliance obligations.
19. Take steps to ensure that the service providers employ the same high standard of care in performing the services as the company would have.
20. Ensure that the partners (clients or service providers) handle data (use, sharing, retention, destruction) in compliance with applicable data protection laws. This shall apply from the origination to the end use of data.
21. Establish a clear chain of responsibility for failures/issues by third-party dependencies.
22. Develop clear guidelines for data storage/computing/movement in a cloud environment.
23. Implement controls to prevent unauthorised disclosure of confidential data within the company and service providers.
24. Follow local laws/standards as applicable, if operating in a jurisdiction other than India.

Transparency & Accountability

25. Engage in fair, transparent[9], and ethical business practices with all stakeholders, including clients, partners, and regulators.
26. Identify, disclose, and appropriately manage conflicts of interest in all business dealings.
27. Maintain transparent pricing structures and clearly outline service terms.

[8] Partnerships with regulated entities and FinTech

[9] Disclose information on products, services, and business practices

28. Maintain records and audit trails demonstrating compliance with regulatory requirements and industry practices.
29. Develop a robust framework to monitor and control performance, adherence to Service Level Agreements, and incident reporting mechanisms.

Employee training & conduct

30. Regularly train employees on relevant laws and industry standards (e.g. data privacy, IT & cybersecurity, AI). Foster a culture of compliance, integrity, and ethical behaviour within the company.
31. Establish mechanisms[10] for employees to report misconduct or non-compliance without fear of retaliation.

Grievance redressal

32. Provide accessible channels for stakeholders (clients, customers, employees) to report grievances. This includes email, phone lines, and dedicated web portals with process and escalation metrics.
33. Establish precise and efficient systems for promptly and transparently resolving customers' and clients' complaints and regulatory queries.
34. Review and improve grievance redressal processes and escalation matrix to ensure effectiveness and adherence to best practices.
35. Report all grievances about regulatory non-compliance and data breaches to the relevant authorities.

[10] Companies are encouraged to have whistle blower policy in place.

Adherence framework

Companies

1. Inform and create awareness amongst the board, employees, clients and partners/service providers about the commitment to the Code.
2. Ensure that all policies, processes, tech stacks, and systems align with the Code's norms and promptly vet any changes for adherence to standards.
3. Implement internal monitoring systems to ensure adherence to the Code and share the report with Senior management and the Board.
4. Train employees on the Code to ensure understanding and commitment and inculcate a culture of adherence to the Code.
5. Display adherence to the Code in public[11] and private communications to clients and other stakeholders as a trust mark to showcase that the company is committed to adhering to the Code.

FACE

6. As per the FACE Article of Association (AoA), members must abide by the Code as it applies to them.
7. As necessary, FACE may ask a member for self-certification and undertaking of adherence to the Code.
8. Each Member will designate a PoC with FACE to take responsibility for the Code, including dissemination and awareness within the company, clarification, compliance, and response to questions related to non-adherence to the Code.
9. The FACE SRO Oversight & Enforcement Committee will examine the evidence[12] of non-adherence to the Code by Members and act as per the process[13] laid out by the Board.

[11] Includes website, social media, and other collateral.
[12] Such evidence will be collected through market intelligence and complaints received from customers and other stakeholders.
[13] Process will be according to regulatory instructions.

Annexures

Annexure 1: Relevant regulations

- Master Direction on Outsourcing of Information Technology Services
- Information Technology Act, 2000
- Master Direction - Know Your Customer (KYC) Direction, 2016
- Aadhaar Act, 2016
- DPDP Rules, 2025
- Prevention of Money Laundering Act, 2002
- CFT-AML
- Directions on Managing Risks and Code of Conduct in Outsourcing of Financial Services by NBFCs Conduct outsourcing

Annexure 2: Relevant certifications

Sl no	Certifications	Requirement
1	ISO/IEC 27001:2013 (Information Security Management)	For securing information and data systems. Required for RegTech companies dealing with sensitive financial or personal data.
2	ISO 22301 (Business Continuity Management)	Often mandated for companies handling critical financial infrastructure or working with banks/insurance.
3	SOC 2 Type II (System and Organisation Controls)	Especially relevant for SaaS-based RegTech companies; important for working with global or enterprise clients.
4	PCI DSS (Payment Card Industry Data Security Standard)	Needed if the companies handle or process payment card data.
5	CERT-In Audits	For cybersecurity

Fintech Association for Consumer Empowerment (FACE) is an RBI-recognised Self-regulatory Organisation in the FinTech sector (SRO-FT). FinTech companies of all kinds come together at FACE to build an industry that enables customer-centric financial services that are safe, suitable, and transparent, delivering positive impacts on society and the economy.