The Reserve Bank of India's (RBI) Department of Supervision, through its Cyber Security and IT Risk Group, has issued Advisory No. 3/2026 dated 25 March 2026 on best practices relating to customer data protection (the 'Advisory'). Drawing on a thematic study conducted across multiple categories of RBI-supervised entities (SEs) in 2025, the Advisory consolidates real-world best practices observed in the field.

The Advisory arrives at a particularly significant moment with India's Digital Personal Data Protection Act 2023 (DPDP Act) anticipated to fully come into force from 13 May 2027. The Advisory serves as a practical guidance document, providing real-world measures and system protocols that SEs have been observed to implement in their ecosystem. It is, in essence, a curated toolkit that other SEs can adapt and customise to their own risk profile, business model, and operating environment.

Salient Features of the Advisory

Governance and Oversight: The Advisory is unambiguous that data protection is a board-level responsibility, not merely an IT function. SEs are expected to maintain formal, periodically reviewed policies, assign clear ownership through accountability structures such as RACI matrices, and ensure that customer data security features as a standing item on board or committee agendas.

Data Collection, Classification, and Consent: SEs are recommended to deploy automated tools to identify and classify data by sensitivity across all environments (i.e., on-premises, cloud, and third-party environments). Equally important is a centralised consent management system and clear communication of privacy practices to customers at key touchpoints such as onboarding and transactions.

Data Security Controls: The Advisory calls for comprehensive mapping of data flows, strong encryption using hardware security modules, and multi-layered data leakage prevention solutions covering various data exit points such as endpoint levels, email, USB, network level, database level, etc. Standardised data dictionaries are also recommended to ensure consistency in how customer data is identified and protected across the enterprise.

Access Management: Controlling who can access customer data and how - is central to the Advisory. SEs can consider enforcing robust remote access controls such as encrypted VPNs restrictions, deploying mobile device management solutions on employee devices, and maintaining comprehensive access logs integrated with real-time monitoring systems that can trigger alerts for unusual or unauthorised activity.

Third-Party Risk Management: Given the financial sector's deep reliance on outsourcing and technology partnerships, the Advisory devotes significant attention to vendor risk. SEs are recommended to share only the minimum data necessary, conduct thorough due diligence on vendors before and after onboarding, require contractual breach-reporting obligations, and prohibit vendors from storing sensitive customer data in plain text.

Incident Response and Recovery: A structured incident response framework, covering scenarios from data leakage to ransomware, is essential. The Advisory recommends periodic cyber drills (including third-party participation), standardised post-incident reviews with root cause analysis, and multi-channel customer communication protocols integrated into the entity's cyber crisis management plan.

Data Retention and Destruction: SEs are to maintain a board-approved retention policy that applies consistently across live systems, test environments, and backups. Deletion events are to be supported by robust audit trails, and data destruction to follow certified methods such as cryptographic erasure or physical destruction in line with NIST 800-88 or equivalent standards.

Customer Rights and Grievance Redressal: The Advisory emphasises that customers are required to be given accessible and effective channels for data-related complaints. This includes CRM systems that generate unique complaint reference numbers, automated status updates, and a multi-channel redressal framework with a published escalation matrix and defined turnaround times.

Audit and Testing: It is recommended that customer data security feature within the scope of internal audit, with coverage extending to design and operating effectiveness, vulnerability assessment and penetration testing findings, and third-party data processors. Audit logs are to be centralised, tamper-proof, and forensically ready.

Emerging Technologies, Cloud Security, and Continuous Monitoring: The Advisory addresses newer risk vectors directly. SEs adopting AI tools, chatbots, or cloud infrastructure are to implement appropriate governance and security controls commensurate with the associated risks. Cloud deployments are to be supported by cloud security posture management tools and a clearly documented shared responsibility framework with the service provider. Across all environments, 24x7 security operations centre monitoring, integrating SIEM, DAM, DLP, and behavioural analytics, is recommended for real-time threat detection and response.

Comment

The Advisory is timely and pragmatic. For SEs, it effectively codifies the industry's leading standard on customer data protection, a benchmark against which existing frameworks can be assessed and strengthened. Critically, the Advisory's themes (i.e., consent management, purpose limitation, breach notification, and grievance redressal) closely mirror obligations under the DPDP Act. SEs that implement these recommendations will be well-positioned to demonstrate compliance readiness across both RBI supervisory expectations and the emerging DPDP framework. The Advisory's strong focus on third-party risk further signals that regulators will hold SEs accountable for the data protection practices of their entire ecosystem, not just their own operations. SEs can treat this Advisory as a strategic framework that can form the foundation of a mature, defensible, and future-proof data protection programme.

- *Supratim Chakraborty (Partner) and Shramana Dwibedi (Principal Associate)*

About Khaitan & Co

Khaitan & Co is a top tier and full-service law firm with over 1300+ legal professionals, including 340+ leaders and presence in India and Singapore. With more than a century of experience in practicing law, we offer end-to-end legal solutions in diverse practice areas to our clients across the world. We have a team of highly motivated and dynamic professionals delivering outstanding client service and expert legal advice across a wide gamut of sectors and industries.

To know more, visit **www.khaitanco.com**