CyberPeace

CyberPeace | Submission to RBI

Public Comments on the Draft

'Guidance on Regulatory Expectations for Data Governance'

Issued by the Reserve Bank of India — Ref. DoR.ORG.REC.XXX/XX-XX-XXXX/2026-27

Submitted by:

CyberPeace

L-29, First Floor, Connaught Place, New Delhi – 110001

secretariat@cyberpeace.net | www.cyperpeace.org

Date: 13th August 2026

Executive Summary

CyberPeace welcomes the Reserve Bank of India's draft Guidance on Regulatory Expectations for Data Governance ("the Guidance") and appreciates the opportunity to provide comments during the public consultation process. The Guidance establishes a robust, principle-based framework for strengthening data governance across Regulated Entities (REs), anchored in board oversight, defined data accountability, lifecycle-based management, a Single Source of Truth (SSOT), and enhanced third-party risk controls. Its architecture is well aligned with internationally recognised standards, particularly the Basel Committee's BCBS 239 principles, and reflects the growing importance of high-quality data governance in ensuring operational resilience, regulatory compliance, financial stability, and consumer protection.

Our review, however, identifies several areas where greater clarity and alignment would strengthen implementation and reduce regulatory uncertainty. These include the limited emphasis on customer-facing data governance measures such as consent management, grievances redressal, and safeguards for automated decision-making; the need to reconcile implementation timelines with the phased enforcement of the Digital Personal Data Protection (DPPP) Rules, 2025; more comprehensive treatment of cross-border personal data transfers; clearer articulation of the Guidance's relationship with existing RBI frameworks on IT governance and outsourcing; and the inclusion of indicative minimum standards for audits, SSOT reconciliation, and data quality metrics. This submission presents cross-cutting recommendations, detailed clause-wise comments, comparative benchmarking against key domestic and international frameworks, and a consolidated set of priority recommendations to support a consistent, risk-based, and future-ready regulatory framework.

About CyberPeace

CyberPeace is a global non-profit organization headquartered in India, working at the intersection of cybersecurity, policy, and peacebuilding. It envisions a safe, resilient, and inclusive cyberspace for all. Through its global initiatives, CyberPeace drives capacity building, policy research, incident response, and public awareness to advance the vision of "CyberPeace and Trust in Technology." From grassroots digital literacy programs to high-level policy and research collaborations, CyberPeace integrates innovation, education, and advocacy to strengthen digital ecosystems worldwide. Championing the future of responsible technology, CyberPeace is building the next generation of Cyber Defenders and Responsible Digital Citizens, aligning its mission with the United Nations Sustainable Development Goals (SDGs) and India's Viksit Bharat 2047 vision.

Scope and Methodology

This note reviews the draft Guidance chapter by chapter (Chapters I–VI), identifying provisions that would benefit from clarification, strengthening, or alignment with existing legal and regulatory frameworks. Each observation is accompanied by a corresponding recommendation to support consistent and practical implementation. The analysis benchmarks the Guidance against:

1. **Digital Personal Data Protection Act, 2023 and DPDP Rules, 2025 –** to assess alignment with India's statutory data protection framework.
2. **EU General Data Protection Regulation (GDPR) –** as a comparative reference where the DPDP framework is silent or less prescriptive.
3. **BCBS 239 and the ECB's 2024 RDARR Guide –** to evaluate consistency with international standards on data governance and risk data aggregation.
4. **Existing RBI regulatory frameworks –** including the 2023 Master Directions on IT Governance and IT Outsourcing to identify overlaps and improve regulatory coherence.

Where the DPDP framework already provides an adequate standard, this note does not recommend additional requirements. Where gaps remain or implementation is phased, it draws on international best practices to propose sector-specific measures that can strengthen the guidance while remaining proportionate to RBI's supervisory mandate.

Table of Abbreviations

Abbreviation	Term
RBI	Reserve Bank of India
RE/REs	Regulated Entity/Entities
SSOT	Single Source of Truth
BCBS 239	Basel Committee on Banking Supervision – Principles for Effective Risk Data Aggregation and Risk Reporting (BCBS 239)
DPDP	Digital Personal Data Protection
EU	European Union
GDPR	Geneeal Data Protection Regulation
ECB	European Central Bank
RDARR	Risk Data Aggregation and Risk Reporting
IT	Information Technology
ITGRCA	IT Governance, Risk, Controls and Assurance (RBI IT Governance framework)
DGF	Data Governance Framework
CISO	Chief Information Security Officer
ITSC	IT Strategy Committee
NBFC	Non-Banking Financial Company
UCB	Urban Co-operative Bank
RRB	Regional Rural Bank
RMCB	Risk Management Committee of the Board
DGC	Data Governance Committee
CGM	Chief General Manager
DPO	Data Protection Officer
RACI	Responsible, Accountable, Consulted, Informed
ISO/IEC	International Organization for Standardization / International Electrotechnical Commission
KYC	Know Your Customer
PMLA	Prevention of Money Laundering Act
DPA	Data Processing Agreement
NDA	Non-Disclosure Agreement(s)
DPIA	Data Protection Impact Assessment
SCCs	Standard Contractual Clauses
BCRs	Binding Corporate Rules
SDF	Significant Data Fiduciary
GSIBs	Global Systemically Important Banks
D-SIBs	Domestic Systemically Important Banks

Part A: Cross-Cutting Recommendations

The following recommendations apply to the Guidance as a whole rather than to a single chapter.

1. **Clarify the Guidance's supervisory status:** The instrument is styled a 'Guidance' and consistently uses 'should' rather than 'shall', unlike RBI 'Directions' issued under statutory powers. RBI should clarify, on the face of the final document, how supervisory expectations under a Guidance will be assessed and what consequences attach to material non-observation so REs can calibrate implementation effort appropriately.

2. **Build explicit proportionality tiers:** The Guidance repeatedly invokes proportionality ("commensurate with" and "proportionate") as a general principle but, apart from part of the NBFC layers already defined in law, does not tier its own obligations (board committee structure, CGM-rank requirement, and audit frequency) to RE size or complexity. An explicit proportionality matrix even if only indicative would material help smaller UCBs, RRRs, and local area banks.

3. **Reconcile the DPDP Rules' phased timeline with RBI's own implementation timeline:** The Guidance state plainly which of its expectations are DPDP-timeline-dependent (and therefore appropriately phased by May 2027) and which are independent RBI expectations that REs must meet on their own schedule.

4. **Fill the automated decision-making gap:** Neither the DPDP Act nor Indian law more broadly provides a right against solely automated decision-making, unlike GDPR Article 22. Given RBI's direct jurisdiction over credit, lending, and risk-s scoring decisions, the Guidance is well placed to require baseline explainability and human review safeguards for automated decisions built on governed data — see Chapters II and IV.

5. **Harmonise explicitly with the ITGRCA and Outsourcing of IT Services Directions, 2023:** Several obligations in this Guidance (board committees, third-party risk assessment, business continuity) already exist in substance under RBI's 2023 IT Governance and Outsourcing Directions. A dedicated 'Interplay with Other RBI Instruments' section in the final Guidance would prevent REEs from building parallel, overlapping compliance programs.

6. **Publish a DGF-to-DPDP-to-ITGRCA role and term crosswalk:** A short glossary annex mapping Data Owner/Steward/Custodian to Data Fiduciary/Processor/Consent Manager and to CISO/Head of IT/ITSC would materialise reduce implementation ambiguity, particularly for smaller REs building their governance structure from scratch.

7. **Give the customer-facing dimension of data governance more weight:** As currently drafted, the Guidance is almost entirely institution-facing. Consent management, data-principal grievance handling, and rights fulfilment (access, correction, and erasure) deserve treatment proportionate to their centrality under the DPDP Act — see Chapters III and IV.

Part B: Chapter-wise Recommendations

This part mirrors the six chapters of the draft Guidance. For each, we summarise our overall assessment before setting out clause-level issues and recommendations in tabular form.

Chapter I: Preliminary (Applicability & Definitions)

The applicability list is comprehensive and appropriately broad across the RBI's regulatory perimeter. The definitions largely track sound data-governance vocabulary; our comments focus on tightening a few definitions and clarifying how DGF terminology interacts with DPPD terminology.

Clause	Issue / Gap Identified	CyberPeace Recommendation
Ch. I, Para (Applicability)	The applicability clause lists eleven categories of Regularized Entities but does not expressly address (a intra-group/ parent/subsidiary data flows within a banking or NBFC group, or (b) data transmitted by India branches of foreign banks to an overseas sea head office or group entity — both high-volume, recurring flows in the sector.	Add a clause clarifying how the Data Governance Framework (DGF) applies to data shared (i) between group entities as defined under the RBI (Commercial Banks – Concentration Risk Management) Directions, 2025, and (ii) by foreign bank branches to their head office/overseas group, with a cross-reference to the third-party (Ch. VI) and cross-border (para 15(4) provisions.
Ch. I, Para 5(9)'(Data Owner')	The Data Owner is defined as the individual "accountable for data governance outcomes". Read in isolation, this risks being conflated with the RE's own statutory liability as 'Data Fiduciary' under the DPPD Act, 2023, which attaches to the entity, not to an individual officer.	Add an explanatory note clarifying that role-based accountability under the DGF is internal and operational and does not dilute or substitute the Board's or the RE's (as Data Fiduciary's) statutory liability under the DPPD Act and other applicable law.
Ch. I, Para 5(13)'(Person Data)	The Guidance importons the DPPD Act's definition of personal data as is. Unlike the GDPR (Art. '9 special categories'), does not create a statutory "sensitive personal data" subcategory yet RE's routinely process intrinsically higher-risk data (financial account, credit history, biometric/Aadhaar).	Introduce a sector-specific 'Sensitive Financial/Personal Data' subcategory within the RE's own classification framework (Ch. V.C) so heightened controls attach regardless of the current gap in national law. See also Ch. V recommendations.
General Definitions	DGF terminology (Data Owner/Steward/Custodian)	Publish an explanatory cross-walk/glossary annexive mapping
	does not map cleanly onto DPPD terminology (Data Fiduciary/Processor/Consent Manager) or onto the terminology already used in the ITGRCA Directions, 2023 (CISO/Head of IT/ITSC), creating a risk of inconsistent implementation and duplicate governance layers across an RE's existing compliance architecture.	DGF roles to DPPD roles and to roles already defined under the ITGRCA and Outsourcing of IT Services Directions.

Chapter II: Governance

This is the Guidance's most developed chapter, and its data risk management provisions (para 15) closely and creditably track BCBS 239. Our recommendations focus on board reporting cadence, avoiding committee duplication with existing RBI instruments, independence safeguards for governance personnel, and closing the cross-border protection-risk gap.

Cause	Issue / Gap Identified	CyberPeace Recommendation
Para 6–7(DGF)	The DGF must be "aligned with" the risk management framework, but its relationship to the board-approved IT Governance Framework and Information Security Policy already mandated under the ITGRCA Directions, 2023, is not addressed risking duplicative or conflicting board-approved documents, especially for REs that have only recently completed ITGRCA implementation.	Require the DGF to be explicitly cross-referenced within (or appended to) the existing IT governance framework/information security policy architecture, with a single integrated board review calendar rather than two parallel annual reviews.
Para 8(Role of the Board)	The Board's oversight duty is open-ended ("review the reports and metrics placed before it") with no minimum reporting cadence — weaker than BCBS 239 Principle 1, which anchors Board accountability in a defined, recurring sign-off, and weaker than the quarterly cadence This very Guidance prescribes for data quality (para 59).	Prescribe a minimum board-level reporting cadence (at least half-yearly) covering DGF effectiveness, data risk exposure, and material incidents, aligned with the quarterly DGC-level data-quality reporting already required.
Paras 9–14 (Board & Executive Committees)	Most REs already operate a Risk Management Committee of the Board (RMCB) and an IT Strategy Committee (ITSC) under the ITGRCA Directions with overlapping data/IT risk mandates. The Guidance is silent on how the new Data Governance Committee (DGC) and Executive Committee interface with these risking committee proliferation. particularly for UCBs/RRBs with limited board bandwidth.	Expressly permit the RMCB or ITSC to absorb the data governance mandate where an RE's scale does not justify a separate committee and require a documented terms-of-reference reconciliation wherever committees co-exist.
Para 13(iii) (Independence of personnel)	The requirement that data governance personnel have "requisite authority, independence, and competence" has no concrete safeguards attached (e.g., protection from adverse action for escalating concerns, prohibition on conflicting duties) — unlike GDPR Article 38's explicit protections for the data protection officer.	Add independence safeguards for data owners/stewards/custodians analogous to GDPR Art. 38(3): protection from dismissal or penalisation for performing data governance duties and a bar on a data custodian both granting and auditing access to the same dataset (segregation of duties).

Cause	Issue / Gap Identified	CyberPeace Recommendation
Para 15(1)(Data risk – seven attributes)	The seven attributes (accountability, integrity, auditability, transparency, traceability, proportionality, standardisation) closely track BCBS 239 but omit an explicit 'resilience' dimension — the capacity to recover data and reporting capability after disruption — which both BCBS 239 and the ECB's 2024 RDARR Guide treat it as integral.	Add 'resilience' as an eighth attribute, cross-referenced to the business continuity/disaster recovery obligations already mandated under the ITGRCA Directions, 2023, so the two frameworks reinforce rather than duplicate each other.
Para 15(4) (Cross-border data risk)	Cross-border risk is framed solely as an operational/access-continuity risk (ensuring the RE can "access, retrieve, and manage its data"). It does not address the data-protection risk of transferring personal data abroad — a materially different question, and one where the DPDP Act (Sec. 16) leaves a gap by adopting a permissive 'blacklist' model (transfers allowed unless a jurisdiction is expressly restricted) rather than GDPR's restrictive, adequacy-based 'whitelist' model.	Require REs to conduct and document a cross-border transfer risk assessment covering both operational-access and data-protection risk before processing, storing, or sharing personal data outside India, particularly via overseas cloud or group/vendor processing centres, given that no equivalent statutory safeguard currently exists under DPDP.
Paras 18–19 (DPDP compliance)	The Guidance treats DPDP Act/Rules compliance as a fixed reference point, but most substantive DPDP Rules obligations (notice, consent standards, breach reporting, retention/erasure, and cross-border conditions) become mandatory only from 13 May 2027. REs implementing this Guidance in the interim may build inconsistent interim compliance postures if the two timelines are not reconciled.	Clarify that DPDP-linked elements of the DGF should track the DPDP Rules' own phased timeline while making clear that RBI's own data governance expectations (roles, SSOT, classification, and quality) proceed on their own schedule and are not contingent on the 2027 DPDP deadline.
Para 20(Audit)	Audit frequency, scope and independence are left to a "risk-based approach" with no floor, and the audit mandate does not explicitly extend to fairness/bias testing of the data inputs to automated or AI-assisted decisions (e.g., credit scoring) – an emerging risk area that neither DPDP nor (in India's case) any GDPR Art. 22-equivalent currently reaches.	Specify a minimum audit periodicity for critical/high-classification data domains, and require audit scope to explicitly cover the data-quality inputs to any automated or algorithmic decision-making system used in credit, pricing, or risk decisioning.

Chapter III: Organisational Structure: Data Roles and Responsibilities

The four roles (Data Function, Owner, Steward, and Custodian) are a clear and workable accountability structure. Our recommendations address proportionality for smaller REs, alignment with DPPD grievances-handling obligations and segregation-of-duties safeguards within the Custodian role.

Cause	Issue / Gap Identified	CyberPeace Recommendation
Para 22(Data Function - CGM rank)	Mandating a chief general manager or equivalent rank to head the data function may not be proportionate for smaller REs (Tier 12 UBCs, local area banks, and regional rural banks) that have no CGM-equivalent grade in their organisational structure.	Tie the seniority requirement explicitly to the RE's regulatory tier/layer (as already done for NBFC-BL/UL/UL in Ch. 1), permitting smaller REs to designate the most senior available officer with board-delegated authority.
Para 24-25(Data Owner)	The Data Owner's responsibilities are not explicitly linked to the DPPD Rules' requirement that every Data Fiduciary designates a contact point (or DPO, for Significant Data Fiduciaries) for data principal grievances—risking two disconnected accountability chains: one for RBI supervisory purposes and another for DPPD grievance redressal.	Require the Data Owner (or a designated Data Steward) for customer data domains to be formally linked to the RE's DPPD grievance/contact point function so data-principal requests (access, correction, erasure, and consent withdrawal) are rooted within the same governance structure used for internal accountability.
Paras 26–27 (Data Steward)	The Data Steward is positioned "within the business function or unit" of the data owner, which does not address the risk that a reporting line embedded in the business could create an incentive to under-report data quality issues that reflect poorly on that unit.	Require a dual/dotted reporting line from the data steward to the data function (para 22) for data governance matters so operational embedding does not compromise independent escalation of quality and compliance issues.
Para 28–29 (Data Custodian)	The Data Custodian is responsible for both "enforcing access controls" and "maintaining technical capabilities", without a segregation-of-duties safeguard preventing the same individual/team from both granting and auditing access to the same dataset.	Require segregation of duties between access-provisioning and access review/audit functions within the Data Custodian role, consistent with ISO/IEC 27001 access-control practice and the security-of-processing expectations under GDPR Art. 32.
Paras 30–31 (Mapping / RACI)	Smaller REs — particularly UBCs and RRBs with limited data governance maturity — may struggle to build a structured roles-to-lifecycle mapping without a reference template, leading to inconsistent quality of implementation across the sector.	Publish an illustrative RACI (Responsible/Accountable/Consulted/informed template as a non-binding annexure, in the manner RBI has provided implementation aids for other Master Directions.

Chapter IV: Data Lifecycle

The lifecycle structure (origination, processing/sharing/transition, retention/archival/disposal) is sound, but consent management, arguably the single most consequential data-governance activity from a customer protection standpoint, is addressed in a single line item. We recommend it be substantially expanded, alongside data minimisation and automated-decision safeguards.

Cause	Issue / Gap Identified	CyberPeace Recommendation
Para 33(v) (Consent management)	Consent management for customer data is currently a single line item within a five-point list disproportionately thin given that (a) consent is the primary lawful basis for processing under the DPDP Act and (b) the DPDP Consent Manager ecosystem becomes operative from November 2026, within the likely working life of this guidance.	Expand consent management into a dedicated lifecycle subsection requiring REs to: (i) maintain machine-readable consent artefacts; (ii) support consent withdrawal with propagation to all downstream systems holding the affected data; and (iii) be technically ready to interoperate with registered Consent Managers, with 'consent lineage' tracked alongside data lineage (Ch. V.B).
Paras 34–37 (Origination & Capture	Data must be captured "only for defined and legitimate purposes", but the Guidance does not explicitly require data minimisation — collecting only what is necessary for the stated purpose, which is a foundational principle under both GDPR Art. 5(1)(c) and the purpose-limitation framing of the DPDP Act.	Add an explicit data-minimisation requirement at the point of capture, alongside the existing purpose-legitimacy requirement in paragraph 34.
Paras 38–40 (Processing, Sharing, Transformation)	Where transformed/derived data feeds automated or algorithmic decisions (credit scoring, underwriting, and fraud triggers), the Guidance requires traceability and an impact assessment of the transformation logic but not disclosure/explainability safeguards for the affected customer, a protection neither the DPDP Act nor (in the Indian context) any GDPR Art. 22-equivalent currently guarantees.	Require REs to document, for any automated or predominantly automated decision materially affecting a customer, the data elements and transformation logic used and to provide for meaningful human review on request, pending a statutory automated-decision-making right in India.
Paras 41–42 (Retention, Archival, Disposal	Retention/disposal is governed by "business, legal, regulatory, or audit requirements" without addressing how REs should reconcile long statutory retention mandates (e.g., KYC/PMLA record-keeping) against the DPDP Rules' erasure obligations and 48-hour pre-erasure notice requirement, effective May 2027.	Provide explicit guidance on the order of precedence between statutory RBI/PMLA retention mandates and DPDP-driven erasure rights, and require REs to document this reconciliation logic within their data retention and archival policy.

Chapter V: Data Architecture

The Single Source of Truth, metadata/lineage, classification, and data quality provisions are well-conceived and, on data quality in particular, closely parallel BCBS 239 Principles 3–6. Our recommendations focus on adding definitional floors (reconciliation frequency, classification tiers, quality dimensions) so implementation is consistent across REs of varying maturity.

Clause	Issue / Gap Identified	CyberPeace Recommendation
Paras 43–46 (Single Source of Truth)	The reconciliation mechanism required between the SDOT and downstream data (para. 46) has no defined frequency or materiality threshold, risking inconsistent implementation across REs of different scale and technical maturity.	Require REs to define and document a risk-based reconciliation frequency and a materiality threshold for escalating unresolved SDOT/ downstream discrepancies to the Data Governance Executive Committee.
Paras 47–51 (Metadata & Lineage)	The prescribed metadata attributes (source, purpose, owner, classification, and retention) do not include the legal basis of processing (consent / contract / legal obligation) at the data element level — a capability increasingly expected of privacy-nature organisations, broadly analogous to GDPR Article 30 Records of Processing Activities.	Add 'legal basis / consent status' as a mandatory metadata attribute, linked to the consent-lineage requirement recommended for Chapter IV.
Paras 52–55 (Data Classification)	The classification framework's criteria (critical, sensitivity, confidentiality, legal/regulatory relevance) are principles-based with no indicative minimum tier structure or mandatory tagging for regulatorially sensitive categories (Aadhaar/biometric, financial account, credit history) — leaving room for inconsistent classification across REs that undermines both supervisory comparability and the third-party controls in Chapter VI.	Prescribe an indicative minimum four-tier classification scheme (e.g., public / internal / confidential / restricted) and mandate a 'sensitive financial/personal data' tag for Aadhaar, biometric, financial account and credit information data — filling the gap left by DPPD's lack of a special category concept.
Paras 56–59 (Data Quality)	REs must 'develop and maintain data quality metrics across multiple dimensions' without RBI defining the dimensions or indicative tolerances, which may produce inconsistencies supervisory comparability. This is otherwise one of the strongest sections of the draft, closely paralleling BCBS 239 Principles 3–6.	Publish indicative data quality dimensions (accuracy, completeness, consistency, timeliness, validity, and uniqueness) with illustrative tolerance ranges REs may calibrate to their risk profile, supporting the quarterly DGC reporting already required.

Chapter VI: Third-Party Arrangements

This chapter appropriately extends data governance obligations to third parties, but stops short of GDPR-equivalent minimum contractual content and is silent on third-party breach notification timelines — a gap that directly affects an RE's ability to meet its own DPDP reporting deadlines.

Clause	Issue / Gap Identified	CyberPeace Recommendation
Para 60 (Group entities)	The chapter addresses "third-parties, including group entities" but does not explicitly extend obligations to subprocessors/sub-contractors engaged by a primary vendor (e.g., a cloud sub-processor engaged by an outsource IT vendor) — a common 'fourth party' risk vector in cloud-heavy technology stacks.	Require RE contracts with third parties to include flow-down obligations binding any sub.processor to equivalent data governance, security, and audit standards, mirroring GDPR Article 28(4).
Paras 61–62 (Sharing purposes & controls)	The Guidance requires "non-disclosure clauses" but does not mandate a comprehensive Data Processing Agreement (DPA)-style contractual instrument specifying subject matter, duration, nature and purpose of processing, data categories, and audit rights—unlike GDPR Article 28(3), which prescribes mandatory processor-contract content.	Require a minimum contractual content standard — subject matter, duration, purpose, data categories, sub-processing conditions, audit rights, and deletion/return obligations on termination — for all third-party arrangements involving classified or personal data.
Para 63 (Traceability , audit, monitoring)	The chapter is silent on the timeline within which a third party must notify the RE of a data breach or security incident affecting shared data. Without this, an RE cannot reliably meet meet its own GDPR-mandated 72-hour breach reporting obligation to the Data Protection Board.	Mandate a maximum third-party-to-RE breach notification window (e.g., 24–48 hours from the third party becoming aware of an incident) as a required contractual term, expressly designed to let the RE meet its own regulatory reporting deadlines.
Cross-reference (Ch. II «15(4) «Ch. VI)	Cross-border data risk (Chapter II) and third-party risk (Chapter VI) are addressed in separate chapters without cross-reference, even though the most common cross-border data-risk scenario for REs is data processed by an offshore third-party vendor or overseas group entity.	Insert an explicit cross-reference requiring REs to apply the Cross-Border Transfer Risk Assessment (recommended for Ch. II) to all third-party arrangements involving offshore processing, storage, or support.

Part C: Comparative Benchmarking Snapshot

The table below summarises, at a glance, how the draft guidance compares with the DDPD Act/Rules, the GDPR, and BCBS 239 across ten dimensions relevant to data governance. It is intended as a quick-reference companion to the clause-wise analysis in Part B, not a substitute for it.

Dimension	RBI Draft Guidance	DPDP Act, 2023 / Rules, 2025	GDPR (EU) 2016/679	BCBS 239
Legal nature	Supervisory 'guidance', expectation-based ("should") rather than binding 'Directions'	Statutory Act + Rules; directly binding, phased in to May 2027	Statutory Regulation; directly binding since 2018	Supervisory principles: binding for G-SIBs, discretionary for D-SIBs
Scope of data covered	All data (not only personal data); 11 categories of REs	Personal data only	Personal data only	Risk data only, for systematically important banks
Board accountability	Board oversight + Board DGC + Executive Committee (Ch. II)	No explicit board mandate; SDFs need a DPO + independent audit	Controller/processor accountability (Art. 5(2)); DPO mandatory for high-risk/public-sector processing	Principle 1: Board approves and owns the RDARR framework
Breach notification	Not addressed in this Guidance	72 hrs to Data Protection Board (all breaches); 'without delay' to affected personnel	Risk-based: 72 hrs to supervisory authority only where risk exists; individuals notified only if risk is high	Not applicable (not a privacy framework)
Impact assessment (DPIA-equivalent)	Not mandated	Annual DPIA required for Significant Data Fiduciaries only	Mandatory (Art. 35) for any high-risk processing, regardless of size	Not applicable
Cross-border transfer	Framed only as operational access/continuity risk (para. 15(4))	Permissive 'blacklist' model (Sec. 16) – transfer allowed unless jurisdiction is notified as restricted	Restrictive 'whitelist' model – adequacy decision, SCCs or BCRs required (Art. 44–49)	Not applicable

Dimension	RBI Draft Guidance	DPDP Act, 2023 / Rules, 2025	GDPR (EU) 2016/679	BCBS 239
Individual / data-subject rights	Not addressed — the Guidance is institution-facing only	Access, correction, erasure, grievance redressal, consent withdrawal; no portability or automated-decision-making right	Broadest: access, rectification, erasure, restriction, portability, objection, and protection from solely automated decisions (Art. 22)	Not applicable
Data quality	Explicit dimensions required + quarterly DGC reporting (paras 56–59)	Not addressed	Accuracy principle (Art. 5(1)(d))	Principles 3–6: accuracy, completeness, timeliness, adaptability
Third-party / processor obligations	Access controls, NDAs, audits, need-to-know basis (Ch. VI)	A data fiduciary remains liable for processor acts (Sec. 8(2)); no prescribed contract content	Mandatory Art. 28 processor contract; sub-processor flow-down required	Not directly covered
Penalties for non-compliance	Supervisory action not specified in this Guidance	Up to ₹250 crore per instance	Up to €20 million or 4% of global annual turnover	Supervisory capital add-ons / restrictions via national regulator

A general observation follows from this comparison: the guidance is, appropriately, broader than any single privacy law in its scope (covering all data, not only personal data) and more prescriptive than DPDP on governance architecture and data quality areas where DPDP is silent. Its principal gaps relative to GDPR and BCBS 239 lie specifically in individual rights operationalisation, impact assessment discipline, and breach notification mechanics exactly the areas this note recommends strengthening in Parts A and B.

Part D: Consolidated Priority Recommendations

For ease of reference, we consolidate what we regard as the highest-priority recommendations from this note. Numbering follows the order of the guidance's chapters, not a ranking of importance.

1. Clarify the guidance's supervisory/enforcement status and how observance will be assessed (cross-cutting).
2. Publish an explicit proportionality matrix tying board-committer structure, seniority requirements, and audit frequency to RE size/layer (cross-cutting: Ch. II, III).
3. Reconcile the DPDP Rules' phased 2027 timeline with the RBI's own implementation expectations under this guidance (Ch. II, para 18–19).
4. Require a documented cross-border transfer risk assessment covering data-protection risk, not only operational access risk, and extend it explicitly to third-party arrangements (Ch. II, para 15(4); Ch. VI).
5. Add an explicit 'Interplay with Other RBI Instruments' section reconciling this Guidance with the ITGRCA Directions, 2023 and the Outsourcing of IT Services Directions, 2023 (cross-cutting; Ch. II, para 6–7, 9–14).
6. Expand consent management into a full lifecycle subsection, including consent lineage and Consent Manager interoperability (Ch. IV, para 33(v).
7. Link the data owner/steward strature to the DPDP Grievance/contact point function so customer rights requests are not handled through a disconnected process (Ch. III, para 24–25).
8. Require baseline explainability and human review safeguards for automated or algorithmic decisions built on governed data (Ch. II, para. 20; Ch. IV, para. 38–40).
9. Mandate a maximum third-party-to-RE breach notification window so REs can meet their own DPDP 72-hour reporting obligation (Ch. VI, para. 63).
10. Prescribe minimum contractual content for third-party data-sharing arrangements, akin to GDPR Article 28(3), including sub-processor flow-down obligations (Ch. VI, para 60–62).
11. Introduce a ‘Sensitive Financial/Personal Data’ classification tag for Aadhaar, biometric, financial account and credit information data to fill the special category gap in the DPDP Act (Ch. I, para. 5(13); Ch. V, para. 52–55).
12. Publish indicative floors for SSOT reconciliation frequency and data quality dimensions/tolerances to support supervisory comparability (Ch. V, para. 46, 56–59).

Parting Note

CyberPeace reiterates its support for the Reserve Bank of India's initiative to establish a comprehensive, sector-wide data governance framework. The draft guidance is a well-structured and largely internationally consistent instrument, and the recommendations in this note are offered in that constructive spirit to help close specific gaps in customer-facing protections, cross-border risk treatment, and interplay with the RBI's existing regulatory architecture and to give regulated entities the definitional clarity needed for consistent, supervisable implementation across a sector as varied as India's banking and financial system. We would welcome the opportunity to discuss any of the recommendations in this note further and to contribute to subsequent stages of this consultation.

CyberPeace

For CyberPeace

With warm regards,

Maj. Vineet Kumar
Founder & Global President
CyberPeace
secretariatacyberpeace.net

CyberPeace

Public Comments on the Draft

'Guidance on Regulatory Expectations for Data Governance'

Issued by the Reserve Bank of India — Ref. DoR.Org.REC.XXX/XX-XX-XXXX/2026-27

Submitted by:

CyberPeace

L-29, First Floor, Connaught Place, New Delhi – 110001

secretariat@cyberpeace.net | www.cyberpeace.org