Foundation of Data Protection Professionals in India
[Not for Profit, Section 8 Company limited by guarantees]
CIN No: U72501KA2018NPL116325: GSTN 29AADCF4963H1ZC
Registered Office: No 37, "Ujvala", 20th Main, BSK first Stage, Second Block, Bangalore 560050
Web: www.fdppi.co.in : www.fdppi.in : E Mail fdppi@fdppi.in: Ph: 08026603490: Mob: +91 8310314516

To

The Reserve Bank of India
Mumbai

Subject: Comments on the Draft "Guidance on Regulatory Expectations for Data Governance

Dear Sir,

FDPPI (A section 8 Company) dedicated to Data Protection in India, is pleased to submit its considered views on the draft "Guidance on Regulatory Expectations for Data Governance" (the "DGF" or "Guidance") published for public comment.

We note at the outset that the Guidance has been released at a time when Regulated Entities (REs) are simultaneously required to implement three other governance obligations: the Digital Personal Data Protection Act, 2023 and the DPDP Rules, 2025 (a legal mandate); the draft "Guidance on Regulatory Principles for Model Risk Management, 2026" (the AI / MRM Guidance); and the Responsible Business Conduct amendments to the Master Directions on IT Governance issued earlier. REs must conform to all four requirements concurrently.

This submission however is restricted to the draft Data Governance Framework alone.

FDPPI is actively engaged in training Banks for DPDPA and in developing a unified compliance-and-audit approach that enables simultaneous conformance to all four requirements with minimal duplication. FDPPI, through its division the Association of Independent Data Auditors (AIDAI), is also building the community of "Independent Data Auditors" envisaged under Section 10 of the DPDPA, 2023.

In this background, we offer the following observations in a constructive spirit for your due consideration.

Part A — General and Cross-Cutting Observations

1. **Converge the frameworks; avoid quadruple compliance.**

   Four parallel governance and protection regimes at once impose a disproportionate burden, most acutely on Cooperative Banks and NBFCs with limited access to affordable expertise.

   We recommend that RBI integrate at least the three RBI guidance into a single Master Data Governance Guideline.

   FDPPI has already developed an integrated model- DGPSI-Banks, in which the DPDPA, AI-governance and data-governance requirements are unified with an ability to audit.

   RBI is invited to examine such integrated compliance models, and FDPPI will provide further details on request.

2. **Primacy of law over guidance.**

The DPDPA is the law of the land, the DGF is administrative guidance. There is a real risk that Bankers treat RBI guidance as the more authoritative source and, in doing so, breach the statute and attract substantial DPDPA penalties while believing they are compliant.

The Guidance should state expressly that, in the event of any conflict, the legal mandate prevails.

The clearest illustration is the handling of minor accounts. RBI permits minors above the age of 10 to operate accounts independently, whereas the DPDPA requires verifiable parental consent for the processing of the data of anyone below 18.

Also, the Guidance should require alignment not only with the DPDPA, 2023 but with the Information Technology Act, 2000 and the Consumer Protection Act, 2019.

3. **. Reconcile mandatory retention with the DPDPA erasure duty.**

Paragraphs 41–42 of the guidance justify retention by business, legal, regulatory or audit need, whereas the DPDPA imposes an erasure obligation on withdrawal of consent or on completion of purpose.
RBI- and PMLA-mandated retention (for example, KYC records) must be expressly recognised in the Guidance as the "legal obligation" exception to erasure, so that Banks are not forced to choose between two mandates.

4. **Ease of compliance and proportionality.**

The Guidance presently omits any "ease of compliance" principle. The quality of data risk may be broadly similar across REs, but its quantum varies with the number of data sets handled and the financial value of the data.

We recommend classifying REs into Categories I, II and III by "Risk Size" (funds at risk / customers served), with progressively reduced rigour for smaller entities, supported by an annexure mapping which provisions apply, are relaxed, or are exempt by category.

5. **Provide a phased transition / glide-path.**

Given the concurrent DPDPA, MRM and Master-Directions load, and the substantial re-architecture the Guidance requires (notably SSOT), RBI should publish a phased implementation timeline with defined milestones, allowing a longer glide-path for smaller REs.

6. **Accommodate external expertise; open the audit ecosystem.**

The Guidance should not restrict the ecosystem of external assistance.

It should expressly permit External Data Governance Consultants to support in-house officers, especially in smaller REs, and it should not confine audit to CERT-In empanelled auditors.

Data-governance, DPDPA and AI-model audits require governance and legal competence that a purely technical CERT-In empanelment does not test. The present reference to CERT-In empanelled auditors is therefore misleading and dysfunctional.

Under Section 10 of the DPDPA, a new class of Independent Data Auditors is emerging. FDPPI, through AIDAI,(Association of Independent Data Auditors of India) is bringing Chartered Accountants, lawyers and CERT-In auditors onto a common platform equipped for DPDPA, DGF and AI audit.

We recommend that the Guidance replace the CERT-In reference with the open, competence-based term "Data Governance and Data Protection Auditors."

7. **Recognise the branch as a governance layer.**

   Banks operate through autonomous branches, and most data governance in practice happens there rather than at Head Office. The framework should recognise at least three tiers — Head Office, Regional Office and Branch — as DGPSI-Banks does through its DGPSI-Bank Branch design. A similar layered approach should be adopted for implementation of this Guidance.

8. **Recognise an aggregation-of-audits model.**

   Banking data governance largely occurs at the branch. The Guidance should recognise an aggregation model - analogous to Standard on Auditing SA 600 for financial audits in which branch-level auditors' work is consolidated by a central auditor into a single opinion for the RE. FDPPI/AIDAI has designed such a system for multi-branch entities.

9. **Data valuation.**

   The Guidance should invite Banks to record a notional rupee value of the data in their custody, consistent with the CAG's recommendation for PSUs and FDPPI's proposed Data Valuation Standard of India (DVSI). This value can also inform the risk-quantum classification proposed in point 3.

Part B — Clause-Specific Comments

Chapter I — Preliminary (Paras 3–5):Applicability and Definitions

(para 3): flexibility should be carved out for smaller Banks. Para 4: the Guidance would benefit from explicit direction on integrating the three RBI guidances and the DPDPA into one unified framework.

(para 5): the term "Data Owner" (introduced at para 24) collides with the DPDPA, under which the Data Principal is the owner of personal data; the internal role should be renamed "Data Manager" to avoid confusion. The "Personal Data" definition should remain aligned to the DPDPA's single-category approach, while the classification framework separately retains a sensitivity gradation for risk purposes.

Chapter II — Governance (Paras 6–21)

Para 6: the proportionality principle is welcome, but the Guidance should specify where flexibility applies (through an annexure) and add a method to risk-profile REs by data-set volume and financial data value.

Paras 10 and 22: a single, individually-accountable designation should be created — the Chief Data Governance and Data Protection Officer (CDGDPO) — supported by associate Data Governance and Data Protection Officers (DGDPOs) at branch level; smaller REs should be permitted to engage external consultants to assist the in-house CDGDPO.

Para 18: the primacy-of-law point applies (minor accounts; alignment with the IT Act, 2000 and the Consumer Protection Act, 2019). Para 20 (audit): the CERT-In restriction should be dropped, per Part A point 4.

Breach and incident-notification harmonisation.

The Guidance should add a provision harmonising incident and breach notification across the DPDPA (intimation to the Data Protection Board and to affected Data Principals within the timelines prescribed under the DPDP Rules, 2025), the CERT-In Directions of 2022 (the six-hour reporting requirement) and RBI's own incident-reporting timelines, so that a single incident does not generate three inconsistent obligations.

Chapter III — Organisational Structure:

a) **Roles and Responsibilities (Paras 22–31)**

The Data Custodian role (para 28) risks overlapping the DPDPA Data Protection Officer (DPO). The Guidance should clarify that the Data Custodian is custodian of non-personal data, while the DPO is custodian of personal data.

b) **DGF-to-DPDPA role-mapping table.**

The Guidance should include a mapping of the DGF roles (Data Owner/Manager, Data Steward, Data Custodian) against the DPDPA roles (Data Fiduciary, Data Processor, Data Principal, DPO and Consent Manager) to prevent role confusion across the two regimes.

c) **Enablement of Data Principal rights.**

The organisational structure and the Data Function should be required to operationalise Data Principal rights under the DPDPA -access, correction, erasure, grievance redressal and nomination, including a defined interface with the RE's grievance-redressal mechanism.

Chapter IV — Data Lifecycle (Paras 32–42)

Consent management (paras 33, 35 and 62) should reference the DPDPA consent architecture explicitly, including the Consent Manager mechanism and the itemised notice requirement. Retention, archival and disposal (paras 41–42) should be reconciled with the DPDPA erasure duty, per Part A.

Chapter V — Data Architecture (Paras 43–59)

The Single Source of Truth (para 43) is the centrepiece of the Guidance but introduces a Single Source of Failure (SSOF) risk. It must therefore be paired with commensurate security controls and a federated access-and-storage model.

Concentration risk from foreign-MNC cloud storage should be addressed by encouraging the use of indigenous cloud services.

Metadata and lineage requirements should be framed to serve two ends beyond internal governance, first, enabling Data Principal rights fulfilment and second, governing AI/ML input data (training-data lineage, quality and bias), with an explicit cross-reference to the parallel MRM Guidance. This is the natural anchor for FDPPI's DGPSI-AI framework and the emerging AIGSI (Artificial Intelligence Governance Standard of India).

Chapter VI — Third-Party Arrangements (Paras 60–63)

Provision should be made for REs to engage external agencies such as Independent Data Auditors for audits under para 63, and external consultants to support the CDGDPO with appropriate security safeguards.

The cross-border elements (read with para 15(4)) should align expressly with the DPDPA's restricted-country transfer regime and with RBI's 2018 directive on storage of payment-system data in India.

Part C — Summary of Key Recommendations

1. Integrate the three RBI guidance into a single Master Data Governance Guideline; examine the DGPSI-Banks model.

2. State expressly that legal mandates (DPDPA, IT Act, Consumer Protection Act) prevail over guidance; resolve the minor-accounts and retention-versus-erasure conflicts.

3. Introduce Category I/II/III proportionality by Risk Size, with an applicability annexure and a phased transition timeline.

4. Replace the CERT-In audit restriction with the open term "Data Governance and Data Protection Auditors"; recognise External Data Governance Consultants and an SA 600-style aggregation-of-audits model.

5. Recognise Head Office / Regional Office / Branch tiers in implementation.

6. Create the CDGDPO designation, with associate DGDPOs at branch level.

7. Rename "Data Owner" as "Data Manager"; separate the Data Custodian (non-personal data) from the DPO (personal data); add a DGF-to-DPDPA role-mapping table.

8. Require the data architecture to enable Data Principal rights and to govern AI/ML input data, cross-referenced to the MRM Guidance.

9. Pair the SSOT with federated controls against Single Source of Failure; encourage indigenous cloud services.

10. Harmonise breach and incident notification across the DPDPA, CERT-In and RBI; align cross-border transfer with the DPDPA and RBI data-localisation.

11. Invite a notional data valuation (DVSI / CAG model), feeding the risk-size classification.

We would be happy to provide further details or supporting frameworks, and to engage with the concerned RBI team on any of the above.

Yours faithfully,

For Foundation of Data Protection Professionals in India

Na. Vijayashankar (Naavi)
Chairman, FDPPI