Data Rakshaq

From consent to compliance - seamlessly

RoPA under DPDP

Record of Processing Activities
A Complete Enterprise Guide

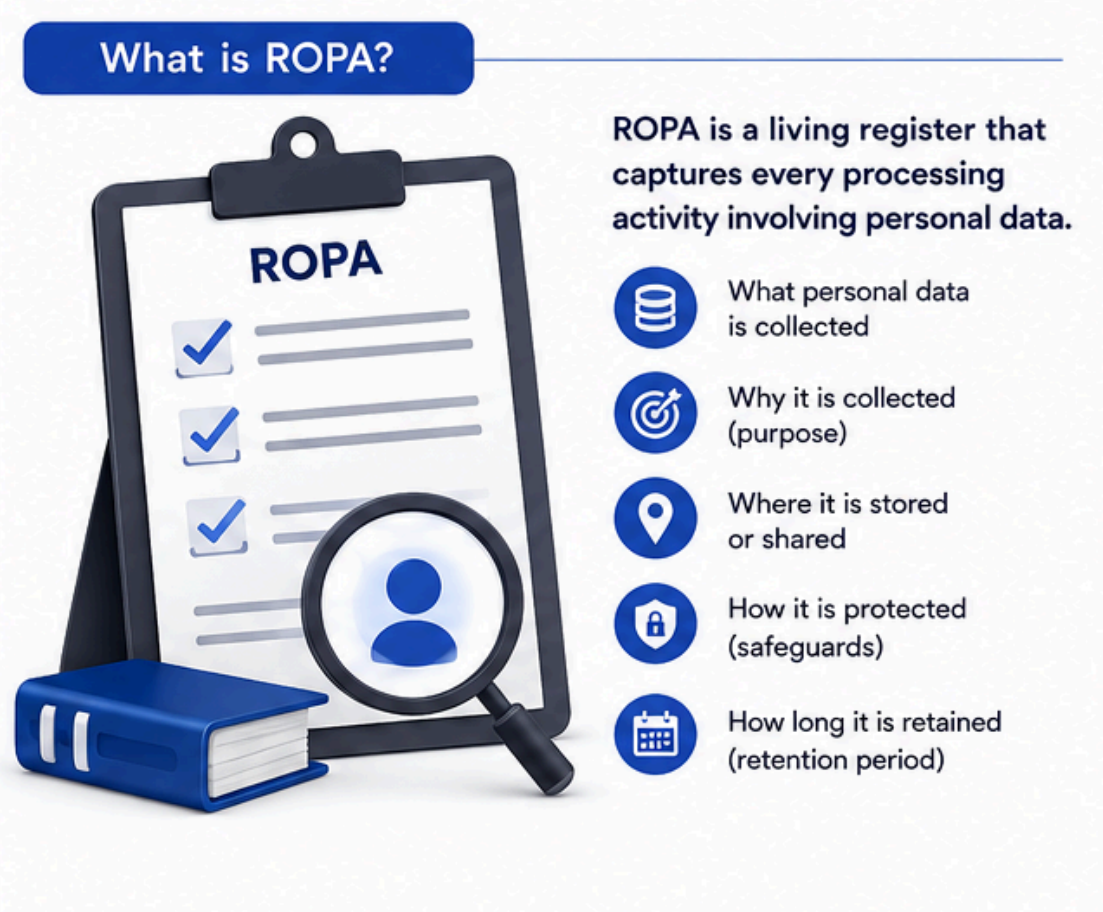
India's Digital Personal Data Protection Act (DPDP), 2023

Table of Contents

What is ROPA?

A **Record of Processing Activities** (ROPA) is the single, authoritative register of how personal data flows through your organisation — what you collect, why you collect it, where it goes, how it is protected, and how long you keep it.

The term comes from GDPR's Article 30, but the concept applies to any data protection law — including India's Digital Personal Data Protection Act (DPDP Act), 2023.



Key insight for Indian enterprises

The DPDP Act and DPDP Rules do not use the phrase 'ROPA' anywhere. But they impose four specific Data Fiduciary duties that are impossible to fulfil without one. In practice, maintaining a ROPA-style register is effectively mandatory for every Indian enterprise handling personal data.

The simplest way to think about a ROPA

Question	Example answer (retail bank)
What data do you collect? 	Name, PAN, Aadhaar, mobile number, income proof
Who does it belong to? 	Retail customers applying for a savings account
Why do you collect it? 	KYC verification under RBI Master Direction
Where is it stored? 	CRM system (Salesforce), Loan Origination System (Finacle)
Who else gets it? 	CIBIL bureau, KYC vendor (DocuVerify), cloud provider
How long do you keep it? 	10 years from account closure (RBI mandate)
Is it sent outside India? 	Yes — analytics SaaS vendor based in USA (flag for DPDP)
How is it protected? 	AES-256 encryption, Aadhaar masking, MFA for all access

An accurate, up-to-date ROPA helps organizations build trust, reduce risk, and stay prepared for evolving privacy regulations.

The three formats a ROPA can take

1. Excel / Google Sheets

Best for

Teams with < 50 staff and 1–4 core systems. Quick to start

Limitations

Static — does not update itself. Prone to version errors (ROPA_final_v6.xlsx).

2. Visual Data Map

Best for

Board presentations, IT architecture reviews, risk identification.

Limitations

Cannot hold granular details like retention periods. Not sufficient alone for audits.

3. Automated platform

Best for

Regulated entities, SDFs, fintechs, high data volumes.

Limitations

Requires significant implementation time and investment.

Why ROPA is unavoidable under DPDP

Section 8(3)— Duty of accuracy

Data Fiduciaries must keep personal data complete, accurate, and consistent across all downstream systems.

Real example: A customer at HDFC Bank updates their mobile number through net banking. **Without a ROPA** mapping all systems, the change may not reach the billing system, the marketing tool or the vendor's records — creating inaccurate data across the enterprise. A **ROPA shows every system that holds that customer's phone number, so the update propagates correctly.**

Section 12(3)— Duty of erasure

When a Data Principal withdraws consent, or when the processing purpose ends, you must erase their data from every system — not just the primary database.

Real example: A loan applicant at an NBFC withdraws consent after rejection. The team deletes the record from the LOS — but forgets the 'Weekly_Leads_Report_Final.xlsx' sitting in a shared Google Drive and the applicant's data in the marketing automation tool. A **ROPA is a verified checklist for full deletion: it lists every system and storage location that touched this applicant's data.**

Records deleted from LOS (Loan Origination System)

Records still their in shared Google and Excel files.

Section 8(7)— Breach Notification

When a Data Principal withdraws consent, or when the processing purpose ends, you must erase their data from every system — not just the primary database.

Real example: A database at a fintech is compromised at 2 AM. The DPO needs to know within hours: which customers were affected, what categories of data were exposed, and which vendors received that data. In the middle of an incident, there is no time to call the IT team. A **ROPA gives instant answers.**

Without ROPA

With ROPA

Section 11(1)— Duty to provide information

Any Data Principal can request details of: (a) their personal data being processed, (b) the processing activities and (c) with whom their data has been shared.

Real example: An employee at a large bank sends a Subject Access Request asking exactly what HR, payroll and IT systems hold their data. **Without a ROPA**, the HR team must scramble across HRMS, payroll SaaS, access logs, and vendor emails — still unable to give a complete answer within a reasonable timeframe.

Cannot delete the data from every system

Data is deleted from every system

What a ROPA must contain

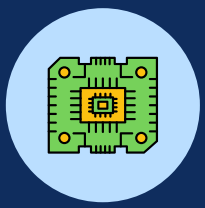
Processing activity / business process

Data principal

Purpose of processing

Data categories

Systems / storage locations



Vendors / processors

Retention period or rule

Cross-border transfers

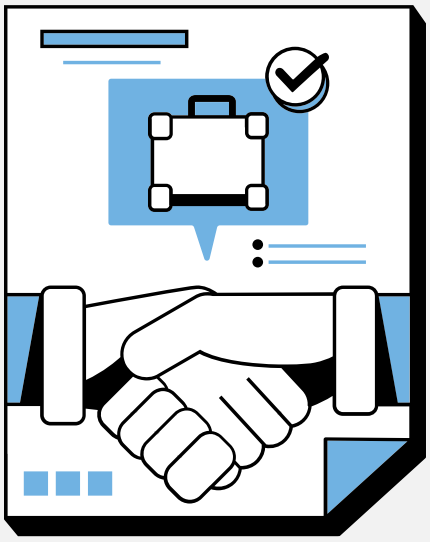
Key safeguards / controls

Source of data

What a completed ROPA register looks like

Customer Onboarding

The organization processes personal data for customer onboarding to complete KYC verification and account setup. The data collected includes the customer's name, PAN, Aadhaar number, phone number, and email address. This information is stored in the CRM and Loan Origination System (LOS), retained for **7 years**, and the processing activity is **complete**.

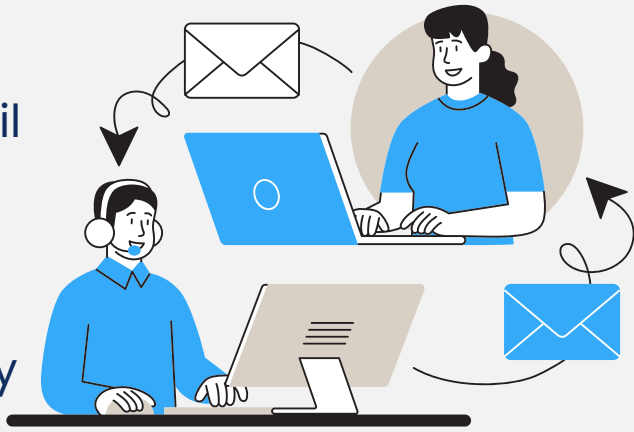


Payroll Processing:

Employee personal data is processed to manage salary disbursement. The information collected includes the employee's name, bank account details, PAN, and salary information. This data is maintained in the HRMS and ERP systems, retained for **10 years** and the processing activity is **complete**.

Email Marketing:

Customer data is processed for promotional and marketing communications. The organization collects the customer's name and email address, which are stored in the marketing platform. However, a data retention period has **not yet been defined,** making this processing activity **incomplete**.



Credit Assessment:

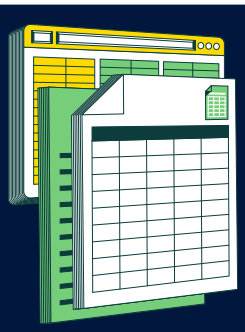
Customer personal data is processed to evaluate creditworthiness during the underwriting process. The data includes income details, PAN, and credit history, which are stored in the Loan Origination System (LOS) and credit bureau systems. The data is retained for **7 years**, and this processing activity is **complete**.

Analytics & Business Intelligence:

The organization uses pseudonymised transaction data from customers to generate business insights and analytics. This data is stored in the data warehouse. However, the retention period has **not been established**, so this processing activity is currently **incomplete**.

Regulatory retention reference — Indian financial sector

Data Type	Regulation	Minimum Retention
KYC documents 	RBI KYC Master Direction	10 years from account closure
Loan records 	RBI Prudential Norms	7 years from loan closure
Payment transaction data 	Prevention of Money Laundering Act (PMLA), 2002	5 years from transaction date
Employee records 	Labour Laws & Employees' Provident Fund (PF) Act	10 years from employee termination
Insurance policy records 	IRDAI Regulations	Policy duration + 3 years
GST / Tax records 	Income Tax Act & GST Act	7 years from the relevant assessment year



How to build your ROPA in Excel

Step 1 Create your workbook structure

Create a new workbook with four sheets:

Sheet 1: Processing Register (this is your main ROPA

Sheet 2: System inventory (all systems that touch personal data)

Sheet 3: Vendor register (all third parties receiving data

Sheet 4: Changelog (date, change, who made it)

In Sheet 1, add columns for all 10 fields from Chapter 3. Freeze the top row. Add ‘Last reviewed’ and ‘Status’ columns.

Step 2 Inventory your systems

Before filling in any row, list every system that processes personal data:

Core systems: CRM, LOS, HRMS, ERP, core banking

SaaS tools: marketing platform, email vendor, analytics tool

Storage: shared drives, S3 buckets, email inboxes

Vendors: credit bureaus, KYC vendors, cloud providers

For each system, identify the owner (the person responsible for that system) and work with them to list what data it holds and from which Data Principals.

Step 3 Fill in one row per processing activity

- Ask the system owner: what data is collected? from whom/why?
- Verify the legal basis — consent, contractual necessity,
- Set a specific retention rule — never leave this field blank
- Flag cross-border transfers (any data leaving India)
- Document at least 2–3 safeguards per activity

Start with your 3–5 most critical processes: customer onboarding, payroll, loan origination.

Step 4 Add data validation and conditional formatting

Use Excel's Data Validation feature:

Status column: dropdown → Complete / Incomplete / Review

Data principal: dropdown → Customers / Employees / Vendors

Cross-border: dropdown → Yes / No

Conditional formatting: amber fill for Incomplete rows, red fill for Review needed

This prevents free-text errors and makes the register easy to filter and audit.

Visual Mockup

Processing activity	Data principal	Purpose	Data categories	Systems	Vendors	Retention	Cross-border	Safeguards	Source
Customer onboarding	Customers	KYC	Name, PAN, Aadhaar	CRM, LOS	DocuVerify	7 years	No	Encryption, MFA	Direct
Payroll	Employees	Salary processing	Name, Bank Account, PAN	HRMS, ERP	Payroll SaaS	10 years	No	HR-only access	Direct
Marketing email	Customers	Promotions	Name, Email	Marketing Tool	Email Vendor	Not set	No	Opt-out mechanism	CRM

Automating your ROPA

Excel vs platform — capability comparison

Criterion	Excel / Sheets	Custom Scripts </>	Data RakshaQ Platform
Setup Effort	Low — Start immediately	Medium — Development resources	Low — Guided onboarding
Data Discovery	Manual only	Partial — Configuration required	Full automated scan
ROPA Updates	Manual edits	Semi-automated	Real-time auto-update
Consent Linkage	Not possible	Custom build required	Built-in workflows
Breach Response	Manual lookup	Partial	Instant impact map
Audit Readiness	Medium — Version control risk	Medium	High — Full audit trail
Best For	Organizations with <50 staff and 1–4	Tech-heavy teams with in-house	Regulated organizations with high data

FEATURES OF ROPA PLATFORM

- Data discovery
- Data mapping
- Real-time updates
- Consent linkage
- Full audit trail
- Breach impact mapping

Integration architecture — what systems connect

Category	Systems	ROPA value delivered
Core data systems 	CRM, LOS, HRMS, ERP, core banking	Auto-populate processing activities and data categories
SaaS & marketing tools 	Marketing platform, analytics, BI warehouse	Identify purpose and cross-border transfer flags
Consent platform 	Consent management, rights portal	Link consent withdrawal to erasure workflows
Unstructured storage 	Google Drive, SharePoint, S3, email inboxes	Discover shadow personal data in files and documents
Incident / SIEM 	Jira, ServiceNow, SIEM tools	Map breach impact to affected ROPA entries instantly
Regulatory 	Data Protection Board portal (S.8(7))	Automated breach notifications to the DPB

Two types of update triggers

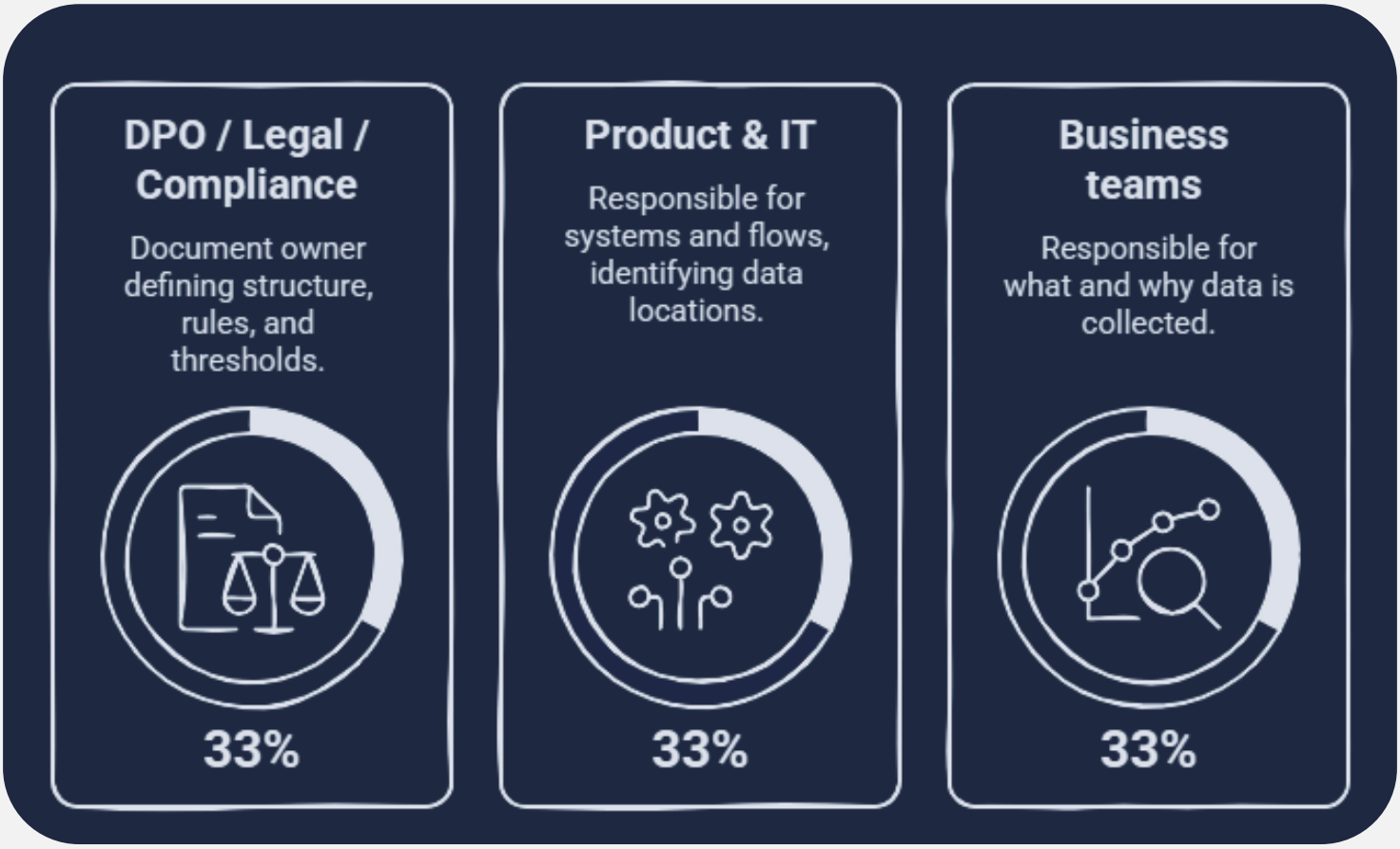
- **Time-based triggers**
  - **Quarterly review**
  - Legal/DPO + IT + Business scan for changes in systems, purposes, and vendors.

  - **Annual deeper review**
  - Align with internal audit. Revisit all retention rules and data minimisation practices.

- **Event-based triggers**

  Do a Privacy Impact Assessment (PIA) whenever:
  - You introduce a new system or major module
  - You onboard a new vendor or processor
  - You launch a new product or business line
  - You make a major change to an existing customer journey
  - You suffer a significant incident or breach

ROPA Ownership Model



A Record of Processing Activities (ROPA) is not owned by a single department—it is a collaborative responsibility across the entire organization. Legal and compliance teams establish the governance framework, IT and product teams provide visibility into systems and data flows, and business teams ensure every instance of personal data collection has a valid purpose and remains limited to what is necessary.

When these teams work together, the ROPA becomes more than a compliance document. It transforms into a living, continuously updated record that improves transparency, strengthens accountability, simplifies audits, accelerates responses to data subject requests, and helps organizations demonstrate compliance with the DPDP Act.

30-day action plan

Timeframe	Key actions	Deliverable
Days 1–7	Form a privacy working group (one person from Legal, IT, and each major business unit). Appoint a DPO or compliance lead. List all major systems: CRM, HRMS, LOS, ERP, etc.	**✓ Privacy working group formed, system inventory started**
Days 8–15	Interview system owners. Identify data categories per system. Document data principals for each system (customers, employees, vendors).	**✓ Data categories mapped to all major systems**
Days 16–22	Map purposes and legal basis for each processing activity. Flag any cross-border data transfers. Identify vendor DPA gaps.	**✓ First draft ROPA entries for 3–5 critical processes**
Days 23–30	Choose your ROPA format (Excel or platform — see Chapters 5 and 6). Conduct first completeness review. Schedule recurring quarterly update cycle.	**✓ Publishable v1.0 ROPA register ready for internal review**

ROPA readiness checklist

ROPA Structure ✅

- All 10 mandatory fields are present as columns in the register
- Header row is frozen and columns have drop-down data validation
- A Status column exists with Complete / Incomplete / Review Needed values
- Last Reviewed and Changed By columns are present
- A changelog sheet or version history is maintained

Processing Activities ✅

- Every system that touches personal data has at least one ROPA entry
- Each entry has a named data principal type (not just "users")
- Each entry has a specific, documented purpose (not "business use" or "analytics")
- All data categories are listed explicitly (not just "customer data")
- Legal basis is documented for every single entry

Retention & Vendors ✅

- Every entry has a retention period or retention rule; none are blank
- Cross-border transfers are flagged with the destination country
- All vendors/data processors are named by company, not listed as "third parties"
- DPA status is confirmed for every vendor processing personal data
- Vendors with cross-border transfers have the transfer mechanism documented

DPDP Duty Readiness ✅

- All downstream systems are mapped so data changes can propagate correctly (Section 8(3))
- Each entry has enough system detail for a complete erasure exercise (Section 12(3))
- Breach response playbook references the ROPA for affected Data Principal identification (Section 8(7))
- ROPA can answer a Data Principal information request within 72 hours (Section 11(1))
- ROPA is reviewed at least quarterly and whenever a material change occurs