mociber

"Simplifying Everything."

DPDP Rules 2025: Guidance to Digital Personal Data Protection Act Implementation

Version: December 2025

Prepared for: Industry Stakeholders, Privacy Leaders & Compliance Teams

Executive Summary

The Digital Personal Data Protection Rules, 2025, issued by the Ministry of Electronics & IT (MeitY), operationalise the Digital Personal Data Protection Act, 2023 and provide the first comprehensive, actionable framework for organisations processing digital personal data in India.

These Rules introduce clarity on consent flows, breach reporting, security safeguards, children's data, cross-border transfers, and retention timelines — enabling organisations to establish predictable, standardised privacy operations.

The DPDP Rules serve as a practical bridge between legislative intent and real-world implementation. They outline the minimum controls and governance expectations that Data Fiduciaries, Data Processors, Consent Managers, and Significant Data Fiduciaries (SDFs) must adopt.

When effectively implemented, the Rules strengthen organisational accountability, reduce compliance ambiguity, and foster a transparent, privacy-first ecosystem that enhances trust with India's rapidly growing digital population.

Enforcement Timelines

The Rules define when obligations under DPDPA become enforceable.

DPDP Act Section	DPDP Rule	Obligation	Timeline
Section 6(8), 6(9)	Rule 4	Consent Manager registration & obligations	1 year from publication
Section 3	NA	Applicability of the Act	18 months from notification
Section 5, 6(10)	Rule 3	Notice to Data Principal	Effective immediately post-notification
Section 9	Rule 10, 12	Processing children's data	As per Rule commencement
Section 10	Rule 13	Obligations of SDF	As per Rule commencement
Sections 11–14	Rule 14	Data Principal Rights	As per Rule commencement
Section 16	Rule 15	Cross-border transfers	As notified by Government

Key Timelines Specified in the Rules

Rule	Obligation	Timeline
Rule 7(1), 7(2)	Data breach intimation to DPB	Immediate (first intimation); 72 hours (detailed)
Rule 8(2)	Retention & deletion (e-commerce/social/gaming)	3-year retention; 48-hour prior deletion notice
Rule 12(1)	DPIA & Data Audits	Annual (from Nov 13, 2025 or SDF designation)
Schedule I, Part B	Consent record retention	7 years
Rule 14(3)	Grievance redressal	Response within 90 days

Additional requirement: Data Fiduciaries and SDFs must publish contact details of their grievance officer/DPO on their website/app.

DATA BREACH ALERT PROTOCOL

Inside India's New 3-Layer Breach Reporting System
When a personal data breach hits, the DPDP Rules 2025 demand speed, clarity, and transparency. No delays. No silence. No excuses.
India's new framework creates a three-tier, time-bound escalation model that every tech team, CISO, and privacy lead must master.

Primary Alert to the DPB — "Tell Us Immediately"

Timeline: Without delay — the moment the organisation becomes aware.

This first alert is a rapid-fire situational report.

It must include:

- What happened (nature of breach)
- How bad it is (extent & likely impact)
- When it occurred (timing)
- Where it occurred (location)

This is the DPB's first window into the incident.

Secondary Report — The 72-Hour Deep Dive

Timeline: Within 72 hours of awareness (unless extended by the Board).

This is the detailed, forensic-grade update.

It must include:

- All updates from the first alert
- Root cause of the breach
- Containment + mitigation actions
- Controls to prevent recurrence

Think of this as the formal incident dossier.

Notify the Data Principals — "Tell the People Affected"

Timeline: Without delay.

This notice must be user-centric, clear, and immediately actionable.

It must include:

- What happened (description + timeline)
- Consequences the user may face
- What the organisation is doing to fix it
- What the user should do (safety steps)
- Contact details of the official handling the breach

Delivery channels:

- User account notifications
- Registered email
- Registered mobile
- Any mode the user has officially provided

This ensures no one stays in the dark when their data is at risk.

REQUIREMENTS
NOTICE & CONSENT

Under the DPDP Rules 2025, every organisation MUST give a proper notice before collecting personal data. This notice must help the user understand exactly what is happening with their data — without confusion, hidden details, or legal jargon.

➤ "Be standalone and understandable without external references"

The notice must explain everything important on its own.

This means:

- Users should not need to click multiple links or open extra documents to understand what the organisation is doing.
- No hiding information in long privacy policies or hard-to-find pages.
- The notice itself should give a complete picture.

Example:

❌ "See our privacy policy for details" → NOT allowed

✓ "We collect your name to create your account and send updates" → Allowed

REQUIREMENTS
NOTICE & CONSENT

Under the DPDP Rules 2025, every organisation MUST give a proper notice before collecting personal data. This notice must help the user understand exactly what is happening with their data — without confusion, hidden details, or legal jargon.

➤ "Be standalone and understandable without external references"

The notice must explain everything important on its own.

This means:

- Users should not need to click multiple links or open extra documents to understand what the organisation is doing.
- No hiding information in long privacy policies or hard-to-find pages.
- The notice itself should give a complete picture.

Example:

❌ "See our privacy policy for details" → NOT allowed

✓ "We collect your name to create your account and send updates" → Allowed

“Use clear, plain language”
The notice must be simple enough for any normal user to understand.
This means:

- No legal wording
- No complicated sentences
- No technical jargon without explanation

Example:
❌ “Your data shall be processed for legitimate business purposes.”
✓ “We use your data to provide our services and improve your experience.”

“Provide itemised purpose and data categories”
The notice must break information into clear bullet points:
● What data is being collected?
(name, email, phone number, location, etc.)
● For what exact purpose?
(account creation, delivery, recommendations, notifications, etc.)
No vague statements like “for service improvement.”
Everything must be specific and itemised.

“Include link/digital mechanism to: withdraw consent, exercise rights, file complaints”
The notice must include a clickable link or digital option that allows the user to:
✓ Withdraw their consent
Users should be able to click a button or follow a clear path to remove their consent.
✓ Exercise their rights
Such as access, correction, erasure, or grievance.
✓ File complaints with the Data Protection Board (DPB)
A link or pathway must exist to guide them to the DPB if they want to escalate.
This ensures transparency and user empowerment.

“Consent withdrawal must be as easy as consent collection.”
This is one of the MOST important rules.
It means:
❌ You cannot make withdrawing consent difficult

- No long forms
- No hidden pages
- No customer-care calls
- No “email us and wait 15 days”
- No forcing users to explain why they’re leaving

✓ It must be as easy as giving consent
If the user gave consent by clicking a button,
they must be able to withdraw it by clicking a button too.
Example:

- If signup consent is one click → withdrawal must also be one click
- If consent is collected in the app → withdrawal must also be available in the app

This prevents dark patterns and user manipulation.

OBLIGATIONS OF CONSENT MANAGERS

A Consent Manager is a specialised entity that helps users give, view, manage, and withdraw consent across different digital services — all from one place.

India introduced this concept to make consent transparent, standardised and user-controlled.

- Operate primarily via a digital platform (website/app)
- Publish corporate and compliance disclosures
- Maintain robust security safeguards
- Ensure unreadable personal data during transfers
- Avoid conflicts of interest
- Not subcontract obligations
- Provide interoperable consent dashboards
- Retain consent records for 7 years
- Undergo periodic audits and submit findings to the Board

Reasonable Security Safeguards

Securing Personal Data

- Encryption
- Tokenisation
- Obfuscation/masking
- Virtual identifiers

Access Controls

- Restrict system access
- Role-based controls
- Prevent unauthorised processing

Contractual Controls

- Processor contracts must mandate safeguards

Monitoring & Detection

- Detect & investigate unauthorised access
- Retain logs for 1 year (unless otherwise required)

Business Resilience

- Backup mechanisms
- Continuity for data integrity/availability events

Empowering Data Principals

Organisations must:

- Publish processes for exercising rights
- Ensure grievance resolution within 90 days
- Provide identifiers (customer ID, email, account reference, etc.) for rights requests

Data Principals may:

- Access, correct, erase their personal data
- Withdraw consent
- Nominate another individual to exercise rights on their behalf

https://www.mociber.com/

CROSS-BORDER DATA TRANSFERS

The DPDP Act and Rules take a liberal, business-friendly approach to international data transfers — but with government-controlled restrictions to ensure national security and data protection.

Organisations ARE allowed to transfer personal data outside India,
BUT only to countries that are not restricted by the Government of India.

Restrictions approving country-by-country transfers (like EU's adequacy decisions), India simply blocks high-risk destinations.

Even when transfer is allowed, the Government may ask organisations to implement extra protections.

You can freely store or process data in countries like the US, EU, UK, Singapore, etc.
Unless the Government explicitly restricts them.

RETENTION TIMELINES

Applies to:

- E-commerce entities (≥ 2 crore users)
- Social media intermediaries (≥ 2 crore users)
- Gaming intermediaries (≥ 50 lakh users)

Retention cap: 3 years for all purposes except:

- Access to user account
- Access to virtual tokens for money/services

Erasure process:

- Notify user 48 hours prior
- Erase unless the user logs in or reaches out

OBLIGATIONS OF SIGNIFICANT DATA FIDUCIARIES

SDFs must review their data processing every year to identify risks to users.
Then, an independent external auditor must verify whether the organisation is following the DPDP Act properly.
This ensures continuous compliance and transparency.

If the organisation uses AI, automated decision-making, or algorithm-based systems, it must check and test those systems to make sure they do not discriminate, cause unfair outcomes, or harm users.
The goal is to prevent biased, unsafe, or harmful algorithmic decisions.

The Government may mark certain datasets as sensitive or high-risk.
If so, SDFs must follow stricter rules for processing these datasets — such as limiting access, adding extra security, and monitoring usage.
This protects nationally important or sensitive personal data.

If the Government declares a type of dataset as “cannot be sent outside India”, SDFs must keep that data within Indian borders only.
They cannot store or process it on foreign servers or allow foreign access.
This protects national security and sensitive data sovereignty.

Exemptions

Child-related Exemptions (For specific entities):

- Clinics, hospitals, educational institutions, crèches, childcare transport providers

Research/Archiving/Statistical Exemptions:

Applicable if:

- Lawful, necessary, minimal, secure
- Accuracy maintained
- Retention limited
- Accountability ensured

Purposes Allowed for Child-Data Processing:

- Government benefits/licenses/subsidies
- Email account creation
- Real-time location determination
- Preventing harmful content exposure

CONCLUSION

DPDPA and the DPDP Rules 2025 mandate a modern, trust-centric, globally aligned privacy regime in India. Organisations that adopt privacy-by-design, automate compliance operations, and prepare early will:

- Minimise regulatory exposure
- Strengthen brand trust
- Improve operational efficiency
- Enable safe digital innovation

This whitepaper is as per our understanding and research. The actual interpretation of the DPDP Act and DPDP rules are with the regulators and concerned authorities.
https://www.mociber.com/

mohsin@mociber.com

+91-7302821607

www.mociber.com

India | Middle East | USA* | Europe* |