

Flash Compliance Update

DPDP Rules 2025

What Organizations Must Do Next

Why This Matters

The DPDP Rules now operationalize the Act as on date 13th Nov 2025 – meaning organizations will be expected to prove compliance, not just declare it.

The rules specify:

- Required security measures
- How to obtain/manage consent
- Breach reporting expectation
- Rights management workflows
- Cross-border data transfer governance
- Children's data processing controls
- Mandatory audits for Significant Data Fiduciaries

The countdown begins now – with 18 months until majority of operational rules become enforceable.

1. Detailed Rule Breakdown With Required Action & Compliance Deadline



Rule	Requirement Summary	Required Actions for Organizations	Compliance Deadline	Relevant Technology Solution
Rule 1	Timeline Enforcement Details	No action (context only)	● Immediate	None
Rule 2	Defines core terms aligned with the Act (verifiable consent, user account, processing, safeguards etc.)	Update internal governance, legal docs, privacy policy	● Immediate	N/A
Rule 3	Privacy notices must be clear, standalone, purpose-specific, include rights, withdrawal, grievance	Rewrite notices across digital touchpoints; Ensure user comprehension	● Within 18 months	CMS updates, UX redesign, Consent banner systems, multilingual support
Rule 4	Registration and obligations of Consent Managers via whom users can manage consent centrally	Prepare for API-based integration with designated Consent Managers	● One year	Consent registry, API gateway, secure token exchange, event logging
Rule 5	Data processed for Government services must meet purpose-limitation and compliance rule	Review and categories government-linked processing; aligns uses with allowed purposes; contractual alignment.	● Within 18 months	Data classification engine, purpose mapping, RBAC controls
Rule 6	Mandates reasonable security controls incl. encryption, IAM, logging, monitoring, vendor controls	Conduct security gap assessment, update security policies, SOPs, vendor contracts and implement required safeguards	● Within 18 months	Encryption-at-rest & transit, masking, obfuscation, DAM, SIEM, SOC, IAM/PAM, immutable logs, backup automation

● Effective immediately | ● Shall come into force in one year | ● Must be implemented within 18 months

Rule	Requirement Summary	Required Actions for Organizations	Compliance Deadline	Relevant Technology Solution
Rule 7	Requires breach notification to users and Board without undue delay with prescribed details within 72 hrs	Establish breach response process, templates & stakeholder matrix	● Within 18 months	SOAR/SIEM alerts, incident management platform, automated user notification workflows (SMS/ email/app)
Rule 8	Organizations must delete data post-purpose; notify user at least 48 hours before deletion	Implement data retention policy, automated deletion workflows and logs	● Within 18 months	Data discovery, data lifecycle management system, archiving engine, deletion automation with audit trail, data cataloguing
Rule 9	Publish a designated privacy contact or DPO for user rights & communication	Assign privacy contact & publish on website/app	● Within 18 months	Ticketing workflow, DPO inbox routing, response SLA tools
Rule 10	Verifiable parental consent required before processing personal data of minors (<18)	Build age-gating & parental consent workflow	● Within 18 months	Age verification engine (KYC/ Aadhaar API), identity proofing, child data tagging logic
Rule 11	Consent for persons with disability must come from verified legal guardian	Create assisted consent path and validate guardian credentials	● Within 18 months	Document verification engine, accessibility UI, identity validation, Consent manager platform
Rule 12	Certain types of child-data processing may be exempt under conditions	Document eligibility, governance & exception controls	● Within 18 months	Exception registry, configurable policy rule engine
Rule 13	Significant Data Fiduciaries (SDFs) require annual DPIA, audits, governance controls, and data localisation safeguards	Identify SDF applicability, prepare annual audit/DPIA process & governance	● Within 18 months (or upon formal designation)	GRC platform , DPIA automation, risk dashboards, algorithmic bias/ testing engine

● Effective immediately | ● Shall come into force in one year | ● Must be implemented within 18 months

Rule	Requirement Summary	Required Actions for Organizations	Compliance Deadline	Relevant Technology Solution
Rule 14	Must enable Data Principal rights: access, correction, withdrawal, deletion, grievance, nomination	Deploy rights management workflows with tracking & SLA	● Within 18 months	Data Principal Rights Portal, workflow automation, identity validation, case management
Rule 15	Cross-border data transfer allowed unless restricted by government & must meet safeguards	Map global data flows; implement contractual + governance safeguards	● Within 18 months	Geo-fencing/ data residency governance, Transfer Impact Assessment engine, SCC contract tracking
Rule 16	Research/statistical/archival processing exempt if data is properly anonymized	Ensure anonymisation meets standards; document controls	● Within 18 months	Pseudonymisation/ anonymisation tools, secure research sandbox environment
Rule 17	Appointment chairperson and other member	No action for organizations. The Data Protection Board will establish this.	● Immediate	N/A
Rule 18	Salary and service rules for Board staffing	No action for organizations. The Data Protection Board will establish this.	● Immediate	N/A
Rule 19	Governs Board procedures, quorum, decision-making	No action for organizations. The Data Protection Board will establish this.	● Immediate	Compliance readiness planning
Rule 20	Board will operate digitally; hearings and compliance online	Prepare regulatory reporting protocols	● Immediate	Regulatory evidence vault, secure upload portal integration
Rule 21	Staffing provisions for Board	No action for organizations. The Data Protection Board will establish this.	● Immediate	N/A
Rule 22	Appeal process established under the tribunal framework	Prepare regulatory engagement + litigation readiness	● Within 18 months	Digital case filing capability, compliance evidence repository
Rule 23	Government may demand specific information under controlled circumstances	Build controlled workflow for lawful disclosure	● Within 18 months	Regulatory action playbooks, secure data extraction tooling, audit registry

● Effective immediately | ● Shall come into force in one year | ● Must be implemented within 18 months

2. Enforcement Model & Penalties

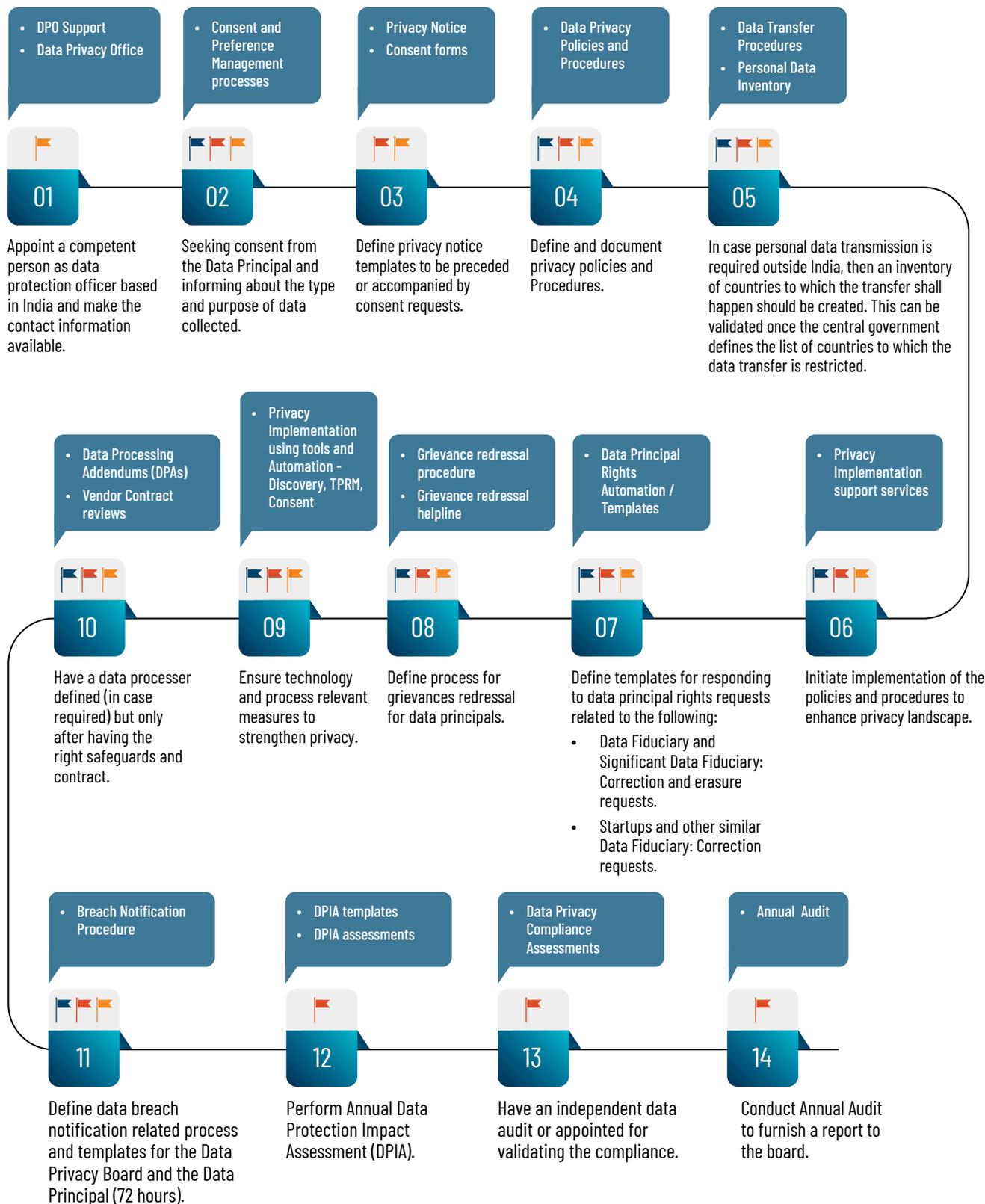
Penalties apply per violation category and may go up to:

Area of Non-Compliance	Indicative Cap
Security Failures	₹250 Cr
Breach Notification Lapse	₹200 Cr
Child Data Misuse	₹200 Cr
Failure to Erase Data Post Retention Period	₹150 Cr
Breach of any other provision of this Act	₹50 Cr

Regulatory actions may also include:

- Corrective orders
- Suspension of data processing
- Blacklisting or restricted operations

Next-Step: Roadmap for Organisations



OUR RECENT REPORTS

INSIGHT



Navigating Data Privacy in Digital India



REPORT



State of Data Privacy in India



WHITEPAPER



Data Privacy in Digital India



WHITEPAPER



Navigating DPDP in Banking



WHITEPAPER



Safeguarding From Within: Insider Risk Management in India



INSIGHT



Harnessing the future: Protiviti's research on AI adoption



WHITEPAPER



AI Driven Collections Strategy for Unsecured Lending



WHITEPAPER



ML Model Validation Best-practice



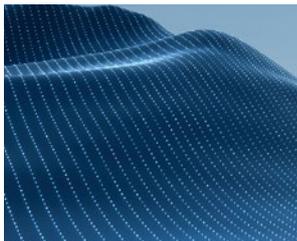
INSIGHT



Top compliance challenges facing the technology industry in 2025



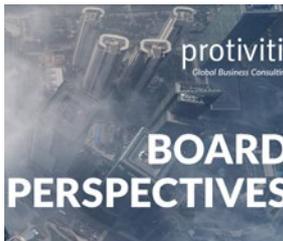
INSIGHT



Technology-modernization projects



NEWSLETTER



The Directors Playbook for Gen AI



REPORT



AI Trends and Future Impact Industry Adoption & Insights



About Protiviti

Protiviti (www.protiviti.com) is a global consulting firm that delivers deep expertise, objective insights, a tailored approach and unparalleled collaboration to help leaders confidently face the future. Protiviti and its independent and locally owned member firms provide clients with consulting and managed solutions in finance, technology, operations, data, digital, legal, HR, risk and internal audit through a network of more than 90 offices in over 25 countries.

Named to the Fortune 100 Best Companies to Work For® list for the 11th consecutive year, Protiviti Inc. has served more than 80 percent of Fortune 100 and nearly 80 percent of Fortune 500 companies. The firm also works with government agencies and smaller, growing companies, including those looking to go public. Protiviti Inc. is a wholly owned subsidiary of Robert Half (NYSE: RHI).

Sandeep Gupta

Managing Director
Sandeep.Gupta@protivitiglobal.in
+91 9702730000

Puneet Gupta

Managing Director
Puneet.Gupta@protivitiglobal.in
+91 9654381181

Dhrubabrata Ghosh

Managing Director
Dhrubabrata.Ghosh@protivitiglobal.in
+91 9739546661

Vaibhav Koul

Managing Director
Vaibhav.Koul@protivitiglobal.in
+91 9819751715

Vijai K

Managing Director
Vijai.K@protivitiglobal.in
+91 9880529503

Sindhu Vethody

Managing Director
Sindhu.Vethody@protivitiglobal.in
+91 9321886905

Prashant Singh

Managing Director
P.Singh@protivitiglobal.in
+91 9739179111

Sarita Padmini

Senior Director
Sarita.Padmini@protivitiglobal.in
+91 9953043552

Sahil Chander

Senior Director
Sahil.Chander@protivitiglobal.in
+91 8800490154

Nagesh Akula

Senior Director
Nagesh.Akula@protivitiglobal.in
+91 9866694411

Face the Future with Confidence®

This publication has been carefully prepared, but should be seen as general guidance only. You should not act or refrain from acting, based upon the information contained in this publication, without obtaining specific professional advice. Please contact the person listed in the publication to discuss these matters in the context of your particular circumstances. Neither Protiviti India Member Private Limited nor the shareholders, partners, directors, managers, employees or agents of any of them make any representation or warranty, expressed or implied, as to the accuracy, reasonableness or completeness of the information contained in the publication. All such parties and entities expressly disclaim any and all liability for or based on or relating to any information contained herein, or error, or omissions from this publication or any loss incurred as a result of acting on information in this presentation, or for any decision based on it.