Introduction

The Digital Personal Data Protection Act, 2023 (DPDPA), outlines comprehensive requirements for handling data breaches in India. These frameworks summarize key provisions related to data breach management, emphasizing accountability for entities processing personal data. The DPDPA establishes a statutory framework that mandates specific obligations for Data Fiduciaries to ensure the protection of personal data in the event of a breach.

1. Core Definitions & Stakeholders

- Personal Data Breach
    - Any incident—accidental or malicious—that leads to loss, alteration, unauthorized disclosure of, or access to personal data.
- Data Fiduciary
    - The entity determining "why" and "how" personal data is processed; bears primary legal responsibility for breach management.
- Data Principal
    - The individual to whom the compromised data belongs; entitled to timely notification and guidance.
- Data Protection Board of India (DPBI)
    - Statutory body empowered to receive breach reports, issue urgent directions, conduct inquiries, and impose penalties.

---

2. Statutory Breach-Response Obligations (DPDPA, 2023)

- Detection & Escalation
    - Deploy continuous monitoring (SIEM, anomaly detection) to flag suspicious events.
    - Document and escalate incidents internally to a dedicated response team.

- 72-Hour Notification Requirement
    - From the moment a breach is confirmed or reasonably suspected, notify both:
        - DPBI via its secure electronic portal.
        - Affected Data Principals in clear, non-technical language.
- Mandatory Notification Contents
    - Brief description of the breach (what happened, when it was discovered)
    - Types/categories of personal data affected
    - Approximate number of records and data principals impacted
    - Potential consequences for individuals (e.g., identity theft risk)
    - Steps taken or planned to contain and mitigate the breach

---

3. Detailed Procedures (Draft DPDP Rules, 2025)

- Standardized Reporting Template
    - Sections for factual summary, risk assessment, and remediation plan.
    - Ensures consistency across notifications to DPBI and Data Principals.
- Communication Guidelines
    - Use simple, concise language; avoid technical jargon.
    - Provide clear guidance on next steps for affected individuals (e.g., password resets, fraud monitoring).
- Record-Keeping & Audit Trails
    - Retain all breach-related logs, investigation reports, and communications for minimum five years.

- File an annual consolidated breach-report to DPBI, highlighting trends and corrective actions.

---

4. DPBI's Enforcement & Penalties

- Investigative Authority
  - Summon records, inspect IT systems, and question personnel to determine root cause and accountability.
- Financial Penalties
  - Up to ₹250 crore for failure to implement reasonable security practices.
  - Up to ₹200 crore for delayed or incomplete breach notifications.
  - Penalty amounts scaled based on severity, negligence, and data-principal impact.
- Non-Monetary Sanctions
  - Suspension of data-processing activities, publication of non-compliance findings, and potential blocking of digital assets for repeated breaches.
- Appeal Mechanism
  - Entities may challenge DPBI orders before the Appellate Tribunal within 60 days through an online process.
- Emergency Powers of DPBI
  - On receiving a breach report, DPBI may order immediate measures—such as suspending processing or enforcing system lockdown—pending full inquiry.

5. Breach Classification & Materiality Thresholds

- Purpose of Classification
  - Prioritize resources and escalation based on breach impact and data sensitivity.

- Severity Categories
    - **High Severity**: Exposure of large volumes (>10,000 records) of sensitive data (e.g., financial, health); immediate risk of significant harm.
    - **Medium Severity**: 1,000–10,000 records of personal data or exposure of moderately sensitive data.
    - **Low Severity**: <1,000 records of non-sensitive data (e.g., preference settings, non-critical identifiers).
- Materiality Thresholds
    - Define internal quantitative thresholds (e.g., >5% of user base) to trigger DPBI notifications and executive-level response even for lower-sensitivity data.
    - Sample Matrix:
        - **High Severity + High Volume** → Immediate DPBI reporting and crisis management team activation.
        - **Medium Severity + Medium Volume** → Standard 72-hour DPBI notification; internal response.
        - **Low Severity + Low Volume** → Document incident; include in quarterly DPBI trend report.

---

6. Cross-Border Data Transfer Notifications

- Scope
    - Breaches affecting data stored or processed outside India must comply with DPDPA breach notification plus any applicable foreign regulations (e.g., GDPR).
- Workflow
    - Identify impacted jurisdictions and applicable foreign breach-notification laws.
    - Engage local counsel for cross-border compliance guidance.
    - Submit parallel notifications:
        - **DPBI** (within 72 hours) detailing cross-border processing.

        - **Foreign Supervisory Authority** (as per local timelines).
- Data Principal Communication
    - Provide consolidated notice outlining cross-border details, local rights, and contact points for queries.

---

7. Incident Response Team Structure & RACI Matrix

- Team Roles
    - **Incident Commander**: Overall responsibility and decision authority.
    - **IT/Forensics Lead**: Technical containment, investigation, and root-cause analysis.
    - **Legal & Compliance Lead**: DPBI liaison, regulatory filings, legal risk management.
    - **Communications Lead**: Notifications to Data Principals, media, partners.
    - **Customer Support Lead**: Helpline setup and remediation services coordination.
- RACI Matrix

Task	Responsible	Accountable	Consulted	Informed
Breach Detection & Triage	IT/Forensics Lead	Incident Commander	Security Operations, DPO	Executive Team
DPBI Notification	Legal Lead	Incident Commander	IT/Forensics, Communications Lead	Board, DPO
Data Principal Advisories	Communications Lead	Incident Commander	Legal, Customer Support	DPO
Media Statements	Communications Lead	CEO/CCO	Legal, Incident Commander	All Staff
Forensic Analysis	IT/Forensics Lead	Incident Commander	External Experts	Legal
Post-Incident Review	DPO	Incident Commander	All Team Leads	Board

8. Breach Notification Channels & Template Samples

- Channels
    - **Email**: Detailed formal notices with branded template.
    - **SMS/Instant Messaging**: Immediate alerts; brief content linking to full notice.
    - **Customer Portal**: Bulletin or notification module for logged-in users.
- Sample Notification Template
    - **Subject:** Important Security Notification: Data Incident on [Date]

    Dear [Name],

    We recently identified an unauthorized access incident on [Date]. Your personal data (e.g., [Data Types]) may have been exposed. We have contained the issue, reset affected credentials, and engaged forensic experts.

    Steps for You:

        - *Change your password immediately.*
        - *Enable multi-factor authentication.*
        - *Monitor your account and financial statements.*

    For assistance, contact [Helpline]. We apologize for any inconvenience.

---

9. Data Protection Impact Assessments (DPIAs) & Pre-Breach Controls

- DPIA Requirement
    - Mandatory for high-risk processing under Draft DPDP Rule 6 (e.g., biometric systems, health data analytics).
- DPIA Process
    - **Define Scope**: Map data flows and stakeholders.
    - **Risk Analysis**: Identify threats and vulnerabilities.

    - **Evaluate Controls**: Review existing security measures.
    - **Mitigation Plan**: Implement additional safeguards (encryption, access controls).
    - **Documentation & Sign-off**: DPO approval; regular reviews.
- Pre-Breach Controls
    - **Data Minimization**: Only collect necessary data.
    - **Encryption**: AES-256 at rest; TLS 1.3 in transit.
    - **Access Management**: Role-based controls with periodic reviews.
    - **Continuous Monitoring**: 24×7 Security Information and Event Management and automated alerts.

---

10. Breach-Simulation Exercises & Table-Top Drills

- Purpose
    - Validate response plans, communication procedures, and decision-making during a breach.
- Exercise Types
    - **Table-Top Drill**: Scenario discussion with key stakeholders; policy and workflow validation.
    - **Live Simulation**: Controlled activation of breach alerts and system isolation.
- Metrics
    - **Mean Time to Detect (MTTD)**: Measure detection speed.
    - **Mean Time to Contain (MTTC)**: Time to halt breach propagation.
    - **Notification Lead Time**: From detection to DPBI/Data Principal notification.

---

11. Consent Manager Breach Obligations

- Role & Scope

    - Consent Managers facilitate consent collection, storage, and revocation on behalf of multiple Data Fiduciaries.

- Notification Requirements
    - Report breaches affecting consent records to DPBI within **48 hours**.
    - Notify downstream Data Fiduciaries whose processing relies on compromised consent data.
    - Retain breach logs and communications for **five years**.

---

12. Privacy by Design & Security by Default Integration

- Embedding in Development
    - **Requirements Phase**: Incorporate data-protection checkpoints in early design.
    - **Secure Coding**: Adhere to OWASP Top 10 countermeasures; periodic code reviews.
    - **Automated Security Testing**: Integrate SAST (Static Application Security Testing) and DAST (Dynamic Application Security Testing) into CI/CD pipelines.
- Default Security Controls
    - **Logging & Auditing**: Default-on for all sensitive operations.
    - **Encryption**: Mandatory for new data stores and service communications.
    - **Least-Privilege Access**: Deny-all default; grant minimal necessary permissions.

Conclusion Adopting a comprehensive breach-management strategy—spanning classification, cross-border protocols, structured incident response, clear notifications, DPIAs, simulations, customer remediation, Consent Manager duties, and privacy-by-design—ensures not just compliance with India's DPDPA and DPDP Rules but also enhances organizational resilience and stakeholder trust.



ConsenSys

Powered by

digio

Data compliance for Legal teams,

Data Access for Business teams,

Data Privacy for Customers.

Schedule a demo today, Get in touch with us at

Email : bd@digio.in

Ph: 080-69489510