DPDP INCIDENT & BREACH REPORTING TEMPLATES

Notices • Timelines • Escalation matrix • Officer roles

Issued by **Senmig GRC Technologies** — single point of contact in India for DPDP Act, GDPR & SOC 2 implementation. Use these working templates to record, notify and escalate personal-data breaches under the Digital Personal Data Protection Act, 2023.

1. Statutory Notification Timeline

When	Action	Detail
T+0	Detection / suspicion	SOC, IT, vendor or employee report logged in incident register.
≤ 6 hrs	Internal escalation	Notify CISO, DPO, Grievance Officer & Incident Commander. Open ticket.
≤ 24 hrs	Triage & containment	Classify severity (S1–S4); isolate systems; preserve evidence & logs.
≤ 72 hrs	Notice to Data Protection Board (DPB)	File initial breach notice via Form A (sample below).
≤ 72 hrs	Notice to affected Data Principals	Send Form B individual notice (email / SMS / in-app).
≤ 7 days	Sectoral regulator notice	RBI / SEBI / IRDAI / CERT-In as applicable; align with sectoral rules.
≤ 30 days	Root-cause & remediation report	Submit RCA, corrective actions and control uplift to DPB.
Ongoing	Post-incident review	Lessons learned, control redesign, board reporting, audit closure.

2. Severity Classification & Escalation Matrix

Sev	Definition	Owner	Escalate to	Board?
S1	Mass PII / financial data leak; >10k principals; cross-border exposure	Incident Commander	CEO, DPO, CISO, Legal, Board Risk Cmte, DPB, Sectoral Reg.	Yes
S2	Targeted breach; <10k principals; sensitive PII (Aadhaar, health, credentials)	DPO	CISO, Legal, Grievance Officer, DPB	Yes
S3	Limited internal exposure; no exfiltration confirmed	CISO	DPO, Legal, internal audit	Notify
S4	Near-miss / control failure; no data loss	SOC Lead	DPO (log only)	No

3. Officer Roles & Responsibilities

Role	Primary responsibility under DPDP
Data Protection Officer (DPO)	Single point of contact for the Data Protection Board (mandatory for Significant Data Fiduciaries). Owns breach notification.
Grievance Officer	Receives Data Principal complaints; resolves within statutory turnaround; closes the loop with DPB filings.
Significant Data Fiduciary	Board-designated entity-level accountability; signs DPIA & periodic audit reports.
CISO / Incident Commander	Leads containment, forensics, evidence preservation; works with SOC, IT and vendors.
Legal & Compliance	Drafts statutory notices, regulator correspondence, contract / SLA enforcement against processors.
Internal Audit	Independent review of RCA, control uplift and DPB submissions.
Board Risk Committee	Oversight, S1/S2 sign-off, ratification of disclosure decisions.

4. Form A — Notice to the Data Protection Board (within 72 hrs)

To: The Chairperson, Data Protection Board of India
From: [Data Fiduciary legal name, CIN, registered address]
DPO: [Name, designation, email, phone]
Date / Time of filing: [DD-MM-YYYY HH:MM IST]
Incident reference: [INC-YYYY-####]

1. Nature of the personal-data breach: [confidentiality / integrity / availability — describe]
2. Date & time of detection: [____] **Date of occurrence (if known):** [____]
3. Categories & approximate number of Data Principals affected: [____]
4. Categories & volume of personal data records: [____]
5. Likely consequences: [identity theft, financial loss, reputational harm, etc.]
6. Measures taken / proposed: containment, mitigation, communication to principals.
7. Cross-border element: [Yes / No — jurisdictions involved]
8. Sectoral regulators notified: [RBI / SEBI / IRDAI / CERT-In — date & reference]
9. Annexures: incident timeline, forensic summary, sample notice to principals.

Signed: _____ (DPO) Counter-signed: _____ (Significant Data Fiduciary / CEO)

5. Form B — Notice to Affected Data Principal

Subject: Important — notice regarding a personal-data incident affecting you

Dear [Principal Name],

We are writing to inform you, in line with the Digital Personal Data Protection Act, 2023, that on **[date]** we identified a personal-data incident at **[Data Fiduciary name]** that may have affected the following categories of your personal data: **[list]**.

What happened: [plain-language description]
What we are doing: containment, forensic investigation, regulator notification, additional security controls.
What you should do: [reset password, monitor statements, enable MFA, ignore suspicious calls quoting this incident].

For any question, contact our Grievance Officer at **grievance@[domain]** or our DPO at **dpo@[domain]**. You also have the right to lodge a complaint with the Data Protection Board of India.

Sincerely,
[Grievance Officer name & designation]

6. Internal Incident Register — Row Template

Field	Value
Incident ID	INC-YYYY-####
Detected at / by	[timestamp] / [name, team]
Severity (S1–S4)	[ ]
Systems / vendors involved	[ ]
Categories of data	[PII / SPI / financial / health / credentials]
Principals affected (count)	[ ]
Containment actions	[ ]

DPB filed (Y/N, ref)	[ ]
Principal notice issued (Y/N, channel)	[ ]
Sectoral regulator notice	[RBI / SEBI / IRDAI / CERT-In]
RCA owner / due date	[ ]
Closure date / sign-off	[DPO + CISO + Legal]

Penal note — contraventions under the DPDP Act, 2023 attract civil penalties up to **Rs. 250 crore** per breach. These templates are working drafts and must be tailored to your sector, contracts and processor footprint.