Complynz

10 SLIDES · SAVE FOR LATER

PRIVACY FIRST · ZERO-TRUST COMPLIANCE

Our approach to *DPDP.*

Six pillars, one operating model — built so a lean team can pass a customer audit without standing up a dedicated compliance function.

SCOPE
DPDP Act, 2023

AUDIENCE
Startup & growth teams

READ TIME
~2 minutes

COMPLYNZ · 2026

SWIPE →

A FOUNDATION, NOT A FIRE DRILL

Going compliant. *From day one.*

The DPDP Act, 2023 is no longer a future event. If you collect personal data of anyone in India — customers, employees, vendors — you're already in scope. The cheapest moment to build compliance is **before** the first regulator notice, customer audit or partnership delay.

MAX PENALTY

₹250 Cr

Per instance of breach for serious failures under DPDP Act, 2023.

TRIGGER

Already applicable

Once your first user is from India, DPDP obligations apply.

COST CURVE

~10× cheaper

To build it in early than retrofit after your first ten-thousand records.

SIX PILLARS, ONE OPERATING MODEL

How we build DPDP *readiness.*

No 300-page deliverables nobody reads. Six tightly-scoped pillars, sequenced so each one makes the next cheaper to deliver — and so an auditor finds exactly what they expect.

01 **Notice & Consent**
Plain-language notices, granular capture, withdrawal.

02 **Data Principal Rights**
Access, correction, erasure, grievance workflow.

03 **Data Mapping & Discovery**
Inventory, flows, classification, sensitivity tags.

04 **DPO & Governance**
Role, SOPs, risk register, compliance calendar.

05 **Breach Response**
72-hour playbook, drill, evidence binder.

06 **Sensitive PI & Cross-Border**
Children's data, health, transfer mechanisms.

Pillar 01

Notice & *consent.*

Where DPDP actually meets your product — every form, every cookie, every signup.

- **Plain-language notices** in English plus key Indian languages, mapped to each processing purpose.
- **Granular consent capture** on contact, careers, marketing and product flows — not a single blanket checkbox.
- **Cookie banner & preference centre** with category-level control and a global "withdraw" link.
- **Versioned consent log** with timestamps — your audit trail when a regulator asks "prove it".
- **Withdrawal workflow** wired into your CRM so a "no" actually propagates downstream.

Pillar 02

Data principal *rights.*

When a user emails "delete my data" — what happens in the next 30 days decides whether you're compliant.

- **Self-service rights portal** for access, correction, erasure and grievance — one link, one workflow.
- **SLA-tracked ticketing** behind it, so requests don't sit in someone's inbox until the deadline.
- **Identity verification** step calibrated to risk — no over-asking, no under-checking.
- **Grievance officer routing** with escalation if the first response doesn't resolve.
- **Audit log of every request** — who asked, who responded, what was disclosed.

Pillar 03

Data mapping, discovery & *classification.*

You can't protect what you can't see — and you can't see it until you've mapped where it lives, where it flows, and how sensitive it is.

- **Systems & data inventory** — register of every system that holds personal data, with owner and purpose.
- **Data flow maps** across product, marketing, hiring, support and vendors — including third-party processors.
- **Classification scheme** — public / internal / confidential / restricted, applied consistently across teams.
- **Sensitive data discovery** — automated scans for high-risk patterns (PAN, Aadhaar, health, payment).
- **Retention rules** per data class — because keeping it forever isn't a strategy, it's a liability.

Pillar 04

DPO & *governance.*

One named owner, one register, one cadence — enough governance to stand up in audit, not enough to slow product down.

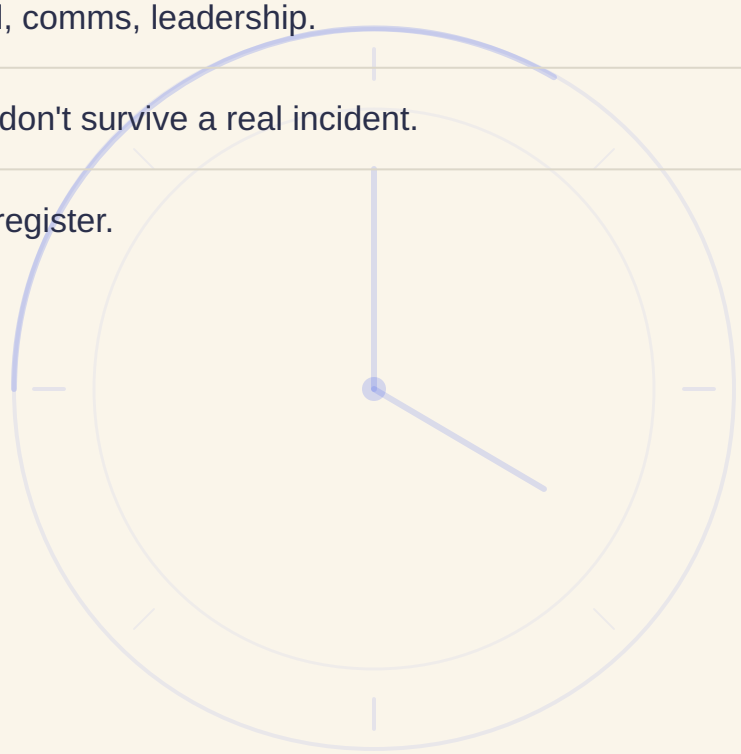
- **DPO role definition** — responsibilities, reporting line, decision rights documented.
- **SOPs & playbooks** for the recurring decisions a DPO actually makes each month.
- **Risk register** — top-25 privacy risks scored, owner and treatment plan per risk.
- **Compliance calendar** with reviews, drills, training and audit windows.
- **Monthly dashboard** — posture, open risks, SLA breaches — one view for leadership.

Pillar 05

Breach *response.*

The 72-hour clock starts ticking the moment your team confirms the incident — not when leadership hears about it.

- **Detection & triage runbook** — what counts as a personal data breach, who decides, in how long.
- **72-hour notification templates** for the Data Protection Board and affected principals.
- **Containment & forensics SOP** with named roles — engineering, legal, comms, leadership.
- **One tabletop drill per year** — because plans you've never rehearsed don't survive a real incident.
- **Post-incident review** that feeds back into policy, controls and the risk register.



Pillar 06

Sensitive PI & *cross-border.*

Where the standard playbook isn't enough — children's data, financial & health PI, and data leaving Indian soil.

- **Children's data handling rules** — parental consent, age-gating and verifiable consent flows.
- **Sensitive personal data inventory** — financial, health, biometric, government-ID — where it sits and who touches it.
- **Cross-border transfer note** — whitelist tracking, contractual safeguards and re-papering as the rules evolve.
- **Vendor & processor inventory** with tiering — who processes, what, under what contract.
- **Annual review cadence** — because both the data and the rules will have moved.

↑ SAVE THIS FOR LATER

PRIVACY FIRST · ZERO-TRUST COMPLIANCE

Compliance, *engineered* as a programme.

If you're an early-stage or growth team thinking about DPDP — let's talk before the regulator does. We help you build all six pillars in **4 to 6 months**, sized for a lean team and an auditor's binder.

REACH US
hello@complynz.com

FOLLOW
@complynz on LinkedIn