



# Is Your Tech Stack Hiding a ₹250 Crore Liability?

Your growth depends on data. But India's new DPDPA law means every API call, every user signup, and every third-party integration now carries legal accountability.

1

## Investors are Watching

DPDPA compliance is now a mandatory part of VC due diligence. Non-compliance can kill your next funding round or M&A exit.

2

## Liability is Universal

The law doesn't care if you have 1 employee or 1,000. If you decide why user data is collected, you are 100% accountable for its safety.

3

## The Real Cost

Beyond the ₹250 crore penalty, a breach costs an average of ₹22 crore in lost trust and downtime.

## The Opportunity

Smart founders are using 'Privacy as a Competitive Advantage'

to win enterprise contracts and build brand trust.

## The Cyberaube Way

We help you move from 'Work in Progress' to 'Secure by Design' using our jargon-free SARAL framework.





# The Founder's 18-Month Countdown

The clock started on November 14, 2025. Full DPDPA enforcement begins May 14, 2027. Every day counts towards securing your future.



📌 **Founder Note:** Complacency is the greatest risk. Re-architecting systems takes time. Start today to avoid expensive retrofitting later.



# Rule 6: Your New Statutory Cybersecurity Baseline

Rule 6 of the DPDPA 2025 Rules mandates stringent cybersecurity measures, transforming data protection into an uncompromising statutory obligation for all Data Fiduciaries and Processors. This isn't just about IT; it's a board-level imperative.



## Advanced Encryption

Implement AES-256 for data at rest and TLS 1.2+ for data in transit, ensuring robust data confidentiality.



## Zero-Trust Access

Enforce Multi-Factor Authentication (MFA) and Role-Based Access Control (RBAC) to limit access strictly to 'need-to-know' principles.



## 1-Year Log Retention

Legally retain all processing and system logs for a minimum of one year to facilitate forensic investigations.



## Continuous Monitoring

Deploy SIEM tools for real-time anomaly detection and proactive investigation of unauthorized access attempts.



## Vendor Linkage

Contractually bind all third-party Data Processors (Cloud/SaaS) to uphold these exact cybersecurity standards; non-compliance is your liability.



**The Cyberaube Advantage:** Cyberaube helps you move from fragmented security to a multi-layered defense strategy that satisfies the "Reasonable Safeguards" legal standard.



# Rule 3: Converting Users through Transparency


Rule 3 mandates a radical overhaul of your app and web UI, transforming privacy from a legal burden into a pathway for user trust and retention.

## Before DPDPA: Ambiguous Practices

- Privacy notices often buried within lengthy Terms of Service.
- Vague descriptions of data categories and processing purposes.
- Notices frequently offered in English only, limiting accessibility.
- Consent implied through pre-ticked boxes or continued use.

## After DPDPA: Clear & Explicit

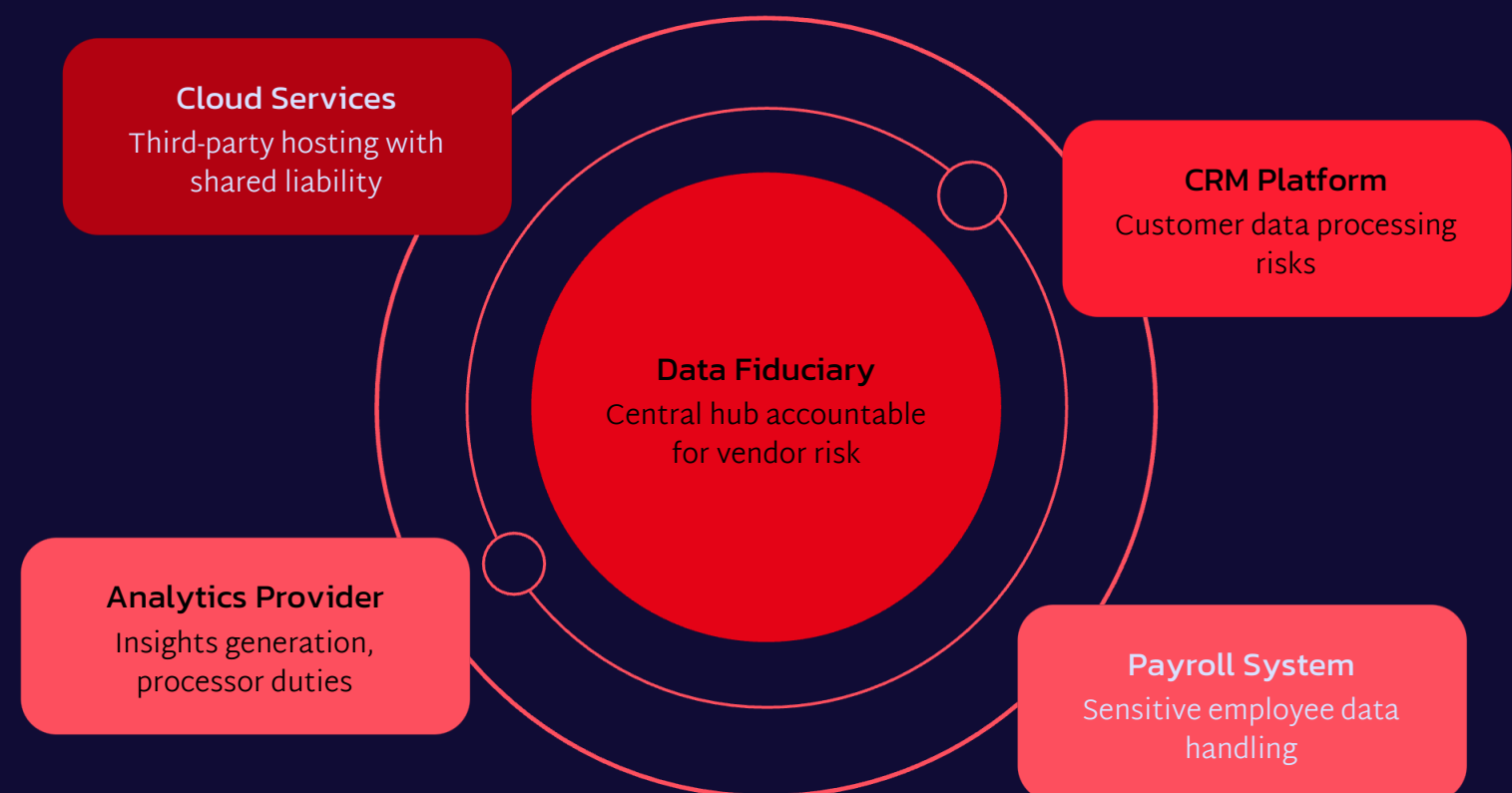
- Standalone, easily understandable privacy notices.
- Itemized listing of data categories and the exact services they enable.
- Available in English and **22 regional Indian languages**.
- Requires 'clear affirmative action' for explicit consent (no pre-ticked boxes).

 **Strategic Sales Point:** Transparent onboarding isn't just about the law—it's about building the trust that drives user retention and converts hesitant prospects into loyal customers.



# Your Vendors, Your Risk: Managing Processor Liability

The DPDPA extends a Data Fiduciary's liability to third-party Data Processors, making diligent vendor management a critical component of your compliance strategy.



## Accountability & Contracts

Data Fiduciaries are fully accountable for vendor processing and must engage them under legally binding contracts defining scope and purpose.

## The "Mirror" Rule

Your contracts must mandate that processors implement identical security safeguards to those required of you under Rule 6.

## Breach & Sub-processor Visibility

Processors must notify breaches immediately, and you must maintain visibility into sub-processors to mitigate 'Fourth-Party Risk'.

❑ Cyberaube: Ensures secure supply chain with vendor audits & DPDPA-aligned DPAs.





Consent

Consent

## Responsible AI: Innovation without the Lawsuits

Navigating the DPDPA in the age of Artificial Intelligence demands a proactive approach to data governance. It's about building trust, not just features.



### Training Transparency

Users must know if their data is training your models and retain the explicit right to opt-out, ensuring full control over their digital footprint.



### Algorithmic Fairness

Rigorously verify that your AI software does not perpetuate or reinforce biases, safeguarding user rights and preventing discriminatory outcomes.



### Data Minimization

Prioritize 'interaction signals' and anonymized data over raw identifiable data for ML training, drastically reducing compliance risks.

 **The Sales Advantage:** Building a compliant AI pipeline from day one transforms you into the preferred partner for enterprise clients who are terrified of data risks.





# From Compliance Anxiety to Strategic Growth

Cyberaube transforms the DPDPA from a regulatory hurdle into a launchpad for your business expansion.

## Why Cyberaube? Your Partner in Growth

### **SARAL (Simple, Accessible, Rational, Actionable) Strategy**

We cut through the 30,000 words of legal text to give you a 10-step actionable technical roadmap for DPDPA compliance.

### **Agile DPO-as-a-Service**

We act as your India-based focal point for the Data Protection Board, managing all communication and compliance requirements.

### **Exit-Ready Compliance**

We ensure your data practices are a strength, not a weakness, during your next funding round or acquisition.

**The 18-month window is closing.**

Visit [cyberaube.com](https://cyberaube.com) for a Free 30-Minute Readiness Audit to protect your growth.

[Request Your Free Audit](#)



72:00:00

# The 72-Hour Rule: Your Crisis Response Clock

The DPDPA 2025 Rules introduce a critical 72-hour window for data breach response, turning incident management into a race against the clock. Miss this deadline, and face severe penalties.

1

## Statutory Deadline

Notify the Data Protection Board within 72 hours of becoming aware of any personal data breach.

2

## Individual Notification

Inform affected users "without undue delay," providing clear details on the breach and protective steps.

3

## Forensic Reporting

Submit a comprehensive report detailing the cause, affected datasets, and all remedial actions taken.

❏ Don't improvise during a breach. Cyberaube provides automated breach detection workflows and pre-built notification templates so you can meet the 72-hour mandate without panic.

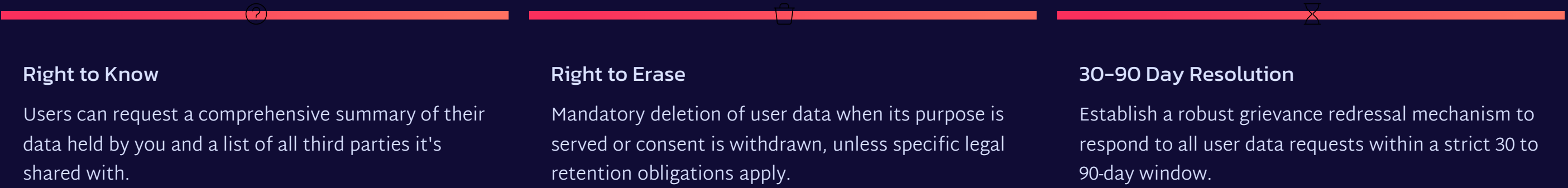






# User Control: Building Your Privacy Dashboard

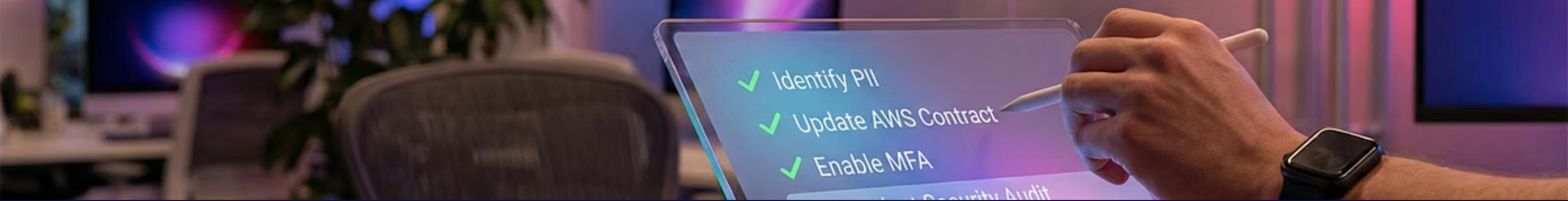
The DPDPA empowers users with unprecedented control over their data, transforming privacy management from a backend compliance task into a front-facing user experience.



Transitioning from manual support to an automated Privacy Dashboard is crucial. It drastically cuts operational overhead and ensures you consistently meet statutory deadlines.

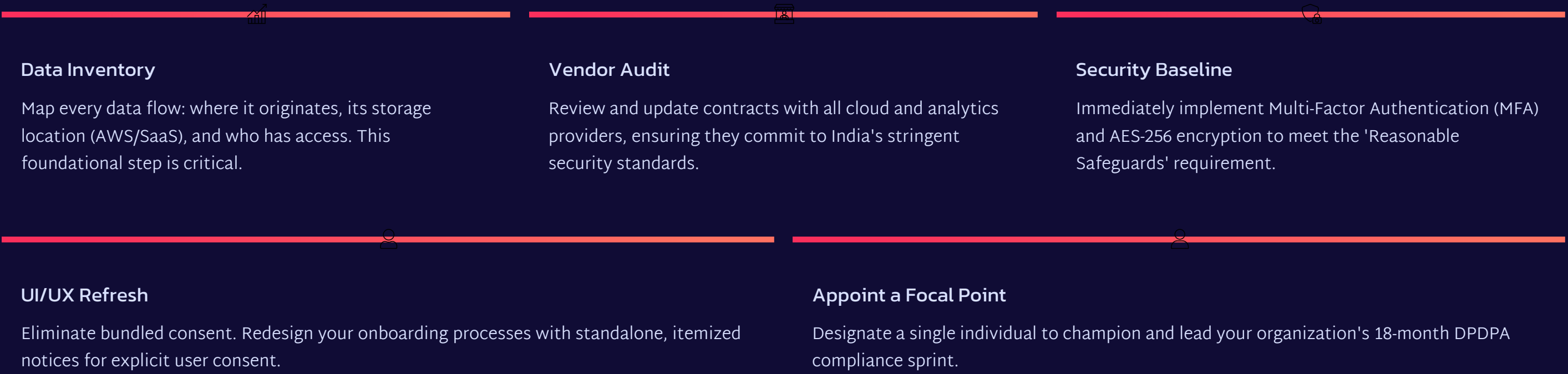
**Cyberaube Value:** We architect intuitive self-service portals, enabling users to access, correct, or erase their data with a single click. This transforms a legal requirement into a premium, trust-building user experience.





# The Founder's DPDPA Checklist: Start Here

Don't wait for DPDPA 2025 to become a reality. These immediate action items will set your foundation for compliance and strategic data governance.



Ready to move from "Work in Progress" to "Secure by Design"? Visit [cyberaube.com](https://cyberaube.com) for a **Free 30-Minute Readiness Audit**.

Request Your Free Audit



# Your DPDPA Implementation Kit: Don't Navigate Alone

Templates are just the starting line. A misconfigured notice or a generic retention policy is a regulatory red flag. We don't just give you the paperwork; we provide the SARAL (Simple, Accessible, Rational, Actionable) strategy to make them work for your specific tech stack.

## What You Get Access To (Upon Request):

- **Statutory Notices:** Standalone, plain-language Privacy Notices (Rule 3).
- **Consent Architecture:** Multi-lingual, itemized Consent Forms for data processing.
- **Crisis Playbooks:** 72-hour Data Breach Response Plans and Board Notification forms.
- **Lifecycle Tools:** Data Retention Policies and User Rights Request portals.

"Reading the Act is the Rules of the Road. Taking a course is Driving School. Using these templates and Cyberaube's guidance is your GPS and Safety Inspection. Let's ensure your startup reaches its destination without a ₹250 crore crash!"

Ready to transform your compliance journey? Book a free 30-minute DPDPA Readiness Audit at [cyberaube.com](https://cyberaube.com) to unlock access to our full template library and receive a personalized implementation roadmap.

[Request a Guided Onboarding Call](#)

### The Statutory Ground Truth

The [DPDPA, 2023: Official Act PDF](#) is the foundation of your legal standing. The [DPDP Rules, 2025: Official Rules PDF](#) outline the operational machinery you must follow.

### Upskilling Your Team

Access the [DPDPA Certificate Course v1.1](#) at [dpdpa.com](https://dpdpa.com) – a free, comprehensive 6-module program covering Data Mapping, AI Compliance, and Third-Party Risk.

