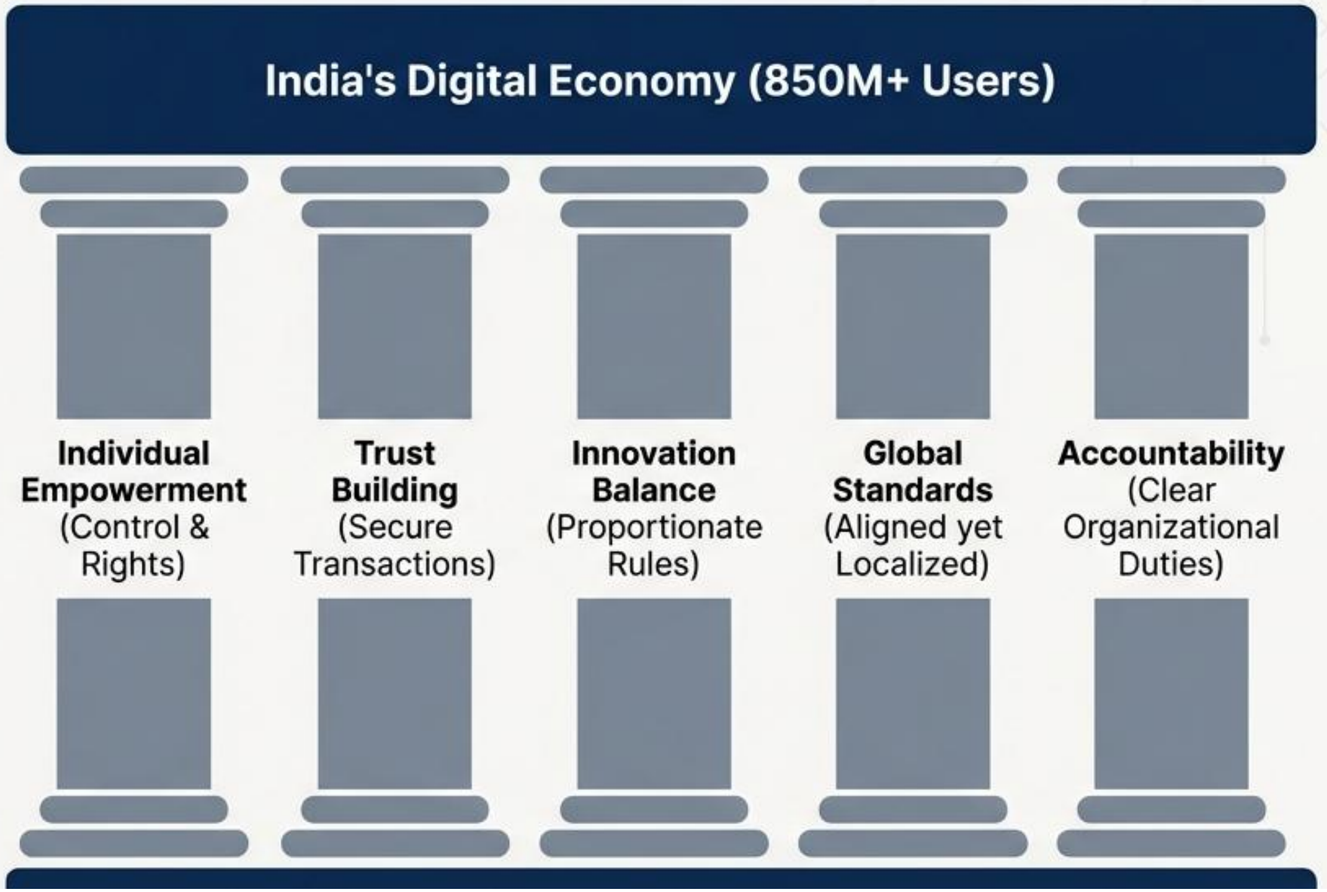
The India DPDP Blueprint: A Primer

By **Kannan Subbiah**

B.Com FCA CISA CGEIT C|CISO CCMP

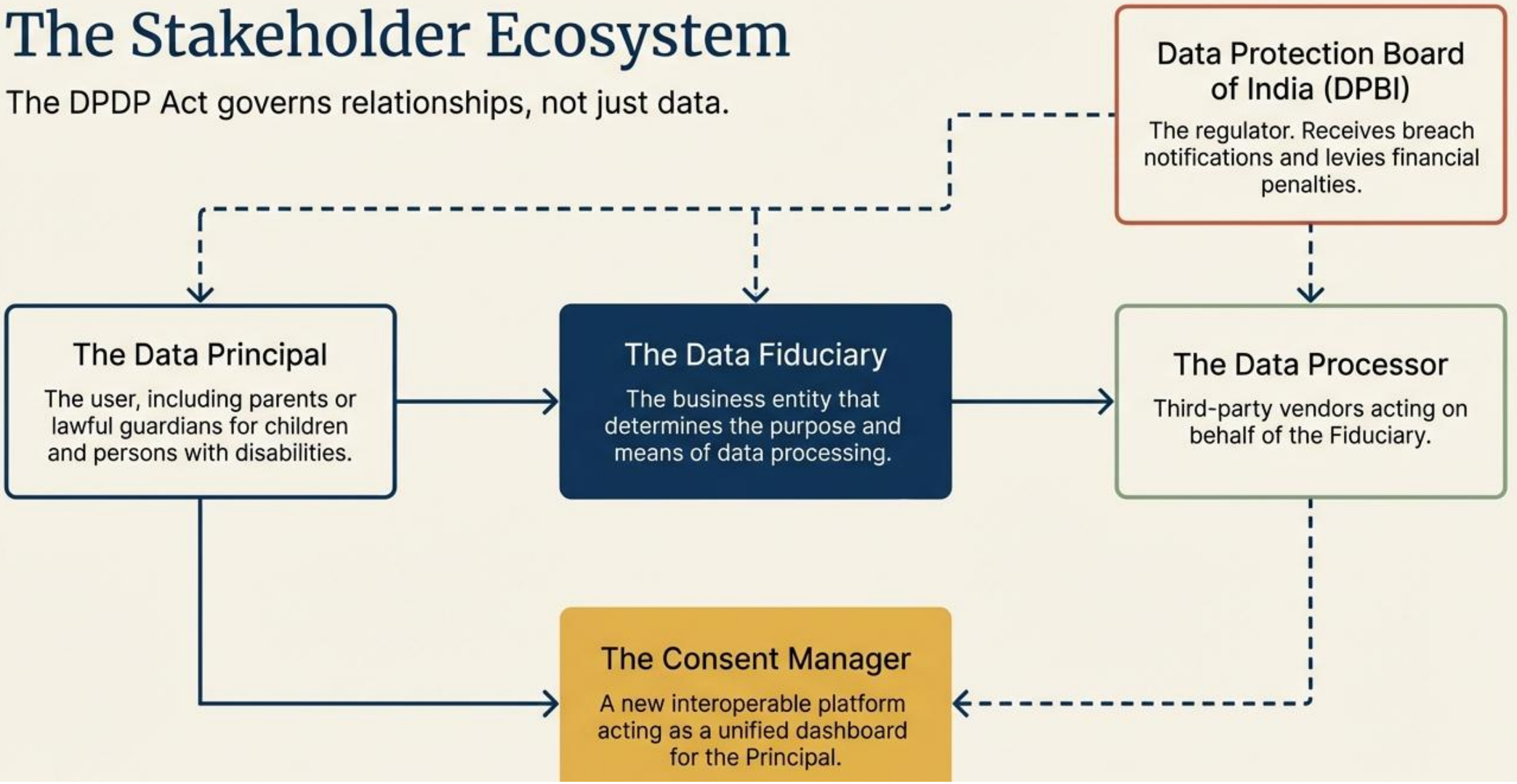
A Decade of Constitutional Evolution

- **Aug 2017: Justice K.S. Puttaswamy v. Union of India** (Right to Privacy = Fundamental Right under Article 21).
- **July 2018: Justice Srikrishna** Committee Report.
- **Aug 2023:** Parliament Passage & Presidential Assent.
- **Nov 2025:** Final DPDP Rules notified.



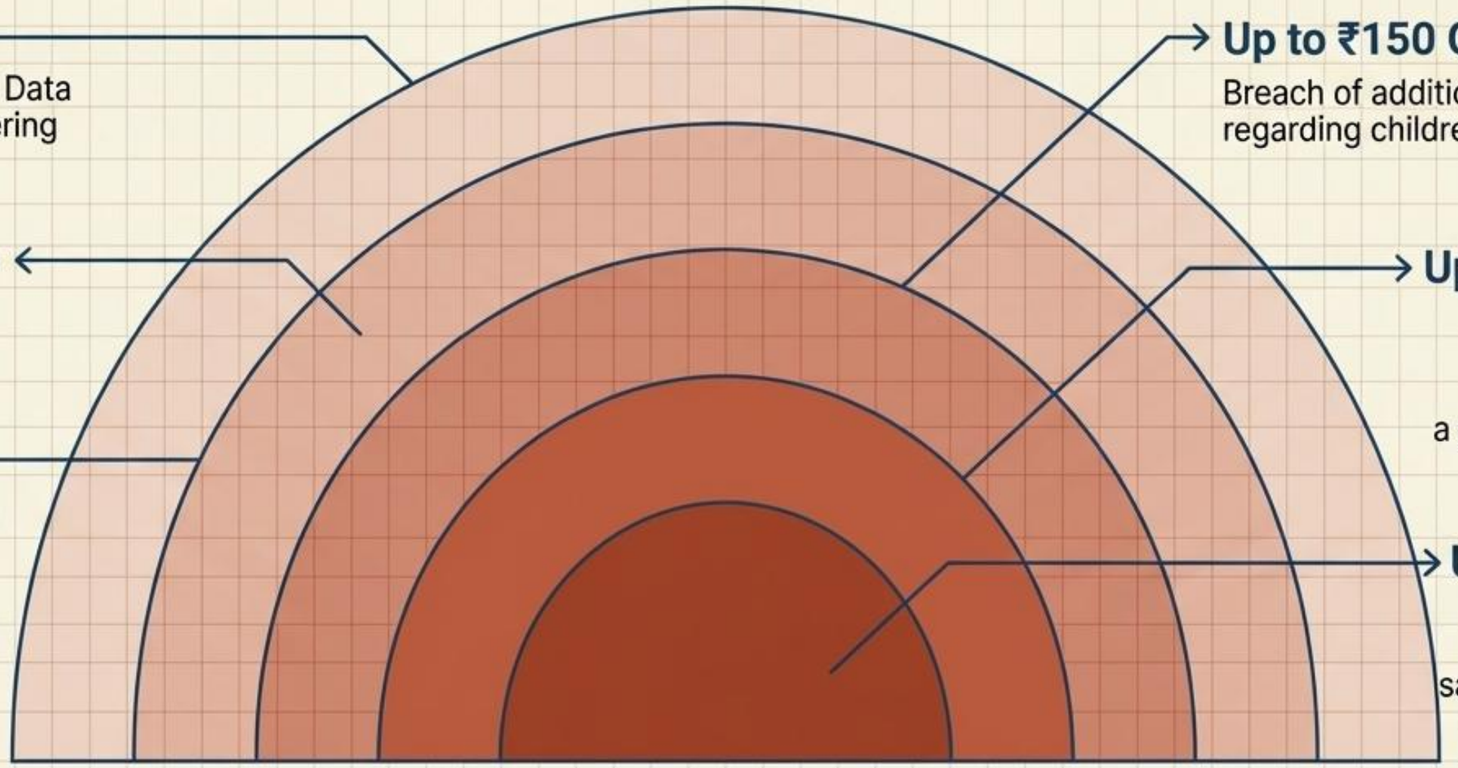
The Stakeholder Ecosystem

The DPDP Act governs relationships, not just data.



The Penalty Blast Radius

The DPBI can levy severe financial penalties for operational failures, credited to the Consolidated Fund of India.



₹10,000

Breach of duties by a Data Principal (e.g., registering false complaints).

Up to ₹50 Crore

Breach of general provisions of the Act or Rules.

₹10,000

Breach of duties by a Data Principal (e.g., registering false complaints).

Up to ₹150 Crore

Breach of additional obligations regarding children or SDF obligations.

Up to ₹200 Crore

Failure to notify the Board or affected Data Principals of a a personal data breach.

Up to ₹250 Crore

Failure to take reasonable security safeguards to prevent a personal data breach.

Meet the Regulator: The Data Protection Board

Board Structure

Appointed by Central Government; experts in law, tech, and economics.

The Civil Court Equivalence

Under Section 28, the Board operates with the exact powers of a Civil Court under the Code of Civil Procedure, 1908.

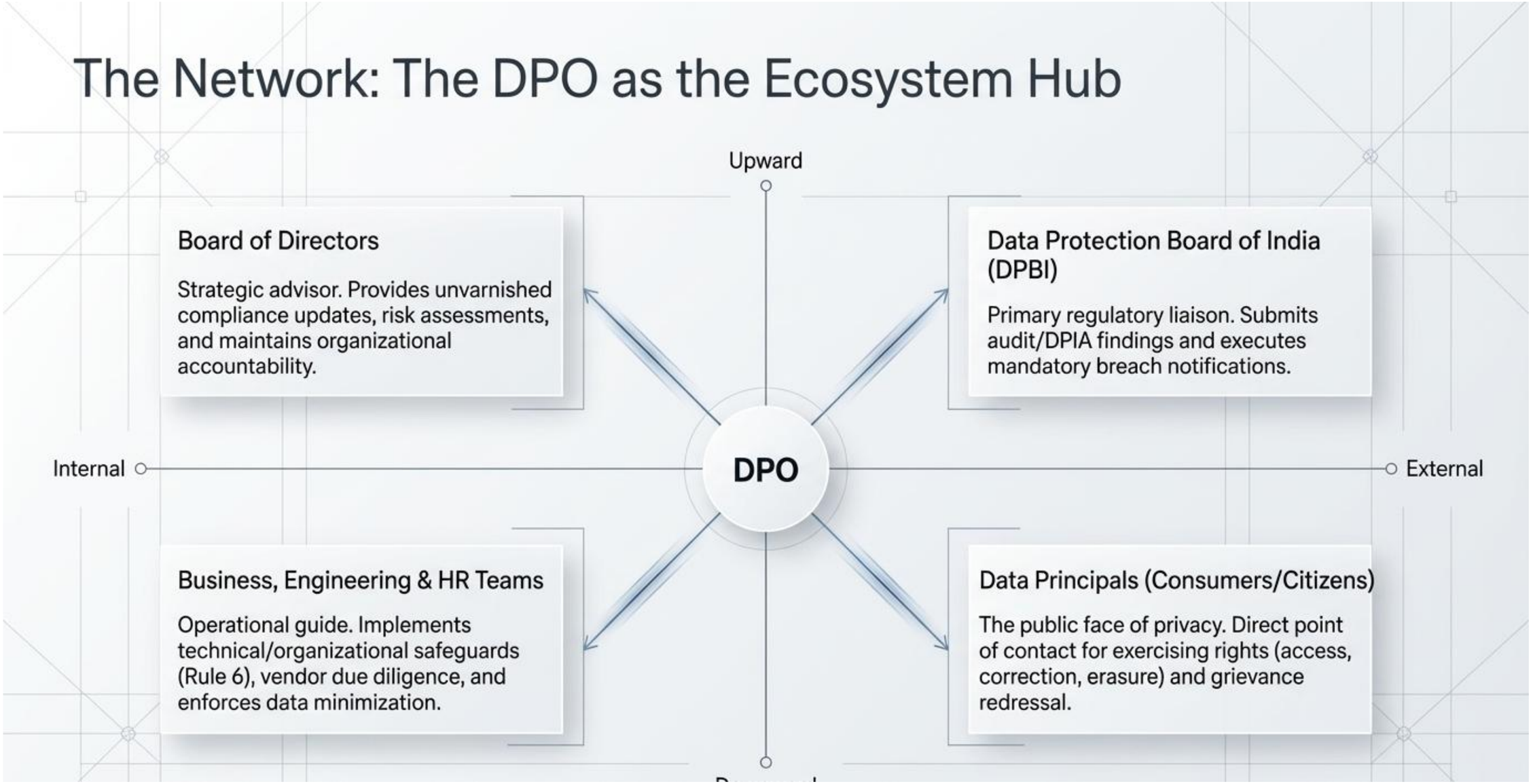
- Initiate Suo Motu Investigations
- Summon Witnesses under oath
- Demand Documents and Records
- Inspect Premises and Server facilities
- Issue legally binding Interim Orders

The Fiduciary Tiering Matrix

The Government assigns ‘Significant’ status based on data volume, sensitivity, and risk to democracy.

Data Fiduciary (Standard)	Significant Data Fiduciary (SDF)
Appoint contact person for grievances	Appoint an India-based Data Protection Officer reporting to the Board
Implement reasonable security	Appoint an Independent Data Auditor
(No requirement)	Conduct periodic Data Protection Impact Assessments (DPIA) and audits
Standard cross-border data flows	Restrict specific data transfers outside India based on Gov. committee limits

The Network: The DPO as the Ecosystem Hub

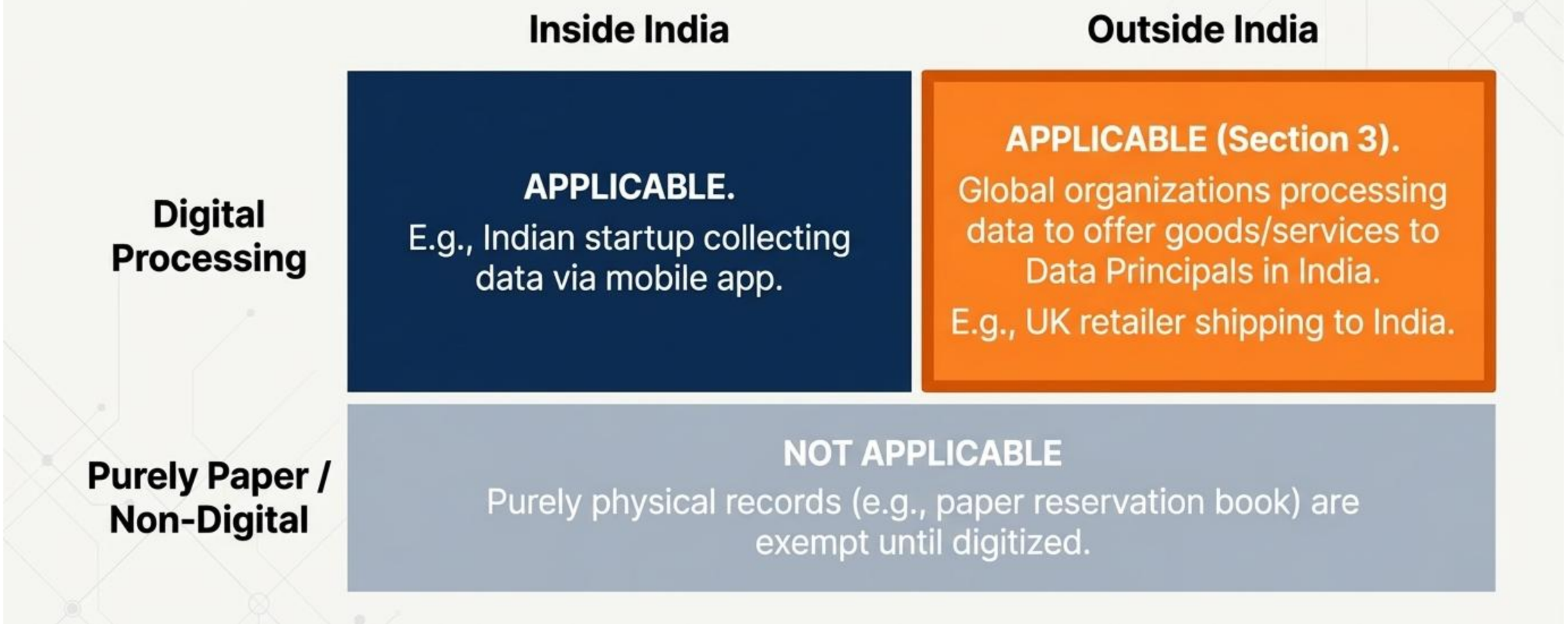


Third-Party Risk & Processor Accountability

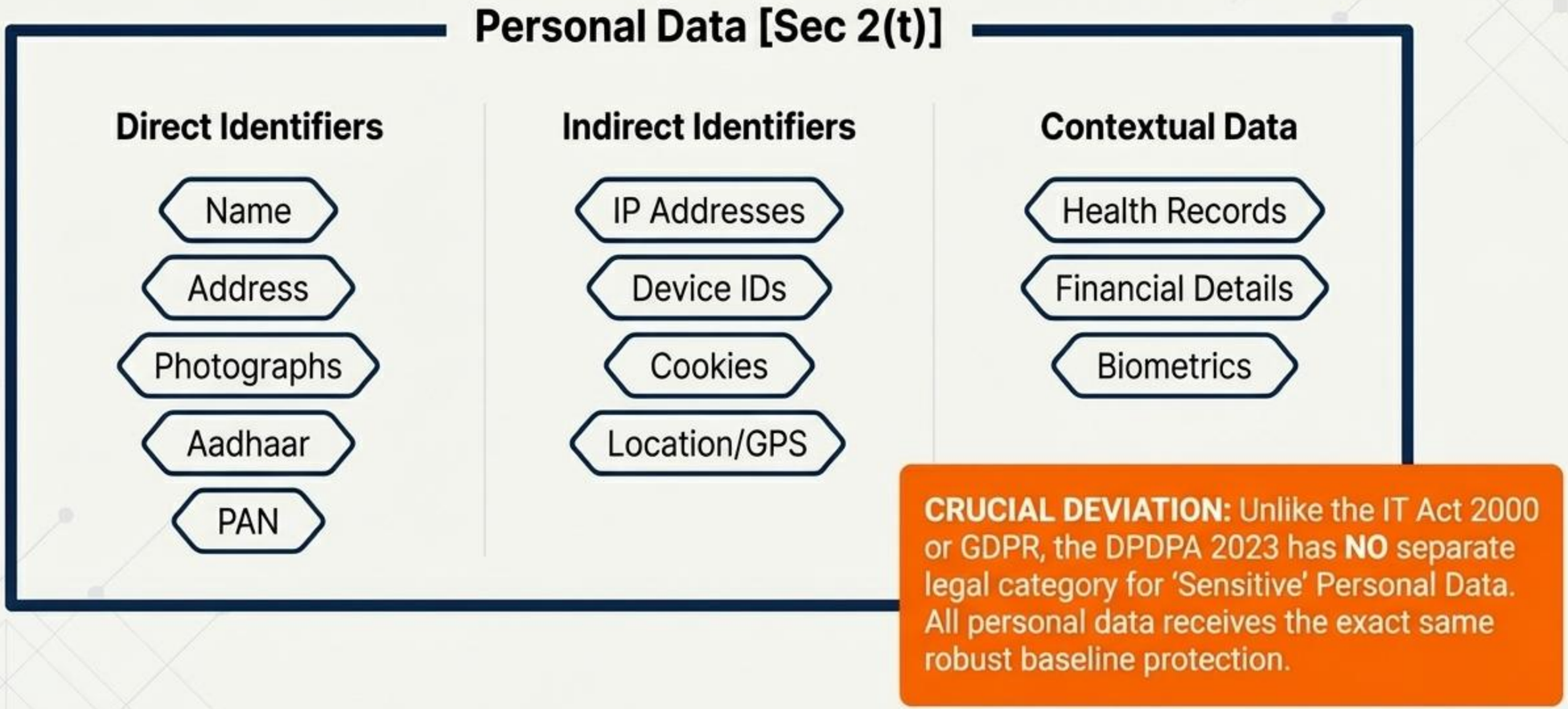
Risk Tier	Characteristics	Due Diligence Level	Mandatory Contract
Critical Risk (e.g., AWS, Razorpay)	High volume, Sensitive data	SOC 2 Type II, Onsite audit, Annual review	Strict DPA, Sub-processor veto
High Risk (e.g., Blue Dart)	Moderate access, Regular processing	Detailed questionnaire, Certification review	Standard DPA
Medium Risk (e.g., Google Analytics)	Limited access, Specific use case	Standard questionnaire, Bi-annual review	Standard DPA
Low Risk (e.g., Design tools)	Peripheral function, No PII	Simplified review, Reactive monitoring	Standard terms

Section 8(8) Liability Insight: You (the Data Fiduciary) remain fully accountable for your processors. You must seek recourse through indemnification clauses in the Data Processing Agreement (DPA).

The Extraterritorial Reach of Indian Data Law

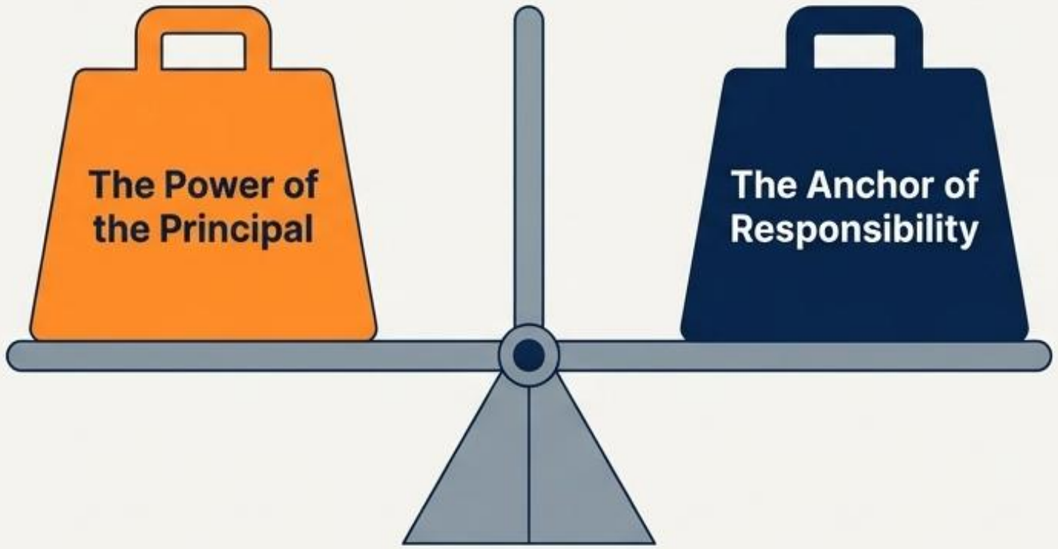


A Universal Standard for Personal Data Protection



The Civic Balance of Digital Rights and Duties

- **Section 11:** Right to Access (Summary of data, processing activities, third-party sharing).
- **Section 12:** Right to Correction & Erasure (Unless retention is legally required).
- **Section 13:** Right to Grievance Redressal.
- **Section 14:** Right to Nominate (Managing digital legacy post-incapacity).



- **Section 15 Duties:** Must comply with applicable law, provide complete identity information, and avoid impersonation.

The Penalty Block:

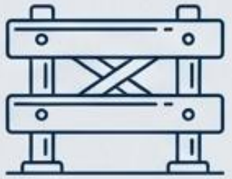
No False Claims.

The Board can impose penalties up to ₹10,000 for frivolous or false grievances.

The Lawful Processing Matrix

Two distinct routing pathways authorize the processing of personal data.

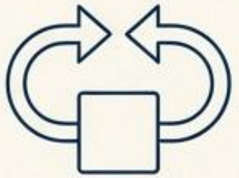
Processing via Consent



Consent must be strictly limited to data necessary for the specified purpose.

Example: A telemedicine app cannot demand access to phone contacts as a condition of service.

Certain Legitimate Uses

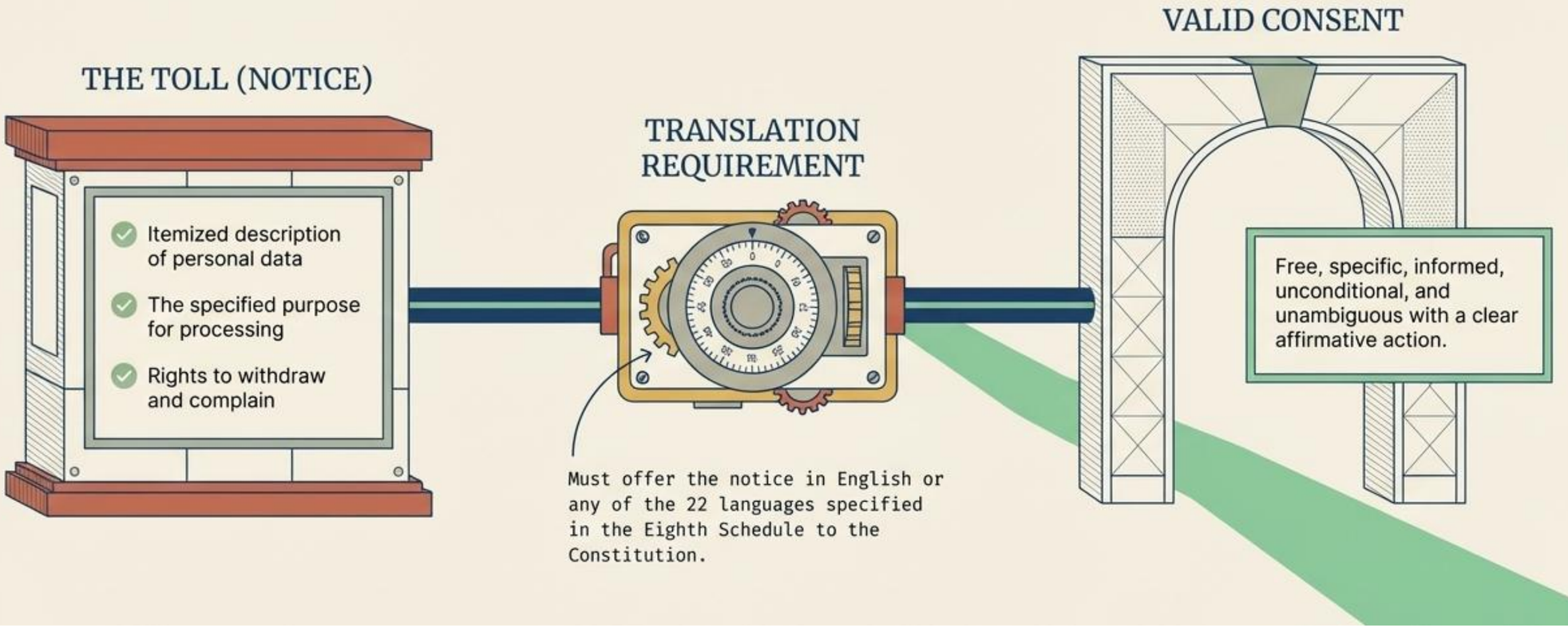


Explicit consent is bypassed in specific scenarios.

- Responding to medical emergencies or epidemics.
- State subsidies, benefits, certificates, or licenses.
- Disaster management and breakdown of public order.
- Employment purposes (preventing corporate espionage, safeguarding trade secrets).

The Notice-to-Consent Gateway

Requests for data cannot proceed without comprehensive, multilingual upfront transparency.



The Diagnostic Criteria for Valid Consent

Freely Given

Active choice required. No coercion, no "accept all or leave" walls, and absolutely no pre-checked boxes.

Specific

The exact purpose must be stated. Consent for delivery does not equal consent for marketing.

Informed

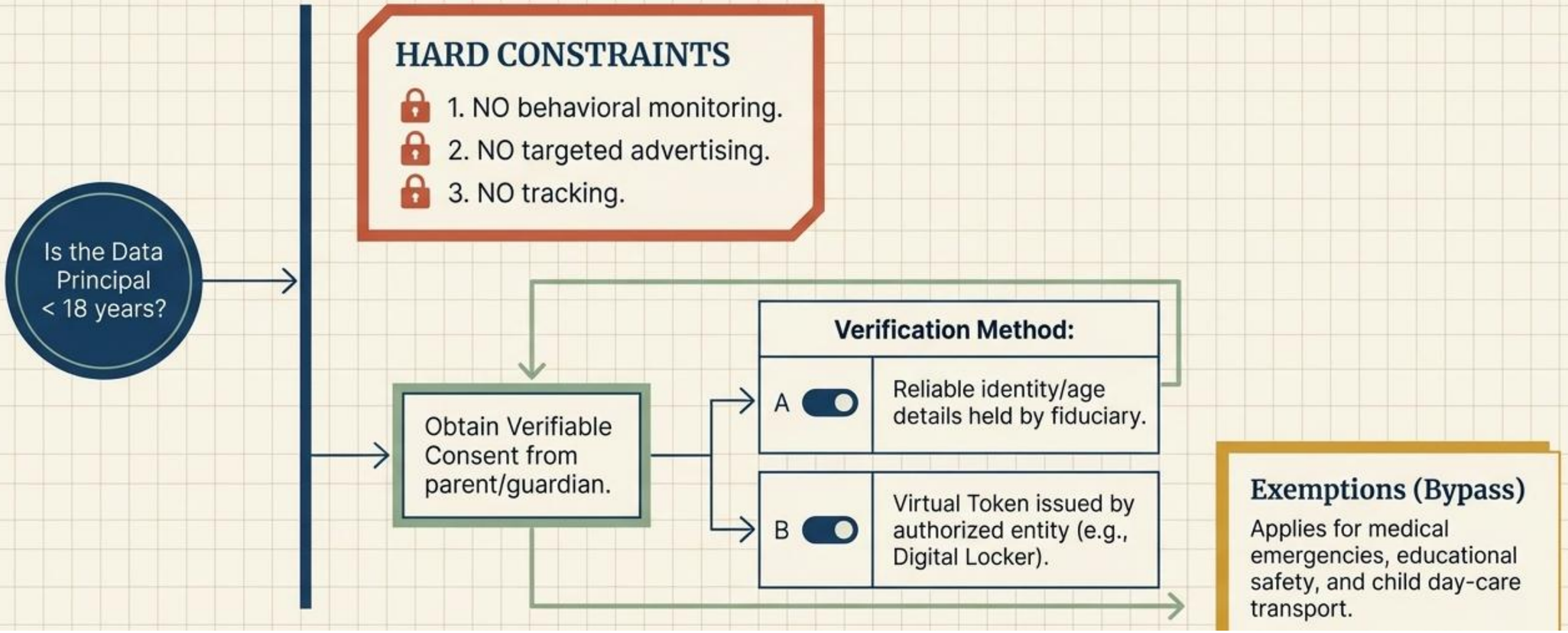
The user must clearly understand what they are agreeing to—no burying terms in dense legal agreements.

Unambiguous

A clear affirmative action indicating consensus ad idem (agreeing upon the same thing in the same sense).

Routing Logic for Minors

Processing data for individuals under 18 requires verifiable parental consent and restricts targeting.



Tech Stack Audit: Mandatory Security Safeguards

Rule 6 dictates specific technical and organizational measures to prevent data breaches.

Data Masking

Secure data through encryption, obfuscation, masking, or the use of virtual tokens.

Access Controls

Implement strict access limitations to computer resources for both Fiduciaries and Processors.

Visibility & Audit

Maintain appropriate logs, monitoring, and review systems to detect unauthorized access.

Log Retention

Retain logs and personal data for a minimum of 1 year for forensic and remediation purposes.

Resilience

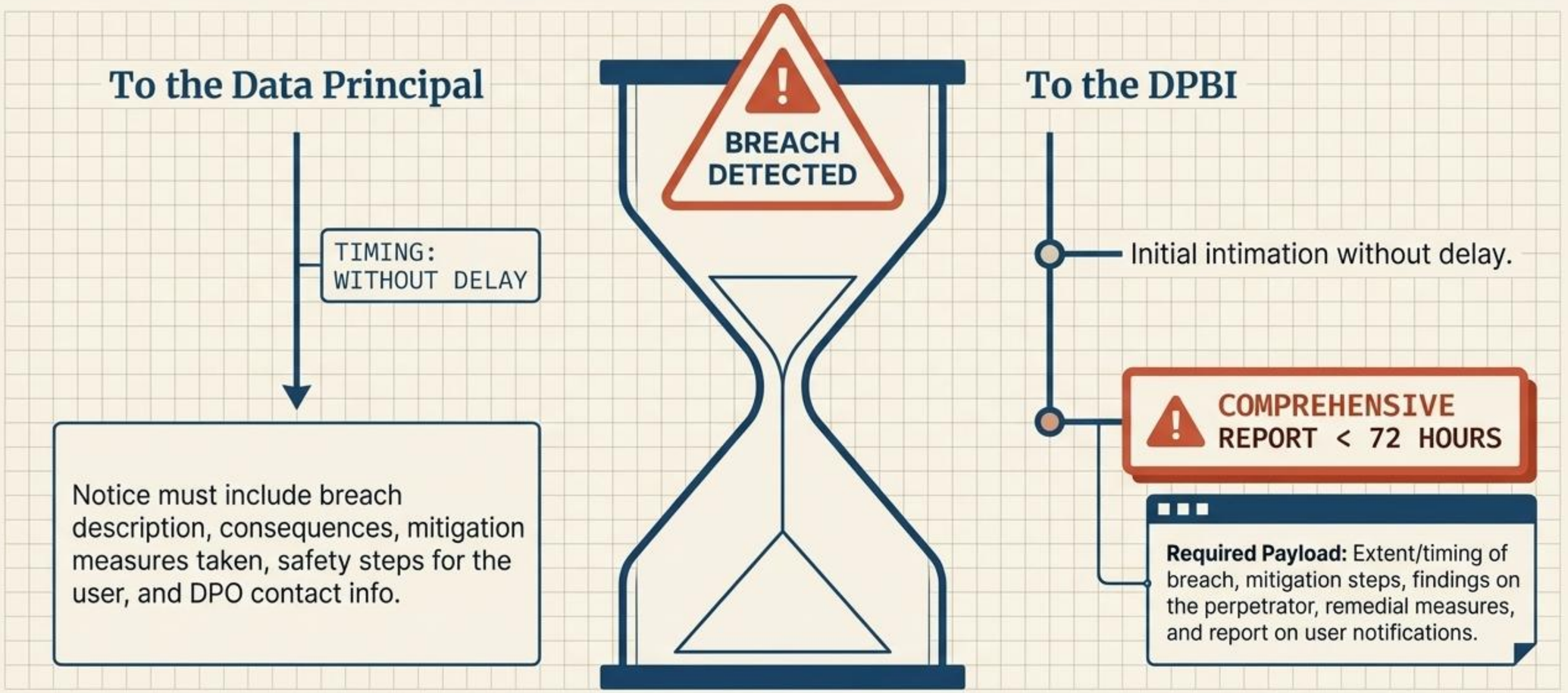
Maintain data-backups to ensure continued processing if integrity or availability is compromised.

Contractual Enforcement

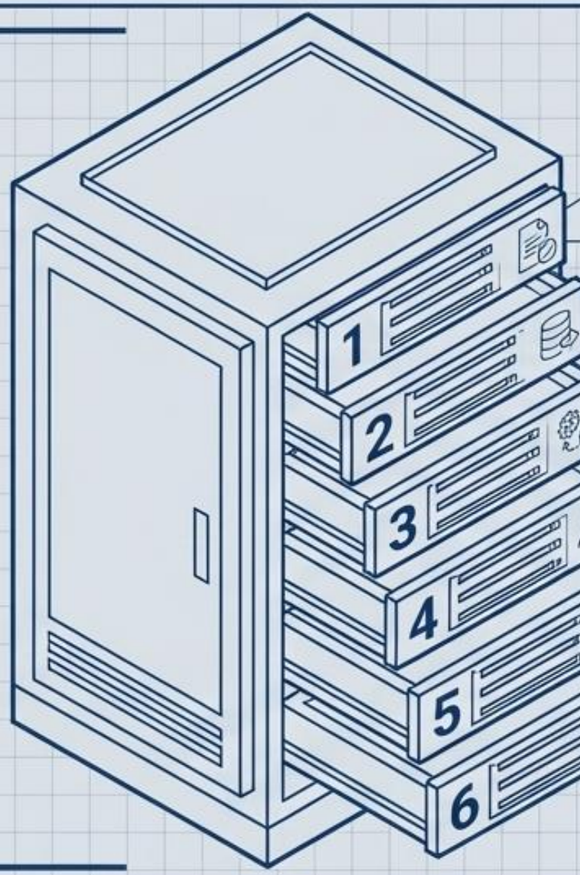
Embed flow-down security requirements in all contracts with Data Processors.

T-Zero: The Breach Notification Countdown

Fiduciaries face a strict window to report compromises in confidentiality, integrity, or availability.



The Evidence Trail: Architecting for Audits



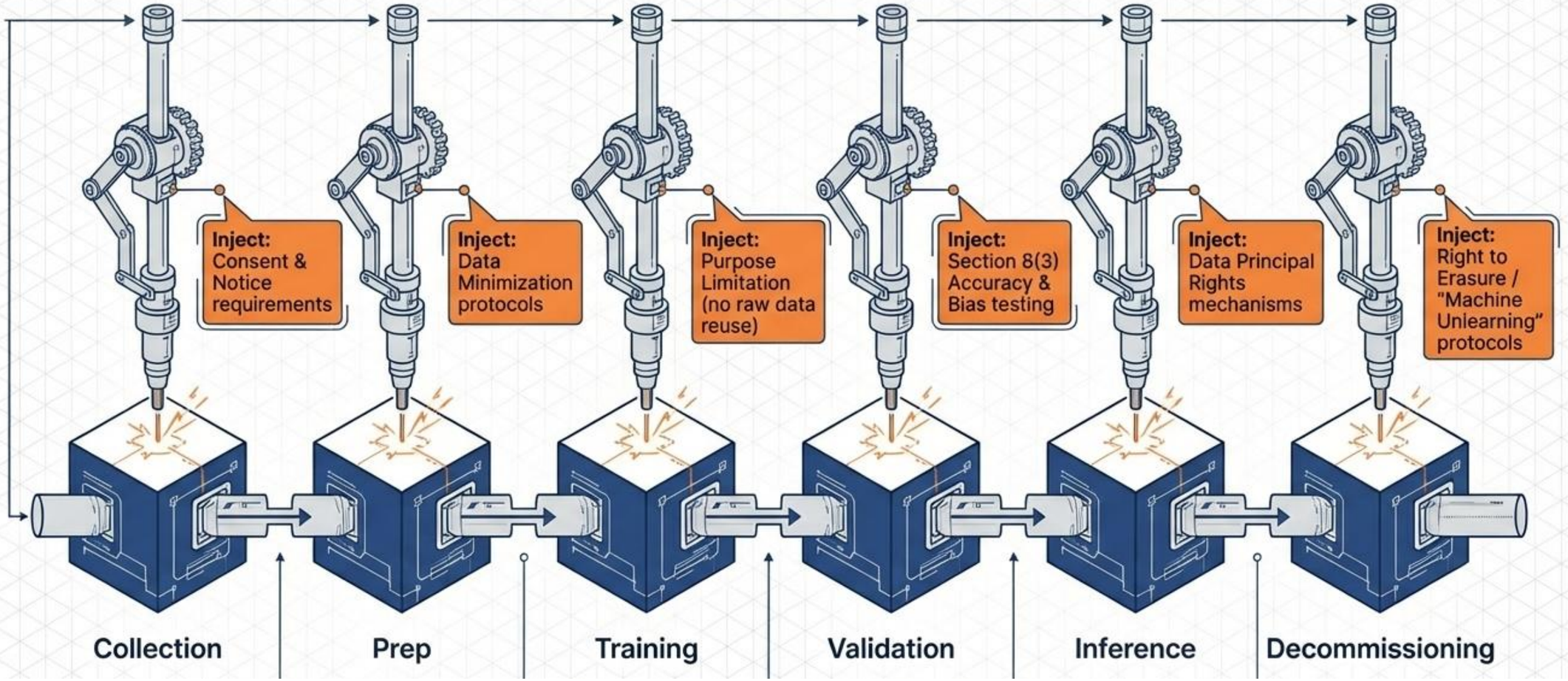
1. **Consent Logs** (Method, purpose, withdrawal)
2. **Processing Records** (Data inventory, retention limits)
3. **Sharing Agreements** (Third-party contracts, cross-border flows)
4. **Principal Requests** (Access, correction, grievance resolutions)
5. **Breach Register** (All incidents and remediation steps)
6. **Security Safeguards** (Vulnerability reports, employee training)

SDF Audit Mandate

SDFs must execute independent external audits evaluating all provisions every 12 months.

Golden Rule Callout:
If it's not documented, it didn't happen.

The AI Frontier: Injecting DPDPA into the ML Lifecycle



The Path to Full Statutory Enforcement

Smart organizations are preparing NOW, not in 2027.

Compliance That Sells

- Privacy Is Now a Market Expectation
- DPDP compliance builds customer confidence
- Reduces regulatory and investor risk

Next Step: Book a DPDP Readiness Assessment