WHITE PAPER- 1

Data Protection in the Digital Economy





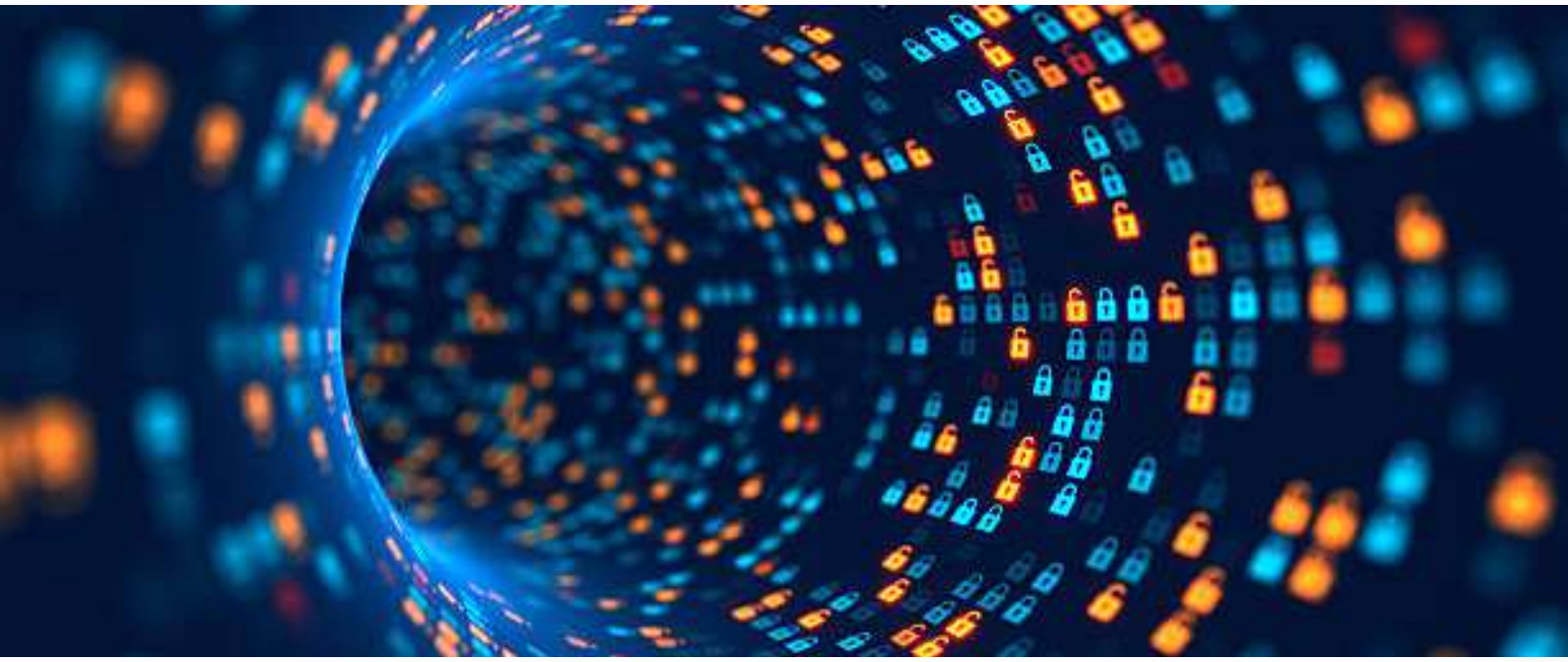


Disclaimer

This paper is based on the DPDP Act, 2023; the DPDP Rules, 2025 (notified on 13 November 2025); official Government of India material; the official texts and regulator guidance of the other jurisdictions discussed; and publicly reported developments available up to **30 September 2026.** Foreign-law summaries have been briefly included only for the limited purpose of providing a global perspective. Penalty figures are described as "up to" the relevant limit and can depend on conditions. Case studies use publicly reported facts; illustrative case studies are clearly labelled and describe fictional organisations. Earlier policy papers are used only for historical context.

This paper is for general awareness and management discussion only. It is **not legal advice.** How any law applies depends on each organisation's facts, sector rules, contracts and later notifications. Readers should obtain specific professional advice before acting.

Table of **Contents**



01

The Global Data Protection Moment

- Executive Summary
- Why Data Protection Is Now a Boardroom Issue
- Data Protection Explained Simply
- Privacy, Data Protection, Cybersecurity, Data Governance and AI Governance – What Is the Difference?
- The Global Data Lifecycle
- The Eight Principles Shared by Most Privacy Laws
- Why This Matters for Indian Businesses and Global MNCs

02

International Data Protection Landscape

- Global Privacy Rules at a Glance
- European Union GDPR and UK GDPR
- United States Privacy Landscape
- Asia-Pacific: Singapore, China and Selected Regional Frameworks
- GCC and Middle East: UAE, DIFC, ADGM and Saudi Arabia
- Brazil LGPD and Other Relevant Growth Markets
- Cross-Border Data Transfers – Why Location, Remote Access and Vendor Access Matter
- Global Comparison – What Leaders Need to Know.

03

India's DPDP Framework

- India's DPDP Journey and Why It Matters
- DPDP Act and Rules at a Glance
- Applicability, Key Terms and Exclusions
- Legal Grounds – Consent and Certain Legitimate Uses
- Notice, Consent and Consent Managers
- Security Safeguards and Data Breaches
- Retention, Erasure and Individual Rights
- Children, Persons with Disability and Significant Data Fiduciaries Cross-Border Transfers, Exemptions, Enforcement and Penalties
- DPDP and Other Indian Laws



The Global Data Protection Moment

Executive Summary

Every modern business runs on personal data. A customer in Mumbai shares a mobile number for a delivery. An employee in London gives bank details for salary. A support engineer in Manila opens a customer record. An AI assistant summarises a contract that contains names and signatures.

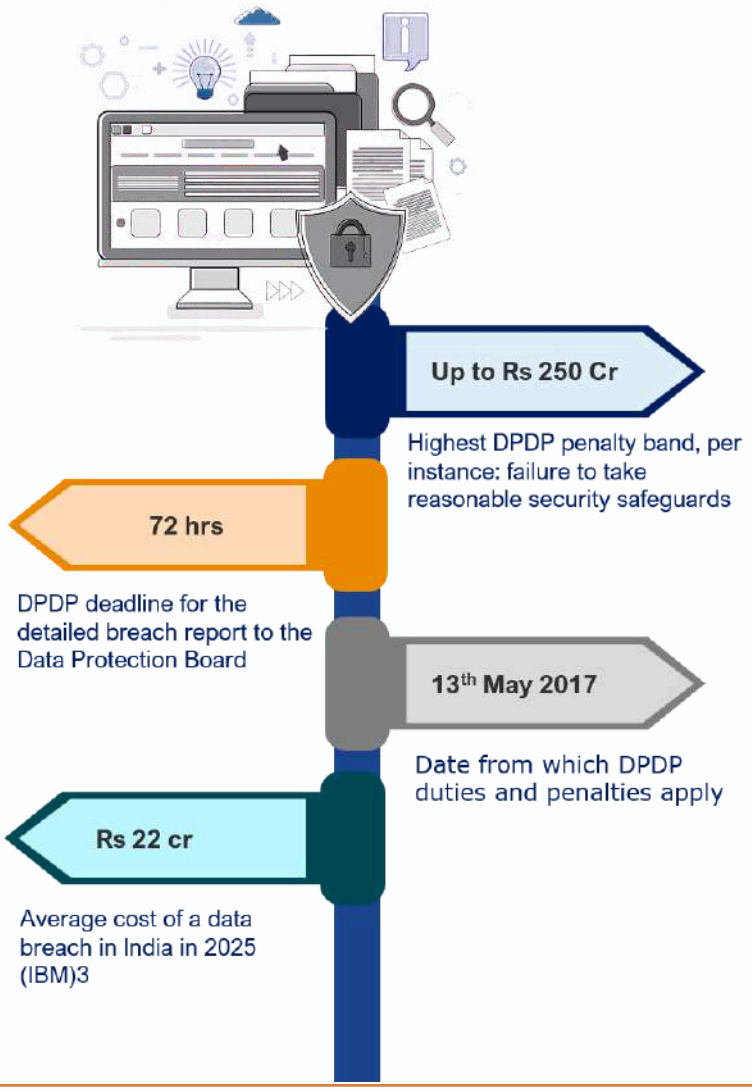
Each of these is a use of personal data. In most major economies, each is now governed by law. The laws differ in detail, but they ask the same basic questions: **Why do you need this data? Did you tell the person? Is it safe? Who else sees it? When will you delete it? Can you prove all of this?**

This paper starts from one central message. **Data protection is a global business issue. It is not only a legal or IT checklist.**

It brings together privacy, responsible data use, cybersecurity, data governance, third-party risk, AI governance and customer trust.

India is now firmly part of this movement. The Digital Personal Data Protection Act, 2023 (DPDP Act), and the Digital Personal Data Protection Rules, 2025 (DPDP Rules), create India's first single law for digital personal data. 1. The rules for consent managers start on **13 November 2026.**[1] Most core duties and the penalties start on **13 May 2027.**[2]

DPDP is best understood as I**ndia's local operating layer inside a global data-protection programme.** Organisations that already follow good global practice have a head start. But India has its own rules, and they need a specific gap assessment.





Ten things every leader should know

	Key message	Why It matters
1	Data-protection laws now cover most major economies, and many reach businesses outside their own borders.	A company can be subject to a law in a country where it has no office.
2	Most laws share the same core principles: purpose, minimum data, security, rights and accountability.	One strong global baseline covers much of the work.
3	Local rules still differ on legal grounds, children, breach timing and transfers.	Every key market needs a local gap check.
4	DPDP covers digital personal data used in India, and use abroad linked to offering goods or services to people in India.	Global firms serving Indian customers are covered.
5	Under DPDP, data may be used only with valid consent or for a listed "certain legitimate use".	There is no general "legitimate interests" ground.
6	Every personal data breach must be reported to the Board and to affected people; a detailed report is due within 72 hours.	Global incident playbooks need an Indian context.
7	Under DPDP, everyone under 18 is a child. Parental consent must be verifiable.	Consumer apps, gaming, EdTech and e-commerce feel this first.
8	The organisation stays responsible for what its vendors do with the data.	Vendor, cloud and AI contracts become central controls.
9	Good data protection runs as a technology-enabled cycle: discover, classify, govern, protect, monitor, respond, assure.	Policies alone will not prove compliance.
10	The build window is short. Core DPDP duties apply from 13 May 2027.	Late 2026 and early 2027 are for building and testing.

Leadership Takeaway

Data protection is not a privacy-policy exercise. It is an operating model in which personal data is collected for a clear purpose, used only as allowed, protected throughout its life, shared only with controlled parties and deleted when the purpose ends, with evidence at every step. Organisations that run it this way earn trust and move faster in global markets.

NOTES
1 DPDP Act, 2023, received Presidential assent on 11 August 2023; DPDP Rules, 2025. Official texts: meity.gov.in/data-protection-framework.
2 Commencement notification under s. 1(2) of the DPDP Act (13 November 2025) and Rule 1 of the DPDP Rules, 2025.
3 IBM, Cost of a Data Breach Report 2025 – India findings (average INR 220 million, 7 August 2025): in.newsroom.ibm.com.

Why Data Protection Is Now a Boardroom Issue

Data protection used to be treated as a legal or IT topic. It is now core business issue . Personal data flows through every customer journey, every HR process, every vendor relationship and, every AI system. A weakness anywhere in that chain can become a regulatory, financial and reputational problem for the whole organisation.



Five forces that moved it to the boardroom

- **Laws are now everywhere.** UN Trade and Development (UNCTAD) tracks data-protection laws worldwide. Its tracker shows that a clear majority of countries now have such laws, and more are in the process of drafting regulation.
- **Breaches cost more.** IBM's 2025 study put the global average cost of a data breach at about USD 4.44 million. In India the average data breach cost is about ₹22 crore, the highest India figure in the study's history.[5]
- **Clients now demand proof.** Global customers send security questionnaires, ask for audit reports and write data-protection duties into contracts. Weak answers can mean lost business.
- **AI multiplies exposure.** Staff can paste data into AI tools in seconds. In IBM's 2025 India findings, unapproved "shadow AI" was among the top three factors that raised breach costs.[6]
- **Trust is a growth asset.** People share more with organisations they trust. Investors, lenders and acquirers now look at data practices during due diligence.

The value of getting it right, and the cost of getting it wrong

Getting it right	Getting it wrong
Customers trust you with their data and stay loyal.	Penalties: under DPDP, up to ₹250 crore per instance for the most serious security failures.
Faster onboarding by global clients who ask for privacy assurance.	Loss of business with clients that demand strong controls.
Less unnecessary data stored, so lower storage cost and smaller breach impact.	Complaints, media attention and damage to reputation.
Better vendor control and stronger cyber resilience.	Fraud and identity theft affecting customers and employees.
Safe, confident use of AI and analytics.	Business disruption during investigations and recovery.
Easier entry into regulated markets abroad.	In repeated serious cases, possible blocking of an online service in India (DPDP Act, Section 37).

The value of getting it right, and the cost of getting it wrong

1. What personal data do we hold, and where is it stored?
2. Why do we need each type of data, and on what legal basis do we use it?
3. Which teams, vendors and AI tools can see or use it, and from which countries?
4. How do we protect it, and when do we delete it?
5. If something goes wrong tonight, who finds out, who decides and how fast can we act?

Business Perspective

If management cannot answer these five questions with evidence, the organisation has a governance gap, even if it already has a privacy policy and good cybersecurity tools.



NOTES
4 UNCTAD, Data Protection and Privacy Legislation Worldwide: unctad.org/page/data-protection-and-privacy-legislation-worldwide.
5 IBM, Cost of a Data Breach Report 2025 (global average USD 4.44 million), and IBM India newsroom release, 7 August 2025.
6 IBM India newsroom release, 7 August 2025 (shadow AI added about INR 17.9 million to average breach cost).

Data Protection explained Simply

Data protection means looking after information about people so that it is used fairly, kept safe and not misused. It applies to customers, employees, job applicants, patients, students, visitors, suppliers' staff and anyone else an organisation deals with.

What is personal data?

Personal data is any information that relates to a person who can be identified, directly or indirectly. Examples include a name, phone number, photo, email address, ID number, bank details, location, voice recording or IP address. Even small details that are harmless on their own can identify someone when combined.

In Simple Words

Personal data relates to an individual. The individual has rights under the law. The organisation that uses the data has legal duties.

An everyday way to think about it

You give a courier your address so that a parcel can reach you. The courier may use the address to deliver the parcel.

It should keep the address safe, should not sell it to a marketer, should tell you if it is leaked, and should not keep it forever. If you ask what it holds about you, it should be able to tell you.

Data-protection law asks every organisation to behave like that good courier: **a clear purpose, honest information, safe handling, limited sharing, respect for the person's rights and deletion when the job is done.**

The four roles

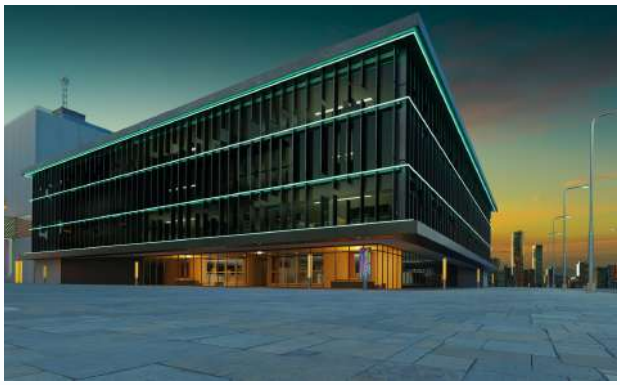
Every privacy law describes the same four roles, though the names change from country to country.



Role in plain words	Common global term	India (DPDP) term	Example
The person the data is about	Data subject	Data Principal (for a child, includes the parent; for a person with a disability, the lawful guardian)	A customer, employee or patient
The organisation that decides why and how the data is used	Controller	Data Fiduciary: the entity that, alone or with others, decides the purpose and means of processing.[7]	A bank, hospital, retailer or employer
A service provider that uses the data only on the organisation's instructions	Processor	Data Processor.[8]	A cloud host, payroll vendor or call centre
The authority that enforces the law	Supervisory authority / regulator	Data Protection Board of India.[9]	Ireland's DPC, the UK ICO, India's Board

Why the word "FIDUCIARY"?

The DPDP Act uses “Data Fiduciary” to signal a duty of care. Legally, however, the role is defined by function: it is the entity that decides the purpose and means of using the data. A company can be a data fiduciary for its own employees and a data processor for a client at the same time.



Key DPDP terms at a glance

Term (Act reference)	Simple meaning	Everyday example
Personal data (s. 2(t))	Any data about an individual who can be identified by or from that data.	Name, mobile number, photo, employee ID.
Digital personal data (s. 2(n))	Personal data in digital form, including data collected on paper and later digitised.	A paper form typed into a CRM.
Processing (s. 2(x))	Any fully or partly automated operation on data: collecting, storing, using, sharing, erasing and more.	Sending an SMS using a stored number.
Consent Manager (s. 2(g))	A Board-registered platform that helps people give, manage, review and withdraw consent.	A single consent dashboard across services.
Significant Data Fiduciary (s. 10)	A Data Fiduciary notified by the Government because of volume, sensitivity or other risk factors.	A large platform or institution, if notified.
Personal data breach (s. 2(u))	Unauthorised processing, or accidental disclosure, use, alteration, destruction or loss of access, that compromises confidentiality, integrity or availability.	A hacked database, or a salary file emailed to the wrong person.
Child (s. 2(f))	A person who has not completed 18 years of age.	A 16-year-old online gamer.

NOTES
7 DPDP Act, 2023, s. 2(i).
8 DPDP Act, 2023, s. 2(k).
9 DPDP Act, 2023, s. 18.

Privacy, Data Protection, Cybersecurity, Data Governance and AI Governance - What is the Difference

These five terms are often used as if they mean the same thing. They do not. Each answers a different question, and each is usually led by a different team. Problems arise in the gaps between them.

A perfectly secure database can still breach privacy if the data inside it is used for a purpose nobody was told about. A well-written privacy notice means little if the same database is unencrypted and exposed to the internet. A model built with good intentions can still harm people if the data it learnt from was inappropriate.

Discipline	The main question it answers	Typical lead	Example of a failure
Privacy	Is this use of information about a person fair, expected and respectful?	Privacy / Legal	Using delivery addresses to build hidden lifestyle profiles.
Data protection	Are we following the law and controls for handling personal data, across its whole life?	DPO / Privacy office	No valid consent or legal ground; data kept for years with no reason.
Cybersecurity	Are our systems and all our data (personal or not) protected from attack, loss and misuse?	CISO / IT Security	Ransomware encrypts servers because backups were never tested.
Data governance	Who owns each data set, what does it mean, is it accurate, and how long do we keep it?	CDO / Data owners	Three copies of the customer list, each with different details.
AI governance	Are our AI systems designed, trained and used responsibly, safely and lawfully?	AI council / Risk	A hiring tool rejects candidates unfairly because of biased training data.
Third-party risk	Do our vendors and partners protect data as per DPDP standard.	Procurement / Risk	A marketing vendor reuses customer lists for its own campaigns.

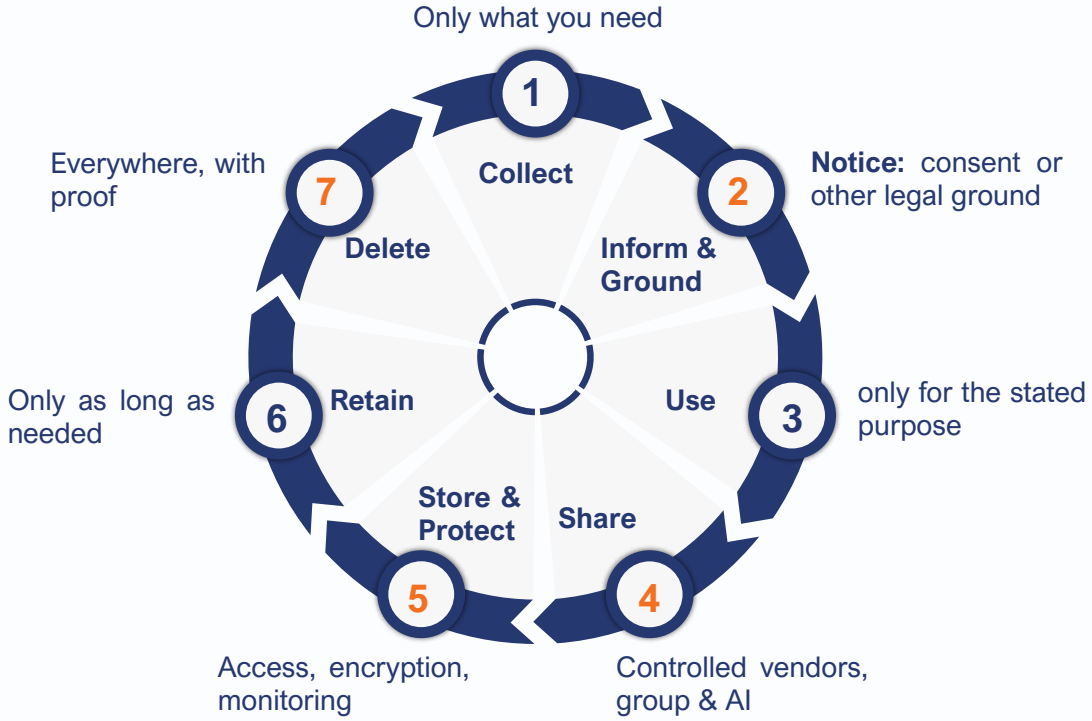
Leadership Takeaway

Run these as one Intergrated programme, with shared data maps, risk registers, and evidence. Separate silos create duplicate work and blind spots, which is exactly where regulators and attackers find problems.

The Global Data - Lifecycle

Every privacy law, in every country, follows personal data through the same life. The legal words differ; the stages do not. If an organisation can control and evidence each stage, it will meet most of the requirements of most laws.

The Personal Data Lifecycle



Individual rights (access correction, erasure, and complaint) can be exercised at any **stage.**

Evidence (notices, consent, logs, access reviews, deletion logs) should be kept at **every step.**

Where lifecycles usually break

- **Collection:** forms ask for more than is needed "just in case".
- **Use:** data collected for one purpose drifts into another, such as delivery numbers used for marketing.
- **Sharing:** a vendor, group company or AI tool receives more data than its job needs.
- **Storage:** copies sit in spreadsheets, email, test systems and backups that no one tracks.
- **Deletion:** the main record is deleted, but copies survive with vendors and in archives.

In Simple Words

Think of personal data as something you are carrying for someone else. You need to know where it is at all times, who has it, and when you will return it or destroy it.



The Eight Principles Shared by Most Privacy Laws

Most modern privacy laws trace back to the same ideas. The OECD Privacy Guidelines of 1980 (updated in 2013) set out an early international version.[10] The EU GDPR lists its principles in Article 5.[11] When the DPDP Act was introduced, the Government highlighted seven principles behind it.[12]



The eight principles below are a practical common language. They are **not identical legal tests** in every country, but an organisation that follows them will be mostly meet compliance requirement almost anywhere.

Principle	What it means	Question to ask
1. Lawful, fair and transparent use	Use data only on a valid legal ground, and tell people clearly what you are doing.	Would the person be surprised by how we use their data?
2. Purpose limitation	Use data only for the purpose you stated, or a compatible one the law allows.	Are we using the data for something new we never mentioned?
3. Data minimisation	Collect only what you need for that purpose.	Do we really need every field on this form?
4. Accuracy	Keep data correct and up to date, especially when it drives decisions.	Could wrong data lead to a wrong decision about someone?
5. Storage limitation	Keep data only as long as needed, then erase or anonymise it.	When exactly will we delete this?
6. Security	Protect data against loss, theft, misuse and unauthorised access.	What would happen if this system were breached tomorrow?
7. Individual rights	Let people see, correct and erase their data, and complain.	How easily can a person find out what we hold about them?
8. Accountability	Be responsible, and be able to prove compliance with evidence.	Can we show evidence, not just policies?

NOTES
10 OECD, Guidelines on the Protection of Privacy and Transborder Flows of Personal Data (1980, revised 2013): oecd.org.
11 Regulation (EU) 2016/679 (GDPR), Art. 5: eur-lex.europa.eu/eli/reg/2016/679/oj.
12 MeitY / PIB, explanatory material on the Digital Personal Data Protection Bill, 2023 (August 2023): pib.gov.in.

Why this matters for Indian Businesses & Global MNCs

India sits in two places in the global data economy at once. It is a **large digital market** with hundreds of millions of online users. It is also a **global operations hub:** IT and business-process services, Global Capability Centres (GCCs), pharmaceutical research and engineering all handle data about people in other countries.

This creates two kinds of exposure. **Indian businesses going global** meet foreign laws, directly when they sell abroad and indirectly through client contracts. **Global groups operating in India** must add India's DPDP layer to their existing programmes.

The map at the end of this section shows how the layers fit together. International principles shape national laws. National laws such as DPDP sit alongside sector rules.

Contracts carry foreign requirements into Indian operations. The organisation's own operating model is where all of this becomes real.



If you are…	Rules that usually follow you	Practical focus
An Indian IT, BPO or GCC provider serving overseas clients	Client-country laws through contracts (for example EU Standard Contractual Clauses); DPDP partly, because s. 17(1)(d) exempts many duties for foreign-contract data but security safeguards still apply	Contract compliance, security evidence, breach escalation, sub-processor control
An Indian consumer platform	DPDP in full; sector rules; foreign laws if you target users abroad	Notice, consent, children, rights, breach readiness
An Indian subsidiary of a global group	DPDP; group policy; home-country law of the parent; transfer rules of other countries in the data chain	India addendum to the global programme; group data-flow map
An Indian company selling into the EU, UK, Gulf or US	Local laws may apply directly, without a local office	Local representative, local notices, transfer tools

GLOBAL-TO-INDIA FRAMEWORK MAP

1 Shared global principles	OECD Guidelines and the eight common principles: lawful use, purpose, minimisation, accuracy, storage limits, security, rights, accountability
2 International laws	EU GDPR · UK GDPR · US state & sector laws · Singapore PDPA · China PIPL · UAE PDPL / DIFC / ADGM · Saudi PDPL · Brazil LGPD
3 India's DPDP framework	**DPDP Act, 2023 + DPDP Rules, 2025: India's local operating layer**
4 Indian sector & cyber rules	CERT-In Directions · RBI · SEBI · IRDAI · Telecom Act 2023 · Aadhaar Act · Consumer Protection · ABDM
5 Contracts & standards	Client DPAs · EU / UK / ANPD clauses · ISO 27001 / 27701 · SOC 2 · Sector outsourcing terms
6 Your operating model	Discover · Classify · Govern · Protect · Monitor · Respond · Assure

Read top to bottom: shared principles shape national laws; DPDP sits beside Indian sector rules; contracts carry foreign requirements into Indian operations; the operating model is where compliance becomes real.

Leadership Takeaway

A mature global privacy programme is a useful baseline, but India requires a specific DPDP gap assessment. Equally, DPDP compliance alone does not satisfy the laws of the other countries your data touches.





International Data Protection Landscape

Global Privacy Rules at a Glance

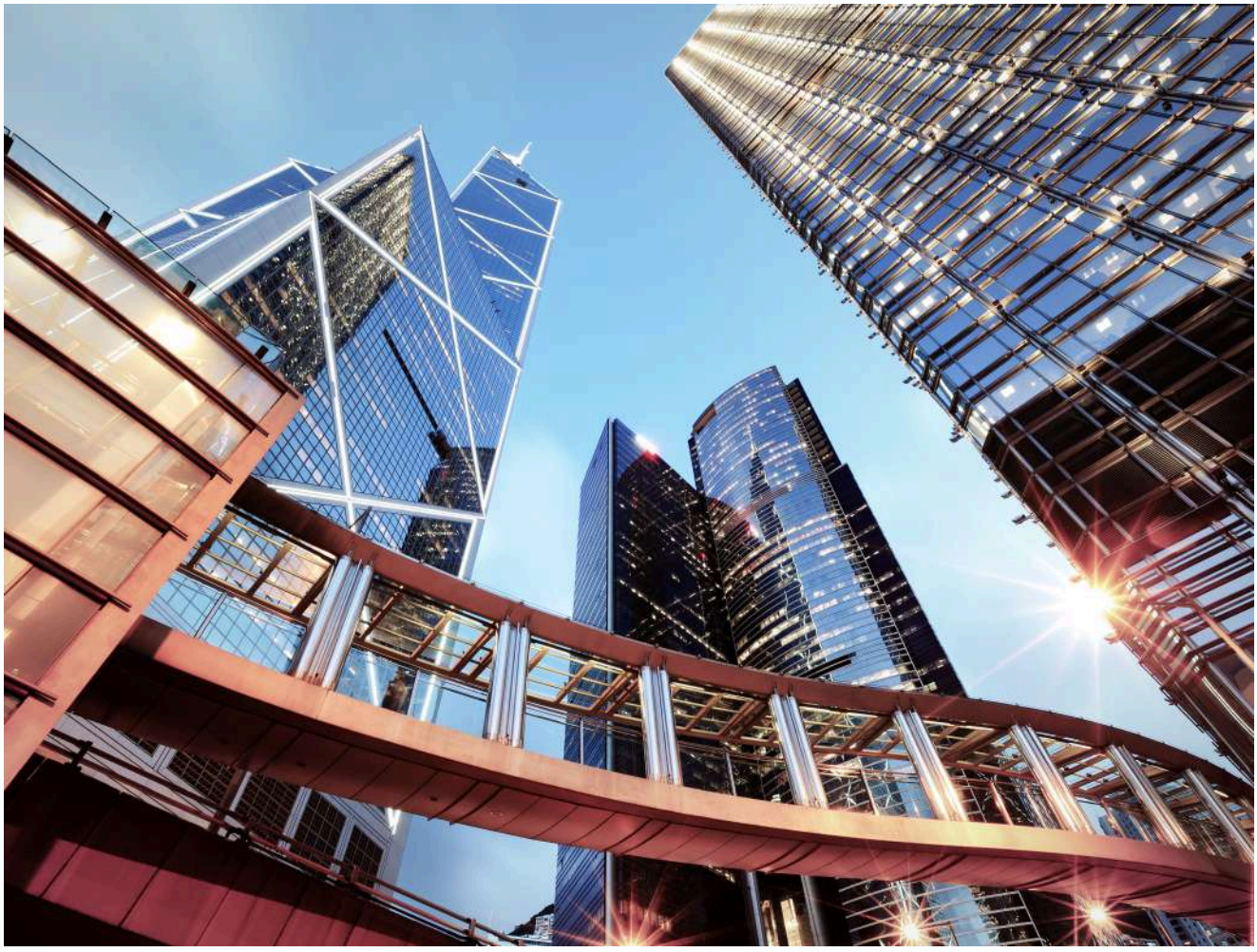
This document does not try to cover every country. It gives practical coverage to eight jurisdictions that matter most to Indian businesses and to global groups operating in India: the **European Union, the United Kingdom, the United States, Singapore, China, the United Arab Emirates, Saudi Arabia and Brazil.** Other laws are listed briefly in Appendix C.

For each jurisdiction we explain only seven things: who may be affected, what the law protects, the main business expectations, the cross-border position, individual rights, the breach-response approach and one practical point for Indian businesses. Summaries are simplified and current as at September 2026; always confirm details with the official sources in Appendix C.



Jurisdiction	Main law(s)	Regulator	Status
European Union	General Data Protection Regulation (GDPR), Regulation (EU) 2016/679	National supervisory authorities; European Data Protection Board	Applies since 25 May 2018
United Kingdom	UK GDPR and Data Protection Act 2018, as amended by the Data (Use and Access) Act 2025	Information Commissioner's Office (ICO)	Main 2025 reforms in force from February 2026
United States	No single federal law: about 20 state privacy laws plus federal sector laws	FTC, state attorneys general, California Privacy Protection Agency, sector regulators	State laws in force on a rolling basis
Singapore	Personal Data Protection Act 2012 (PDPA)	Personal Data Protection Commission (PDPC)	Amended 2020; in force

China	Personal Information Protection Law (PIPL) 2021, with the Data Security and Cybersecurity Laws	Cyberspace Administration of China (CAC)	In force since 1 November 2021
UAE	Federal Decree-Law No. 45 of 2021 (PDPL); DIFC Data Protection Law 2020; ADGM Data Protection Regulations 2021	UAE Data Office; DIFC Commissioner; ADGM Office of Data Protection	Federal implementing regulations awaited
Saudi Arabia	Personal Data Protection Law (PDPL) and implementing regulations	Saudi Data & AI Authority (SDAIA)	Enforced since 14 September 2024
Brazil	General Data Protection Law (LGPD), Law No. 13,709/2018	National Data Protection Authority (ANPD)	In force since 2020



European Union GDPR and UK GDPR

The EU's General Data Protection Regulation (GDPR) is the most influential privacy law in the world. It applies across all 27 EU member states and the wider European Economic Area. Many Privacy laws borrowed its ideas, although, as this paper shows, they are not copies.

After leaving the EU, the UK kept the GDPR as "UK GDPR". The **Data (Use and Access) Act 2025** then made targeted changes. Its main data-protection reforms took effect on 5 February 2026, and a new duty to handle complaints followed in June 2026.[13] The EU is also debating a "Digital Omnibus" package that would amend parts of the GDPR. As at September 2026 these GDPR changes remain proposals.[14]

Penalties can be significant: under the GDPR, up to €20 million or 4% of worldwide annual turnover, whichever is higher, for the most serious breaches.[15] UK maximums penalties are up to £17.5 million or 4% of turnover.

Key point	European Union – GDPR	United Kingdom – UK GDPR as amended
Who may be affected	Organisations established in the EU; and organisations outside the EU that offer goods or services to, or monitor the behaviour of, people in the EU.[16]	Same approach for the UK: UK establishments, and non-UK organisations targeting or monitoring people in the UK.
What it protects	The fundamental right to protection of personal data. Covers digital and structured paper records. Extra rules for special categories such as health, biometrics and religion.	Same scope and special categories.
Main business expectations	One of six lawful bases, including contract, legal obligation, legitimate interests and consent. Records of processing, impact assessments for high-risk uses, processor contracts, privacy by design, a DPO in certain cases, and an EU representative for many non-EU firms.	Similar to the EU. New list of "recognised legitimate interests" (such as crime prevention, safeguarding and emergencies) that need no balancing test; more flexible rules on automated decisions; a duty to handle complaints; some low-risk cookies exempt from consent.
Cross-border transfers	Allowed to countries with an EU adequacy decision (India has none). Otherwise use safeguards such as Standard Contractual Clauses (SCCs) or Binding Corporate Rules, with a transfer risk assessment.[17]	UK adequacy regulations, the UK International Data Transfer Agreement or the UK Addendum to EU SCCs. The 2025 Act uses a "not materially lower" protection test.
Individual rights	Access, correction, erasure, restriction, portability, objection, and protection from solely automated decisions with significant effects.	Same core rights. Searches for access requests must be reasonable and proportionate.
Breach response	Notify the regulator within 72 hours unless the breach is unlikely to create a risk; tell affected people without undue delay if the risk is high.[18]	Same: ICO within 72 hours where there is risk; tell people if the risk is high.

For Indian businesses	Indian vendors usually sign SCCs as “data importers”. Expect audit rights, sub-processor approval and contract breach-notice windows of 24–48 hours.	UK and EU client contracts now differ in detail. Keep separate UK and EU clause sets rather than one merged template.



NOTES
13 Data (Use and Access) Act 2025 (c. 18): legislation.gov.uk/ukpga/2025/18; ICO, “One year on” (June 2026): ico.org.uk.
14 European Commission, Digital Omnibus proposals (19 November 2025); European Parliament Legislative Train Schedule: europarl.europa.eu/legislative-train.
15 GDPR, Art. 83(5).
16 GDPR, Art. 3.
17 GDPR, Chapter V (Arts. 44–50).
18 GDPR, Arts. 33–34.

United States Privacy Law

The United States has **no single, comprehensive federal privacy law.** Instead, it has a patchwork. More than twenty states have comprehensive consumer privacy laws, led by California.[19] Federal laws cover specific sectors, such as health (HIPAA), financial services (Gramm-Leach-Bliley Act) and children under 13 online (COPPA). The Federal Trade Commission (FTC) acts against "unfair or deceptive" data practices.

Two newer federal measures matter to Indian service providers. Listed companies must disclose material cybersecurity incidents, generally within four business days of deciding that an incident is material.[20] And the Department of Justice's Data Security Program (from April 2025) restricts giving certain "countries of concern" access to bulk sensitive personal data of Americans.[21]

Key point	United States – state laws and key federal sector laws
Who may be affected	State laws usually apply to businesses above size or data-volume thresholds that do business in the state or target its residents, wherever the business is based. Sector laws follow the activity: health providers and their "business associates", financial institutions, online services directed at children.
What it protects	Consumers' control over the sale and sharing of their data; protection of sensitive data (health, precise location, biometrics, children); and protection against deceptive practices.
Main business expectations	Clear privacy notices; opt-out of sale, sharing and targeted advertising; opt-in consent for sensitive data in many states. Contracts with "service providers" or "processors"; data-protection assessments for high-risk processing. California now also regulates automated decision-making technology, risk assessments and cybersecurity audits, phased in from 2026.[22]
Cross-border transfers	No general transfer restriction. The DOJ Data Security Program restricts certain data deals involving countries of concern (such as China and Russia). India is not a country of concern, but US clients now pass these restrictions down to vendors.
Individual rights	Access, deletion, correction, portability, and opt-out of sale, sharing, targeted advertising and some profiling. California requires businesses to honour browser-based opt-out signals such as Global Privacy Control.
Breach response	All 50 states have breach-notification laws with different triggers and timelines. HIPAA requires notice to individuals without unreasonable delay and within 60 days. Listed companies have SEC disclosure duties.
For Indian businesses	US clients flow down HIPAA business associate agreements, GLBA security terms, state-law service-provider clauses and DOJ restrictions on access from countries of concern. Indian delivery centres must evidence these controls, including who can access data and from where.

NOTES
19 IAPP, US State Privacy Legislation Tracker: iapp.org/resources/article/us-state-privacy-legislation-tracker.
20 US SEC, Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure, Release No. 33-11216 (2023), Form 8-K Item 1.05.
21 US Department of Justice, Data Security Program, 28 CFR Part 202: justice.gov/nsd/data-security.
22 California Privacy Protection Agency, regulations on ADMT, risk assessments and cybersecurity audits (approved September 2025; effective 1 January 2026 with phased dates): cppa.ca.gov.

Asia-Pacific: Singapore, China and Selected Regional Frameworks

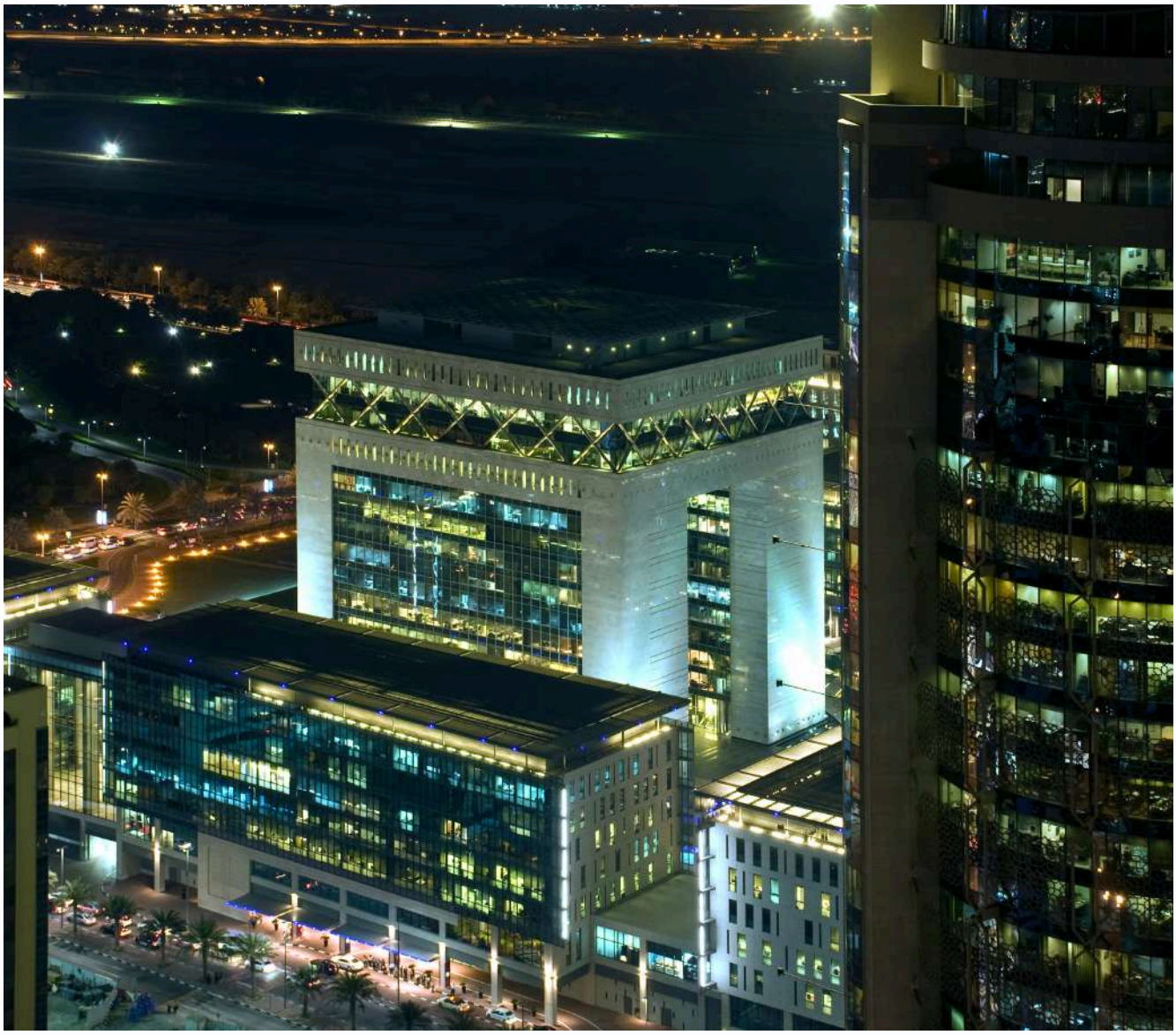
Asia-Pacific has no single model. **Singapore** takes a practical, business-friendly but firm approach. **China** combines privacy with national-security controls on data leaving the country. Many Indian groups run regional hubs from Singapore and buy from, sell to or manufacture in China, so both matter.

China's framework has been tightened and clarified in stages. The Cybersecurity Law was amended with effect from 1 January 2026, raising penalties. New measures on personal-information compliance audits (from May 2025) and on certification for data exports (from January 2026) also apply.[23]

Other regional laws are relevant for some groups: Japan's APPI, South Korea's PIPA, Australia's Privacy Act (amended in 2024), Indonesia's PDP Law (fully in force from October 2024) and Vietnam's Personal Data Protection Law (effective 1 January 2026). See Appendix C.

Key point	Singapore – PDPA	China – PIPL
Who may be affected	Private organisations that collect, use or disclose personal data in Singapore, including foreign organisations doing so there.[24]	Processing in China; and processing outside China to provide products or services to, or analyse the behaviour of, people in China.[25]
What it protects	Personal data, balancing individual rights with organisations' legitimate needs.	Personal information rights. "Sensitive" information (biometrics, health, finance, location, children under 14) needs extra care.
Main business expectations	Consent (including deemed consent) or a listed exception, such as legitimate interests or business improvement. Mandatory Data Protection Officer; reasonable security; retention limits; Do Not Call rules for marketing.	Consent (separate consent for sensitive data, sharing and export) or another listed basis such as contract or HR management. No general legitimate-interests basis. Impact assessments, a responsible officer, compliance audits, and a representative in China for foreign processors in scope.
Cross-border transfers	Allowed if the recipient gives a comparable standard of protection, for example through contracts, binding corporate rules or certifications.	Needs a CAC security assessment, the standard contract or certification, unless an exemption applies (for example, some contract-necessity and HR transfers). Stricter rules for critical operators and large volumes.
Individual rights	Access and correction. (A portability right has been legislated but is not yet in force.)	Know, decide, access, copy, portability, correction, deletion, and an explanation of processing rules; can refuse decisions made solely by automated means that significantly affect them.

Breach response	Assess a suspected breach promptly; notify the PDPC within 3 calendar days of deciding it is notifiable, and affected people if significant harm is likely.	Take remedial action immediately and notify the authorities and, generally, affected individuals. Separate cyber-incident rules set very short reporting times.
For Indian businesses	Singapore is a common regional headquarters. Indian vendors serving Singapore clients should expect the PDPC's protection standard to be written into contracts.	Assume China-origin personal data cannot leave China without an approved mechanism. Plan group reporting and shared-service designs around this.



NOTES
23 CAC, Measures for Personal Information Protection Compliance Audits (effective 1 May 2025); Measures for Certification of Personal Information Outbound Transfer (effective 1 January 2026); amended Cybersecurity Law (effective 1 January 2026): cac.gov.cn.
24 Personal Data Protection Act 2012 (Singapore): sso.agc.gov.sg/Act/PDPA2012.
25 Personal Information Protection Law of the PRC (2021), Art. 3 (official English translation: npc.gov.cn).

GCC and Middle East: UAE, DIFC, ADGM and Saudi Arabia

The Gulf is a major market and workplace for Indian businesses and professionals. Its data-protection rules are relatively new and still developing.

In the **United Arab Emirates,** the first question is always: **which rulebook applies?** The UAE has a federal law for the "mainland". Two financial free zones have their own, separate laws: the **Dubai International Financial Centre (DIFC)** and **Abu Dhabi Global Market (ADGM).** Health and banking data may also be covered by their own sector laws. As at 2026, the federal law's implementing regulations had not yet been issued, so some details (such as breach timelines) remain open.[26] Data moving between the mainland and a free zone can count as a cross-border transfer.

The DIFC and ADGM laws closely follow the GDPR model, and here the label "GDPR-style" is fair.[27]

Saudi Arabia's Personal Data Protection Law has been fully enforced since 14 September 2024, supervised by the Saudi Data & AI Authority (SDAIA).[28] Penalties can include fines of up to SAR 5 million, which can be doubled for repeat breaches, and criminal penalties for disclosing sensitive data with intent to harm.

Key point	United Arab Emirates – Federal PDPL, DIFC, ADGM	Saudi Arabia – PDPL
Who may be affected	Federal: processing in the UAE mainland, and processing abroad of data about people in the UAE. Excludes government data, the DIFC and ADGM, and health or banking data covered by their own laws. DIFC and ADGM: entities in those zones.	Processing in the Kingdom, and processing outside it of personal data about people living in the Kingdom.
What it protects	Personal data and sensitive personal data (such as health, biometrics and religion).	Personal data, with stricter rules for sensitive, credit, health and genetic data.
Main business expectations	Consent or another listed ground; security; records; impact assessments for high-risk uses; a DPO in defined cases. DIFC/ADGM: fuller GDPR-like duties and registration or notification with the regulator.	Consent or another legal basis (legitimate interest is not available for sensitive data); records of processing; privacy policy; impact assessments. A DPO in defined cases; registration on SDAIA's National Data Governance Platform for some controllers.
Cross-border transfers	Federal: to countries with adequate protection or under other listed conditions. DIFC/ADGM: adequacy lists or appropriate safeguards.	To adequate countries, or with appropriate safeguards (standard clauses, binding corporate rules, certification) and a risk assessment; transfer only the minimum needed.

Individual rights	Information, access, correction, erasure, restriction, objection and, in the free zones, portability.	To be informed, access, obtain a copy, correction and destruction.
Breach response	Federal: notify the Data Office on becoming aware (details await regulations). DIFC: notify the Commissioner as soon as practicable. ADGM: within 72 hours.	Notify SDAIA within 72 hours where harm is likely; tell affected people without undue delay if harm is likely.
For Indian businesses	Map which licence each Gulf entity holds (mainland, DIFC or ADGM) before designing notices and transfers. Indian staff working in the UAE are usually covered by UAE law, not DPDP.	Indian contractors and IT providers on Saudi projects often handle employee and resident data. Moving it to India needs a documented transfer mechanism and risk assessment.



NOTES
26 Federal Decree-Law No. 45 of 2021 on the Protection of Personal Data (UAE); status of executive regulations as reported in Chambers Global Practice Guide, Data Protection & Privacy 2026 – UAE.
27 DIFC Data Protection Law, DIFC Law No. 5 of 2020 (as amended): difc.ae; ADGM Data Protection Regulations 2021: adgm.com.
28 Saudi Personal Data Protection Law (Royal Decree M/19 of 1443H, as amended) and Implementing Regulation; Regulation on Personal Data Transfer outside the Kingdom (as amended 2024): sdaia.gov.sa.

Brazil LGPD and Other Relevant Growth Markets

Brazil's General Data Protection Law (LGPD) is Latin America's most important privacy law. It is enforced by the National Data Protection Authority (ANPD), which has issued detailed regulations on breach reporting and international transfers.[29] Penalties can reach up to 2% of revenue in Brazil, capped at R$50 million per incident.

Beyond Brazil, fast-growing markets such as **Indonesia, Vietnam, Nigeria, Kenya and South Africa** now have modern data-protection laws. Indian firms expanding into these markets should run a short local check before launch. Appendix C lists these laws and their regulators.

Key point	Brazil – LGPD
Who may be affected	Processing in Brazil; processing to offer goods or services to people in Brazil; and data collected in Brazil, wherever the organisation is based.
What it protects	Fundamental rights of freedom and privacy. "Sensitive" data (health, biometrics, religion, political opinion and similar) has stricter rules.
Main business expectations	One of ten legal bases, including consent, contract, legal obligation, legitimate interests and credit protection. A Data Protection Officer ("encarregado") in most cases; records of processing; impact reports on request; security measures.
Cross-border transfers	Adequacy, or safeguards such as the ANPD's Standard Contractual Clauses. Organisations relying on contractual clauses had to adopt the ANPD text by August 2025.
Individual rights	Confirmation, access, correction, anonymisation or deletion, portability, information about sharing, withdrawal of consent, and review of automated decisions.
Breach response	Notify the ANPD and affected people within 3 working days where the incident may create relevant risk or damage.
For Indian businesses	Indian IT, pharma and manufacturing groups with Brazilian entities should use the ANPD clauses word for word in intra-group and vendor agreements.



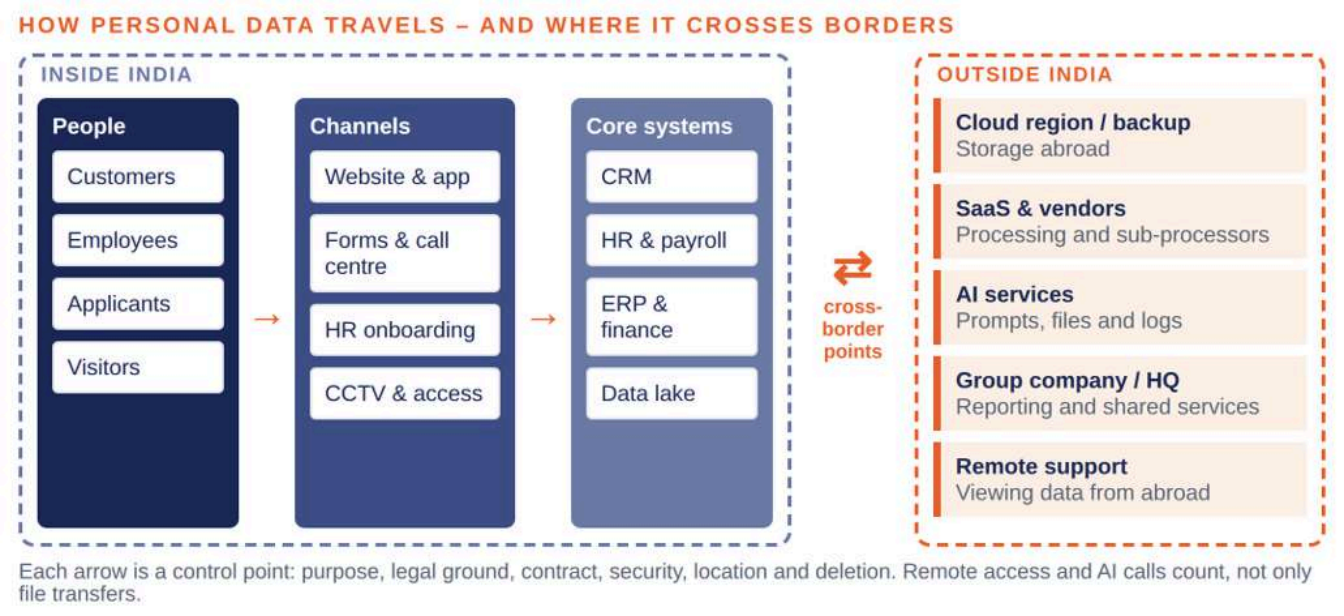
Cross-Border Data Transfers – Why Location, Remote Access and Vendor Access Matter

Many people think a "data transfer" means sending a file to another country. In practice it is much wider. **Viewing** a record on a screen from another country, a vendor's engineer **logging in** to fix a system, a cloud **backup** in another region, or an **AI service** processing a prompt abroad can all move data across borders.

Laws take three broad approaches:

- **Open unless restricted.** Transfers are allowed unless the Government blocks a country. This is India's approach under s. 16 of the DPDP Act.[30]
- **Conditional.** Transfers need adequacy or safeguards such as standard clauses. This is the EU, UK, Brazil, Saudi, UAE and, in its own way, Singapore model.
- **State-controlled**. Some transfers need government assessment or approval. China is the main example.

On top of these, **sector rules** can require data to stay in the country. In India, for example, the Reserve Bank of India requires payment-system data to be stored in India.[31]



Each arrow is a control point: purpose, legal ground, contract, security, location and deletion. Remote access and AI calls count, not only file transfers.

What a transfer register should record

- Data set and people affected
- Sending and receiving entities and their legal roles
- Countries of storage, processing and remote access
- Transfer tool used (for example, SCCs, IDTA, ANPD clauses)
- Vendors and sub-processors in the chain
- Date of last risk assessment and review

In Simple Words

Data location is not the same as data access. Keeping servers in India does not stop a transfer if people outside the organization or geography have access the data.

NOTES
30 DPDP Act, 2023, s. 16; DPDP Rules, 2025, Rule 15.
31 Reserve Bank of India, Storage of Payment System Data, circular RBI/2017-18/153 (6 April 2018): rbi.org.in.

Global Comparison – What Leaders Need to Know

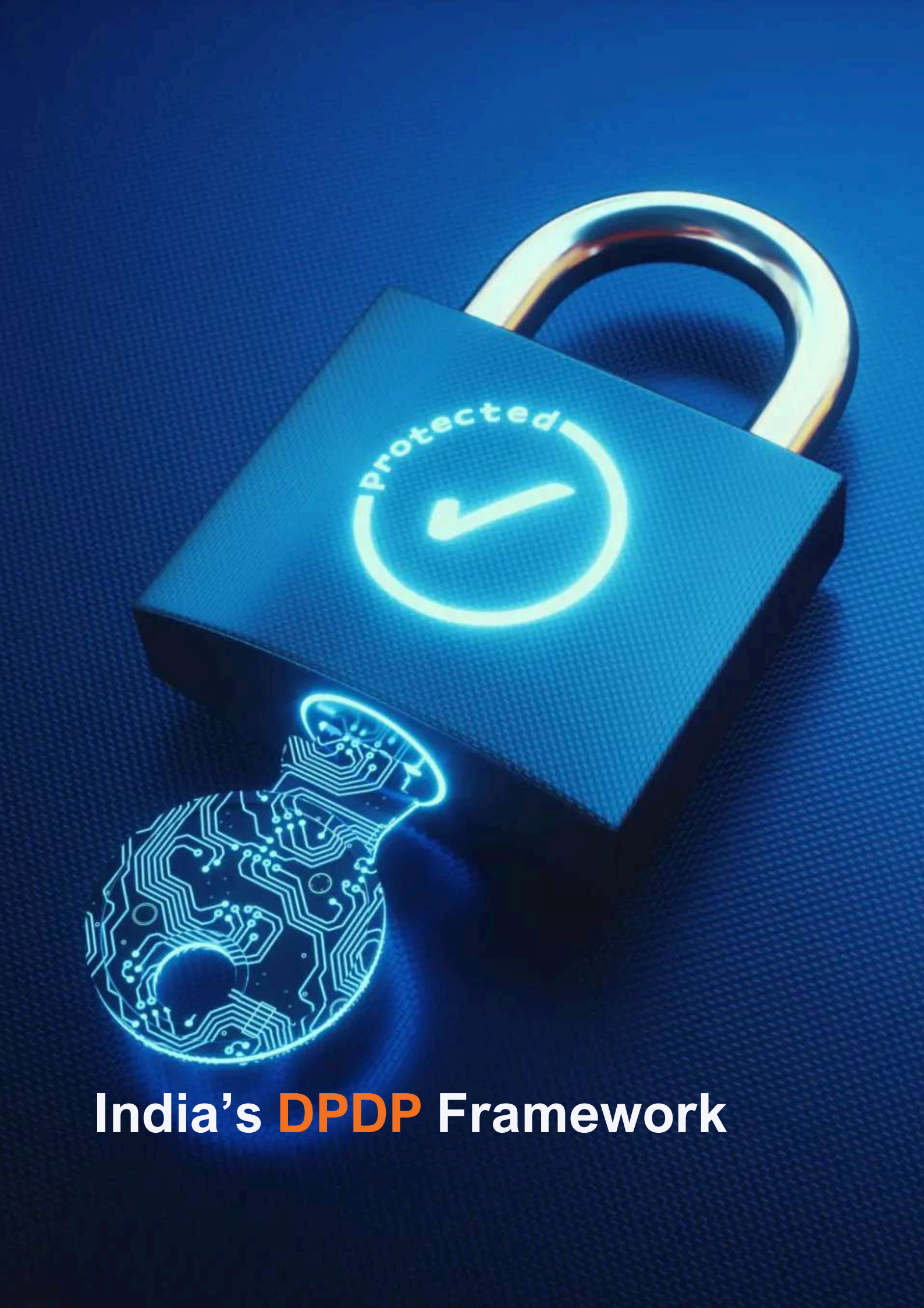
The table below compares the jurisdictions on the points that most often change how a global programme must work. It is a simplified guide for management discussion, not legal advice.

Jurisdiction	Main legal grounds	Breach notice to regulator	Cross-border approach	Person Responsible
India (DPDP)	Consent or listed "certain legitimate uses"	Every breach, without delay; detailed report within 72 hours	Allowed unless a country is restricted	DPO in India only for SDFs; published contact for all
EU (GDPR)	Six bases, incl. legitimate interests	Within 72 hours if there is risk	Adequacy or safeguards	DPO in some cases; EU representative for many non-EU firms
UK	Six bases plus "recognised legitimate interests"	Within 72 hours if there is risk	Adequacy, IDTA or Addendum	DPO in some cases; UK representative in some cases
United States	Mostly notice and opt-out; opt-in for sensitive data in many states	Varies by state; SEC for listed companies	No general restriction; DOJ rule on countries of concern	None generally
Singapore	Consent, deemed consent or exceptions	Within 3 calendar days of assessing it as notifiable	Comparable protection	DPO mandatory
China	Consent or listed bases; no legitimate interests	Immediately	Assessment, standard contract or certification	Officer; representative in China for foreign processors
UAE (Federal)	Consent or listed grounds	On becoming aware (details awaited)	Adequacy or listed conditions	DPO in defined cases
Saudi Arabia	Consent, legitimate interest (not for sensitive data) and others	Within 72 hours if harm is likely	Adequacy or safeguards plus risk assessment	DPO in defined cases
Brazil	Ten bases, incl. legitimate interests	Within 3 working days if risk	Adequacy or ANPD clauses	DPO in most cases

Where India is different

Topic	India – DPDP	What global teams should do
Scope	Digital personal data only (including digitised paper records)	Do not ignore paper-to-digital workflows such as scanned forms.
Legal grounds	No general legitimate-interests ground	Do not copy EU balancing tests into India; map each use to consent or section 7 of DPDP Act.
Children	Everyone under 18; verifiable parental consent; no tracking or targeted ads	Add an India child-control layer to global products.
Breach	All personal data breaches reported to the Board and to affected people	Add an India branch to global incident playbooks.
Sensitive data	DPDP does not create a separate statutory special-category data regime	Higher-risk data (health, finance, biometrics, children) still needs proportionate safeguards; keep stronger global controls.
Transfers	Open unless a geography is restricted; SDFs may face localisation of specified data	Keep a live transfer map so restrictions can be applied quickly.
Unique features	Consent Managers; duties on individuals; right to nominate	Build nomination into rights workflows; decide on Consent Manager integration.
Penalties	Fixed maximum amounts per instance, up to ₹250 crore	Treat as board-level risk, alongside turnover-based fines abroad.





India's DPDP Framework

India's DPDP Journey and Why It Matters

India's DPDP framework developed through a long policy journey after the Supreme Court recognised privacy as a fundamental right in **Justice K.S. Puttaswamy (Retd.) v. Union of India** in August 2017.[32] Before that, India relied mainly on the Information Technology Act, 2000 and the 2011 rules on "sensitive personal data".

Earlier policy white papers and consultations shaped the debate. They included the November 2017 White Paper of the Committee of Experts chaired by Justice B.N. Srikrishna, which invited public comment on the design of a data-protection framework for India.[33] Draft bills followed in 2018, 2019 and 2022. **However, the current legal position must be based on the DPDP Act, 2023, the DPDP Rules, 2025 and later official notifications**, not on earlier drafts.



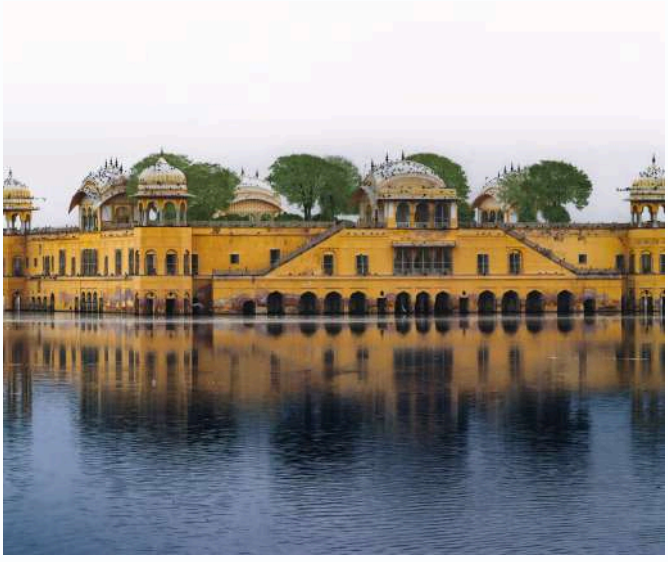
Historical milestones for context. Current obligations come only from the DPDP Act, 2023, the DPDP Rules, 2025 and later notifications.

Why it matters beyond India

- **Scale.** India has one of the world's largest online populations and extensive digital public infrastructure for identity, payments and documents.
- **Global operations.** Much of the world's IT, business-process and GCC work is delivered from India. How India treats data affects clients everywhere.
- **Trust in trade.** Clear, enforceable rules support cross-border digital trade and investment.

Leadership Takeaway

Read the history for context, but act on the current law. Older drafts contained ideas, such as a separate "sensitive personal data" category and strict localisation, that did not become part of the final Act.



NOTES

32 Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 SCC 1 (nine-judge bench, 24 August 2017).

33 Committee of Experts under the Chairmanship of Justice B.N. Srikrishna, White Paper on Data Protection Framework for India (MeitY, 27 November 2017); summary at en.vikaspedia.in (e-governance section). Cited for historical context only.

DPDP Act and Rules at a Glance

The DPDP Act sets the main duties and rights. The DPDP Rules, notified on 13 November 2025, give the practical detail: what a notice must say, the minimum security measures, how to report breaches, time limits for erasure and more.[34]

A corrigendum to the Rules was issued in December 2025.

The Government chose a **phased start** so that businesses have time to prepare. The Act's structure is summarised in Appendix A and each Rule's start date in Appendix B.

Phase	Date	What comes into force	What it means for business
Phase 1	13 Nov 2025	Definitions; Data Protection Board provisions (ss. 18–26); Rules 1, 2 and 17–21; amendment to the RTI Act (s. 44(3))	The regulator exists in law. Start readiness work.
Phase 2	13 Nov 2026	Consent Manager registration and obligations (s. 6(9), s. 27(1)(d); Rule 4 and First Schedule)	Registered Consent Managers can begin operating. Decide whether and how to integrate with them.
Phase 3	13 May 2027	All core duties: notice, consent, legitimate uses, security, breach reporting, children, SDFs, rights, transfers, exemptions, penalties; omission of IT Act s. 43A; Rules 3, 5–16, 22, 23	Full compliance expected. Penalties can be imposed.

Where things stand in September 2026

- **Data Protection Board.** The Board was established in law on 13 November 2025. In May 2026 MeitY invited applications for the Chairperson and four Members.[35] Public reporting in August 2026 indicated that appointments had not yet been announced.[36] Readers should check the latest position.
- **Proposal to accelerate.** In January 2026, MeitY consulted industry on shortening parts of the 18-month window, including for Significant Data Fiduciaries and cross-border rules. As at the date of this paper, no amendment has been notified, so the dates above remain the reference dates.[37]
- **Consent Manager ecosystem.** MeitY has published non-binding technical guidance on consent management systems and run an innovation challenge to encourage prototypes.

What this means?

Treat late 2026 as the build period and early 2027 as the test period. Organisations that wait until May 2027 will not have time to redesign notices, renegotiate vendor contracts, build rights workflows and test breach response.

NOTES

34 DPDP Rules, 2025, published in the Gazette of India; MeitY press release and explanatory note (November 2025): meity.gov.in/data-protection-framework.

35 MeitY, advertisement inviting applications for Chairperson and Members of the Data Protection Board of India, F. No. 2(1)/2026-Pers.I (May 2026): meity.gov.in.

36 LiveLaw, "India's Data Protection Board: Established in Law, Absent in Fact" (1 August 2026).

37 As reported in Mondaq / Chambers & Partners, "MeitY plans to cut short DPDP compliance timeline" (2026). Monitor the e-Gazette for any amending notification.

Applicability, Key Terms and Exclusions

The DPDP Act applies to the processing of **digital personal data within India,** whether collected in digital form or collected on paper and digitised later. It also applies to processing **outside India** if it is connected with offering goods or services to people in India.[38]

in Simple words

If your company in London, New York or Dubai sells an app, a course or a product to people in India, the DPDP Act can apply to you even if you have no office in India.

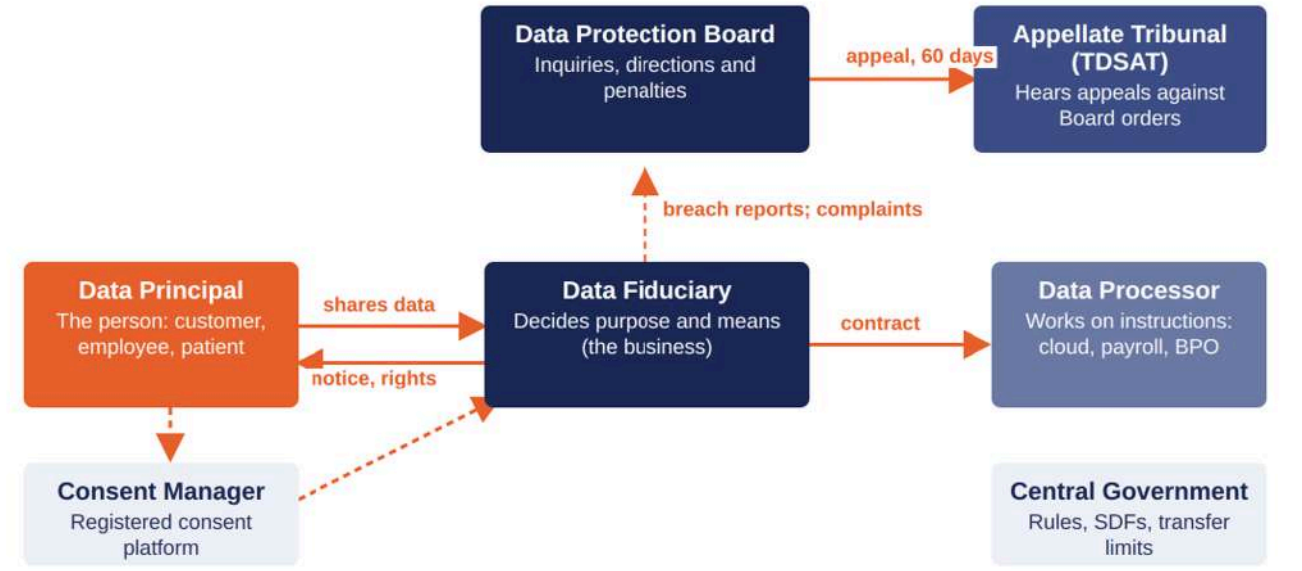
The Act does **not** apply to personal data used by an individual for purely personal or domestic purposes, or to personal data made publicly available by the person themselves or by someone under a legal duty to publish it.[39]

Truly anonymised data that can no longer identify anyone is not personal data. Pseudonymised data, where identity can be restored with a key, remains personal data.

Nuances leaders often miss

- **B2B is not exempt.** Names, emails and phone numbers of business contacts, employees, contract workers and visitors are personal data.
- **Public does not mean free to use.** The public-data exclusion is narrow. Scraping social-media profiles or websites for a new purpose needs careful legal review.
- **No special-category regime.** DPDP does not create a separate statutory special-category data regime, but higher-risk data still requires proportionate safeguards.

THE KEY PLAYERS UNDER DPDP



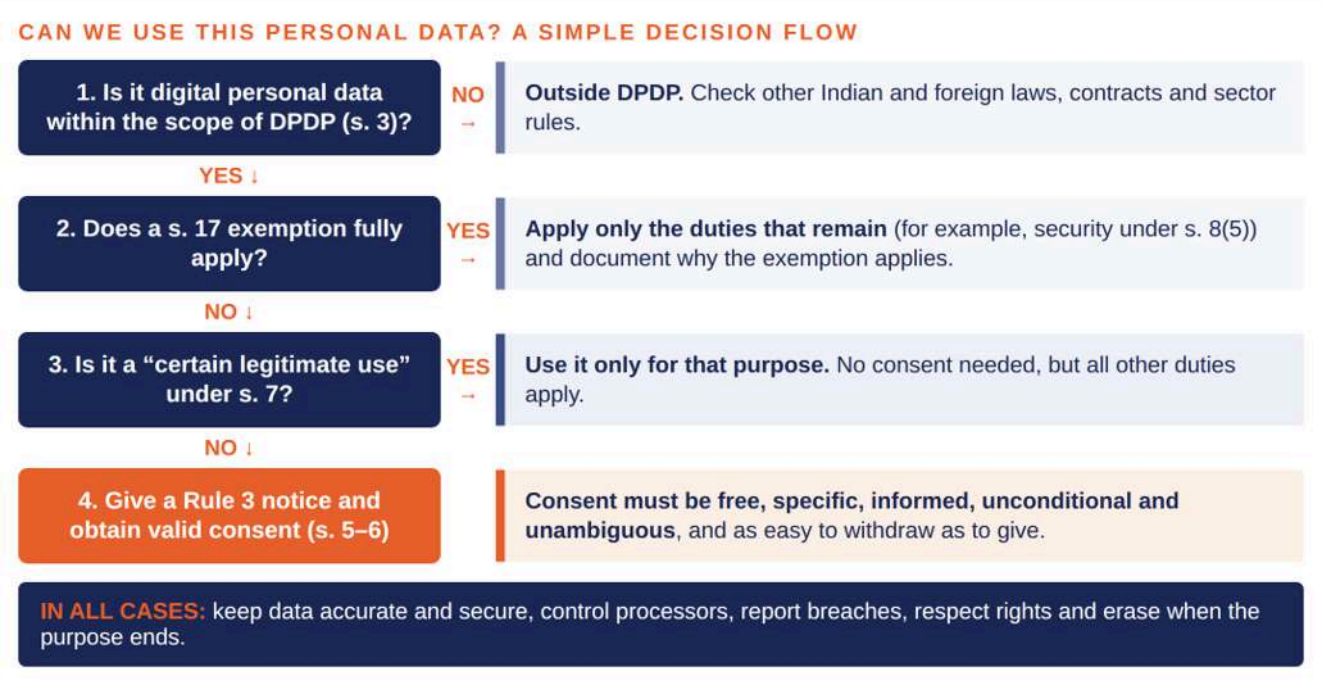
A person must first complain to the business; only then can they approach the Board.

NOTES
38 DPDP Act, 2023, s. 3(a)–(b).
39 DPDP Act, 2023, s. 3(c).

Legal Grounds – Consent and Certain Legitimate Uses

Under s. 4, personal data may be processed only for a lawful purpose, and only on one of two grounds: the person has given consent, or the use falls within a "certain legitimate use" listed in s. 7.[40] There is no third option.

This is a major difference from the EU, UK, Brazil and Singapore, where a general "legitimate interests" ground exists. If an Indian use is not clearly within s. 7, the business will usually need consent.



The certain legitimate uses under section 7

S. 7	Legitimate use (no consent needed)	Simple example
(a)	The person voluntarily gave data for a specified purpose and has not said they object to its use.	A buyer shares a phone number so the shop can send the bill by SMS.
(b)	The State provides a subsidy, benefit, service, certificate, licence or permit.	Using existing records to credit a scholarship.
(c)	The State performs a legal function, or acts for sovereignty, integrity or security.	A department carrying out a statutory duty.
(d)	Meeting a legal duty to disclose information to the State.	Providing data required by a tax authority.

(e)	Complying with a judgment or order under Indian law, or a foreign judgment on contractual or civil claims.	Producing records under a court order.
(f)–(g)	Responding to a medical emergency, or giving treatment during an epidemic or public-health threat.	Treating an unconscious accident victim.
(h)	Ensuring safety or giving help during a disaster or breakdown of public order.	Locating employees during a flood.
(i)	Employment purposes, or protecting the employer from loss or liability (such as espionage or leaks of trade secrets), or providing a benefit the employee asked for.	Running payroll, attendance and background checks.

WHAT THE LAW REQUIRES	Every use of digital personal data must rest on consent or a s. 7 legitimate use. The business must be able to show which ground applies.
GOOD PRACTICE	Keep a register that maps each processing activity to its ground, notice and retention period. Review it when a purpose changes.
ILLUSTRATION	A company may process payroll data under s. 7(i). If it later wants to use employee contact details to market a partner's insurance product, that is a new purpose and will usually need consent.



NOTES
40 DPDP Act, 2023, ss. 4 and 7.

Notice, Consent and Consent Managers

Notice: telling people clearly

Whenever a business asks for consent, it must first (or at the same time) give the person a notice.[41] The notice must be understandable on its own, in clear and plain language, with an itemised list of the data and the specific purposes. It must explain how to withdraw consent, use rights and complain to the Board. People must be able to read it in English or any of the 22 languages in the Eighth Schedule to the Constitution.[42] For data collected before the Act, a notice must be given as soon as reasonably practicable.

Poor notice	Good notice
"We may collect your information to improve our services and share it with	"We will use your mobile number to send delivery updates. We will not use it for marketing unless you tick the box below."
Hidden in a 20-page privacy policy.	Shown on screen before the "Submit" button, with a link to more detail.
Only in English legal language.	Available in the customer's preferred language.
No way to withdraw consent.	"Change your mind at any time from Settings > Privacy."

Consent: what makes it valid

Consent must be **free, specific, informed, unconditional and unambiguous**, given by a clear affirmative action, and limited to the data necessary for the stated purpose.[43] Pre-ticked boxes, silence and "by continuing to browse" do not work. Bundled consent ("agree to marketing or you cannot use the app") fails the "free" test where marketing is not needed for the service.

A person can withdraw consent at any time, and withdrawing must be **as easy as giving it.**[44] After withdrawal, the business and its processors must stop processing within a reasonable time, unless another law requires the data to be kept. If there is a dispute, **the business must prove** that proper notice was given and valid consent obtained.[45]

A strong consent record contains

- Person or account reference
- Date and time stamp
- Notice version shown
- Purpose(s) agreed
- Channel (app, web, call centre, paper)
- Withdrawal date and proof that downstream systems were updated

Consent Managers

A Consent Manager is a Board-registered platform that lets people give, manage, review and withdraw consent across many businesses from one place. It must be a company incorporated in India with a net worth of at least ₹2 crore, act in a fiduciary capacity for the person, avoid conflicts of interest, keep consent records for at least seven years and be unable to read the personal data it helps share.[46] These provisions start on **13 November 2026.**

WHAT THE LAW REQUIRES	Standalone plain-language notice (Rule 3); valid consent (s. 6); withdrawal as easy as giving; business bears the burden of proof.
GOOD PRACTICE	Version-control every notice; test withdrawal end to end; decide early whether to accept consent through Consent Managers.
ILLUSTRATION	A bank's app shows a one-screen notice in Hindi or English, with separate unticked boxes for credit-card offers and partner insurance offers.

NOTES
41 DPDP Act, 2023, s. 5; DPDP Rules, 2025, Rule 3.
42 DPDP Act, 2023, s. 5(3).
43 DPDP Act, 2023, s. 6(1).
44 DPDP Act, 2023, s. 6(4)–(6).
45 DPDP Act, 2023, s. 6(10).
46 DPDP Rules, 2025, Rule 4 and First Schedule (Parts A and B).

Security Safeguards and Data Breaches

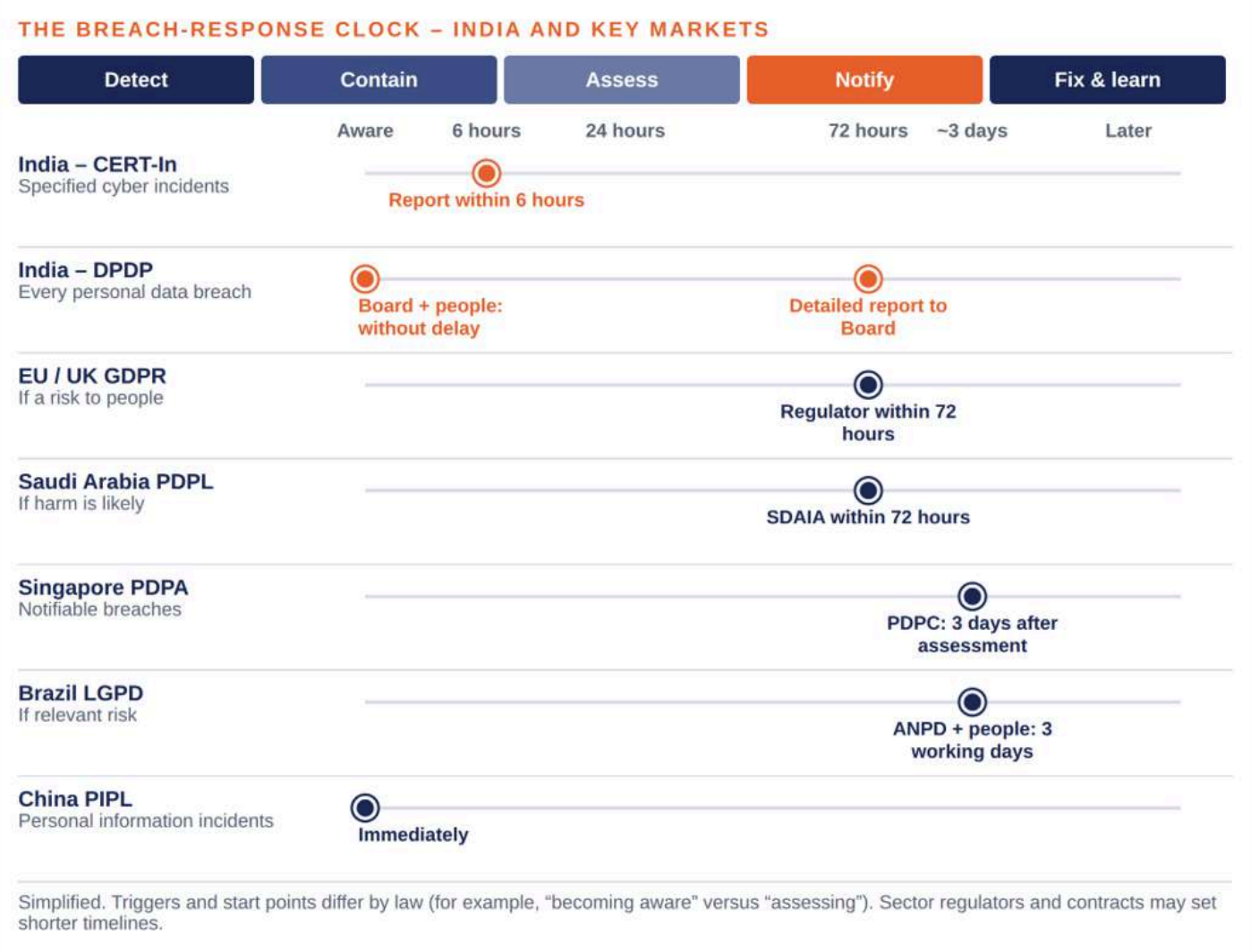
Every Data Fiduciary must protect personal data in its possession or control, including data held by its processors, by taking reasonable security safeguards to prevent a breach.[47] This duty carries the highest penalty band in the law: up to ₹250 crore per instance. Rule 6 sets out the minimum measures.[48]

Rule 6 minimum safeguard	What it means	Typical control
Encryption, obfuscation, masking or virtual tokens	Make data unreadable to anyone who should not see it.	Encrypt databases and laptops; mask ID and card numbers.
Access control	Only the right people can reach the data.	Role-based access, multi-factor login, quarterly reviews.
Visibility of access	Know who accessed what and when.	Logs, monitoring and alerts for unusual downloads.
Continuity	Data stays available even if systems fail or are attacked.	Backups, tested restoration, disaster recovery.
Log and data retention for one year	Keep logs and related data for at least a year to detect and investigate breaches, unless another law says otherwise.	Central log store or SIEM with one-year retention.
Processor contracts	Vendors must commit to the same safeguards.	Security clauses and audit rights.
Technical and organisational measures	People and process, not just technology.	Policies, training, secure development, patching.

What counts as a breach

A personal data breach is not only a cyber-attack. It includes any unauthorised processing, and any accidental disclosure, use, alteration, destruction or loss of access that affects the confidentiality, integrity or availability of personal data.[49] A lost laptop, a misdirected email, an ex-employee who still has access, a ransomware outage or a vendor's leak can all be breaches.





What must be reported, and to whom

To whom	When	What to include
Each affected person	Without delay, in clear and plain language, through their account or registered contact	What happened; likely consequences; what the business is doing; what the person can do to stay safe; contact details.
Data Protection Board – first intimation	Without delay	Description of the breach, including its nature, extent, timing, location and likely impact.
Data Protection Board – detailed report	Within 72 hours of becoming aware (or longer if the Board allows on request)	Updated facts; causes; mitigation; findings on who caused it; steps to prevent recurrence; report on notices sent to affected people.

Source: DPDP Act, s. 8(6); DPDP Rules, Rule 7.

Point	CERT-In Directions (IT Act)	DPDP Act and Rules
Regulator	CERT-In (under MeitY)	Data Protection Board of India
What is reported	Specified cyber incidents, whether or not personal data is involved	Any personal data breach, cyber or not
Deadline	Within 6 hours of noticing	Without delay; detailed report within 72 hours
Tell individuals?	Not required by the Directions	Yes, every affected person
Log retention	180 days, maintained in India	At least one year (Rules 6 and 8)

Source: CERT-In Directions under s. 70B(6) of the IT Act, 2000 (28 April 2022): cert-in.org.in.

Business Leaders Questions

If a serious incident happens at 11 pm tonight, do we know who owns it, who decides to notify, who writes to customers and who calls CERT-In, within minutes rather than days?



NOTES
41 DPDP Act, 2023, s. 5; DPDP Rules, 2025, Rule 3.
42 DPDP Act, 2023, s. 5(3).
43 DPDP Act, 2023, s. 6(1).
44 DPDP Act, 2023, s. 6(4)–(6).
45 DPDP Act, 2023, s. 6(10).
46 DPDP Rules, 2025, Rule 4 and First Schedule (Parts A and B).

Retention, Erasure and Individual Rights

How long can data be kept?

A business must erase personal data, and make its processors erase it, when the person withdraws consent or when the specified purpose is no longer being served, whichever is earlier, unless another law requires it to be kept.[50] For certain large platforms, the Rules set a fixed three-year inactivity period.

- 48-hour warning: at least 48 hours before erasure, the platform must tell the person their data will be erased unless they log in or make contact.
- Account access: data needed only to let the person access their account or virtual tokens need not be erased.
- One-year minimum: every Data Fiduciary must keep personal data, traffic data and processing logs for at least one year for purposes such as security and investigations, unless another law requires longer.[51]

Class of Data Fiduciary (Third Schedule)	Registered users in India	Erase after
E-commerce entity	2 crore or more	3 years from the person's last contact or use of rights (or from commencement of the Rules, if later)
Online gaming intermediary	50 lakh or more	Same 3-year period
Social media intermediary	2 crore or more	Same 3-year period

Practicle Example

"We keep everything because storage is cheap" is no longer a strategy. Every extra year of data kept is an extra year of breach exposure, and deletion must reach backups, email, spreadsheets, test systems and vendors too.sation, that did not become part of the final Act.

Individual rights

- The Act gives every Data Principal four rights and places five duties on them.[52]

Right	What the person can ask for	What the business must do
Access (s. 11)	A summary of their data and how it is processed; the identities of other Fiduciaries and Processors it was shared with, and what was shared.	Search all systems and provide a clear summary.
Correction and erasure (s. 12)	Correct, complete or update data; erase data no longer needed.	Update or erase in all connected systems unless law requires retention.
Grievance redressal (s. 13)	A readily available way to complain to the business.	Respond within the published period, not exceeding 90 days (Rule 14). The person must use this route before going to the Board.

Nomination (s. 14)	Nominate someone to exercise their rights on death or incapacity.	Provide a nomination facility.

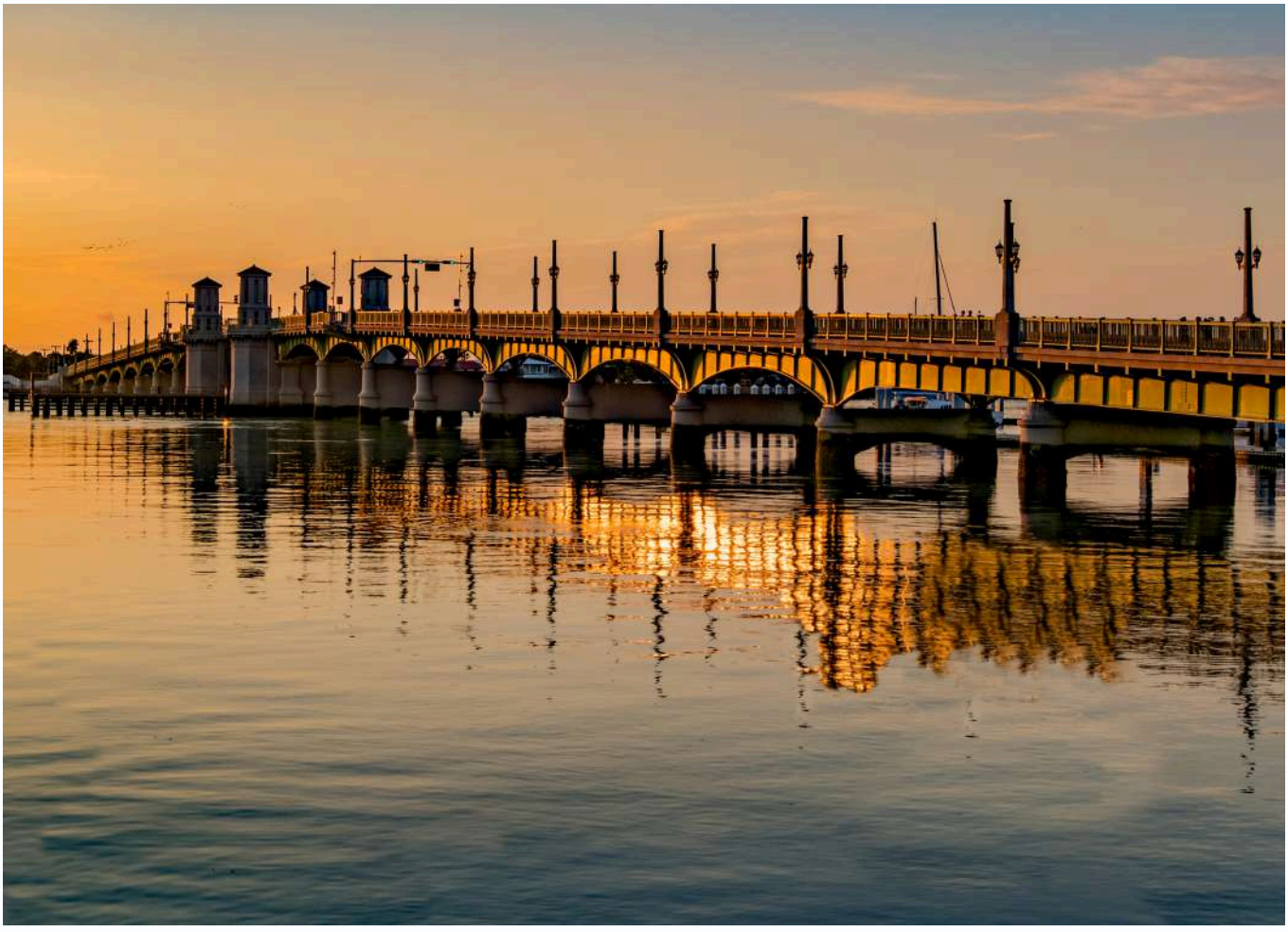
Duties of individuals (s. 15): follow the law; do not impersonate anyone; do not suppress material information for government documents; do not file false or frivolous complaints; give only verifiably authentic information when asking for correction. Breach can attract a penalty of up to ₹10,000.

In Simple Words

If a customer says "Please delete my account" or "What do you know about me?", that is a legal rights request, even if they never mention DPDP. Front-line staff must recognise and route it.

Making rights work in practice (Rule 14)

1. Publish how to make a request and which identifiers are needed (for example, customer ID).
2. Log every request with a case number and date.
3. Verify identity proportionately.
4. Route the request to every system and vendor that holds the data.
5. Check completeness and legal exceptions.
6. Reply within the published timeline and keep evidence.



NOTES
50 DPDP Act, 2023, s. 8(7)–(8).
51 DPDP Rules, 2025, Rule 8 and Third and Seventh Schedules.
52 DPDP Act, 2023, ss. 11–15.

Children, Persons with Disability and Significant Data Fiduciaries

Children and persons with disability

Under DPDP, **a child is anyone under 18,** a higher age than in most other laws. Before processing a child's data, the business must obtain verifiable consent of a parent. For a person with a disability who has a lawful guardian, the guardian's **verifiable consent is needed.** The business must not process data in a way likely to harm a child's well-being, and must not track, behaviourally monitor or target advertising at children.[53]

How consent is verified (Rule 10). The business must check that the person consenting is an identifiable adult. It can rely on reliable identity and age details it already holds (for example, a verified existing customer), details the parent provides, or a virtual token linked to identity and age issued by an authorised entity, such as a DigiLocker-based service.

Who or what is exempt from some child-data rules (Rule 12, Fourth Schedule)	Condition
Clinical and mental-health establishments; healthcare professionals	Only as needed to provide health services.
Educational institutions	For tracking and monitoring for educational activities or the child's safety.
Crèches and child day-care centres	For the safety of children in their care.
Transport services for children engaged by educational institutions or crèches	For tracking location during travel, for safety.
Specified purposes	For example: exercising legal powers, providing benefits, creating a user account limited to email, ensuring content is not harmful, confirming that a user is not a child.

Leadership Question

Even if our product is not meant for children, could under-18 still be using it? If yes, how do we check age and obtain verifiable parental consent?

Significant Data Fiduciaries (SDFs)

The Government can notify any Data Fiduciary, or a class of them, as a Significant Data Fiduciary.

It considers the volume and sensitivity of data, risk to people's rights, and effects on sovereignty, electoral democracy, security of the State and

public order.[54] No business can self-declare, and as at September 2026 no Significant Data Fiduciary had been publicly notified.

Practical Point

Large banks, insurers, telecom operators, big social-media and e-commerce platforms, and health-data businesses should prepare as if they may be notified. Building DPIA capability and independent audit arrangements takes months.



Extra duty for SDFs	Details
Data Protection Officer	Based in India; represents the SDF; responsible to the Board of Directors or similar body; point of contact for grievances.
Independent data auditor	Appoint an independent auditor to evaluate compliance.
Annual DPIA and audit (Rule 13)	Data Protection Impact Assessment and audit at least once every 12 months; report significant
Algorithmic due diligence (Rule 13)	Verify that technical measures, including algorithmic software, do not pose a risk to people's rights.
Localisation of specified data (Rule 13(4))	Ensure personal data specified by the Government, on a committee's recommendation, and related traffic data, is not transferred outside India.



NOTES
53 DPDP Act, 2023, s. 9; DPDP Rules, 2025, Rules 10–12 and Fourth Schedule.
54 DPDP Act, 2023, s. 10(1).

Cross-Border Transfers, Exemptions, Enforcement and Penalties

Sending data outside India

India follows a **negative-list** approach. Personal data may be transferred to any country **unless** the Government restricts transfers to that country by notification.[55] Rule 15 adds that transfers must meet any requirements the Government specifies about making data available to a foreign State or its entities. Any Indian law that gives **higher protection or restriction**, such as RBI's payment-data storage rule, continues to apply.[56] SDFs may also face localisation of specified data under Rule 13(4).

Keeping data in India does not by itself make processing lawful, and sending data abroad is not by itself unlawful.

Exemptions

Some situations are fully or partly exempt. Use exemptions carefully and document why they apply.[57]

Exemption (s. 17)	What is exempt	Example
Legal rights and claims	Processing needed to enforce a legal right or claim.	Using customer data to recover dues in court.
Courts and regulators	Processing by courts, tribunals and bodies with judicial or quasi-judicial functions.	A tribunal reviewing evidence.
Crime	Preventing, detecting, investigating or prosecuting offences.	A fraud investigation with police.
Foreign-contract data	Processing in India of data about people outside India under a contract with a foreign entity.	An Indian BPO serving a US client's customers.
Approved restructuring	Processing needed for a merger, demerger or similar scheme approved by a court, tribunal or competent authority.	Moving employee data in an approved merger.
Loan defaulters	Ascertaining financial information and assets of a person who has defaulted on a loan.	A lender tracing a defaulter's assets.
Notified State bodies; research	Notified State instrumentalities; research, archiving or statistics where no decision is taken about a specific person and Rule 16 standards are met.	An anonymised academic study.
Notified classes, including startups	The Government may exempt some businesses from ss. 5, 8(3), 8(7), 10 and 11.	A notified early-stage startup.

Approved restructuring	Processing needed for a merger, demerger or similar scheme approved by a court, tribunal or competent authority.	Moving employee data in an approved merger.
Loan defaulters	Ascertaining financial information and assets of a person who has defaulted on a loan.	A lender tracing a defaulter's assets.
Notified State bodies; research	Notified State instrumentalities; research, archiving or statistics where no decision is taken about a specific person and Rule 16 standards are met.	An anonymised academic study.
Notified classes, including startups	The Government may exempt some businesses from ss. 5, 8(3), 8(7), 10 and 11.	A notified early-stage startup.
Approved restructuring	Processing needed for a merger, demerger or similar scheme approved by a court, tribunal or competent authority.	Moving employee data in an approved merger.

Note For IT/ITES and GCCS

The foreign-contract exemption in s. 17(1)(d) is important for Indian service providers. It switches off many duties, but s. 8(1) (responsibility) and s. 8(5) (security safeguards) still apply, and client contracts will usually impose the foreign law's standards anyway.

How enforcement works

1. **Trigger:** a complaint (after using the business's grievance route), a breach intimation, a Government reference or a court direction.
2. **Inquiry:** the Board decides if there are grounds, then inquires as a digital office; it can summon people and inspect documents.[58]
3. **Alternatives:** the Board may refer parties to mediation or accept a voluntary undertaking from the business.[59]
4. **Order:** a penalty, directions, or closure of the case.
5. **Appeal:** to the Telecom Disputes Settlement and Appellate Tribunal (TDSAT) within 60 days.[60]

Breach (Schedule to the Act)	Maximum penalty per instance
Failure to take reasonable security safeguards to prevent a breach (s. 8(5))	Up to ₹250 crore
Failure to notify the Board or affected people of a breach (s. 8(6))	Up to ₹200 crore
Failure to meet additional obligations for children (s. 9)	Up to ₹200 crore
Failure to meet additional obligations of a Significant Data Fiduciary (s. 10)	Up to ₹150 crore

Breach of a voluntary undertaking accepted by the Board (s. 32)	Up to the penalty for the original breach
Breach of any other provision of the Act or Rules	Up to ₹50 crore
Breach of duties by a Data Principal (s. 15)	Up to ₹10,000

Source: DPDP Act, s. 33 and the Schedule. In deciding the amount, the Board considers the nature, gravity and duration of the breach, type of data, repetition, gain or loss avoided, mitigation and its timeliness, proportionality and likely impact of the penalty (s. 33(2)).

Blocking Risk

The foreign-contract exemption in s. 17(1)(d) is important for Indian service providers. It switches off many duties, but s. 8(1) (responsibility) and s. 8(5) (security safeguards) still apply, and client contracts will usually impose the foreign law's standards anyway.



NOTES
55 DPDP Act, 2023, s. 16(1).
56 DPDP Act, 2023, s. 16(2).
57 DPDP Act, 2023, s. 17.
58 DPDP Act, 2023, ss. 27–28; DPDP Rules, 2025, Rule 20.
59 DPDP Act, 2023, ss. 31–32.
60 DPDP Act, 2023, s. 29.

DPDP and Other Indian Laws

The DPDP Act is **in addition to** other laws, not a replacement. If there is a conflict, DPDP prevails to the extent of the conflict (DPDP Act, s. 38). Many businesses are also subject to cyber, sector, identity, consumer, tax, company and employment rules. Keep **one regulatory map** rather than running these as separate projects.

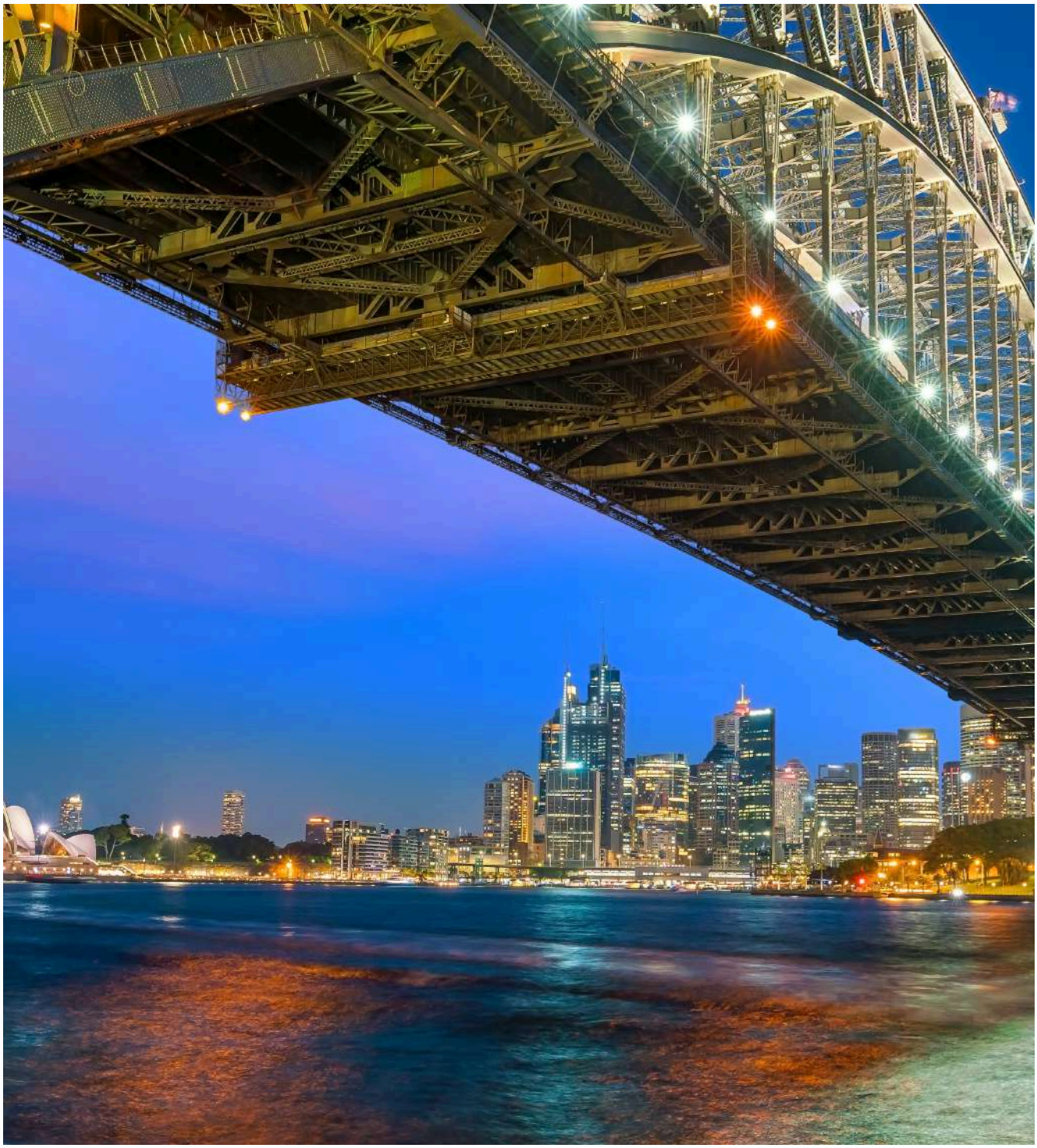
Law or regulation	How it interacts with DPDP
IT Act, 2000 and SPDI Rules, 2011	Section 43A (compensation for failing to protect sensitive data) is omitted when s. 44(2) of the DPDP Act comes into force on 13 May 2027; the SPDI Rules fall away with it.
CERT-In Directions, 2022	Continue to apply: 6-hour reporting of specified cyber incidents; ICT logs kept in India for a rolling 180 days.
Right to Information Act, 2005	Section 8(1)(j) amended by s. 44(3) of the DPDP Act (in force from 13 November 2025): personal information is exempt from disclosure.
RBI directions	Payment-data storage in India, IT outsourcing and cyber-security directions continue; stricter rules prevail (s. 16(2)).
SEBI and IRDAI frameworks	SEBI's Cybersecurity and Cyber Resilience Framework (2024) and IRDAI's cyber-security guidelines continue for regulated entities.
Telecommunications Act, 2023	Subscriber-data, interception and security duties for telecom entities.
Aadhaar Act, 2016	Specific limits on collecting, storing and sharing Aadhaar numbers and biometrics.
Consumer Protection Act, 2019; health data (ABDM)	Unfair trade practices, dark-patterns guidelines and e-commerce grievance duties; consent-based health-data exchange under the Ayushman Bharat Digital Mission.
Company, tax and labour laws	Set minimum retention periods that override erasure duties for those records.

One incident, several reporting routes

One ransomware attack on a bank's vendor could trigger a CERT-In report, a DPDP intimation, an RBI report and foreign notifications. Build **one incident record** and a decision tree that identifies all routes at once.

Leadership Question

Can our incident team identify DPDP, CERT-In, sector and foreign reporting duties from the same playbook, without starting a new legal analysis at the time of the incident?



GLOBAL FIRM.

THAT UNLOCKS VALUE FOR Global Business.



What we do

- Global Tax & Compliance
- Global Transfer Pricing
- AI & Cyber Security
- Risk Advisory
- Accounting Outsourcing
- Advisory & Strategy
- Assurance & IT Audit
- Technology & Data Analytics

Ready to go global ? contact@sw-india.com www.sw-india.com LinkedIn: sw-india