Two regimes, one data estate: governing the EU GDPR and India’s DPDP at once

A multinational with a mature GDPR programme already holds roughly seventy per cent of what India’s DPDP demands. The remaining thirty per cent is where the money and the risk sit, because the divergences are structural rather than cosmetic.

Cambridge Cyber International | 6 June 2026

The General Data Protection Regulation has been directly applicable across the European Economic Area since 25 May 2018. India’s Digital Personal Data Protection Act 2023 received presidential assent in August 2023 but lay dormant pending subordinate rules. Those rules, the Digital Personal Data Protection Rules 2025, were notified on 13 November 2025, triggering a phased commencement: the Data Protection Board provisions took effect immediately, registration duties for Consent Managers follow at the one-year mark, and the substantive obligations and data-principal rights become enforceable from 13 May 2027 (Ministry of Electronics and Information Technology 2025; Shardul Amarchand Mangaldas 2025). What follows therefore contrasts a mature, fully enforced regime with a young one that is legally complete but operationally still inside its compliance runway. The status of the law is stated as at 6 June 2026, which leaves roughly eleven months before the DPDP’s substantive duties and data-principal rights become enforceable on 13 May 2027. For a programme that must re-base lawful processing on consent, integrate a Consent Manager and stand up an under-eighteen regime, eleven months is a single planning horizon, not a comfortable margin.

The shared ancestry, and the three divergences that matter

The two laws share a common ancestry. India’s drafters borrowed the GDPR’s vocabulary of accountability, purpose limitation, data minimisation and consent, and the resemblance is close enough that a multinational with a working GDPR programme already holds roughly seventy per cent of what the DPDP demands. The remaining thirty per cent is where the money and the risk sit, because the divergences are structural rather than cosmetic.

Three differences dominate everything else. First, lawful processing: the GDPR offers six lawful bases including the elastic legitimate-interests balancing test, whereas the DPDP recognises only consent and a closed list of enumerated legitimate uses, leaving no general-purpose fallback when consent is impractical. Second, the rights catalogue: the GDPR grants eight data-subject rights including portability, objection and protection against solely automated decisions, while the DPDP grants a narrower set and adds an idiosyncratic right of nomination. Third, the enforcement economics: the GDPR caps fines at the greater of twenty million euro or four per cent of worldwide annual turnover and gives individuals a private right to compensation, whereas the DPDP imposes fixed monetary penalties up to two hundred and fifty crore rupees with no turnover linkage, no criminal liability and no private right of action.

For the dual-subject organisation the practical lesson is that GDPR compliance is necessary but not sufficient. A GDPR-grade programme must be extended, not merely copied, to absorb the DPDP’s consent-first architecture, its under-eighteen children’s regime, its negative-list approach to cross-border transfers and its breach-notification rule that tolerates no risk threshold.

Two numbers frame the stakes. The GDPR governs the personal data of roughly four hundred and fifty million people across the European Economic Area; the DPDP governs that of nearly one and a half billion data principals in India, about three times as many. So although the

DPDP's per-instance penalty ceiling is lower and fixed, the operational load it imposes, consent capture and withdrawal, rights handling and no-threshold breach notification, runs at a far larger population scale. Capacity that is comfortable for a European user base can be overwhelmed by an Indian one, and that capacity has to be built before the clock runs out: with the substantive duties enforceable from 13 May 2027, roughly eleven months from the date of writing, the window to engineer consent, rights and breach pipelines for a billion-plus principals is narrow.

Instruments, status and regulatory architecture

The GDPR is a regulation, meaning it applies directly in every Member State without national transposition, although Member States retain limited room to legislate on specific points such as the age of digital consent and employment data. It is enforced by a network of independent national Supervisory Authorities coordinated through the European Data Protection Board, with the consistency mechanism and the one-stop-shop resolving cross-border cases. Rulemaking, guidance and enforcement thus sit with independent regulators and, ultimately, the courts and the Court of Justice of the European Union (our GDPR framework page summarises its obligations, who it binds and the official source in brief).

The DPDP architecture is more centralised and more executive-led. The DPDP Act is primary legislation; the operational detail lives in the DPDP Rules, which the Central Government makes and can amend (our DPDP framework page sets out the act's key obligations, who it binds and the official source in brief). The Data Protection Board of India is the adjudicatory body, but it is narrower than a European Supervisory Authority: it investigates breaches and imposes penalties yet does not issue binding codes or guidance, and substantive rulemaking power rests with the Central Government rather than the Board. Appeals from the Board run to the Telecom Disputes Settlement and Appellate Tribunal. The design consequence is that, in India, the political executive retains levers (exemptions, transfer restrictions, rule amendments) that in Europe sit with independent authorities or courts.

Scope and reach

The GDPR governs personal data processed wholly or partly by automated means, and non-automated processing where the data form or are intended to form part of a filing system. It carves out a special category of sensitive data under Article 9: racial or ethnic origin, political opinions, religious beliefs, trade-union membership, genetic and biometric data, health, and sex life or orientation, each subject to heightened conditions. The DPDP is narrower in one respect and flatter in another. It governs only digital personal data, that is, data in digitised form or data collected on paper and then digitised, and it does not regulate purely non-digital records. Critically, it draws no statutory distinction between ordinary and sensitive personal data. There is no special-category tier; health records and shopping histories sit under the same baseline rules, with extra protection arriving only indirectly through the Significant Data Fiduciary mechanism and the children's provisions. For a dual-subject organisation this asymmetry cuts both ways: Indian law imposes no Article 9 conditions, but a mature controller will usually keep its GDPR sensitive-data controls in place globally rather than maintain two data-classification schemes.

Both laws reach beyond their home territory. The GDPR, under Article 3, applies to processing in the context of an EU establishment regardless of where processing occurs, and to controllers outside the Union that offer goods or services to, or monitor the behaviour of, individuals in the Union. The DPDP, under section 3, applies to processing of digital personal data within India, and to processing outside India where it is in connection with offering goods or services to data principals in India. The DPDP omits the GDPR's explicit monitoring-of-behaviour limb, so pure profiling of Indian residents without an offer of goods or services sits in a greyer zone than its European equivalent.

Dimension	GDPR	DPDP
Form of data covered	Automated, plus structured manual filing systems	Digital only (born-digital or subsequently digitised)

Dimension	GDPR	DPDP
Sensitive-data tier	Yes (Article 9 special categories)	No statutory tier
Extraterritorial trigger	Establishment; offering; monitoring behaviour	Offering goods or services to principals in India
Excluded processing	Purely personal or household; law enforcement under a separate directive	Personal or domestic; certain published data; broad state exemptions

Actors and vocabulary

The role architecture maps cleanly enough that translation is mostly one-to-one, which helps when drafting bilingual policies. The GDPR controller becomes the DPDP Data Fiduciary, a trust-based framing whose operative obligations nonetheless resemble those of a controller. The GDPR processor becomes the Data Processor, though the DPDP routes most processor duties through the fiduciary's contract rather than imposing many direct statutory duties. The data subject becomes the Data Principal, and for a child the principal is the child while consent is exercised by a parent or lawful guardian. The Supervisory Authority finds its analogue in the Data Protection Board of India, which adjudicates and penalises but does not issue binding guidance and is therefore not a full-spectrum regulator. Two DPDP roles have no GDPR counterpart: the Significant Data Fiduciary, a government-designated class carrying heightened duties, and the Consent Manager, an India-specific registered intermediary through which principals grant, review and withdraw consent.

Lawful processing: the central divergence

This is where the two regimes part company most consequentially. The GDPR, under Article 6, provides six lawful bases: consent, performance of a contract, compliance with a legal obligation, protection of vital interests, performance of a task in the public interest, and the controller's or a third party's legitimate interests subject to a balancing test against the data subject's rights. The legitimate-interests basis is deliberately open-textured; it is the workhorse that lets organisations process data for fraud prevention, network security, direct marketing and intra-group administration without seeking consent for every operation.

The DPDP recognises only two routes to lawfulness: consent under section 6 and a closed list of certain legitimate uses under section 7. The legitimate-uses list is enumerated and finite: the voluntary provision of data by the principal for a specified purpose, state functions and the provision of subsidies or services, compliance with law or court orders, medical emergencies, employment-related purposes, and disaster or public-order situations, among a handful of others. There is no residual balancing test. If a processing activity does not map onto an item on the list, the only lawful path is consent. This is the single most important operational difference for a multinational, because data flows that Europe handles comfortably under legitimate interests, for example broad analytics, marketing enrichment or cross-border group reporting, may require an explicit consent architecture in India.

The consent standard itself is similar on paper. Both require consent to be free, specific, informed, unambiguous and signalled by clear affirmative action, and both require withdrawal to be as easy as giving. The DPDP layers two India-specific features on top. First, the notice that accompanies a consent request must be itemised and, on request, available in English or any of the languages in the Eighth Schedule to the Constitution. Second, consent may be mediated through a Consent Manager, a registered platform that gives principals a single dashboard to grant and revoke permissions across fiduciaries, an institutional construct with no GDPR equivalent.

> GDPR compliance is necessary but not sufficient. A GDPR-grade programme must be extended, not merely copied, to absorb the DPDP's consent-first architecture.

Rights, obligations and children

The GDPR confers a broad suite of rights: access, rectification, erasure, restriction of processing, data portability, objection including to direct marketing, the right not to be subject to a solely automated decision producing legal or similarly significant effects under Article 22, and the right to lodge a complaint with a Supervisory Authority. The DPDP confers a narrower set: access to a summary of personal data and processing, correction and erasure, grievance redressal, and a distinctive right of nomination that lets a principal designate another individual to exercise their rights in the event of death or incapacity. The gaps matter. The DPDP contains no standalone right to data portability, no general right to object, no right to restriction, and no Article 22-style protection against automated decision-making. Conversely, the right of nomination has no European counterpart.

Right	GDPR	DPDP
Access	Yes (Art 15)	Yes (summary of data and processing)
Rectification or correction	Yes (Art 16)	Yes
Erasure	Yes (Art 17)	Yes (on withdrawal or purpose completion)
Restriction of processing	Yes (Art 18)	No
Data portability	Yes (Art 20)	No
Objection	Yes (Art 21)	No
Safeguards on automated decisions	Yes (Art 22)	No
Grievance redressal	Via complaint to Supervisory Authority	Yes (statutory right against the fiduciary)
Nomination	No	Yes

Both regimes are built on accountability, but they distribute the heavier duties differently. Under the GDPR every controller carries a baseline of accountability documentation: records of processing activities under Article 30 with a small-organisation carve-out, data protection by design and by default under Article 25, a data protection impact assessment for high-risk processing under Article 35, and binding processor contracts under Article 28. A data protection officer is mandatory under Article 37 where the core activities involve large-scale systematic monitoring or large-scale processing of special-category data, and controllers outside the Union must appoint an EU representative under Article 27. The DPDP applies a lighter universal baseline and concentrates the heavy duties on the Significant Data Fiduciary. Every fiduciary must implement reasonable security safeguards, honour notice and consent, erase data on withdrawal or once the purpose is served, and ensure processor compliance through contract. Only entities the Central Government designates as Significant Data Fiduciaries must additionally appoint an India-based Data Protection Officer, engage an independent data auditor, and conduct periodic impact assessments and audits. The trigger is therefore governmental designation rather than the GDPR's self-assessed risk test.

Both regimes single out children, and here the DPDP is the stricter. The GDPR, under Article 8, sets the age of valid consent for information-society services at sixteen, permitting Member States to lower it to no less than thirteen. The DPDP treats anyone under eighteen as a child and requires verifiable parental or lawful-guardian consent before processing a child's data. It goes further by prohibiting processing likely to cause detrimental effects on a child's well-being, and by banning behavioural tracking, behavioural monitoring and targeted advertising directed at children outright, subject to limited exemptions the government may notify. For a global digital service this is a meaningful design constraint: an age-assurance and parental-consent layer calibrated to a thirteen-to-sixteen European threshold will not satisfy India's under-eighteen rule, and advertising-technology stacks must be able to switch off behavioural targeting for Indian minors at population scale.

Cross-border transfers: mirror-image defaults

The transfer models are almost mirror images in their default posture. The GDPR, in Chapter V, starts from prohibition: personal data may leave the EEA only under an adequacy decision, appropriate safeguards such as standard contractual clauses or binding corporate rules, or a narrow set of derogations. The burden is on the exporter to establish a lawful transfer mechanism, and the Schrems II jurisprudence requires a transfer impact assessment of the destination country's surveillance environment. This is a whitelist model: prohibition by default, permitted only where a mechanism is in place.

The DPDP starts from permission. Transfers are allowed to any country by default, and the Central Government may issue a negative list restricting transfers to specified jurisdictions. This is a blacklist model: permission by default, blocked only where a destination is named. In principle it is far more permissive, but two caveats temper that. First, no negative list has yet been populated, so the practical contours remain uncertain. Second, sectoral data-localisation rules, notably from the Reserve Bank of India for payment data, continue to apply on top of the DPDP and can be stricter than the general regime. For a multinational the asymmetry is stark: moving EU data to India requires a documented Article 46 mechanism, whereas moving Indian data to the EU currently requires nothing under the DPDP itself, though prudent governance keeps contractual safeguards in place either way.

Breach notification: the missing materiality filter

Both regimes converge on a seventy-two-hour clock but diverge sharply on threshold and audience. The GDPR requires notification to the Supervisory Authority without undue delay and, where feasible, within seventy-two hours of becoming aware, but only where the breach is likely to result in a risk to individuals' rights and freedoms; affected individuals are notified only where the risk is high. The risk threshold filters out trivial incidents. The DPDP Rules impose no risk threshold at all. On becoming aware of any personal-data breach the fiduciary must inform affected data principals without delay and must furnish the Data Protection Board with an initial intimation followed by a detailed report within seventy-two hours covering the breach, its circumstances, mitigation and the identity of any responsible party (MediaNama 2025; Ministry of Electronics and Information Technology 2025). The absence of a materiality filter means Indian breach-reporting volumes will run higher than their European equivalents, and against a population of nearly one and a half billion principals the notification machinery must scale accordingly. Incident-response runbooks tuned to the GDPR's risk gate must be re-papered to notify every qualifying breach to both the Board and the affected individuals.

Aspect	GDPR	DPDP
Authority notification	Within 72 hours, if risk to rights	Initial intimation, then detailed report within 72 hours, no threshold
Individual notification	Only if high risk	Always, without delay
Materiality filter	Yes (risk-based)	None

Enforcement economics

The enforcement economics differ in kind, not just degree. The GDPR's administrative fines run up to ten million euro or two per cent of worldwide annual turnover for the lower tier, and up to twenty million euro or four per cent of worldwide annual turnover for the higher tier, whichever is greater. The turnover linkage scales the deterrent to the size of the undertaking. The GDPR also creates a private right: data subjects may seek compensation for material and non-material damage under Article 82, and may lodge complaints and pursue judicial remedies. The DPDP imposes fixed monetary penalties untethered to turnover, set by reference to schedules and capped per instance: up to two hundred and fifty crore rupees for failure to take reasonable security safeguards, up to two hundred crore rupees for failures in breach notification or in children's-data obligations, and lower ceilings for other defaults. There is no criminal liability under the DPDP and, importantly, no private right of action and no statutory compensation to individuals; enforcement runs through the Data Protection Board, with

penalties paid to the state. The DPDP also introduces penalties on data principals for filing false or frivolous complaints, which has no GDPR analogue. The net effect is that, for a very large enterprise, the GDPR's turnover-based ceiling can dwarf the DPDP's fixed cap, while for the same enterprise the DPDP removes the class-action and individual-litigation exposure that shadows GDPR compliance in Europe.

Exemptions

The GDPR keeps exemptions narrow and rule-bound. Article 23 lets Member State law restrict rights only where necessary and proportionate for enumerated public-interest objectives, and there are specific carve-outs for journalism, academic, artistic and literary expression, and for research and archiving subject to safeguards. The DPDP grants broader and more executive-controlled exemptions. Section 17 allows the Central Government to exempt state instrumentalities from most of the Act in the interests of sovereignty, security, public order and friendly relations, and provides exemptions for processing necessary for research, archiving or statistical purposes, for certain start-ups by notification, and for the enforcement of legal rights. The width of the state-facing exemptions, and the fact that they are conferred and bounded by the executive rather than by an independent authority or court, is one of the most debated features of the Indian regime and a recurring theme in civil-society commentary (Internet Freedom Foundation 2025).

Which controls a dual-subject programme must add

For an organisation inside both regimes, the operating model is convergence with deliberate divergence. The pragmatic architecture is to run a single, GDPR-grade global baseline and bolt on India-specific modules rather than maintain two independent programmes. The reusable GDPR assets are substantial: the records of processing, the security and breach-response controls, the data-subject-rights tooling for access, correction and erasure, the processor-contracting templates and the privacy-by-design discipline all transfer to the DPDP with minor adaptation. The India-specific additions are where effort concentrates, and they are precisely the controls a GDPR-only programme will be missing on the 13 May 2027 enforcement date: a consent-first lawful-basis design that does not lean on legitimate interests; integration with or readiness for a Consent Manager; an under-eighteen children's regime with verifiable parental consent and behavioural-advertising suppression; a nomination workflow; a breach process that notifies every qualifying incident with no risk gate; and a watch on the government's cross-border negative list and sectoral localisation rules. Conversely, the organisation cannot retire any GDPR machinery, because the DPDP's narrower rights set and permissive transfer model do not relax European duties.

What CCI's tooling changes

A dual-regime programme fails most often not on policy but on not knowing, in evidence terms, where personal data sits, which lawful basis each flow relies on, and what an enforcement event would cost. CCI's primitives attack exactly those gaps, and each claim below is a likelihood-reduction supported by an existing product rather than a guarantee.

NetDiagramer maps the actual data estate, the flows between systems and the jurisdictions each flow crosses. For the transfer problem this is foundational: you cannot apply the GDPR's whitelist of Article 46 mechanisms or watch the DPDP's blacklist if you cannot see which flows leave the EEA or land in India. The same topology surfaces every flow currently leaning on legitimate interests, which is the precise population that must be re-based on consent before the DPDP bites.

EviGen turns accountability from a documentation exercise into automated evidence. Records of processing under Article 30, consent ledgers, and the impact-assessment and audit artefacts a Significant Data Fiduciary must produce are generated and kept current from the live estate rather than reconstructed from spreadsheets at audit time. One evidence pipeline serves both the European records duty and the Indian accountability and audit duties.

Evidence Vault gives the breach process the tamper-evident timeline it needs to survive the DPDP's no-threshold rule. When every qualifying incident must reach the Board within

seventy-two hours and every affected principal without delay, the constraint is not willingness but the ability to assemble a defensible account of what happened, when and to whom, fast. The same vault satisfies the GDPR's Article 33 and 34 record-keeping.

cVaR prices the divergent enforcement economics in money. It quantifies exposure under both ceilings, the GDPR's turnover-linked four per cent and the DPDP's fixed two hundred and fifty crore per instance, so a board sees its dual-regime penalty surface as a single number rather than two legal abstractions, and can rank remediation by expected loss reduction.

Domain Separation keeps the European and Indian data estates logically separable, so localisation requirements, a future negative list and the differing lawful-basis regimes can be enforced per jurisdiction without forking the whole programme into two. It is the control that makes convergence-with-deliberate-divergence operable rather than aspirational.

Getting the dual mandate stood up in time

The DPDP's substantive duties land on 13 May 2027. From the date of writing that is about eleven months, which reads as distant and is not: a consent-first re-architecture, a Consent Manager integration and an under-eighteen regime are multi-quarter programmes, and they run in series more often than in parallel because each depends on a clean view of the data estate that most organisations do not yet have. Counting backward from May 2027, the discovery and data-mapping work has to begin this quarter for the build, test and audit phases to fit before enforcement. Where an organisation needs senior privacy leadership to drive that build without adding permanent headcount, CCI's CISO-as-a-Service offers a pool of eight or more CISSP-certified practitioners for interim, fractional, on-call or post-incident cover, with independence preserved because CCI does not audit where it leads. That pool is not Europe-only: CCI has India-based CISSP-certified practitioners, senior data-privacy specialists who know the DPDP, the Consent Manager model and the Eighth Schedule language obligations from the inside. That matters in practice, because a Significant Data Fiduciary must appoint an India-domiciled Data Protection Officer, and a local privacy lead also shortens the distance to Indian counsel, the Data Protection Board and the realities of consent at national scale.

The other recurring gap is foundational rather than legal: most organisations cannot say, in evidence, where their personal data actually sits. CCI's data-inventory specialists map exactly that across legacy estates, hot data in live systems and cold data in archives and backups, structured records in databases and the far harder unstructured sprawl in documents, mailboxes, file shares and object stores. That inventory is the precondition for everything downstream, the consent re-basing, the rights and erasure workflows, the cross-border transfer view and the breach-scope assessment, none of which can be trusted if the map of the estate is incomplete. Where the gap is bespoke tooling, the in-house R&D team, the academics, doctoral researchers and engineers who built NetDiagramer, EviGen, cVaR and DORA-MAST, can compose those primitives, inventory ingestion, configuration evidence, topology mapping and quantification, into a rapid dual-regime readiness toolset. That is stated as capability, with the shipped products as the proof, not as a stopwatch promise. To scope a dual-regime readiness assessment, talk to a practitioner.

Side-by-side master matrix

Dimension	GDPR	DPDP
Instrument	Regulation (EU) 2016/679	DPDP Act 2023 + DPDP Rules 2025
In force	25 May 2018	Phased; substantive duties from 13 May 2027
Data covered	Automated and structured manual; sensitive tier	Digital only; no sensitive tier
Extraterritorial trigger	Establishment; offering; monitoring	Offering goods or services to principals in India
Lawful bases	Six, including legitimate interests	Consent plus closed list of legitimate uses

Dimension	GDPR	DPDP
Sensitive-data regime	Article 9 special categories	None (indirect via SDF and children)
Children's age	16 (Member States may lower to 13)	Under 18; behavioural-advertising ban
Rights	Eight, including portability, objection, Art 22	Access, correction, erasure, grievance, nomination
Data protection officer	Risk-based mandatory	Significant Data Fiduciaries only; India-based
Cross-border model	Whitelist (prohibition by default)	Blacklist (permission by default)
Breach notice	72h to SA if risk; individuals if high risk	72h to Board plus all affected principals, no threshold
Maximum penalty	EUR 20m or 4% of global turnover	INR 250 crore per instance, no turnover link
Private right of action	Yes (Art 82)	None
Regulator	Independent Supervisory Authorities	Data Protection Board (adjudicatory only)
Rulemaking	EDPB, Commission, Supervisory Authorities	Central Government

Acronyms

Acronym	Expansion
BCR	Binding Corporate Rules
CJEU	Court of Justice of the European Union
DPDP	Digital Personal Data Protection
DPIA	Data Protection Impact Assessment
DPO	Data Protection Officer
EDPB	European Data Protection Board
EEA	European Economic Area
GDPR	General Data Protection Regulation
MeitY	Ministry of Electronics and Information Technology (India)
RBI	Reserve Bank of India
SA	Supervisory Authority
SCC	Standard Contractual Clauses
SDF	Significant Data Fiduciary
TDSAT	Telecom Disputes Settlement and Appellate Tribunal

References

European Parliament and Council (2016). Regulation (EU) 2016/679 (General Data Protection Regulation). https://eur-lex.europa.eu/eli/reg/2016/679/oj

Government of India (2023). The Digital Personal Data Protection Act, 2023. https://www.meity.gov.in/static

Ministry of Electronics and Information Technology (2025). Government notifies DPDP Rules to empower citizens and protect privacy. Press Information Bureau. https://www.pib.gov.in/PressReleasePa

Ministry of Electronics and Information Technology (2025). Digital Personal Data Protection Rules, 2025 (notification). https://static.pib.gov.in/WriteReadData/specificdocs/documents/2025/nov/doc20

Shardul Amarchand Mangaldas & Co (2025). Enforcement of the DPDP Act and notification of the DPDP Rules. https://www.amsshardul.com/insight/enforcement-of-the-dpdp-act-and-notification-of-the-dpdp-rules/

MediaNama (2025). Data breach reporting timeline of DPDP Rules 2025 explained. https://www.medianama.com/2025/11/223-data-breach-reporting-timeline-of-dpdp-rules-2025-explained/

Internet Freedom Foundation (2025). Statement on DPDP Rules 2025. https://internetfreedom.in/

India Briefing (2025). Digital Personal Data Protection (DPDP) Rules 2025 notified. https://www.india-briefing.com/news/dpdp-rules-2025-india-data-protection-law-compliance-40769.html