INDIA JURIS
International Law Firm

Digital Data Protection

CONTENTS

INTRODUCTION

For most of its life, India's Digital Personal Data Protection Act, 2023 ("DPDP Act") was a law without an engine. Parliament passed it and the President assented to it in August 2023, but for two years it sat without the rules needed to make its obligations operational, without a functioning regulator, and without a compliance clock running against anyone. That changed on 13 November 2025, when the Ministry of Electronics and Information Technology ("MeitY") notified the Digital Personal Data Protection Rules, 2025 ("DPDP Rules"), following consultations held across seven cities and thousands of public submissions.

2026 has been the year that notification turned into practice. The Data Protection Board of India ("DPBI") has been constituted. A phased, eighteen-month compliance timeline is now running, with deadlines falling through late 2026 and into May 2027. Courts, meanwhile, have not waited for the statute to catch up: the Delhi High Court's decision on the right to be forgotten shows judges filling gaps the Act does not address. This publication surveys the major legal developments shaping data protection in India in 2026: the phased rollout of the DPDP Rules, the parallel breach-reporting regimes businesses must now navigate, the judicial evolution of the right to be forgotten, and the unresolved questions around cross-border data transfer and enforcement readiness.

THE DPDP RULES, 2025: A LAW GETS ITS ENGINE

The Digital Personal Data Protection Act, 2023 set out the framework: it defines personal data, creates the roles of "Data Fiduciary" (the entity that decides why and how personal data is processed) and "Data Principal" (the individual to whom the data belongs), and lists obligations around consent, notice, and data security. What it left to delegated legislation was the operational detail, and it is the DPDP Rules, 2025 that now supply it. MeitY's consultation process before finalising the Rules was extensive. Draft rules were opened for public comment, and in-person consultations were held in Delhi, Mumbai, Guwahati, Kolkata, Hyderabad, Bengaluru, and Chennai. Startups, MSMEs, industry associations, civil society groups, government departments, and individual citizens together contributed 6,915 inputs during the process, which MeitY has described as shaping the final text.

Some parts of the Act and Rules came into force immediately on notification. Chief among these are the provisions establishing the Data Protection Board of India under Section 18 of the Act, including its digital-first functioning and institutional set-up. The Board is therefore legally constituted, with its chairperson and members appointed and its headquarters in the National Capital Region. But legal existence is not the same as full operational readiness as an adjudicatory body, and industry commentary has been careful to draw that distinction through 2026.

The remaining obligations are being phased in over eighteen months from notification. Consent Manager registration requirements, for entities that wish to operate as intermediaries managing an individual's consent across multiple platforms, fall due at roughly the twelve-month mark, around November 2026. The bulk of substantive Data Fiduciary obligations, covering notice content, consent architecture, data principal rights such as access, correction and erasure, and grievance redressal, along with the Board's power to impose penalties, become fully enforceable at the eighteen-month mark, around May 2027. Significant Data Fiduciaries, a category the Central Government designates by separate notification for entities processing especially large volumes or particularly sensitive categories of personal data, face additional duties: appointment of a Data Protection Officer based in India, annual independent data audits, and periodic data protection impact assessments.

The stakes for getting this compliance work done are considerable. Penalties under the DPDP Act can reach up to two hundred and fifty crore rupees for a single serious violation, calibrated to the nature, gravity, and duration of the breach and the entity's response to it. For most businesses operating in India, or serving Indian users from abroad, 2026 is therefore best understood as what several compliance advisories have called a "build year": the period to map personal data flows, stand up consent and rights-management systems, and prepare for audits, before the Board's penalty powers become fully live.

The extraterritorial reach of the Act is worth flagging for any client with cross-border operations. The DPDP Act applies not only to processing of digital personal data within India, whether collected online or digitised after offline collection, but also to processing by entities located outside India where that processing is connected with offering goods or services to individuals in India, or with profiling such individuals. A foreign SaaS company with an Indian user base, in other words, is squarely within scope even if it has no Indian corporate presence.

BREACH NOTIFICATION: TWO REGULATORS, TWO CLOCKS

One of the more demanding features of the new framework is that India now runs two parallel, overlapping breach-reporting regimes, and organisations operating here need to satisfy both.

The first is the Indian Computer Emergency Response Team ("CERT-In") framework under its Directions of 28 April 2022, issued under the Information Technology Act, 2000. Directions require specified categories of cyber incidents, including ransomware attacks, data breaches, identity theft, unauthorised access, website defacement, and attacks on critical infrastructure, to be reported to CERT-In within six hours of the entity noticing them.

Directions also require ICT system logs to be maintained for one hundred and eighty days, and mandate that such logs be stored within India.

The second is the data-protection-specific regime under Section 8(6) of the DPDP Act and the DPDP Rules, which is aimed at protecting individual privacy rather than at cybersecurity incident management as such. Under this regime, a Data Fiduciary must notify the Data Protection Board of India without delay upon becoming aware of a personal data breach, and must follow up with a more detailed report within seventy-two hours. Separately, and just as importantly, the Data Fiduciary must also notify each affected Data Principal directly, describing the incident, its likely consequences, and the steps being taken to address it.

A feature that surprises many organisations used to European practice is that the DPDP Act, unlike the EU's General Data Protection Regulation, does not currently build in a risk-based threshold for reporting. GDPR allows a controller to avoid notifying a breach that is unlikely to result in a risk to individuals. India's framework, as presently drafted, does not draw that distinction between major and minor incidents, which means organisations may need to over-report even comparatively minor incidents in order to stay compliant, rather than exercising the kind of materiality judgment that is common practice elsewhere.

The practical risk this creates was illustrated in October 2025, when a global communications platform with more than two hundred million active users disclosed a significant breach that did not originate in its own systems at all. An attacker had instead compromised a third-party customer service provider, gaining access to a support ticket queue containing sensitive customer information. The episode is a reminder that under the DPDP framework, a Data Fiduciary's breach-notification exposure extends to the conduct of its vendors and processors, not merely its own infrastructure

The Data Protection Board's enforcement toolkit, once fully operational, is broad. It can investigate complaints from individuals whose rights have not been respected, demand information from entities, conduct inquiries, direct urgent remedial or mitigation measures following a breach, and impose financial penalties calibrated to the violation. It can also refer disputes for alternative dispute resolution, accept voluntary undertakings from Data Fiduciaries in lieu of a full inquiry, and, in serious cases, recommend that the government block access to a non-compliant platform.

COURTS FILL THE GAP: THE RIGHT TO BE FORGOTTEN

Not every question in Indian data protection law has waited for a statute. The right to be forgotten, the idea that an individual can ask for old, outdated, or no-longer-relevant personal information to be delinked from name-based searches, has developed almost entirely through case law, since neither the DPDP Act nor the Rules codify it directly.

Its constitutional roots trace back to the Supreme Court's nine-judge bench decision in Justice K.S. Puttaswamy v. Union of India (2017), which recognised privacy, including informational privacy, as a fundamental right flowing from Article 21 of the Constitution. In his concurring opinion in that case, Justice Sanjay Kishan Kaul explored the idea of a right to erasure, drawing on the European Union's General Data Protection Regulation, though those observations were expressly exploratory rather than a binding rule.

In the years since, High Courts have taken inconsistent positions. The Karnataka High Court, in Sri Vasunathan (2017), permitted redaction of a petitioner's daughter's name from court records, treating the right to be forgotten as an evolving principle to be balanced against modesty and privacy in a sensitive case. The Madras High Court partially recognised the right in 2021 by directing That a petitioner's name be removed from an acquittal judgment is a position a Division Bench affirmed in 2024. The Gujarat High Court took the opposite view in Dharanraj Bhanushankar Dave (2017), declining to order removal of non-reported judgments from search engines on the ground that their publication did not infringe any fundamental right. This left the law genuinely unsettled going into 2026, with courts applying a similar constitutional foundation to reach different outcomes.

The most significant development this year came from the Delhi High Court. In a 144-page order delivered on 29 May 2026 in a batch of more than thirty petitions, Justice Sachin Datta addressed claims from individuals who had been acquitted, discharged, or were otherwise parties to concluded proceedings, whose names nonetheless continued to surface prominently in search results tied to old court documents and accusations. The Court held that the right to a dignified life and personal liberty under Article 21 includes a right to leave behind the record of failed or concluded proceedings, and that this right operates even against private commercial entities, not merely the state. Rather than ordering deletion of judicial records outright, the Court endorsed de-indexing as the practical remedy: removing records from name-based search results while leaving the underlying judgment accessible through case numbers, citations, or direct court records. In some circumstances, the order extended to global de-indexing. The judgment also set out what commentators have called a structured proportionality test, requiring that continued retention or indexing of a record serve a legitimate purpose, weighed against the harm to the individual's privacy and dignity.

The picture at the level of the Supreme Court is less settled. In a separate matter, the Supreme Court stayed a lower court order that had directed the removal of news reports and judicial records from the public domain on right-to-be-forgotten grounds, while acknowledging that Indian law already

recognises limited protection in sensitive categories of cases, such as those involving the modesty of women, without creating a general, freestanding right of erasure. A broader petition asking the Supreme Court to settle the contours of the right to be forgotten remains pending. Until that is resolved, the Delhi High Court's approach stands as the most detailed judicial framework available, but it is a High Court decision operating in a landscape the Supreme Court has not yet definitively mapped.

It is worth being precise about how this judicial right relates to the statutory scheme. The DPDP Act does give a Data Principal a right to correction and erasure of personal data under Section 12, but that right runs against a Data Fiduciary in respect of data the Data Principal supplied for a specific purpose, and it operates through the Fiduciary's own grievance process rather than through a court order directed at a search engine or a news publisher. It is a narrower, consent-linked tool, not a general mechanism for delinking old judgments or news coverage from a person's name. The right to be forgotten as the Delhi High Court has articulated it fills a distinct gap: it addresses information a person never supplied and has no contractual relationship over, such as a court judgment or a news report about them, which the DPDP Act's erasure right was never designed to reach. The two tracks are complementary rather than overlapping, and practitioners advising on reputation or record-clearing matters need to identify which one actually fits the client's situation.

CROSS-BORDER TRANSFERS AND THE COMPLIANCE COUNTDOWN

Unlike the European Union's adequacy-based model, which permits transfers only to jurisdictions the European Commission has approved as offering an equivalent level of protection, the DPDP Act takes a more permissive default position: cross-border transfer of personal data is generally allowed, except to countries the Central Government specifically restricts by notification. This is a narrower, blacklist-style restriction rather than a broad whitelist requirement, and it is one of the more business-friendly features of the Indian framework compared to its European counterpart.

That relative permissiveness does not mean transfers are unregulated. Significant Data Fiduciaries face heightened obligations regardless of where their processing occurs, including the appointment of an India-based Data Protection Officer, annual independent data audits, and periodic impact assessments, precisely because the volume or sensitivity of the data they hold raises the stakes of getting cross-border handling wrong. Sector-specific rules, particularly in financial services, also continue to impose their own data-localisation requirements independent of the DPDP framework.

Awareness remains a genuine obstacle to compliance on the ground. A PwC India survey found that only sixteen percent of Indian consumers say they understand the Digital Personal Data Protection law, and more than half report being unaware that they have any rights over their personal data at all. That gap matters for Data Fiduciaries too: notice and consent obligations are only meaningful if the individuals receiving them understand what they are agreeing to, and low public awareness increases the risk of complaints once the Board's enforcement powers are fully active.

For businesses, the practical guidance converging across the compliance advisory industry is consistent: use 2026 to build, not to wait. That means completing a data-mapping exercise to understand what personal data is held and why, standing up consent-management and rights-fulfilment systems capable of handling access, correction, and erasure requests, preparing breach-response playbooks that satisfy both the CERT-In six-hour and DPDP seventy-two-hour clocks, and, for larger organisations, beginning the process of appointing a Data Protection Officer and scoping an independent data audit well ahead of the Board's move to full enforcement around May 2027

A PRACTICAL CHECKLIST FOR THE BUILD YEAR

Advisories converging across the compliance industry point to a broadly similar set of priorities for organisations that have not yet started preparing. Setting these out plainly is more useful, at this stage, than restating the statute.

Map personal data flows across the organisation, including what is collected, why, where it is stored, and which third-party processors or vendors touch it.

Review and rewrite consent notices so they meet the DPDP Rules' requirements for clear, itemised, and specific information, rather than relying on bundled or pre-ticked consent.

Build a rights-fulfilment process capable of handling access, correction, and erasure requests from Data Principals within a reasonable timeframe.

Draft a breach-response playbook that satisfies both the CERT-In six-hour reporting clock and the DPDP Act's without-delay and seventy-two-hour requirements, and that accounts for breaches originating with vendors and processors, not only internal systems.

Review vendor and processor contracts to ensure data-processing obligations, audit rights, and breach-notification duties are passed down contractually, since liability under the Act does not stop at the Data Fiduciary's own systems.

Track Significant Data Fiduciary designations and sectoral notifications as they are issued, since obligations attach on notification rather than on a single fixed date for the whole economy.

WHAT THESE DEVELOPMENTS HAVE IN COMMON

Taken together, the developments surveyed in this publication point to a single underlying theme: India's data protection regime is being assembled in parallel, by different institutions, on different timelines, rather than arriving all at once from a single source. Parliament supplied the statute in 2023. The executive supplied the operational rules and the regulator only in November 2025, after a long gap in between. The judiciary, faced with individuals whose privacy interests could not wait for a statutory right to be forgotten, has stepped in to build one out of Article 21 case law, reaching results the Delhi High Court itself acknowledged were filling a legislative vacuum.

This creates a genuinely unusual compliance environment. A business operating in India today must track a statute that is only partially in force, a regulator that exists on paper but is still building out its adjudicatory capacity, two separate breach-notification clocks running on different triggers, and a body of privacy case law developing independently of, and in places ahead of, the statutory text. None of these tracks is static: the DPBI's enforcement posture once its full powers activate in 2027, the Supreme Court's eventual ruling on the right to be forgotten, and the pace at which Significant Data Fiduciaries are designated will each reshape the picture further.

The comparison to more mature regimes is instructive rather than flattering. The GDPR took effect as a single, fully operational instrument in 2018, backed by data protection authorities with years of prior enforcement experience under predecessor directives. India's framework, by contrast, is being built and tested in real time, with courts, regulators, and businesses all learning the shape of the law as they go. That is not necessarily a weakness: the phased approach gives businesses a genuine runway to prepare, and the judiciary's willingness to act, as in the Delhi High Court's May 2026 judgment, shows a system capable of protecting individual rights even where the legislature has not yet spoken. But it does mean that legal advice in this space carries an unusually short shelf life, and that compliance strategies need to be revisited as each phase of the DPDP Rules, each new Board ruling, and each appellate development comes into effect.

CONCLUSION

India's digital personal data protection law does not suffer from the kind of foundational uncertainty that has dogged Bitcoin's legal status elsewhere; the DPDP Act gives it a clear statutory basis, and 2026 has been the year that basis started to function as a working system. The Data Protection Board of India has been constituted. A phased timeline is now running toward full enforcement in May 2027. Courts have shown they will act where the statute is silent, as the Delhi High Court did on the right to be forgotten in May 2026. And businesses, regulators, and individuals alike are still learning to operate two breach-notification clocks, a developing body of privacy case law, and a compliance calendar that will keep adding deadlines through next year.

How the Data Protection Board approaches its first real enforcement actions, how the Supreme Court eventually resolves the right to be forgotten, and whether organisations meet the May 2027 compliance deadline will do more to define the practical shape of data protection in India than the text of the Act itself. For now, the clearest guidance available to any organisation handling personal data in India is to treat 2026 as the year to prepare, not the year to wait.

About India Juris

India Juris is a full-service international law firm providing comprehensive legal solutions to a diverse range of clients, including corporates, financial institutions, and individuals. With a strong focus on delivering practical and result-oriented advice, the firm combines deep legal expertise with a clear understanding of business needs across sectors.

Follow us on :

www.indiajuris.com

Our Offices

New Delhi
Lajpat Nagar-1 New Delhi
newdelhi@indiajuris.com

Gurugram
Sohna Road, Gurugram
gurugram@indiajuris.com

Bengaluru
Indira Nagar, Bengaluru
bengaluru@indiajuris.com

Mumbai
Andheri East, Mumbai
mumbai@indiajuris.com

GIFT CITY, Gujarat
Processing Area GIFT SEZ, GIFT CITY
giftcity@indiajuris.com