Navigating digital education in India: The DPDPA's role in building trust and privacy

April 2026

Education in India is evolving faster than ever before. As of 2025, there were 24.8 crore students, 14.72 lakh schools, 100 lakh teachers,[1] 1,150+ universities, and 45,000+ colleges.[2]

With the education sector experiencing transformation at an unprecedented scale with a CAGR of 23.28% during 2026–34, the online learning market is projected to touch $23.9 billion by 2034.[3]

As learning continues to shift towards digital ecosystems, trust emerges as a core pillar and privacy as a critical test to pass for all stakeholders. Against this backdrop, the Digital Personal Data Protection Act (DPDPA), 2023, becomes even more significant.

Due to digital education taking the front stage where minors are the primary data principals, compliance with the Digital Personal Data Protection Act (DPDPA) isn't just a mandate, it's a duty of care. Considering low awareness, vulnerable groups, and rising digital adoption, the education sector must lead the shift towards transparent, responsible, privacy-first learning environments.

Learners want to control their data. Educators must earn their trust. Regulators demand accountability, and the DPDPA ensures everyone is well prepared with a clear and enforceable framework.

EdTech companies, operating at scale and handling large volumes of sensitive learner data, may potentially be classified as Significant Data Fiduciaries under the DPDPA. While the law does not yet provide absolute clarity on thresholds, the nature and magnitude of data processed by large EdTech platforms places them firmly within the regulator's heightened lens of scrutiny..

Why DPDPA is a game-changer for the education sector

India's education sector processes some of the most sensitive and intimate data in the country where the stakes aren't just high—they include personally identifiable information of minors. Profiles, biometrics, behavioural patterns, chats—the education ecosystem touches data at its most personal. The list goes on.

The DPDPA essentially suggests that 'If you collect it [data], you justify it. If you store it, you secure it.' If a student or parent wants it deleted, you delete it.

Impact on the education sector

- No more hoarding of student data (clear purpose)
- Student/parental consent (verifiable, clear): Section 9(1) – Verifiable parental consent required before processing children's data
- Eliminating tracking, profiling, and ads for children:
  - Section 9(3) – Absolute ban on tracking, behavioural monitoring, and targeted advertising for children:

  During the COVID-19 pandemic when remote learning became the norm, institutions widely used AI-based proctoring tools which monitored students through webcams, tracked eye movement and behaviour, and generated automated suspicion scores. Investigations by the Electronic Frontier Foundation (EFF)[4] and other academic research show these practices caused heightened anxiety, stress, and fear of false accusations, particularly harming younger students and those with disabilities—illustrating real psychological harm from behavioural tracking. Such practices had adverse effects on children's well-being.

  - Section 9(2) – Prohibition on processing likely to cause harm to a child's well being:

  Global bodies like WHO and UNICEF have long warned about the risks of advertising aimed at children. While many education platforms block direct ads targeting users under 18, indirect pathways continue to exist. Such targeted exposure can pressure young minds, erode privacy, and exploit limited judgment, fostering impulsive buying, early materialism, and potential mental health concerns such as anxiety and low self-esteem.

1 Economic Survey 2024 25, Press Information Bureau (PIB), Govt. of India
2 AISHE 2021-2022 report, released in January 2024
3 ET Education
4 Electronic frontier foundation

Compliance isn’t optional

Under the act, violations involving the mishandling of children’s personal data attract fines of up to ₹200 crore to prevent harm and mandatory consequences designed to strongly deter profiling, tracking, or unsafe processing of minors’ data.[5]

GDPR taught the world a simple lesson: privacy fines aren’t merely symbolic—they can have significant operational impacts.

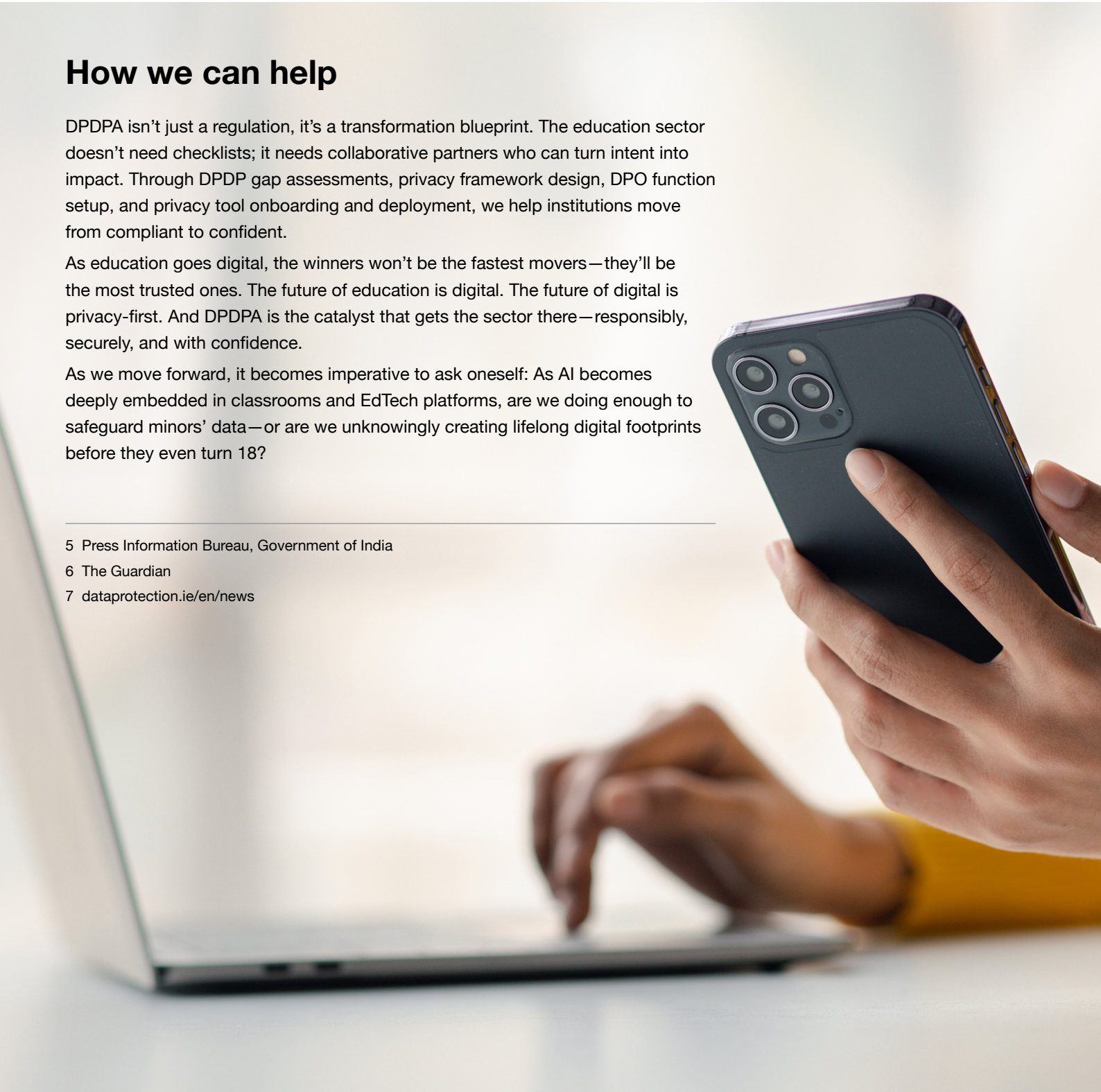
- Children’s data exposed by default: €405 million for Instagram (2022)[6]
- Weak data protection for minors: €345 million for a leading short video platform (2023)[7]

How we can help

DPDPA isn’t just a regulation, it’s a transformation blueprint. The education sector doesn’t need checklists; it needs collaborative partners who can turn intent into impact. Through DPDP gap assessments, privacy framework design, DPO function setup, and privacy tool onboarding and deployment, we help institutions move from compliant to confident.

As education goes digital, the winners won’t be the fastest movers—they’ll be the most trusted ones. The future of education is digital. The future of digital is privacy-first. And DPDPA is the catalyst that gets the sector there—responsibly, securely, and with confidence.

As we move forward, it becomes imperative to ask oneself: As AI becomes deeply embedded in classrooms and EdTech platforms, are we doing enough to safeguard minors’ data—or are we unknowingly creating lifelong digital footprints before they even turn 18?



5 Press Information Bureau, Government of India

6 The Guardian

7 dataprotection.ie/en/news

About PwC

We help you build trust so you can boldly reinvent

At PwC, we help clients build trust and reinvent so they can turn complexity into competitive advantage. We're a tech-forward, people-empowered network with more than 364,000 people in 136 countries and 137 territories. Across audit and assurance, tax and legal, deals and consulting, we help clients build, accelerate, and sustain momentum. Find out more at www.pwc.com.

PwC refers to the PwC network and/or one or more of its member firms, each of which is a separate legal entity. Please see www.pwc.com/ structure for further details.

Contact us

Anirban Sengupta
Partner and Co-Lead – Cyber and Digital Risk
PwC India
anirban.sengupta@pwc.com

Sundareshwar Krishnamurthy
Partner and Co-Lead – Cyber and Digital Risk
PwC India
sundareshwar.krishnamurthy@pwc.com

Nebha Maheshwari
Partner – Cyber and Digital Risk
PwC India
nebha.maheshwari@pwc.com

Heena Vazirani
Partner – Cyber and Digital Risk
PwC India
heena.vazirani@pwc.com

pwc.in

Data Classification: DC0 (Public)

SG/April2026 - M&C 52571