THE DPDP ACT 2023: WHAT CORPORATES NEED TO PREPARE FOR

Ronald Philips, Advocate

ABSTRACT

The Digital Personal Data Protection Act, 2023 is India's first comprehensive law on how personal data must be collected, stored and used. It came after the Supreme Court held, in K.S. Puttaswamy v. Union of India, that privacy is a fundamental right. This article looks at what the Act actually requires of companies: getting clear and specific consent from users, honouring their rights over their own data, and meeting extra obligations if a company qualifies as a Significant Data Fiduciary. It also covers the rules on sending data outside India, the penalties the Data Protection Board can impose, and how the Act affects different sectors such as technology, banking, e-commerce and healthcare differently. Recent surveys show that many Indian businesses are still not prepared for these obligations. The article ends by setting out the practical steps companies need to take now to bring their data practices in line with the law.

BACKGROUND

For years, there were no clear rules governing how Indian Businesses collected, stored and handled people's personal data. The method in which data was collected was largely unregulated and rarely any real accountability when things went wrong. Companies designed consent forms in a way which led to confusion and doubt in the minds of the users. Also, data was shared to third parties without the consent of the users.

Things changed when India passed the Digital Personal Data Protection Act, 2023 ("the Act") in August 2023, which is India's first comprehensive legislation governing the processing of digital personal data.[1] The legislation was introduced following the ruling in K.S. Puttaswamy v Union of India,[2] where the Hon'ble Supreme Court of India held that Privacy is a fundamental right under Article 21 of the Constitution of India. The ruling made it clear that the people's personal information can only be collected and stored with their consent and with proper reasons and justification as to how much data and why the data is being collected. The Act was thus designed to protect citizens without hindering fast growing digital economy.

SCOPE AND APPLICABILITY

The Act applies to all the entities whether domestic or foreign that collects and processes digital personal data of the people in India. Merely offering goods or services to Indian users or operating a digital platform within the country is sufficient to attract its obligations.[3]

The Act defines personal data as any information capable of identifying an individual, including names, contact details, health information and location data. The Act establishes a foundational distinction between two parties, the Data Fiduciary and the Data Principal. The Data Fiduciary is the entity that determines the means and purpose of processing the data, while the Data Principal is the individual to whom the data relates. The Scope of rights and obligations under the Act are purely based on the relationship between these two parties.

[1]Ministry of Electronics and Information Technology, Government of India, Data Protection Framework, https://www.meity.gov.in/data-protection-framework (last visited Jul. 16, 2026).
[2]Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 S.C.C. 1 (India).
[3]DPDP Act India Checklist for MNCs: Data Compliance Guide, KSandK.com, https://ksandk.com/data-protection-and-data-privacy/dpdp-act-india-checklist-for-mncs/ (last visited Jul. 16, 2026).

WHAT THE LAW MANDATES

Consent must be clear and specific

The most important aspect is that the users are entitled to free specific, informed and unambiguous consent before collecting their personal data. Businesses can no longer bury permissions in lengthy and complex terms and conditions without giving valid reasons to accept each one of them. Moreover, the users are also entitled to withdraw their consent at any given time. This has major implications on how Businesses design their app interfaces and customer communication.

Design tricks such as pre-ticked boxes or consent hidden within "Accept all" buttons are now considered as unfair trade practices and are termed as Dark Patterns.[4]

Enforceable rights over user data

The Act confers four substantive rights upon the Data Principals[5] that the Business Entities are obligated to honour. The users are to be informed about the data that is being collected from them, the users have the right to get their data corrected if it is inaccurate, have their data erased when it is no longer needed and are also entitled to raise grievances if they believe that their data was mishandled. If the Business Entity fails to respond to the requests made by the users they are at breach. It is extremely significant for Business entities to have clear processes, designated points of contact and the technical infrastructure to respond to the requests made by the users.

Significant Data Fiduciaries

The Act recognizes that not all Data Fiduciaries pose the same degree of risk. The Central Government is empowered to designate certain entities as Significant Data Fiduciaries (SDFs)[6] based on the volume and the sensitivity of the data processed, potential risk to the rights of the

[4]The Legal Perils of Dark Patterns in India: Intersection Between Data Privacy and Consumer Protection, SCC Online Blog (Sept. 16, 2025), https://www.scconline.com/blog/post/2025/09/16/the-legal-perils-of-dark-patterns-in-india-intersection-between-data-privacy-and-consumer-protection/ (last visited Jul. 16, 2026).
[5]DPDP Act 2023: Rights of Data Principals Explained, KSandK.com, https://ksandk.com/data-protection-and-data-privacy/dpdp-act-2023-rights-of-data-principals-explained/ (last visited Jul. 16, 2026).
[6]Significant Data Fiduciaries: DPDP Act Compliance Guide, KSandK.com, https://ksandk.com/data-protection-and-data-privacy/significant-data-fiduciaries-dpdp-act-compliance-guide/ (last visited Jul. 16, 2026).

users and broader implications for National Security and Public order.

The SDFs must appoint a Data Protection Officer (DPO) residing in India, engage an Independent Data Auditor and also conduct Data Protection Impact Assessments (DPIAs) before processing their activities. Large Technology platforms, Financial Institutions, Healthcare Aggregators and major e-commerce operators are the various entities who will be designated as Significant Data Fiduciaries.

Cross-Border Transfers and Restrictions

Under the Act, cross border transfers of data are allowed to all the countries that the Indian Government has not specifically restricted. The Government reserves the right to block transfer of data to certain countries if it determines that the data protection standards are inadequate.[7] This is great news for Multinational Businesses and Companies that rely on Global Cloud infrastructure. The Businesses with international data flows are obligated to monitor and abide by the restrictions imposed by the Government so as to prevent regulatory action against them.

PENALTY FRAMEWORK

The financial consequences of non-compliance are serious under the Act. The Data Protection Board of India is the Central, independent regulatory authority tasked with monitoring data compliance, investigating data breaches, adjudicating disputes and enforcing penalties. The Penalties are imposed based on the nature of violation and in the most serious cases, the penalty can go up to Rs. 250 Crores.[8]

The Board considers several factors while determining the penalties to be imposed on the Business Entities based on how severe the breach is and if the entity took necessary steps to mitigate risk. A Business Entity that notifies the breach and co-operates fully will be treated differently compared to an entity that conceals the breach.

Moreover, compliance breaches may lead to regulatory audits, media scrutiny and the loss of consumer confidence. Wilful breach or gross negligence by the directors or employees of the Companies may face personal liability which could end up tarnishing the reputation of the

[7]India's New Cross-Border Data Transfer Framework, KSandK.com, https://ksandk.com/data-protection-and-data-privacy/indias-new-cross-border-data-transfer-framework/ (last visited Jul. 16, 2026).
[8]Penalties and Adjudication Under India's DPDP Act, 2023, KSandK.com, https://ksandk.com/data-protection-and-data-privacy/penalties-adjudication-under-indias-dpdp-act-2023/ (last visited Jul. 16, 2026).

entities.

SECTORAL IMPLICATIONS

The impact of the Act will be perceived differently across industries based on the nature and volume of data processed by each sector:

Global Technology Companies: Multinational Companies operating in India especially sectors like telecom, social media, fintech and large digital platforms are expected to fall within the ambit of Significant Data Fiduciaries. These Large Companies require a comprehensive governance overhaul. This includes appointment of resident DPOs, conducting annual independent audits and undertaking DPIAs before deploying new data intensive features.

Digital Platforms and E-Commerce: Businesses that process large volumes of data face significant exposure under the act. These Platforms need to consider how permissions are sought from the users, how they handle data breaches and how they respond to requests of the users to change or delete their data.

Banking and Financial Services: Banking and NBFCs handle sensitive categories of data such as income records, credit histories, identity documents and transaction history. These sectors are obligated to prevent breach as a large-scale data breach may attract penalties up to Rs. 250 Crore. The average cost of a data breach in India reached an all-time high of INR 195 million in 2024,[9] underlining the real financial exposure beyond regulatory penalties.

Healthcare and Health Tech: The Healthcare sector processes large scale sensitive data. The Organizations processing medical records and diagnostic data are subject to intensive scrutiny under the Act. The data collected is highly confidential and any unauthorized disclosure may seriously affect an individual's privacy and dignity. This is the reason why Healthcare sectors would face heightened compliance obligations under the Act.

COMPLIANCE GAP

Despite the law being in place, India's corporate readiness remains a concern. EY India

[9]IBM, Cost of a Data Breach Report 2024: India, IBM Newsroom (Jul. 31, 2024), https://in.newsroom.ibm.com/2024-07-31-IBM-Report-Escalating-Data-Breach-Disruption-Pushes-Average-Cost-of-a-Data-Breach-in-India-to-All-Time-High-of-INR-195-Million-in-2024 (last visited Jul. 16, 2026).

recently surveyed close to 150 professionals across sectors,[10] and the picture that comes out of it is mixed: momentum toward compliance is building, but actual readiness on the ground is still patchy. A big part of the problem is awareness itself — around 71% of the businesses surveyed said they are not really familiar with the Act or its Rules, and this gap shows up not just among operational teams but at leadership level too. Healthcare, education and infrastructure appear to be lagging the furthest behind, largely due to fragmented data systems and legacy processes. Financial services, e-commerce and technology platforms are doing comparatively better, likely because they are already used to dealing with regulatory scrutiny in other forms. Budget constraints, a shortage of trained data protection professionals and outdated IT systems[11] keep coming up as the main reasons companies are struggling to close this gap.

These are the problems that need to be analysed and necessary steps need to be taken to fix the issues. The Data Protection Board is set up and enforcement will follow. The Companies that have not prepared will end up paying a much higher price and will find themselves scrambling to remediate under pressure in comparison to the ones that have shown awareness about the changing landscape of the data governance in India under the Act.

WHAT COMPANIES ARE REQUIRED TO DO NOW

The Businesses that stay ahead of this law will be the ones that treat compliance as an ongoing commitment rather than a one-time exercise. To achieve this, Businesses must:

- Know exactly what personal data they collect and the reason for collecting it.
- Ensure that the consent processes are clear and up to date.
- Have a clear plan to resolve issues and respond to user data requests promptly.
- Assess whether they are likely to be designated as Significant Data Fiduciaries based on the scale of data being collected.

[10]EY India, India's Data Privacy Shift: Steering the DPDP Compliance and Readiness, EY (2025), https://www.ey.com/en_in/insights/cybersecurity/india-s-data-privacy-shift-steering-the-dpdp-compliance-and-readiness (last visited Jul. 16, 2026).
[11]Over 70% Indian Firms Struggle to Interpret DPDP Act: EY, Businessworld, https://www.businessworld.in/article/over-70-indian-firms-struggle-to-interpret-dpdp-act-ey-592272 (last visited Jul. 16, 2026).

- Be prepared for a data breach before it actually happens.

WHERE DOES THIS LEAVE US?

The Act represents a shift in how India expects to treat personal data. It is not an impossible standard but requires intentionality, systems and accountability that Companies never had to build before. Those who see this as an opportunity are more likely to be better positioned with customers and their stakeholders. Those who treat it as a compliance burden will face consequences that will go beyond financial penalty. In an era where data breaches in India are growing in both frequency and cost[12] and where customers are increasingly aware of their rights, strong data governance is no longer an option but a legal and business necessity.

[12]Supra note 10.