



Same rules, different realities: MSMEs under the DPDP Act

The Digital Personal Data Protection Act, 2023 (**DPDP Act**) marks a fundamental shift in India's data governance regime. One of the significant features of the DPDP Act is its size-neutral design, *i.e.*, the statute does not differentiate between large enterprises and smaller players such as micro, small and medium enterprises (**MSMEs**). As a result, every data fiduciary regardless of turnover, scale, digital maturity or operational sophistication is subject to the same baseline obligations. This creates a challenging compliance landscape for MSMEs, which must meet enterprise-level standards despite having limited resources, lean teams, fragmented digital systems and limited legal or technical support.

This primer outlines how the DPDP Act is likely to impact MSMEs and the strategic compliance and advocacy measures they should consider adopting as the regulatory framework is phased in.

WHAT ARE MSMEs?

MSMEs are micro, small, and medium enterprises, a category defined by the government based on investment in plant and machinery or equipment and annual turnover. Recently, the central government revised¹ the definition of MSMEs as under the Micro, Small and Medium Enterprises Development Act, 2006 and the updated definitions have been in effect since April 1, 2025.

MSMEs form the backbone of the Indian economy, forming a key pillar of growth. For FY 2024-25, the MSME sector contributed ~30% to the GDP and over 45% to the country's exports.² MSMEs contribute significantly to the economy and social development of the country by fostering entrepreneurship and generating large employment opportunities at comparatively lower capital cost, next only to agriculture.³ However, despite their crucial role in the economy, the MSME sector faces several constraints such as limited access to timely and adequate formal credit; inadequate infrastructure and technology adoption hindering productivity and difficulty in attracting talent.⁴ On top of this regulatory burden, the absence of a differential treatment further increases compliance costs for MSMEs and exposes them to heightened legal risks.

¹ *Ministry of Micro, Small and Medium Enterprises Notification, 21st March, 2025*, available at <https://www.dcmsme.gov.in/Notification-S.O-no-1364-E-dated-21.03.2025-Revised-Definition.pdf>. Broadly, enterprises with capital investment not exceeding INR 2.5 crore, INR 25 crore, INR 125 crore and turnover not exceeding INR 10 crore, INR 100 crore and INR 500 crore would qualify as micro, small and medium enterprises, respectively.

² *Udyami Diwas-MSME Day 2025: Driving Innovation, Enabling Inclusion*, available at <https://www.pib.gov.in/PressNoteDetails.aspx?NoteId=154772&ModuleId=3®=3&lang=2>.

³ Annual Report 2024-25, Ministry of Micro, Small and Medium Enterprises, available at <https://www.msme.gov.in/sites/default/files/MSME-ANNUAL-REPORT-2024-25-ENGLISH.pdf>.

⁴ *Understanding MSME sector, progress and challenges*, SIDBI available at <https://www.sidbi.in/uploads/Understanding Indian MSME sector Progress and Challenges 13 05 25 Final.pdf>.

ONE SIZE MAY NOT FIT ALL

The DPDP Act adopts a strictly size-neutral approach, imposing the same baseline obligations on every data fiduciary regardless of any metric, for example annual turnover or employee strength.⁵ What this means is that MSMEs must be compliant with the obligations under the DPDP Act, at the same level of rigour as a larger corporation. These sets of obligations on a data fiduciary are significant, for example implementing purpose-specific notices to secure consent, establishing robust consent and withdrawal mechanisms, ensuring strict data-security safeguards, putting in place grievance redressal systems, etc. Since MSMEs do not benefit from economies of scale typically associated with large corporations, this could potentially lead to disproportionate compliance friction, especially for traditional MSMEs that may have only recently digitized their operations.

Consider a semi-digital retail MSME, such as a small apparel store or electronics shop. Customer data is often collected informally through a mix of UPI receipts, handwritten records, and WhatsApp based communication. Implementing notice and consent processes, maintaining consent logs, providing withdrawal mechanisms, and responding to access or correction requests all require digitization of workflows that were never designed with data protection in mind. In many tier-two and three city businesses, limited awareness of the forthcoming obligations may further constrain their ability to implement any meaningful compliance measures.

EXEMPTIONS IN THEORY, STRENUOUS COMPLIANCE IN PRACTICE

The DPDP Act vests the central government with wide-ranging powers to shape the compliance landscape, including the power to notify certain data fiduciaries as *significant*,⁶ frame rules on cross-border data flows,⁷ and importantly exempt⁸ certain data fiduciaries or classes of data fiduciaries from specific provisions of the DPDP Act, among others. This discretionary power, set out under Section 17(5), is particularly significant for the MSME sector, which operates with resource constraints, limited digital maturity, and low economies of scale to absorb rising foreseeable compliance costs.

However, despite the importance of this provision, Section 17(5) will come into force only 18 months from now,⁹ i.e., at the very end of the DPDP Act's staggered implementation timeline.

This creates a major concern - MSMEs will need to invest time, capital, training, and operational changes into full DPDP compliance over the next 18 months, even though the eventual scope of exemptions, if at all, remains unknown. In practice, they are asked to operationalize compliance first and learn later whether those efforts were necessary. This uncertainty is not just inefficient, it risks misallocating scarce MSME resources.

SO, WHAT NEXT?

The timing mismatch places MSMEs in regulatory limbo, i.e., bearing compliance costs upfront while waiting for a relief framework that may never materialize. For many MSMEs, whose margins are already thin and whose digital processes are still evolving, these sunk compliance costs could be disproportionate and potentially distortionary. **The next 18 months therefore cannot be spent in passive anticipation but must be strategically utilized for both compliance and pro-active targeted advocacy.**

⁵ Interestingly, as per Article 30(5) of EU's General Data Protection Regulation, organisations with fewer than 250 employees are generally exempt from maintaining records of processing activities, except where the processing is regular (not occasional), poses risks to individuals' rights and freedoms, or involves special category or criminal-offence data.

⁶ Section 10(1), DP\DP Act.

⁷ Section 16(1), DPDP Act.

⁸ Section 17(5), DPDP Act: "The Central Government may, before expiry of five years from the date of commencement of this Act, by notification, declare that any provision of this Act shall not apply to such Data Fiduciary or classes of Data Fiduciaries for such period as may be specified in the notification."

⁹ Ministry of Electronics and Information Technology (MeitY), Notification dated November 13, 2025, available at <https://www.meity.gov.in/static/uploads/2025/11/c56ceae6c383460ca69577428d36828b.pdf>.

- **Putting together a compliance roadmap:** Absent a clear indication from the central government on exemption, MSMEs must still chart a workable compliance roadmap in the interim to avoid non-compliance.
 - **MSMEs as data fiduciaries and/ or data processors.** Depending upon the nature of business, MSMEs could qualify as data fiduciaries, data processors or both.
 - o As **data fiduciaries**, MSMEs would need to comply with a suit of obligations. Since the obligations emanate from processing digital personal data, **data minimization** (collecting personal data that is **necessary**) is key for MSMEs to reduce compliance burden. They should begin by mapping all personal data they collect, and setting up simple notice, consent, and grievance workflows that meet DPDP Act requirements without heavy infrastructure. They must put in place basic but reliable security safeguards, train staff handling data, and establish clear protocols for deletion, correction, and breach reporting. In cases of third-party vendor data processing, MSMEs should ensure robust contractual protections to avoid exposure to disproportionate risk.
 - o As **data processors**, MSMEs will be bound by contracts with data fiduciaries, who will typically require processors to implement the very same obligations that the DPDP Act imposes on fiduciaries themselves. In practice, this means MSMEs may face contractual terms demanding stringent security measures, tight breach-reporting timelines, and full alignment with the fiduciary's compliance framework. Therefore, MSMEs should watch out for absolute and wide representations and warranties, uncapped or broad indemnities, and obligations that go beyond what the DPDP Act actually requires. They should negotiate for clarity, proportionality, and capped liability so that processing engagements do not expose them to disproportionate commercial or regulatory risk.
- **Targeted advocacy:** Historically, across multiple iterations of the DPDP Bill, MSMEs were never explicitly recognized as a distinct category even though “small enterprises,” were, at one stage (DPDP Bill, 2018, 2019 and 2021), proposed to receive limited relief (such as exemptions for manual processing). Given the DPDP Act excludes non-automated processing from its scope, in effect, nothing has meaningfully changed for the sector with the DPDP Act coming into force. This makes coordinated advocacy by the MSMEs and their industry associations crucial on two fronts:
 - **Full exemption.** Seek full exemption under Section 17(5) for a specified time-period enabling a smooth transition for MSMEs.
 - **Partial exemption.** Alternatively, if a full carve-out is not accepted, engage with MeitY on tailored relaxations. The central government has wide powers under Section 17(5) and limited powers under Section 17(3) to exempt certain data fiduciaries entirely or with respect to specified obligations, respectively. MSMEs should appeal to the central government's wider power under Section 17(5) given the limitations under Section 17(3), in particular with respect to seeking consent.
 - **Institutional support.** In any event, MSMEs should also consider seeking institutional support from MeitY to ease the compliance burden. This could include creating templated notices for MSMEs, providing them with a simple checklist of when the DPDP Act will apply to them or not or other forms of legal support.
- **Upfront clarity.** Finally, because the central government can exercise its exemption powers only at the end of the transition-period, MSMEs should consider seeking policy clarity upfront to avoid compliance costs.

We hope you have found this information useful. For any queries/clarifications please write to us at insights@elp-in.com or write to our authors:

Ravisekhar Nair, Partner – Email – ravisekharnair@elp-in.com

Parthsarathi Jha, Partner – Email – parthjha@elp-in.com

Ketki Agrawal, Principal Associate – Email – ketkiagrawal@elp-in.com

Disclaimer: The information provided in this update is intended for informational purposes only and does not constitute legal opinion or advice.