INTERNATIONAL JOURNAL OF LEGAL STUDIES AND SOCIAL SCIENCES [IJLSSS]

ISSN: 2584-1513 (Online)

Volume 4 | Issue 3 [June, 2026]| Page 348 - 359

COMPLIANCE OBLIGATIONS FOR MSMES UNDER INDIA'S DIGITAL PERSONAL DATA PROTECTION ACT, 2023: A CRITICAL ANALYSIS WITH REGULATORY FRAMEWORK APPROACH

-Debarshi Roy Choudhury[1]

ABSTRACT

India's Digital Personal Data Protection Act, 2023 and the notified Digital Personal Data Protection Rules, 2025 constitute the nation's inaugural comprehensive statutory framework for the governance of digital personal data. Although the legislation is viewed as a means to regulate large technology platforms, its non-discriminatory approach mandates key obligations on all Data Fiduciaries ranging from global e-commerce conglomerates to local pharmacies that digitize customer records. This article provides a critical assessment of how the DPDP Act and the DPDP Rules impact Micro, Small and Medium Enterprises, which together contribute about 30.1% to India's Gross Domestic Product and employ more than 28 crore individuals. By fully leveraging the provisions of the statute, the notified rules, a comparative study of the European Union's General Data Protection Regulation, and expert insights, the article posits that while the DPDP Act commendably upholds the constitutional right to privacy recognized in Justice K.S. Puttaswamy v. Union of India (2017), its uniform compliance framework imposes a structurally disproportionate burden on MSMEs. The article delineates key obligations, reviews the governance structure for Significant Data Fiduciaries, lists the phased enforcement timeline, and suggests a proportionate regulatory pathway tailored to the operational realities of India's small business landscape.

Keywords: Regulatory Compliance, Platform Accountability, DPDP Act, GDPR, Proportionate Regulation, Data Governance

[1] Designation- Student (3rd year), Course – BA LLB , Institutional Affiliation – Jalpaiguri Law College, University of North Bengal , West Bengal , Email – debarshirchoudhury2164@gmail.com , Contact - 8293710070

INTRODUCTION

India's digital economy stands among the fastest growing globally with over 900 million internet users and a projected trillion dollar digital economy by 2026. The expansion of digital payment infrastructure has underscored the necessity of robust personal data governance, elevating it from a policy preference to a constitutional imperative. In a landmark judgment, the Supreme Court's nine-judge bench in *Justice K.S. Puttaswamy (Retd.) & Ors. V. Union of India & Ors.*, (2017) 10 SCC 1 unequivocally established that the right to privacy is a fundamental right enshrined in Article 21 of the Constitution of India.[2] This ruling laid the normative groundwork for the legislative framework that would follow.

On August 11, 2023, the Digital Personal Data Protection Act, 2023 (Act No. 22 of 2023), received Presidential assent. Following over two years of rule-drafting, the Central Government operationalized the framework through a series of notifications on November 13, 2025, which included the notification of the Digital Personal Data Protection Rules, 2025, the establishment of the Data Protection Board of India, and a phased implementation timeline stretching over 18 months until May 12, 2027.[3] While the regulatory discourse of the DPDP Act has primarily focused on its implications for large technology companies, social media intermediaries, and multinational data processors, this emphasis masks a more fundamental challenge of the uniform application of the law to micro, small, and medium enterprises. These entities, which constitute the socio-economic backbone of India, often operate with limited resources, nascent digital infrastructure, and restricted access to legal counsel.

This article adopts a doctrinal and comparative research methodology by analysing primary sources and secondary sources to evaluate MSME compliance burdens under the DPDP Act. As noted by Economic Laws Practice, the DPDP Act does not differentiate between large enterprises and small enterprises, thereby imposing enterprise-level standards on MSMEs despite their resource constraints, fragmented digital systems, and limited legal or technical support. This article will proceed as follows: Section 2 will map the MSME landscape in India. Section 3 will outline the key obligations imposed by the DPDP Act on all fiduciaries. Section 4 will examine the structured compliance structure distinguishing ordinary Data Fiduciaries from Significant Data Fiduciaries. Section 5 will trace the phased enforcement timeline under the DPDP Rules. Section 6 will provide a critical analysis of the practical challenges faced by MSMEs. Section 7 will draw comparative lessons from the GDPR's

[2] *Justice K.S. Puttaswamy (Retd.) & Ors. v. Union of India & Ors.,* (2017) 10 SCC 1.

[3] Ministry of Electronics and Information Technology (MeitY), Notification G.S.R. 843(E) dated 13 November 2025 (Digital Personal Data Protection Rules, 2025).

approach to small enterprises. Finally, Section 8 will offer a forward looking analysis of what a proportionate regulatory framework for Indian MSMEs should entail.

CURRENT LANDSCAPE OF MSMES IN INDIA

MSME is defined under the Micro, Small and Medium Enterprises Development Act, 2006. The classification underwent major changes in 2020 with the Notification S.O. 2119 (E), which introduced an investment and turnover criterion, replacing the earlier investment-only metric and eliminating the distinction between manufacturing and service enterprises.

The aggregate economic impact of these entities is significant, yet individual MSMEs are characterized by several challenges that directly influence their data management practices and minimal in-house legal or technical expertise. According to SME Forum's 2025 digitalization survey, concerns over data privacy, cyber fraud, and unauthorized access continue to be major barriers to digital adoption among MSMEs.[4] These characteristics necessitate a specific analytical deep dive through which DPDP Act obligations must be evaluated.

OBLIGATIONS UNDER THE DPDP ACT

The DPDP Act uses the term "Data Fiduciary" to refer to any person or persons who determine the purpose and means of processing of personal data which ensures that entities ranging from large tech firms to small and medium-sized enterprises that digitize personal information of Indian citizens are covered under the Act. Any MSME that processes personal data of Indian residents is classified as a Data Fiduciary and subject to the Act's provisions. The duties of Data Fiduciaries will become enforceable during Phase 3 starting from May 12, 2027.

CONSENT AND NOTICE REQUIREMENTS

Under Section 6, a Data Fiduciary must secure the free, specific, informed, unconditional, and unequivocal consent of the Data Principal before processing their personal data with a notice. Section 5 requires that the notice include all the personal data required for collection; the purpose of its processing; the mechanisms available to the Data Principal for exercising rights; the process for

[4] India SME Forum, *The State of Digitalisation in Indian MSMEs: A Study on the Evolving Digital Landscape of MSMEs in India* (December 2025) https://indiasmeforum.org/digishaastra/assets/docs/Final-META-Report-Card-2025.pdf accessed 14 June 2026.

lodging complaints with the Data Protection Board; and the availability of the notice in any of the languages listed in the Eight Schedule to the Constitution.

Rule 3 of the DPDP Rules provides additional specifications regarding the format and delivery of these notices. The responsibility of proving that consent has been obtained lies with the Data Fiduciary. For MSMEs that frequently gather personal data via paper forms, WhatsApp queries, or informal UPI transactions, establishing a legally robust consent framework represents a significant operational overhaul rather than a mere procedural adjustment.

PURPOSE LIMITATION AND DATA MINIMIZATION

The consent provided by a Data Principal is strictly purpose-limited as it authorizes processing only for the specified purpose and only of the personal data essential for that purpose. Any additional processing for a different purpose requires new consent. Pursuant to Section 8, the Data Fiduciary is obligated to maintain the completeness, accuracy, and consistency of personal data that is likely to be utilized to influence the Data Principal or shared with another Data Fiduciary.

REASONABLE SECURITY SAFEGUARDS

Section 8(5) of the DPDP Act obliges that every Data Fiduciary should implement data security and privacy protection measures to prevent personal data breaches. Rule 6 operationalises this requirement by setting forth a minimum set of security measures applicable to all Data Fiduciaries.[5]

Every company must strictly follow these measures, and failure to implement these reasonable security safeguards can result in a personal data breach penalty of up to ₹250 crore which is the highest penalty tier under the Act.[6]

BREACH NOTIFICATION

Upon discovering a personal data breach, a Data Fiduciary must notify both the Data Protection Board and the affected Data Principals without further delay. Rule 7 further stipulates that a detailed breach report must be submitted to the DPB within 72 hours. It is equally important to notify the affected Data Principals about the details about the nature of the breach, its gravity and the further steps required to mitigate the issue.

[5] DPDP Act, 2023, Section 8(5); DPDP Rules, 2025, Rule 6.
[6] DPDP Act, 2023, First Schedule read with Section 33.

DATA RETENTION AND ERASURE

A Data Fiduciary must erase personal data and ensure that its data processors do the same, once the specified purpose for which it was collected is no longer served, unless retention is mandated by law. Rule 8 states that the Data Principal must be absolved from all their rights related to the data and the purpose is no longer served if it does not engage with the Data Fiduciary within a stipulated period. The Third Schedule to the DPDP Rules outlines specific retention timelines for different categories of Data Fiduciaries, such as e-commerce platforms, social media intermediaries, and gaming companies, typically three years after the last interaction or triggering event. Notably, Data Principals must be informed at least 48 hours before their data is erased. For MSMEs, this obligation poses significant challenges, as customer records are often retained indefinitely for business continuity, warranty claims, or informal credit histories, without a structured deletion protocol.

DATA PRINCIPAL RIGHTS

The DPDP Act grants Data Principals four fundamental rights enforceable against all Data Fiduciaries:

- Right to Access Information (Section 11): A Data Principal can request a summary of personal data being processed, the purposes of processing, and the identities of Data Fiduciaries and processors with whom the data has been shared.
- Right to Correction, Completion, Updating, and Erasure (Section 12): A Data Principal can request corrections to inaccurate data, completion of incomplete data, and deletion of data no longer necessary for the specified purpose.
- Right to Grievance Redressal (Section 13): A Data Principal can lodge complaints with the Data Fiduciary, who must respond within 90 days.
- Right to Nomination (Section 14): A Data Principal can designate another individual to exercise her rights in the event of death or incapacity. Each of these rights imposes corresponding obligations on Data Fiduciaries to establish accessible mechanisms for their exercise, requiring technological infrastructure and organizational processes that many MSMEs have not previously needed.

GRIEVANCE REDRESSAL

Every Data Fiduciary must publish the business contact information of a Data Protection Officer or a designated contact person to handle queries from Data Principals regarding data processing. An

effective grievance redressal mechanism is mandatory for all Data Fiduciaries to resolve the queries of Data Principals regarding their data and retention policies which must be transparent with responses required within 90 days.

PROCESSING OF CHILDREN'S DATA

Section 9 imposes additional obligations when processing personal data of children under 18 years. Every Data Fiduciaries must verify parental consent and are prohibited from processing children's data in ways that could cause harm. They should never track behavioural patterns in children or target advertise with visuals that may affect them. Rule 10 details the process for obtaining verifiable parental consent. For MSMEs in sectors like education, retail, entertainment, or healthcare that serves families or minors, this obligation necessitates a dedicated verification infrastructure.

COMPLIANCE STRUCTURE OF SIGNIFICANT DATA FIDUCIARIES

The DPDP Act establishes a framework by differentiating between ordinary Data Fiduciaries and Significant Data Fiduciaries. This distinction, however, does not absolve ordinary fiduciaries of their fundamental responsibilities; instead, it imposes additional obligations specifically on SDFs.

DESIGNATION OF SDFS

The Central Government retains the authority to designate any Data Fiduciary as a Significant Data Fiduciary.

Crucially, SDF status is determined based on the nature and risk profile of the processing activities rather than solely on revenue, company size, or employee numbers. A small-scale startup handling sensitive data of millions of students could potentially be designated an SDF, whereas a large manufacturing MSME collecting only basic supplier contact details might not be.

ENHANCED OBLIGATIONS OF SDFS

Upon designation, SDFs are required to maintain additional obligations outlined in Section 10 and Rule 13 of the DPDP Rules:

- Appointment of a Data Protection Officer ("DPO"): The DPO must be based in India and act as the primary point of contact for Data Principals and the DPB.

- Annual Data Protection Impact Assessments ("DPIAs"): SDFs must perform DPIAs to evaluate risks to Data Principals, the necessity and proportionality of the processing, and the adequacy of safeguards in place.
- Independent Audits: Periodic independent compliance audits are mandatory.
- Algorithmic Risk Assessments: SDFs using algorithms for profiling or automated decision-making must conduct risk assessments.
- Detailed Compliance reports must be submitted to the DPB.

THE PHASED ENFORCEMENT TIMELINE

Under the DPDP Act and DPDP Rules, a strict phased enforcement timeline is provided which is required for the implementation of provisions over three distinct phases.[7]

Phase 1: On 13th November 2025, immediate force was brought to put forth the definitional provisions under Section 2, the framework under Sections 18-26, and the government's rule-making powers under Section 35, 38-43. On the Rules notification, Rules 1, 2, and 17–21 took immediate effect by establishing the procedural framework and the constitution and functioning of the DPB. This phase primarily ensured that the DPB existed and the regulatory architecture was operational.

Phase 2: On 12th November 2026, immediate force was brought to put forth for registration requirements for Consent Managers under Section 6(9) and Section 27(1)(d) for the DPB's jurisdiction over breaches of registration conditions by Consent Managers, along with Rule 4 which governs the registration and obligations of Consent Managers. A Consent Manager, under the DPDP Act, helps the Data Principal to give, manage, review, and withdraw consent. While MSMEs are unlikely to become Consent Managers themselves, they may be required to integrate with Consent Manager platforms to route and record consent, especially in consumer-facing applications.

Phase 3: 12 May 2027 is the most consequential phase. It brings into force all substantive and operational obligations, including:[8]

- Sections 3–5, 6(1)–(8) and (10): Notice and Consent requirements;
- Section 7: Legitimate uses (processing without Consent);
- Sections 8–10: General and additional obligations of Data Fiduciaries and SDFs;

[7] Ministry of Electronics and Information Technology (MeitY), Notification S.O. 4858(E) and G.S.R. 843(E) dated 13 November 2025.

[8] Digital Personal Data Protection Rules, 2025, rr 3, 5-16, 22-23.

- Sections 11–15: Data Principal rights and duties;
- Sections 16: Cross-border Data transfer restrictions;
- Section 17: Exemptions;[9]
- Sections 27–34, 36–37: DPB's powers and functions, penalties, and information-seeking powers.

Rules 3, 5-16, 22, and 23 take effect covering notices, security safeguards, breach intimation, retention and erasure, verifiable parental consent, SDF obligations, cross-border transfers, and the appeals procedure. From a compliance perspective, the 18-month window between November 2025 and May 2027 is the compliance readiness period. However, as analyzed in Section 6, this window carries a critical structural paradox.

CRITICAL GAPS IN MSMES

THE SIZE OF MSMES AND ITS LIMITATIONS

The structural feature of the DPDP Act, and the most important point of criticism from the MSME perspective, is clearly the size-neutral design. Unlike the GDPR, which contains size-sensitive adjustments discussed in Section 7 of this article, the DPDP Act applies the same baseline compliance obligations regardless of turnover, number of employees, amount of data processed. In India, mid-sized businesses with sales of ₹500 crore and internal legal teams face the same consent architectures, breach notifications and complaint handling obligations as microenterprises with sales of ₹ 10 crore and 3 employees.

COMPLIANCE COST

The costs associated with the DPDP framework disproportionately impact smaller enterprises. Larger entities can incur these costs over economies of scale, dedicated legal and privacy teams, and robust governance structures. But the new startups and micro, small, and medium-sized enterprises face significant challenges while dealing with a liability and consume a much larger portion of an MSME's limited budget.

[9] DPDP Act, 2023, Section 17(5).

ABSENCE OF EXEMPTION FOR SMALL-BUSINESSES

Unlike the GDPR, the DPDP Act lacks an express size-based exemption. The potentially relevant exemption mechanism is Section 17(5), which permits the Central Government to declare, within five years of commencement, that any provision of the Act shall not apply to such Data Fiduciary or classes of Data Fiduciaries for such period as may be specified. However, Section 17(5) does not come into effect until Phase 3, which is 18 months after the November 2025 notification, specifically on May 12, 2027. This timing creates a significant limitation as micro, small and medium-sized enterprises are required to invest fully in DPDP compliance over the next 18 months, despite the uncertainty regarding the eventual scope of any exemptions.

As ELP's analysis highlights, for MSMEs "whose margins are already thin and whose digital processes are still evolving, these sunk compliance costs could be disproportionate and potentially distortionary."[10]

PENALTY CONSEQUENCES

The DPDP Act's penalty framework is adjusted for absolute maximum rather than percentage sales. The highest level penalties resulting from breaches due to failure to implement proper security protections have nothing to do with the size of or the revenue of the Data Fiduciary. For a micro MSME with an annual sales of ₹5-10 crore and the ₹250 crore penalties is existential rather than a deterrent adjusted to action. In contrast, the GDPR provides for a maximum fine of up to 4% of global annual sales or 20 million euros whichever is higher with the actual penalty calibrated to factors including the size, nature and the cooperation of the offender under Article 83(2). [11]

This absolute penalty design creates two perverse incentives. First, MSMEs may escape the scope of application of the Act which is applicable only to digital personal data by simply avoiding digitizing operations or moving data processing to unofficial third party vendors. Second, it has the effect of deterring investment in MSME into data-led business models and weakens the very digital transformation that India's economic policy is about to accelerate.

[10] Economic Laws Practice, 'Same Rules, Different Realities: MSMEs under the DPDP Act' (December 2025) https://elplaw.in/wp-content/uploads/2025/12/Same-rules-different-realities-MSMEs-under-the-DPDP-Act.pdf accessed 14 June 2026.

[11] GDPR, Art. 83(2).

AWARENESS

MSMEs face challenges related to general compliance and awareness, with most micro enterprises are unaware of their obligations under the DPDP Act, while others struggle with the technical capacity required to implement compliance structures, even when they understand them. Unlike GST compliance, DPDP compliance involves a far more multidisciplinary approach, necessitating legal, cyber security, and organizational expertise that is often lacking within most MSME teams. The discourse surrounding the DPDP Act has primarily centered on large enterprises and listed companies, whereas the enforcement implications may disproportionately affect smaller businesses.

THIRD-PARTY RISK

Many micro, small, and medium-sized enterprises (MSMEs) function as Data processors for larger enterprises, offering services such as payroll processing, management, logistics, or sales support within the framework. Under the DPDP Act, although direct obligations typically lie with the Data Fiduciary, contracts often mandate that the MSME processor must follow the same stringent safeguards, comply with breach-reporting timelines, and provide comprehensive indemnities and warranties. For MSMEs that lack negotiating power with their larger clients, these contractual requirements can expose them to significant commercial and contractual risks that extend beyond what the DPDP framework mandates, potentially including uncapped indemnities and absolute representations that surpass industry standards.

COMPARATIVE ANALYSIS WITH GDPR'S APPROACH TO SMALL ENTERPRISES

The EU's General Data Protection Regulation, known as GDPR, Regulation (EU) 2016/679), effective since 25 May 2018, applies universally to entities processing personal data of EU residents, irrespective of their size. Unlike the DPDP Act, which includes no blanket exemption for small businesses, the GDPR features several size-sensitive adjustments that significantly ease compliance burdens for smaller enterprises.[12]

- Article 30- Recordkeeping exemption: Enterprises with fewer than 250 employees are generally exempt from maintaining detailed records of processing activities, commonly known as RoPAs, unless the processing is not occasional, poses risks to individuals' rights, or involves

[12] Regulation (EU) 2016/679 (General Data Protection Regulation),OJ L. 119, 4.5.2016, p. 1.

special categories of sensitive data or criminal records. This provision offers substantial practical relief to small businesses whose data processing is routine and low risk.[13]

- Article 37- Data Protection Officer (DPO): The requirement to appoint a DPO is limited to entities where personal data processing is a core business activity posing specific threats such as large-scale monitoring or processing of sensitive data. Small businesses whose data processing is in support to their main business activity are not automatically required to appoint a DPO.
- Article 25- Privacy by Design: Although no small-business exemption exists, Article 25 allows organizations to consider the costs of implementation as a factor in determining appropriate technical and organizational measures. This proportionality principle enables small businesses to adopt lower-cost safeguards suitable to their scale and the nature of their processing.
- Article 32- Security of Processing: Similar to Article 25, the security obligation includes the "costs of implementation" and "scope" of processing as relevant factors, implicitly calibrating the security standard to the enterprise's capacity.[14]
- Article 35- Data Protection Impact Assessments (DPIAs): DPIA obligations are triggered only when processing is "likely to result in a high risk" to individuals' rights, with the scope and context of processing as relevant considerations. Small businesses with low processing activities are unlikely to need DPIAs.

The GDPR's approach to small enterprises is practically better organized and represents a model of proportionate regulation. It gives enough relief to small businesses and newly established entities. It allows for a flexible guided principle for businesses according to the scale, nature and the volume of the data being processed.

TOWARDS A COMPREHENSIVE REGULATORY FRAMEWORK

A risk-calibrated regulatory approach must first recognize that processing 500 customers' contact details for order fulfillment requires a different privacy risk than a social media platform processing data of 50 million users. A well designed framework should calibrate its requirements to the actual risk

[13] GDPR, Art 30(5).
[14] GDPR, Articles 25 and 32.

posed by a given processing activity, rather than imposing a uniform regulatory floor that imposes excessive costs on smaller entities.

The DPB's approach as a digital-first regulatory body should prioritize proactive engagement with MSME associations, issue interpretive guidance on the application to small businesses, and adopt an approach that focuses initial enforcement energy on high-risk, high-volume processing activities also while creating a safe-harbor framework for good-faith MSMEs that demonstrate sincere effort.

A forward looking analysis must always recognize that achieving DPDP compliance offers strategic upside for MSMEs, in highly privacy conscious marketplace, where enterprise clients, foreign buyers, and sophisticated consumers scrutinize data handling practices. MSMEs that demonstrate DPDP compliance can differentiate themselves in procurement decisions, qualify for export contracts where international counterparts require data protection assurances, and build the consumer trust.

The question is not whether MSMEs should comply, but rather how the compliance structure should be designed to make compliance achievable for the 7 crore enterprises that form the backbone of India's economy.

CONCLUSION AND RECOMMENDATIONS

In conclusion, a proposed regulatory framework for Indian MSMEs under the DPDP Act demands structured and practical action. Parliament should consider targeted amendments to introduce a turnover-linked penalty calculation for enterprises below certain thresholds and authorize the Central government to notify size based exemptions prior to Phase 3 enforcement. Ministry of Electronics and Information Technology should exercise its powers within the existing framework to issue early notifications of exemptions for micro enterprises handling non-sensitive, non-systematic personal data. The Data Protection Board must adopt and publish an enforcement prioritization policy for a risk-based, capacity-sensitive approach to enforcement. The DPDP Act holds transformative potential for India's digital governance but only if its implementation accounts for the demographic and economic diversity of India's data ecosystem. Enterprises with sales turnover below ₹5 crore and processing data of fewer than 5,000 data principals should be made eligible for the first phase compliance with notice and security measures only. A fair and inclusive regulatory approach with the GDPR model regarding enterprise size, nature and the total volume of data processed must be strictly complied with. By applying these measures we can advance the fundamental right to privacy and push for a more inclusive data governance and compliance mechanisms.