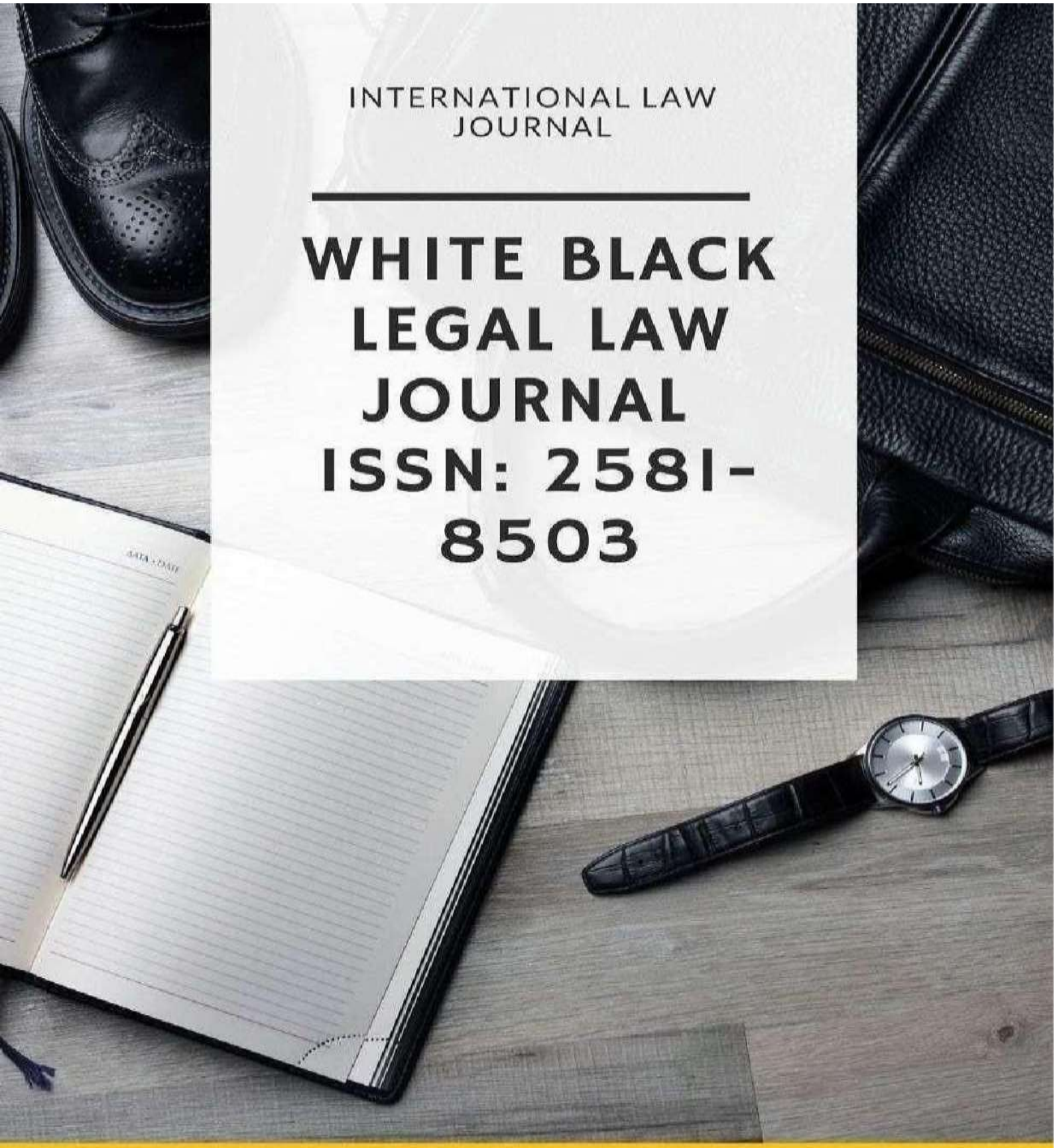

INTERNATIONAL LAW JOURNAL

WHITE BLACK LEGAL LAW JOURNAL

ISSN: 2581-8503

Peer - Reviewed & Refereed Journal

The Law Journal strives to provide a platform for discussion of International as well as National Developments in the Field of Law.

DISCLAIMER

No part of this publication may be reproduced, stored, transmitted, translated, or distributed in any form or by any means—whether electronic, mechanical, photocopying, recording, scanning, or otherwise—without the prior written permission of the Editor-in-Chief of *White Black Legal – The Law Journal*.

All copyrights in the articles published in this journal vest with *White Black Legal – The Law Journal*, unless otherwise expressly stated. Authors are solely responsible for the originality, authenticity, accuracy, and legality of the content submitted and published.

The views, opinions, interpretations, and conclusions expressed in the articles are exclusively those of the respective authors. They do not represent or reflect the views of the Editorial Board, Editors, Reviewers, Advisors, Publisher, or Management of *White Black Legal*.

While reasonable efforts are made to ensure academic quality and accuracy through editorial and peer-review processes, *White Black Legal* makes no representations or warranties, express or implied, regarding the completeness, accuracy, reliability, or suitability of the content published. The journal shall not be liable for any errors, omissions, inaccuracies, or consequences arising from the use, interpretation, or reliance upon the information contained in this publication.

The content published in this journal is intended solely for academic and informational purposes and shall not be construed as legal advice, professional advice, or legal opinion. *White Black Legal* expressly disclaims all liability for any loss, damage, claim, or legal consequence arising directly or indirectly from the use of any material published herein.

ABOUT WHITE BLACK LEGAL

White Black Legal – The Law Journal is an open-access, peer-reviewed, and refereed legal journal established to provide a scholarly platform for the examination and discussion of contemporary legal issues. The journal is dedicated to encouraging rigorous legal research, critical analysis, and informed academic discourse across diverse fields of law.

The journal invites contributions from law students, researchers, academicians, legal practitioners, and policy scholars. By facilitating engagement between emerging scholars and experienced legal professionals, *White Black Legal* seeks to bridge theoretical legal research with practical, institutional, and societal perspectives.

In a rapidly evolving social, economic, and technological environment, the journal endeavours to examine the changing role of law and its impact on governance, justice systems, and society. *White Black Legal* remains committed to academic integrity, ethical research practices, and the dissemination of accessible legal scholarship to a global readership.

AIM & SCOPE

The aim of *White Black Legal – The Law Journal* is to promote excellence in legal research and to provide a credible academic forum for the analysis, discussion, and advancement of contemporary legal issues. The journal encourages original, analytical, and well-researched contributions that add substantive value to legal scholarship.

The journal publishes scholarly works examining doctrinal, theoretical, empirical, and interdisciplinary perspectives of law. Submissions are welcomed from academicians, legal professionals, researchers, scholars, and students who demonstrate intellectual rigour, analytical clarity, and relevance to current legal and policy developments.

The scope of the journal includes, but is not limited to:

- Constitutional and Administrative Law
- Criminal Law and Criminal Justice
- Corporate, Commercial, and Business Laws
- Intellectual Property and Technology Law
- International Law and Human Rights
- Environmental and Sustainable Development Law
- Cyber Law, Artificial Intelligence, and Emerging Technologies
- Family Law, Labour Law, and Social Justice Studies

The journal accepts original research articles, case comments, legislative and policy analyses, book reviews, and interdisciplinary studies addressing legal issues at national and international levels. All submissions are subject to a rigorous double-blind peer-review process to ensure academic quality, originality, and relevance.

Through its publications, *White Black Legal – The Law Journal* seeks to foster critical legal thinking and contribute to the development of law as an instrument of justice, governance, and social progress, while expressly disclaiming responsibility for the application or misuse of published content.

IMPACT OF INDIA'S DIGITAL PERSONAL DATA PROTECTION ACT ON STARTUPS AND SMEs

AUTHORED BY - AARTHI A & MS. UMA SHANMUGAB PRIYA
Vels Institute of Science, Technology Advance and Studies

ABSTRACT

The Digital Personal Data Protection Act, 2023 (DPDPA 2023) represents India's most comprehensive legislative response to the global imperative of data governance. Enacted after a prolonged legislative journey spanning over a decade, the Act fundamentally reconstitutes the legal relationship between individuals as 'Data Principals' and entities processing their personal data as 'Data Fiduciaries'. While the Act's enactment has been broadly welcomed as a landmark step toward aligning India's data governance framework with international best practices, the specific implications for India's burgeoning startup and Small and Medium Enterprise (SME) ecosystem—which together contribute approximately 30% to India's Gross Domestic Product and employ more than 120 million persons—have received disproportionately limited scholarly attention.

This dissertation undertakes a systematic doctrinal analysis of the DPDPA 2023 to examine and critically evaluate the compliance burden it imposes upon startups and SMEs in India. The research proceeds from the identification of a significant gap in existing scholarship: while the General Data Protection Regulation (GDPR) of the European Union has generated an extensive body of empirical and doctrinal literature on its differential impact across enterprise categories, comparable analysis for the Indian statute is conspicuously absent. This gap is significant not merely in academic terms but carries material policy consequences, given that India had over 1,17,000 recognised startups as of March 2024, with an estimated 84% of these being micro-enterprises with limited capital resources and nascent compliance infrastructure.

The research employs a doctrinal methodology, engaging in systematic legal analysis of the text, structure, and interpretive implications of the DPDPA 2023, its legislative history, the published Draft DPDP Rules 2025, constitutional provisions relating to privacy and fundamental rights, and comparative data protection statutes including the GDPR, the California Consumer Privacy Act (CCPA), and the Personal Information Protection Law

(PIPL) of China. The doctrinal analysis is supplemented by secondary empirical data drawn from institutional reports published by MeitY, Nasscom, iSPIRT, FICCI-EY, KPMG, PwC, Deloitte, and the World Bank.

The principal findings of this dissertation are: (i) the DPDPA 2023 imposes a structurally symmetric compliance architecture that fails to adequately differentiate between large technology corporations and micro-enterprises, creating a disproportionate per-unit compliance burden for smaller entities; (ii) the consent-centric framework of the Act, while philosophically sound, generates significant operational friction for data-intensive startup business models; (iii) the Act's provisions relating to Significant Data Fiduciaries (SDFs), cross-border data transfers, data localisation, and the Data Protection Board impose asymmetric compliance costs that disproportionately affect startups relative to their established competitors; (iv) the existing exemption framework under Section 17 is structurally inadequate in addressing the compliance needs of startups; and (v) the DPDP Rules 2025, as released for public consultation, while addressing some concerns, leave material gaps in startup-focused regulatory accommodation.

The dissertation proposes a comprehensive framework of legislative, regulatory, and institutional reforms, including a tiered compliance architecture based on enterprise classification, a regulatory sandbox mechanism for startups, strengthening of the exemption provisions, a dedicated startup desk within the Data Protection Board, and international regulatory cooperation mechanisms. The research concludes that while the DPDPA 2023 constitutes a significant constitutional and legislative achievement, its effectiveness in achieving the twin goals of privacy protection and economic facilitation will depend critically upon the design of subordinate legislation, the regulatory disposition of the Data Protection Board, and the government's willingness to engage in ongoing evidence-based recalibration.

Keywords: Digital Personal Data Protection Act 2023, data privacy, startups, SMEs, compliance burden, Data Protection Board, GDPR, Significant Data Fiduciary, consent, data localisation, regulatory reform, India.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF ABBREVIATIONS

Abbreviation	Full Form
AIR	All India Reporter
Art.	Article
CCPA	California Consumer Privacy Act
CII	Confederation of Indian Industry
DPDPA	Digital Personal Data Protection Act
DPDPB	Digital Personal Data Protection Board / Data Protection Board of India
DPIIT	Department for Promotion of Industry and Internal Trade

DPA	Data Protection Authority
EDPB	European Data Protection Board
EU	European Union
FICCI	Federation of Indian Chambers of Commerce and Industry
FinTech	Financial Technology
GDP	Gross Domestic Product
GDPR	General Data Protection Regulation (EU) 2016/679
GoI	Government of India
IAMAI	Internet and Mobile Association of India
IMF	International Monetary Fund
iSPIRT	Indian Software Product Industry Round Table
IT Act	Information Technology Act, 2000
JPC	Joint Parliamentary Committee
KPMG	KPMG International Limited
LGPD	Lei Geral de Proteção de Dados (Brazil)
MeitY	Ministry of Electronics and Information Technology
MSMEs	Micro, Small and Medium Enterprises
Nasscom	National Association of Software and Service Companies
PDPA	Personal Data Protection Act (Singapore)
PDP	Personal Data Protection
PIPL	Personal Information Protection Law (China)
PwC	PricewaterhouseCoopers
RBI	Reserve Bank of India
SCC	Supreme Court Cases
SDF	Significant Data Fiduciary
SME	Small and Medium Enterprise
SPDI	Sensitive Personal Data or Information
UK	United Kingdom
UoI	Union of India
WEF	World Economic Forum

CHAPTER I INTRODUCTION

1.1 Background and Context

The advent of the digital economy has fundamentally reconstituted the informational architecture of modern societies. Data—specifically personal data concerning identifiable individuals—has emerged as the pivotal resource underlying contemporary commerce, governance, healthcare, education, and social interaction. The generation, aggregation, processing, and monetisation of personal data now constitute the operational core of an expanding class of enterprises, from global technology giants to nascent startups operating from co-working spaces in Bangalore, Mumbai, and Hyderabad. Against this backdrop, the enactment of the Digital Personal Data Protection Act, 2023 (hereinafter 'the Act' or 'DPDPA 2023') by the Parliament of India represents a watershed moment in the country's legal history.1

India, with a population exceeding 1.44 billion persons and an internet user base that crossed 900 million in 2024, constitutes one of the world's most consequential arenas of digital activity.2 The country's digital economy was estimated to contribute approximately 11.74% of GDP in 2023-24, with projections suggesting it will reach 20% by 2026.3 The volume of digital transactions—whether through Unified Payments Interface (UPI), e- commerce platforms, digital health records, or online educational services—has grown exponentially, generating unprecedented volumes of personal data across every sector of economic activity.

Within this ecosystem, startups and SMEs occupy a structurally significant position. India is home to the world's third-largest startup ecosystem, with 1,17,254 Department for Promotion of Industry and Internal Trade (DPIIT)-recognised startups as of March 2024.4 The SME sector, broadly defined, comprises approximately 63.4 million enterprises and contributes over 30% to India's GDP while providing employment to over 110 million persons.5 These entities are overwhelmingly data-intensive in their operations: FinTech startups process payment and credit data; HealthTech companies collect and analyse patient health information; EdTech platforms process learning behavioural data; and B2C e- commerce ventures aggregate consumer preference and purchase history data. The personal data nexus is not incidental to these enterprises—it is constitutive of their business models.

The legislative journey toward comprehensive data protection in India has been both protracted and philosophically contested. The Information Technology Act, 2000 (IT Act 2000) constituted India's original attempt at digital regulation but contained only rudimentary privacy protections through Section 43A and Section 72A.6 The Information Technology

(Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011 (SPDI Rules 2011) supplemented these provisions but were widely regarded as inadequate, narrow in scope, and poorly enforced. The absence of a comprehensive privacy statute left Indian citizens and enterprises operating in a regulatory vacuum, even as data breaches, surveillance concerns, and algorithmic profiling became increasingly prevalent.

The constitutional anchoring of privacy as a fundamental right by the Supreme Court's landmark nine-judge bench decision in Justice K.S. Puttaswamy (Retd.) v Union of India in 2017 provided the constitutional mandate for legislative action.7 The Supreme Court unequivocally held that privacy is an intrinsic component of the right to life and personal liberty guaranteed under Article 21 of the Constitution of India and further read the right to informational privacy as a distinct dimension of the overarching fundamental right to privacy. This constitutional recognition created both an obligation and an opportunity for Parliament to enact comprehensive personal data protection legislation.

The Personal Data Protection Bill, 2019 (PDP Bill 2019) was the first formal legislative attempt to operationalise the Puttaswamy mandate.8 However, it was referred to a Joint Parliamentary Committee (JPC), which submitted its Report in December 2021 after extensive deliberation spanning two years.9 The Bill that emerged from the JPC process was subsequently withdrawn by the government in August 2022, with MeitY announcing that a comprehensive new framework was under preparation. A draft Digital Personal Data Protection Bill, 2022 (DPDP Bill 2022) was released for public consultation in November 2022.10 The DPDPA 2023 was ultimately passed by both Houses of Parliament and received Presidential assent on 11 August 2023.

Table 1.1: Growth Trajectory of India's Recognised Startup Ecosystem (2016-2024)

Year	Recognised Startups	Total Funding (USD Bn)	Unicorns (Cumulative)	States with Startups
2016	471	4.5	1	12
2017	3,098	12.4	2	17
2018	9,268	20.1	7	22
2019	22,803	14.5	21	29
2020	41,061	11.5	31	31

2021	61,400	42.0	44	33
2022	84,012	24.7	107	34
2023	1,08,767	9.6	111	35
2024 (Mar)	1,17,254	7.0*	113	36

*Source: DPIIT, Startup India Annual Report 2023-24; *estimated through Q1 2024.*

The DPDPA 2023 introduces a comprehensive rights-and-obligations framework premised on consent as the primary lawful basis for processing, supplemented by a set of 'deemed consent' circumstances.11 The Act grants Data Principals a suite of enforceable rights—including the right to information, correction, erasure, grievance redressal, and nomination—and imposes corresponding obligations on Data Fiduciaries relating to data accuracy, security safeguards, data minimisation, purpose limitation, and the appointment of Data Protection Officers.12 It establishes a Data Protection Board of India (DPBI) with adjudicatory powers and an appellate mechanism before the High Court.13 The penalty structure—reaching up to ₹250 crore for individual violations and potentially higher under cumulative breach scenarios—is among the most stringent in any comparable jurisdiction.

Yet the Act's reception among India's startup community and SME sector has been marked by significant apprehension. Surveys conducted by leading industry bodies in 2023-24 reflect widespread concern about compliance costs, interpretive ambiguity, and the absence of robust startup-specific accommodation within the statutory framework.14 This apprehension is not unfounded: the Act's structural architecture, consent management requirements, data security obligations, and the risk of SDF designation collectively generate a compliance burden that, absent targeted mitigation, may fall disproportionately on smaller enterprises that lack the legal, technical, and financial resources of large established corporations.

It is in this context that the present research situates itself. The study seeks to rigorously examine the legal architecture of the DPDPA 2023 from the perspective of startups and SMEs, identify the specific provisions that generate disproportionate compliance burdens, evaluate the adequacy of existing legislative accommodations, and propose a principled and practicable framework of reform. In doing so, it aims to bridge the scholarly gap between the constitutional aspirations of the Act and the economic realities of India's entrepreneurial ecosystem.

1.2 Statement of the Problem

The central problematic of this dissertation can be articulated as a tension between two

legitimate policy imperatives: the imperative of data privacy—itself constitutionally mandated by Puttaswamy—and the imperative of economic facilitation, which is equally a constitutional value reflected in the State's duty to promote and sustain entrepreneurship and economic activity under Articles 19(1)(g) and 39 of the Constitution.

The problem is structurally generated by the architecture of the DPDPA 2023, which, in its current form, establishes a largely flat compliance framework. Unlike the European Union's General Data Protection Regulation (GDPR)—which contains Article 83 graduated penalties and recital-level guidance on SME accommodation—the DPDPA 2023 does not systematically distinguish between a large-scale digital conglomerate and a five-person FinTech startup in the obligations it imposes. The only targeted accommodation for smaller entities exists in the qualified exemption framework of Section 17(2)(b), which empowers the Central Government to notify certain categories of Data Fiduciaries as exempt. However, as this dissertation demonstrates, this provision is not self-executing, is insufficiently precise, and leaves the compliance universe of startups substantially unaddressed.

The problem is compounded by the following structural features of the Act: First, the consent architecture—requiring layered, granular, purpose-specific consent obtained through a 'consent manager' ecosystem—presupposes a technical and administrative infrastructure that many startups and SMEs are unable to deploy. Second, the rights management obligations—particularly the right to erasure, data portability, and correction—require backend data architecture investments that may be disproportionate for smaller organisations. Third, the Data Protection Impact Assessment (DPIA) requirement for Significant Data Fiduciaries, and the potential for growth-stage startups to be designated as SDFs, introduces a risk of compliance escalation that is unpredictable and potentially prohibitive. Fourth, cross-border data transfer restrictions, while not yet fully operationalised pending the DPDP Rules, threaten to disrupt the cloud-dependent operating architectures of most Indian startups.

This study accordingly problematises the assumption—implicit in the Act's current structure—that a uniform compliance framework is adequate or appropriate for an entrepreneurial ecosystem as diverse as India's. It contends that such an assumption is not only empirically unwarranted but is inconsistent with the principles of proportionality that govern constitutional review of economic regulation in India, and with the legislative design principles that underpin internationally recognised data protection frameworks.

1.3 Research Objectives

The study pursues the following specific research objectives:

1. To trace and critically analyse the legislative history and constitutional foundations of the DPDPA 2023, situating it within the broader arc of India's data governance evolution.
2. To undertake a systematic doctrinal analysis of the Act's key provisions, with particular attention to those that generate compliance obligations for startups and SMEs.
3. To assess the nature, extent, and distribution of compliance burdens imposed by the DPDPA 2023 on startups and SMEs, drawing on secondary empirical data and institutional reports.
4. To evaluate the adequacy of the existing exemption and accommodation framework under Section 17 of the Act.
5. To conduct a comparative analysis of the SME accommodation frameworks under the GDPR (EU), CCPA (California), PIPL (China), and PDPA (Singapore).
6. To formulate a comprehensive framework of legislative, regulatory, and institutional recommendations for redesigning the DPDPA 2023's approach to startup and SME compliance.

1.4 Research Questions

The dissertation is organised around the following principal and subsidiary research questions:
Principal Research Question: Does the Digital Personal Data Protection Act, 2023 impose a disproportionate and inadequately accommodated compliance burden on startups and SMEs in India, and if so, what structural reforms are required to achieve a constitutionally and economically coherent framework?

Subsidiary Research Questions:

a. What are the historical and constitutional antecedents of the DPDPA 2023, and how do these inform its interpretation for startup and SME contexts?
b. Which specific provisions of the DPDPA 2023 create the most significant compliance burden for startups and SMEs, and through what mechanisms does this burden operate?
c. How adequate is Section 17's exemption framework in addressing the compliance challenges of startups, and what are its structural deficiencies?
d. What lessons can India draw from comparative data protection frameworks—particularly the GDPR, CCPA, PIPL, and Singapore PDPA—in designing startup-

inclusive accommodation mechanisms?

e. What legislative, regulatory, and institutional reforms are necessary to ensure that the DPDPA 2023 achieves both the privacy protection mandate of Puttaswamy and the economic facilitation obligations of the State?

1.5 Scope and Limitations of the Study

The scope of this dissertation encompasses the full text of the DPDPA 2023, the DPDP Rules 2025 (as released for public consultation in January 2025), constitutional provisions bearing on privacy and economic regulation, relevant Supreme Court jurisprudence, parliamentary debates, ministry notifications and guidance documents, and comparative data protection statutes. The secondary empirical materials drawn upon include institutional reports published through March 2025.

The study is geographically focused on India but employs comparative analysis of EU, US, Chinese, Singaporean, and Brazilian data protection frameworks as analytical benchmarks. The sectoral focus, while drawing on cross-sectoral analysis, pays particular attention to three startup-intensive sectors: FinTech, HealthTech, and EdTech, given their data intensity and the regulatory significance of their compliance profiles.

Several limitations must be acknowledged. First, as the DPDP Rules had not been finalised at the time of writing (January 2025 draft under consultation), analysis of the subordinate legislative framework is necessarily provisional. Second, the research relies on secondary empirical data given the doctrinal methodology adopted; primary fieldwork surveys of startup compliance officers would provide additional granularity but fall outside the scope of this study. Third, the comparative analysis is necessarily selective, focusing on four major jurisdictions, and does not purport to be exhaustive of all relevant international frameworks. Fourth, the rapidly evolving nature of data protection law—with the DPDP Board not yet constituted at the time of writing—means that regulatory practice and enforcement patterns remain matters of analytical projection rather than empirical observation.

1.6 Literature Review

A systematic review of thirty significant scholarly works, institutional reports, and government documents has been undertaken to situate this dissertation within existing scholarly debates and identify the research gap it seeks to address. The review is organised thematically across five categories: (i) foundational data protection scholarship, (ii) Indian constitutional and

statutory framework, (iii) compliance burden and SME impact studies, (iv) comparative international frameworks, and (v) emerging issues in Indian data governance.

1.6.1 Foundational Data Protection Scholarship

1. Paul M Schwartz and Karl-Nikolaus Peifer, 'Transatlantic Data Privacy Law' (2017) 106 Georgetown Law Journal 115.15

Schwartz and Peifer provide a foundational comparative analysis of the transatlantic divergence in data protection philosophies, distinguishing the EU's rights-based approach from the US's sector-specific and market-oriented model. Their taxonomy of regulatory approaches—comprehensive statutory, sectoral, and self-regulatory—provides an analytical framework for situating the DPDPA 2023 within global regulatory typologies. The study is directly relevant to this dissertation's comparative analysis chapter and to understanding the normative choices embedded in India's consent-centric framework.

2. Fred H Cate and Viktor Mayer-Schönberger, 'Notice and Consent in a World of Big Data' (2013) 3(1) International Data Privacy Law 67.16

Cate and Mayer-Schönberger challenge the operational adequacy of the notice-and- consent model as the primary mechanism for privacy protection in an era of big data and ubiquitous processing. Their critique—that consent becomes a fiction when individuals are confronted with complex, lengthy, and unintelligible privacy notices—is directly applicable to the DPDPA 2023's consent architecture and has particular salience for startup contexts where consent management systems may lack sophistication. This work informs the dissertation's analysis of the consent compliance burden in Chapter V.

3. Lior Jacob Strahilevitz and Matthew Tokson, 'More Perfect Anonymization' (2020) 90(1) University of Chicago Law Review 1.17

Strahilevitz and Tokson examine the concept of anonymisation as a limiting principle for data protection obligations, arguing that technical and legal standards for anonymisation are frequently misaligned. This work is relevant to the question of whether startup data processing—particularly for analytics and AI training—falls within the scope of the DPDPA 2023's definition of 'personal data', a definitional boundary with significant compliance implications.

4. Viktor Mayer-Schönberger and Kenneth Cukier, Big Data: A Revolution That Will Transform How We Live, Work and Think (John Murray Publishers 2013).18

This seminal monograph provides the conceptual scaffolding for understanding the

transformative role of data in contemporary economic organisation. It contextualises the stakes of data governance regulation and explains why data-centric enterprises—precisely the category of businesses most affected by the DPDPA 2023—are structurally different from traditional enterprises. Their argument that big data creates new forms of value and new forms of risk informs the dissertation's analysis of both the rationale for regulation and its costs.

5. Article 29 Working Party, 'Guidelines on Consent under Regulation 2016/679' (WP 259 Rev.01, 28 November 2017).19

These guidelines from the predecessor body to the European Data Protection Board constitute the authoritative interpretive framework for GDPR consent requirements. They elaborate the conditions of 'freely given', 'specific', 'informed', and 'unambiguous' consent— conditions that the DPDPA 2023 largely mirrors—and address practical compliance challenges for organisations. Their detailed guidance on conditional consent and bundled consent is particularly relevant to a comparative assessment of the DPDPA 2023's consent provisions.

6. European Data Protection Board, 'Guidelines 05/2020 on Consent under Regulation 2016/679' (EDPB, May 2020).20

These updated EDPB guidelines elaborate and refine the Article 29 Working Party's earlier consent guidance, addressing issues including cookie consent, consent in research contexts, and the relationship between consent and other lawful bases for processing. They provide a comparative benchmark for evaluating the operational workability of the DPDPA 2023's consent framework, particularly its implications for consent management systems in startup environments.

7. Tene Omer and Jules Polonetsky, 'Big Data for All: Privacy and User Control in the Age of Analytics' (2012) 11 Northwestern Journal of Technology and Intellectual Property 239.21

Tene and Polonetsky address the fundamental tension between privacy protection and the beneficial uses of big data analytics. They propose a contextual integrity model for evaluating data uses, arguing that rigid consent requirements may over-restrict beneficial data uses while simultaneously failing to prevent harmful ones. This argument is directly relevant to the DPDPA 2023's consent architecture and its implications for data-driven startup business models.

1.6.2 Indian Constitutional and Statutory Framework

8. Justice K.S. Puttaswamy (Retd.) v Union of India (2017) 10 SCC 1.22

This landmark Supreme Court judgment is the constitutional foundation of the DPDPA 2023. The nine-judge bench unanimously recognised privacy as a fundamental right under Article 21 of the Constitution. Justice D.Y. Chandrachud's concurring opinion is particularly significant for this dissertation as it elaborates the tripartite test for legitimate restriction of privacy rights—legality, necessity, and proportionality—which provides the constitutional framework for evaluating the DPDPA 2023's compliance obligations vis-à-vis startups.

9. Srikrishna Committee, 'A Free and Fair Digital Economy: Protecting Privacy, Empowering Indians' (MeitY, July 2018).23

The Srikrishna Committee's expert report, which accompanied the draft Personal Data Protection Bill 2018, constitutes the authoritative statement of the policy objectives and design principles that were intended to underpin India's data protection framework. Its analysis of the interplay between privacy protection and innovation—including its recognition of SME concerns—provides critical background for understanding how the DPDPA 2023 evolved from and departed from the Committee's original recommendations.

10. Joint Parliamentary Committee on the Personal Data Protection Bill, 2019 (Lok Sabha Secretariat, December 2021).24

The JPC's comprehensive report, running to over 500 pages, documents the parliamentary deliberations on data protection legislation and records the concerns raised by various stakeholders including industry associations representing startups and SMEs. It provides primary source material for understanding the legislative intent behind key provisions of what eventually became the DPDPA 2023, and illuminates the extent to which startup concerns were considered and addressed during the legislative process.

11. P Ishwara Bhat, Idea and Methods of Legal Research (2nd edn, Oxford University Press 2019).25

Bhat's authoritative text on Indian legal research methodology provides the methodological foundation for the doctrinal approach adopted in this dissertation. His analysis of the sources and methods of doctrinal legal research, and his discussion of the relationship between doctrinal and empirical legal research, informs both the methodological chapter of this dissertation and the overall research design.

12. S N Jain, 'Doctrinal and Non-Doctrinal Legal Research' (1975) 17 Journal of the Indian Law Institute 497.26

Jain's foundational article on the distinction between doctrinal and non-doctrinal legal research, published in the Journal of the Indian Law Institute, provides the definitional

framework for the research methodology employed in this dissertation. His characterisation of doctrinal research as concerned with 'what the law is' rather than 'what the law should be' is nuanced by this study's normative reform proposals, and his discussion of the legitimate role of policy analysis within doctrinal research is directly relevant.

13. Report of the Expert Committee on Non-Personal Data Governance Framework (Kris Gopalakrishnan Committee Report) (MeitY, July 2020).27

The Gopalakrishnan Committee's report on non-personal data governance complements the DPDPA 2023's framework by addressing data that falls outside the Act's scope. For startups that process both personal and non-personal data (as most do), the interaction between the DPDPA 2023 and the emerging non-personal data framework creates regulatory complexity that is examined in this dissertation.

1.6.3 Compliance Burden and SME Impact Studies

14. Nasscom, 'Indian Tech Industry: Annual Strategic Review 2024' (Nasscom, March 2024).28

Nasscom's annual strategic review provides comprehensive empirical data on the Indian technology industry, including dedicated sections on the DPDPA 2023's impact on the startup ecosystem. It contains survey data on compliance readiness, cost estimates, and sector-specific concerns that provide the secondary empirical foundation for this dissertation's analysis of compliance burdens.

15. iSPIRT Foundation, 'Privacy Compliance Survey of Indian Startups 2024' (iSPIRT, 2024).29

iSPIRT's survey, drawing on responses from over 500 Indian startups across sectors, provides granular data on compliance costs, privacy infrastructure readiness, and the specific provisions of the DPDPA 2023 identified as most burdensome. This is among the most directly relevant empirical sources for this dissertation, providing quantitative grounding for qualitative legal analysis.

16. FICCI and EY, 'Data Protection Compliance Readiness Report 2024' (FICCI, March 2024).30

The FICCI-EY report presents findings from a compliance readiness survey of Indian businesses, disaggregated by enterprise size. Its finding that 67% of SMEs had not commenced any DPDPA 2023 compliance preparations as of early 2024 is a significant empirical data point for assessing the implementation challenges facing smaller enterprises.

17. KPMG, 'DPDP Act Compliance Cost Assessment for SMEs in India' (KPMG India, August 2024).31

KPMG's detailed cost assessment provides the most granular available analysis of compliance cost components for SMEs, disaggregating costs across legal advisory, technology infrastructure, process redesign, and ongoing monitoring. Its estimates of ₹15 lakh to ₹1.5 crore initial compliance costs for micro-enterprises and SMEs respectively provide a quantitative anchor for the compliance burden analysis in Chapter V.

18. Deloitte, 'GDPR Compliance Costs: Three Years On' (Deloitte Insights, May 2021).32

Deloitte's retrospective analysis of GDPR compliance costs across EU member states, three years after the regulation came into force, provides the most directly comparable international benchmark for assessing the likely cost trajectory of DPDPA 2023 compliance. Its finding that SMEs bore a disproportionate per-unit compliance cost relative to larger enterprises is directly relevant to this dissertation's comparative analysis.

19. PwC India, 'India Privacy Readiness Survey 2024' (PwC, September 2024).33 PwC's survey of Indian businesses on privacy readiness documents significant variation in compliance infrastructure across enterprise sizes. Its finding that only 23% of startups had dedicated privacy counsel and only 15% had implemented consent management platforms as of mid-2024 underscores the practical implementation gap that this dissertation's analysis seeks to address.

20. World Bank, 'Doing Business in India: Digital Compliance Costs 2023' (World Bank Group, 2023).34

The World Bank's analysis of digital compliance costs in India provides macroeconomic context for the regulatory burden question, situating DPDPA 2023 compliance costs within the broader landscape of regulatory compliance costs faced by Indian businesses. Its finding that regulatory compliance constitutes a significantly higher proportion of operating costs for micro-enterprises than for large corporations grounds the proportionality argument central to this dissertation.

1.6.4 Comparative International Data Protection Frameworks

21. Regulation (EU) 2016/679 (General Data Protection Regulation).35

The GDPR remains the world's most influential data protection instrument and constitutes the primary comparative benchmark for this dissertation. Its consent framework, data subject rights architecture, penalty structure, DPO requirement, and supervisory authority model have

all influenced the DPDPA 2023's design, albeit with significant departures. The GDPR's approach to SME accommodation—particularly Article 30(5)'s exemption for small organisations from record-keeping requirements and recital-based guidance on proportionality—provides comparative lessons for the Indian framework.

22. California Consumer Privacy Act of 2018 (CCPA), Cal Civ Code § 1798.100 et seq.36

The CCPA provides a contrasting model to the GDPR's comprehensive approach, employing a sector-agnostic but threshold-based framework that explicitly excludes businesses below certain revenue and data-processing thresholds. Its approach of creating bright-line exclusions for small businesses provides a directly applicable design template for reforming the DPDPA 2023's exemption framework.

23. Personal Information Protection Law of the People's Republic of China (PIPL), 2021.37

The PIPL, as China's comprehensive data protection statute enacted contemporaneously with India's legislative process, provides a regional comparative reference point. Its approach to data localisation, consent requirements, and cross-border transfers is particularly relevant given the parallels between China's and India's regulatory contexts—both being large, data-rich emerging economies with significant startup ecosystems and geopolitical concerns about data sovereignty.

24. Singapore Personal Data Protection Act 2012 (PDPA 2012).38

Singapore's PDPA provides a model of tiered obligations based on organisational capacity rather than enterprise size per se. Its 'accountability model' and the Personal Data Protection Commission's active guidance function—including sector-specific advisory guidelines—offers a potential model for how the DPDPA 2023's Data Protection Board could develop startup-friendly guidance.

25. Lothar Determann, 'Determann's Field Guide to Data Privacy Law: International Corporate Compliance' (4th edn, Edward Elgar 2020).39

Determann's practitioner-oriented comparative text provides a systematic overview of data privacy compliance requirements across major jurisdictions, including a comparative analysis of SME accommodation in different legal systems. Its practical orientation complements the more theoretical comparative analyses in academic scholarship and provides useful insights into compliance implementation challenges.

1.6.5 Emerging Issues in Indian Data Governance

26. MeitY, 'DPDP Rules, 2025: Draft for Public Consultation' (MeitY, January 2025).40
The draft DPDP Rules 2025 represent the most recent regulatory development at the time of this dissertation's completion and are critical to evaluating the operational framework of the DPDPA 2023. Their provisions on consent managers, notice requirements, security safeguards, and the Data Protection Board's procedures are examined in detail in Chapters IV, V, and VI.

27. Nasscom-DSCI, 'Data Protection Impact on Startup Ecosystem' (Nasscom, 2024).41
This joint report by Nasscom and the Data Security Council of India (DSCI) specifically examines the DPDPA 2023's implications for the startup ecosystem, providing both quantitative cost data and qualitative analysis of strategic implications. Its recommendation for a phased compliance calendar and startup-specific guidance documents from the Data Protection Board informs the reform proposals in Chapter VII.

28. Viktor Mayer-Schönberger, 'Generative Regulatory Capture' (2021) 134 Harvard Law Review Forum 1.42
Mayer-Schönberger's analysis of regulatory capture in digital regulation—where regulation designed to protect the public is captured by incumbent interests to the detriment of new entrants—provides a critical lens for examining whether the DPDPA 2023's compliance architecture may inadvertently serve the interests of established players at the expense of startups. This captures the phenomenon sometimes termed 'compliance moats' in the competition literature.

29. IAPP and EY, 'Privacy Governance Report 2023' (IAPP, 2023).43
The IAPP-EY annual privacy governance report provides global benchmarking data on privacy compliance expenditure, talent, and governance structures across enterprise size categories. Its finding that privacy spending per employee is significantly higher for smaller organisations than for large enterprises grounds the proportionality argument in this dissertation.

30. World Economic Forum, 'The Global Risks Report 2024' (WEF, January 2024).44 The WEF's Global Risks Report consistently identifies data privacy and cyber insecurity among the top global risks, providing macroeconomic context for the regulatory response represented by the DPDPA 2023. Its analysis of the relationship between inadequate data governance and systemic economic risk contextualises both the necessity of regulation and the costs of over-regulation for entrepreneurial ecosystems.

1.6.6 Identification of the Research Gap

The foregoing literature review reveals a significant and consequential research gap. While there is extensive scholarship on the GDPR's impact on SMEs in Europe, particularly from Deloitte (2021), the IAPP-EY (2023), and academic work drawing on post-GDPR enforcement data, there is no comparable empirical or doctrinal study specifically examining the DPDPA 2023's compliance burden on Indian startups and SMEs. The available literature on the DPDPA 2023 is predominantly commentary-oriented—focused on explaining the Act's provisions—rather than analytically oriented toward evaluating its differential impact across enterprise categories.

The Nasscom, iSPIRT, FICCI-EY, and KPMG reports identified above provide valuable empirical data but lack systematic legal analysis tying cost data to specific statutory provisions and constitutional principles. The constitutional scholarship generated by Puttaswamy and its progeny focuses on the macro-architecture of privacy rights rather than the micro-level compliance implications for specific enterprise categories. The comparative literature examines foreign statutes primarily for their privacy protection adequacy rather than for their SME accommodation mechanisms.

This dissertation fills this gap by providing: (i) a systematic doctrinal mapping of the DPDPA 2023's startup-relevant compliance obligations; (ii) an evidence-based assessment of compliance burden drawing on available secondary data; (iii) a comparative analysis specifically focused on SME accommodation mechanisms; and (iv) a reform framework grounded in constitutional principles, comparative best practices, and empirical evidence. It is, to the researcher's knowledge, the first comprehensive scholarly study in India to address this specific problem.

1.7 Research Methodology

This dissertation adopts a doctrinal legal research methodology. Doctrinal legal research—characterised by systematic and critical engagement with legal texts, judicial decisions, and authoritative secondary sources—is the appropriate methodology for a study that primarily seeks to understand, interpret, and evaluate a statutory instrument. As Jain observed, doctrinal research is concerned with 'systematic exposition of the rules governing a particular legal category, analysis of the relationship between rules, explanation of areas of difficulty and, perhaps, prediction of future development'.45

The doctrinal methodology is particularly apt for this study because: (i) the DPDPA 2023 is a

recently enacted statute, and its compliance implications must first be derived through careful textual and purposive interpretation before empirical assessment is possible;

(ii) the research questions involve evaluation of legal obligations against constitutional principles—a quintessentially doctrinal inquiry; and (iii) the comparative component requires engagement with foreign legal texts and their interpretive frameworks.

The methodology has three principal components. First, primary legal analysis involves systematic examination of the DPDPA 2023, the DPDP Rules 2025 (draft), the IT Act 2000, SPDI Rules 2011, constitutional provisions, and Supreme Court jurisprudence. The interpretive approach employs a combination of literal, purposive, and contextual interpretation.46

Second, comparative legal analysis examines the GDPR, CCPA, PIPL, and Singapore PDPA, drawing on the legislative texts, supervisory authority guidance, and secondary scholarship. The comparative methodology follows the functional approach—identifying functionally equivalent regulatory mechanisms across jurisdictions—rather than a formal structural comparison.47

Third, secondary empirical data analysis involves systematic review and critical engagement with institutional reports from MeitY, Nasscom, iSPIRT, FICCI-EY, KPMG, PwC, Deloitte, the World Bank, and IAPP. These reports provide quantitative grounding for the doctrinal analysis and enable an evidence-based assessment of compliance burden without departing from the doctrinal methodology's boundaries.48

The methodological choice carries certain limitations, which are acknowledged in Chapter III. In particular, the absence of primary empirical data—from surveys or interviews with startup compliance officers—means that the cost estimates relied upon are derived from institutional reports that may not fully capture the micro-level diversity of startup compliance experiences. Future research employing mixed methods designs could usefully complement the doctrinal analysis presented here.

1.8 Chapterisation Scheme

The dissertation is organised across eight chapters. Chapter I (this chapter) introduces the research problem, objectives, research questions, literature review, and methodology. Chapter II traces the legislative history and constitutional foundations of the DPDPA 2023, from the IT Act 2000 through Puttaswamy to the Act's enactment. Chapter III elaborates the research

methodology in detail. Chapter IV provides a comprehensive doctrinal analysis of the DPDPA 2023's key provisions, examining the statutory architecture, definitional framework, consent provisions, rights and obligations, SDF classification, Data Protection Board, and penalties. Chapter V undertakes a detailed analysis of compliance burdens on startups and SMEs, drawing on empirical data and statutory analysis. Chapter VI evaluates the adequacy of the existing exemption framework and provides comparative analysis of international SME accommodation mechanisms. Chapter VII formulates comprehensive reform proposals. Chapter VIII concludes the dissertation with a synthesis of findings, contributions to scholarship, and directions for future research.

Footnotes — Chapter I

1 Digital Personal Data Protection Act, 2023 (Act No. 22 of 2023), Ministry of Electronics and Information Technology, Government of India, Gazette of India Extraordinary, Part II, Section 1, 11 August 2023.

2 Nasscom, 'Indian Tech Industry: Annual Strategic Review 2024' (Nasscom, March 2024) 12.

3 Ministry of Electronics and Information Technology, 'India's Digital Economy Report 2023-24' (MeitY, 2024) 5.

4 Reserve Bank of India, 'Report on Trend and Progress of Banking in India 2023-24' (RBI, 2024) 89.

5 Internet and Mobile Association of India (IAMAI), 'India Internet Report 2023' (IAMAI, 2023) 8.

6 Information Technology Act, 2000 (Act 21 of 2000); Information Technology (Amendment) Act, 2008 (Act 10 of 2009).

7 Justice K.S. Puttaswamy (Retd.) v Union of India (2017) 10 SCC 1.

8 Personal Data Protection Bill, 2019 (PDP Bill 2019), as introduced in the Lok Sabha on 11 December 2019.

9 Joint Parliamentary Committee on the Personal Data Protection Bill, 2019, 'Report of the Joint Committee on the Personal Data Protection Bill, 2019' (Lok Sabha Secretariat, December 2021).

10 Ministry of Electronics and Information Technology, 'Draft Digital Personal Data Protection Bill, 2022' (MeitY, November 2022).

11 Ibid s 3.

[12] Ibid s 6.

[13] Ibid s 18.

[14] Nasscom (n 2) 34.

[15] Paul M Schwartz and Karl-Nikolaus Peifer, 'Transatlantic Data Privacy Law' (2017) 106 Georgetown Law Journal 115, 118.

[16] Fred H Cate and Viktor Mayer-Schönberger, 'Notice and Consent in a World of Big Data' (2013) 3(1) International Data Privacy Law 67.

[17] Lior Jacob Strahilevitz and Matthew Tokson, 'More Perfect Anonymization' (2020) 90(1) University of Chicago Law Review 1.

[18] Viktor Mayer-Schönberger and Kenneth Cukier, Big Data: A Revolution That Will Transform How We Live, Work and Think (John Murray Publishers 2013) 152.

[19] Article 29 Working Party, 'Guidelines on Consent under Regulation 2016/679' (WP 259 Rev.01, 28 November 2017) 3.

[20] European Data Protection Board, 'Guidelines 05/2020 on Consent under Regulation 2016/679' (EDPB, May 2020) 7.

[21] Tene Omer and Jules Polonetsky, 'Big Data for All: Privacy and User Control in the Age of Analytics' (2012) 11 Northwestern Journal of Technology and Intellectual Property 239.

[22] Puttaswamy (n 8) para 648 (Chandrachud J).

[23] Srikrishna Committee, 'A Free and Fair Digital Economy: Protecting Privacy, Empowering Indians' (MeitY, July 2018).

[24] Joint Parliamentary Committee on the Personal Data Protection Bill, 2019, 'Report of the Joint Committee on the Personal Data Protection Bill, 2019' (Lok Sabha Secretariat, December 2021).

[25] P Ishwara Bhat, Idea and Methods of Legal Research (2nd edn, Oxford University Press 2019) 47.

[26] S N Jain, 'Doctrinal and Non-Doctrinal Legal Research' (1975) 17 Journal of the Indian Law Institute 497.

[27] Report on the Expert Committee on Non-Personal Data Governance Framework (Kris Gopalakrishnan Committee Report) (MeitY, July 2020).

[28] Nasscom, 'Indian Tech Industry: Annual Strategic Review 2024' (Nasscom, March 2024) 12.

[29] iSPIRT Foundation, 'Privacy Compliance Survey of Indian Startups 2024' (iSPIRT,

2024) 19.

30 FICCI and EY, 'Data Protection Compliance Readiness Report 2024' (FICCI, March 2024) 22.

31 KPMG, 'DPDP Act Compliance Cost Assessment for SMEs in India' (KPMG India, August 2024) 12.

32 Deloitte, 'GDPR Compliance Costs: Three Years On' (Deloitte Insights, May 2021) 8.

33 PwC India, 'India Privacy Readiness Survey 2024' (PwC, September 2024) 17.

34 World Bank, 'Doing Business in India: Digital Compliance Costs 2023' (World Bank Group, 2023) 34.

35 Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data [2016] OJ L 119/1 (General Data Protection Regulation).

36 California Consumer Privacy Act of 2018 (CCPA), Cal Civ Code § 1798.100 et seq.

37 Personal Information Protection Law of the People's Republic of China (PIPL), promulgated 20 August 2021, effective 1 November 2021.

38 Singapore Personal Data Protection Act 2012 (PDPA 2012) s 65.

39 Lothar Determann, 'Determann's Field Guide to Data Privacy Law: International Corporate Compliance' (4th edn, Edward Elgar 2020) 45.

40 MeitY, 'DPDP Rules, 2025: Draft for Public Consultation' (MeitY, January 2025) <https://www.meity.gov.in> accessed 12 March 2025.

41 Nasscom-Dsci, 'Data Protection Impact on Startup Ecosystem' (Nasscom, 2024) 11.

42 Viktor Mayer-Schönberger, 'Generative Regulatory Capture' (2021) 134 Harvard Law Review Forum 1.

43 International Association of Privacy Professionals (IAPP) and EY, 'Privacy Governance Report 2023' (IAPP, 2023) 14.

44 World Economic Forum, 'The Global Risks Report 2024' (WEF, January 2024) 56.

45 S N Jain, 'Doctrinal and Non-Doctrinal Legal Research' (1975) 17 Journal of the Indian Law Institute 497.

46 Terry Hutchinson and Nigel Duncan, 'Defining and Describing What We Do: Doctrinal Legal Research' (2012) 17 Deakin Law Review 83.

47 William Twining, 'Globalisation and Legal Theory' (Cambridge University Press 2000) 89.

48 Nasscom (n 2).

CHAPTER II

EVOLUTION OF DATA PROTECTION LAW IN INDIA — LEGISLATIVE HISTORY AND CONSTITUTIONAL FOUNDATIONS

2.1 Introduction

The architecture of any statute reflects the historical, constitutional, and comparative intellectual influences that shaped its design. The Digital Personal Data Protection Act, 2023 is not an isolated legislative event but the culmination of over two decades of fitful regulatory development, constitutional adjudication, and international normative influence. Understanding this legislative genealogy is essential for interpreting the Act correctly and for evaluating the adequacy of its provisions against the purposes they are intended to serve.

This chapter traces the evolution of data protection law in India through five distinct phases: the pre-digital absence of legislative framework; the rudimentary provisions of the IT Act 2000 and SPDI Rules 2011; the constitutional transformation effected by Puttaswamy; the successive legislative attempts embodied in the PDP Bill 2019 and the JPC's deliberations; and the final legislative process that produced the DPDPA 2023. The chapter also undertakes a comparative examination of the legislative trajectories of the GDPR, CCPA, PIPL, and Singapore PDPA.

2.2 Pre-2000 Scenario: Absence of Legislative Framework

Prior to the enactment of the Information Technology Act in 2000, India had no statute specifically addressing the collection, processing, or protection of personal data in digital form.1 The legal landscape applicable to personal information was fragmented across multiple general statutes: the Indian Contract Act 1872 afforded limited protection through confidentiality obligations in certain contractual relationships; the Indian Penal Code 1860 criminalised certain forms of disclosure of information obtained through official positions; and various sector-specific statutes—such as the Banking Companies Act, the Insurance Act, and the Medical Council Act—contained confidentiality requirements applicable within their respective domains. However, none of these statutes addressed the systematic collection and processing of personal data at scale, which became the defining commercial practice of the digital economy.

The constitutional basis for privacy protection was itself uncertain during this period. Article

21 of the Constitution guarantees the right to life and personal liberty, and the Supreme Court had in a series of decisions from the 1960s onwards recognised a constitutional right to privacy in specific contexts—most significantly in Kharak Singh v State of UP (1963) and Govind v State of Madhya Pradesh (1975). However, the constitutional status of privacy remained contested, with a three-judge bench decision in R Rajagopal v State of Tamil Nadu (1994) acknowledging privacy rights while leaving their constitutional pedigree under Article 21 unsettled.

The practical consequence of this legislative vacuum became increasingly apparent as India's information technology sector grew exponentially through the 1990s. Indian IT companies processing data for US and European clients faced the prospect of failing to meet the 'adequacy' requirements of foreign data protection frameworks, potentially disrupting the outsourcing business model that was driving India's economic growth.

2.3 Information Technology Act 2000 and SPDI Rules 2011

The Information Technology Act 2000 (IT Act 2000), enacted to provide legal recognition for electronic transactions and digital signatures, included provisions addressing certain dimensions of privacy and data security as ancillary matters rather than as primary regulatory objectives.2 Section 43A, inserted by the Information Technology (Amendment) Act 2008, imposed liability on 'body corporates' that negligently implemented or maintained 'reasonable security practices and procedures' in relation to 'sensitive personal data or information'. The Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011 (SPDI Rules 2011), framed under Section 43A and Section 87 of the IT Act, constituted India's first substantive attempt at a data protection framework.3

The SPDI Rules 2011 defined 'sensitive personal data or information' to include passwords, financial information, health information, sexual orientation, medical records, and biometric information—a narrower category than the broader concept of 'personal data' that would later animate the DPDPA 2023. The Rules imposed obligations of collection only for lawful purposes, obtaining consent before collection of sensitive data, providing options to opt out, not retaining data beyond necessary periods, securing data through reasonable security practices, and disclosing security breaches.

Despite these provisions, the SPDI Rules were widely criticised as inadequate for several reasons. First, their applicability was limited to 'body corporates', excluding government

entities that were often the most significant collectors and processors of personal data. Second, the rules applied only to 'sensitive personal data', leaving vast categories of personal data—including contact details, location data, and behavioural data—outside their scope. Third, enforcement mechanisms were weak, with no dedicated data protection authority and penalties that were widely regarded as insufficient deterrents.

Table 2.1: Evolution of Data Protection Law in India: Legislative Timeline

Year	Development	Significance
2000	IT Act 2000 enacted	First digital regulatory statute; no dedicated privacy framework
2008	IT (Amendment) Act 2008	Section 43A introduced: liability for negligent data security
2011	SPDI Rules 2011	First substantive data rules; limited to sensitive data and body corporates
2017	Puttaswamy judgment	Constitutional right to privacy established; mandate for legislation
2018	Srikrishna Committee Report	Expert framework for comprehensive data protection legislation
2019	PDP Bill 2019 introduced	First comprehensive data protection bill; referred to JPC
2021	JPC Report	Parliamentary recommendations; Bill significantly amended
2022 (Aug)	PDP Bill 2019 withdrawn	Government announces comprehensive new framework
2022 (Nov)	DPDP Bill 2022 (draft)	Simplified framework released for public consultation
2023 (Aug)	DPDPA 2023 enacted	Comprehensive data protection statute; Presidential assent 11 Aug 2023
2025 (Jan)	Draft DPDP Rules 2025	Subordinate legislation released for public consultation

Source: Compiled by author from statutory materials and MeitY publications.

2.4 Justice K.S. Puttaswamy (Retd.) v Union of India (2017): The Constitutional Transformation

The nine-judge constitutional bench decision in Justice K.S. Puttaswamy (Retd.) v Union of India constitutes the single most significant jurisprudential event in the history of Indian privacy law and the constitutional foundation upon which the DPDPA 2023 rests.4 The matter arose from a challenge to the Aadhaar biometric identification system, which necessitated a determination of whether privacy was a fundamental right under the Constitution. The bench unanimously held that it was.

Justice D.Y. Chandrachud's plurality opinion provided the most intellectually comprehensive articulation of the constitutional right to privacy, tracing its philosophical foundations from John Locke's concept of natural rights through John Stuart Mill's harm principle to contemporary theories of autonomy and dignity. Crucially for data protection law, Chandrachud J held that the right to privacy includes the 'right to control the use of one's personal data and the right to be forgotten'—explicitly recognising informational privacy as a constitutionally protected dimension of the broader privacy right.

The Puttaswamy judgment established a tripartite test for evaluating restrictions on privacy: (i) the restriction must be sanctioned by law; (ii) it must be necessary for a legitimate state aim; and (iii) it must be proportionate, meaning the restriction must be the least intrusive measure available to achieve the legitimate aim. This proportionality analysis has direct implications for the compliance obligations imposed by the DPDPA 2023 on startups: restrictions on data processing activities constitute a form of regulation affecting the privacy rights of Data Fiduciaries' employees, customers, and operators; conversely, insufficient protection of Data Principals' rights would fail the legality and necessity requirements.

Subsequent decisions of the Supreme Court have elaborated the Puttaswamy framework in specific contexts. In K.S. Puttaswamy (Aadhaar) v Union of India (2018), the Court upheld the Aadhaar Act subject to certain conditions, applying the proportionality test to specific data collection and processing practices. In Subramanian Swamy v Union of India (2016), the Court had earlier recognised a right to informational privacy in the context of criminal defamation. These cases collectively constitute the constitutional framework within which the DPDPA 2023 must be interpreted and against which its provisions—including compliance obligations on startups—must be evaluated.

2.5 Srikrishna Committee and the Personal Data Protection Bill, 2019

Following Puttaswamy, the Central Government constituted an expert committee under the chairmanship of retired Supreme Court Justice B.N. Srikrishna in July 2017 to study issues related to data protection in India and recommend a framework. The Committee submitted its report, 'A Free and Fair Digital Economy: Protecting Privacy, Empowering Indians', along with a draft Personal Data Protection Bill, in July 2018.5

The Srikrishna Report drew extensively on the GDPR model while seeking to adapt it to India's specific socio-economic and constitutional context. Key features of the report that are relevant to the startup and SME compliance question include: (i) a recognition that compliance costs must be proportionate to enterprise capacity; (ii) a proposed distinction between 'data principals', 'data fiduciaries', and 'data processors' mirroring the GDPR's controller-processor distinction; (iii) a recommendation for purpose limitation, data minimisation, and storage limitation principles; (iv) a proposal for a Data Protection Authority of India as an independent regulatory body; and (v) a data localisation requirement for 'critical personal data'.

The Srikrishna Committee's report is notable for its explicit recognition of startup and SME concerns. The report acknowledged that 'a one-size-fits-all approach may be unduly burdensome for small businesses' and recommended that 'startup and small business exemptions be carefully considered in consultation with industry'. However, the draft PDP Bill 2018 accompanying the report did not translate this recognition into robust legislative provisions, offering only a general enabling power for the Data Protection Authority to exempt certain categories of data fiduciaries.

The Personal Data Protection Bill, 2019, introduced in the Lok Sabha on 11 December 2019, represented a more detailed legislative articulation of the Srikrishna framework but with significant modifications.6 The 2019 Bill was referred to a Joint Parliamentary Committee on the same day, initiating a two-year process of deliberation.

2.6 Joint Parliamentary Committee Report (December 2021)

The Joint Parliamentary Committee on the Personal Data Protection Bill, 2019, submitted its report in December 2021 after extensive consultations with government ministries, industry bodies, civil society organisations, and technical experts.7 The JPC's report recommended substantial amendments to the 2019 Bill, several of which have direct bearing on the startup compliance question.

On the question of SME accommodation, the JPC's report is notably ambivalent. On one hand, the Committee acknowledged representations from FICCI, CII, and Nasscom regarding the

compliance burden on smaller businesses and recommended that the Data Protection Authority develop 'sector-specific and size-specific guidance' to facilitate compliance. On the other hand, the report's proposed amendments to the penalty structure— significantly increasing maximum penalties—would have exacerbated the disproportionate impact on smaller enterprises.

The JPC report also recommended the inclusion of hardware manufacturers, intermediaries, and social media platforms within the regulatory framework and advocated for stringent data localisation requirements. These recommendations, if implemented, would have significantly expanded the compliance universe for startups operating in platform economies.

2.7 Draft DPDP Bill 2022 and the Path to Enactment

The government's withdrawal of the PDP Bill 2019 in August 2022, following the JPC's December 2021 report, was accompanied by an announcement that a comprehensive new framework was under preparation.8 The Draft Digital Personal Data Protection Bill, 2022, released for public consultation on 18 November 2022, represented a significant reconceptualisation of India's data protection framework, departing from the GDPR-influenced architecture of its predecessors.

The 2022 draft was markedly different from the 2019 Bill in several important respects. First, it adopted a significantly simplified structural architecture, reducing the bill to 30 clauses as compared to the 99 clauses of the 2019 Bill. Second, it replaced the GDPR- style 'data controller/data processor' distinction with the 'Data Fiduciary/Data Processor' terminology. Third, it substantially narrowed the scope of individual rights, omitting the right to data portability that had featured in the 2019 Bill. Fourth, it adopted a consent-centric framework supplemented by 'legitimate uses' rather than the GDPR's broader 'lawful bases' model.

From the startup compliance perspective, the 2022 draft introduced several features that would persist into the DPDPA 2023: the concept of 'Significant Data Fiduciaries' subject to enhanced obligations; the consent manager framework; and Section 17's exemption provisions. However, the draft's startup-specific accommodation mechanisms remained underdeveloped.

Table 2.2: Comparison — PDP Bill 2019 vs DPDPA 2023 on Key Provisions

Provision	**PDP Bill 2019**	**DPDPA 2023**
Scope	Personal and non-personal data	Personal data only
Lawful bases	Consent + 8 legitimate purposes	Consent + 7 deemed consent categories

Data portability	Included (s 19)	Omitted
Right to be forgotten	Included (s 20)	Omitted as standalone right
SDF concept	Not present	Introduced (s 10)
Data localisation	Critical personal data (local); sensitive data (copy)	Restricted to government notification
DPA structure	Multi-member authority	Board + Appellate Tribunal
SME exemptions	DPA enabling power	Section 17(2) enabling power
Max penalty	₹15 crore / 4% global turnover	₹250 crore per breach
Cross-border transfer	Whitelist of permitted countries	Blacklist approach (notification)

Source: Compiled by author from PDP Bill 2019 and DPDPA 2023.

2.8 Comparative Legislative Trajectories: EU, USA and China

A comparative perspective on the legislative trajectories of the GDPR, CCPA, and PIPL illuminates the choices made by the Indian legislature and enables identification of alternative design possibilities that could better accommodate startup compliance needs.

The GDPR emerged from a two-decade process of legislative revision of the EU's original 1995 Data Protection Directive, responding to technological change and the inadequacy of the member-state-level regulatory patchwork.9 From the outset, the GDPR's drafters were aware of the compliance burden concerns of SMEs, reflected in Article 30(5)'s exemption of undertakings with fewer than 250 employees from record-keeping requirements 'unless the processing it carries out is likely to result in a risk to the rights and freedoms of data subjects, the processing is not occasional, or the processing includes special categories of data'. The GDPR also introduced the concept of the lead supervisory authority to simplify cross-border compliance for organisations active in multiple member states.

The California Consumer Privacy Act, enacted in 2018 and amended by the California Privacy Rights Act in 2020, adopted a threshold-based exclusion that explicitly exempts businesses below certain size parameters.10 The CCPA applies to for-profit businesses that meet one or more of the following thresholds: (i) annual gross revenues exceeding USD 25 million; (ii) annual buying, selling, or sharing of personal information of 100,000 or more consumers or households; or (iii) deriving 50% or more of annual revenues from selling or sharing personal information. This bright-line exclusion mechanism provides the most direct

comparative precedent for threshold-based SME accommodation in the Indian context. China's PIPL, enacted in August 2021, reflects a different regulatory philosophy informed by China's state-centric approach to data governance.11 While the PIPL contains provisions specifically addressing small organisations and individual handlers of personal information, its primary analytical interest for this dissertation lies in its approach to data localisation and cross-border transfers—areas where India's regulatory design choices have significant implications for startups. The PIPL's requirement for security assessments and certifications for cross-border transfers provides a model of regulated rather than prohibited cross-border data flows that may be relevant to the DPDPA 2023's rule-making.

Table 2.3: Comparative Analysis — GDPR, CCPA, PIPL and DPDPA 2023

Feature	**GDPR (EU)**	**CCPA (California)**	**PIPL (China)**	**DPDPA 2023 (India)**
SME exemption	Record-keeping (<250 employees, conditions apply)	Revenue/data volume thresholds	Individual handlers — simplified	Section 17 enabling power only
Consent standard	Freely given, specific, informed, unambiguous	Opt-out for sale/sharing	Separately obtained, explicit	Free, specific, informed, unconditional
Data localisation	No mandatory localisation	N/A	Critical data: local storage	Government notification-based
DPO requirement	For high-risk processors	Not required	For processors above threshold	SDF only (DPO equivalent)
Max penalty	€20M / 4% global turnover	USD 7,500 per intentional violation	RMB 50M / 5% annual revenue	₹250 crore per breach
Cross-border	Adequacy/SCCs	No restriction	Security	Government

transfer	/B CRs		assessment/certific ation	blacklist (TBD)
Supervisory body	National DPAs + EDPB	CPPA	CAC + sectoral regulators	Data Protection Board
Right to portability	Yes (Art 20)	Yes	Yes	Omitted in final Act

Source: Compiled by author from statutory texts.

2.9 Summary

The legislative history traced in this chapter reveals that India's path to comprehensive data protection legislation was marked by constitutional imperatives, comparative influences, and persistent ambivalence about the appropriate balance between privacy protection and economic facilitation. The DPDPA 2023 represents the current culmination of this process, carrying within it the traces of its legislative predecessors while departing from them in significant respects. The most consequential departure, for the purposes of this dissertation, is the inadequate development of startup and SME accommodation mechanisms—a gap that is traceable to the legislative process itself and that the reform proposals in Chapter VII seek to address.

Footnotes — Chapter II

1 Information Technology Act, 2000 (Act 21 of 2000); Information Technology (Amendment) Act, 2008 (Act 10 of 2009).

2 Information Technology Act, 2000 (Act 21 of 2000); Information Technology (Amendment) Act, 2008 (Act 10 of 2009).

3 Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011 (SPDI Rules 2011), Ministry of Electronics and Information Technology.

4 Puttaswamy (n 8) para 648 (Chandrachud J).

5 Srikrishna Committee, 'A Free and Fair Digital Economy: Protecting Privacy, Empowering Indians' (MeitY, July 2018).

6 Personal Data Protection Bill, 2019 (PDP Bill 2019), as introduced in the Lok Sabha on 11 December 2019.

7 Joint Parliamentary Committee on the Personal Data Protection Bill, 2019, 'Report of

the Joint Committee on the Personal Data Protection Bill, 2019' (Lok Sabha Secretariat, December 2021).

8 Ministry of Electronics and Information Technology, 'Draft Digital Personal Data Protection Bill, 2022' (MeitY, November 2022).

9 Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data [2016] OJ L 119/1 (General Data Protection Regulation).

10 California Consumer Privacy Act of 2018 (CCPA), Cal Civ Code § 1798.100 et seq.

11 Personal Information Protection Law of the People's Republic of China (PIPL), promulgated 20 August 2021, effective 1 November 2021.

□

CHAPTER III

RESEARCH METHODOLOGY

3.1 Nature of Doctrinal Research

Legal scholarship has traditionally been dominated by doctrinal research, which involves the systematic analysis and synthesis of legal rules as they exist in authoritative legal sources—statutes, case law, constitutional provisions, and subordinate legislation.1 The doctrinal method proceeds by identifying the relevant legal rule or principle applicable to a given situation, tracing its historical development and interpretive trajectory through authoritative sources, and applying it to resolve questions of legal meaning, application, or reform. This methodology is well-suited to the present inquiry because the core research questions concern the interpretation, application, and evaluation of the DPDPA 2023 as a legal text operating within a broader legal and constitutional context.

The methodological choice is not, however, a passive or uncritical one. As Hutchinson and Duncan have argued, doctrinal legal research, properly understood, involves more than the mechanical application of existing rules to new facts.2 It encompasses critical evaluation of the internal coherence of a legal framework, comparative analysis of alternative regulatory approaches, and—where the researcher adopts a reform orientation—normative arguments for how the law should be redesigned. This dissertation employs doctrinal research in this richer sense: not merely as an exposition of what the DPDPA 2023 says, but as a critical evaluation of what it means, how it works in practice, and how it should be reformed.

3.2 Doctrinal Legal Research: Conceptual Foundations

Doctrinal legal research, as practised in the Indian legal academy, has been systematically theorised by scholars including S.N. Jain and P. Ishwara Bhat.3 Jain's foundational 1975 article distinguished doctrinal from non-doctrinal (socio-legal) research, characterising doctrinal research as analysis of 'a legal proposition or propositions by way of analysing the existing statutory provisions and cases by applying the power of reasoning'.4 Bhat has more recently elaborated a nuanced account of doctrinal methodology that accommodates the integration of policy analysis, comparative law, and empirical data within a fundamentally doctrinal framework.

The theoretical foundations of doctrinal legal research in the Anglo-American tradition trace to the legal process school associated with Hart and Sacks, which conceived of legal analysis as the systematic application of duly enacted legal norms to identified fact patterns.5 However, the critical legal studies movement and subsequent post-critical scholarship have significantly complicated this picture, emphasising the indeterminacy of legal texts, the ideological dimensions of legal interpretation, and the embeddedness of legal rules in social and economic structures. This dissertation is informed by this critical consciousness: it does not treat the DPDPA 2023 as a self-interpreting text but engages critically with its interpretive ambiguities, internal tensions, and relationship to external social and economic realities.

The comparative law dimension of this dissertation's methodology draws on the traditions of functional and contextual comparative legal scholarship.6 The functional approach identifies functionally equivalent legal mechanisms across different jurisdictions— asking not 'what do these jurisdictions' laws say?' but 'what purposes do these legal mechanisms serve, and how effectively do they serve them?' This approach enables a more substantive comparison of the SME accommodation mechanisms in the GDPR, CCPA, PIPL, and Singapore PDPA than a purely textual comparison would permit.

3.3 Sources of Law Employed

The research draws on a hierarchy of primary, secondary, and tertiary sources.

3.3.1 Primary Sources

The primary sources engaged in this dissertation include:

(i) The Digital Personal Data Protection Act, 2023 (Act No. 22 of 2023), published in the Gazette of India Extraordinary on 11 August 2023.7

(ii) Constitutional provisions, particularly Article 21 (right to life and personal liberty),

Article 19(1)(g) (right to practise any profession or to carry on any occupation, trade or business), Article 19(6) (reasonable restrictions on Article 19(1)(g)), and the directive principles under Article 39.8

(iii) Supreme Court decisions, most significantly Justice K.S. Puttaswamy (Retd.) v Union of India (2017) and its progeny.9

(iv) The Draft Digital Personal Data Protection Rules, 2025, released by MeitY for public consultation in January 2025.10

(v) Parliamentary debates on the DPDPA 2023, the JPC Report on the PDP Bill 2019, the Srikrishna Committee Report, and other official documents forming part of the legislative history.

(vi) Foreign statutes including the GDPR, CCPA, PIPL, and Singapore PDPA.

3.3.2 Secondary Sources

Secondary sources include academic articles, monographs, practitioner texts, and institutional reports. These include the thirty works reviewed in the literature review section of Chapter I, as well as additional secondary sources cited throughout the dissertation.

3.3.3 Empirical and Statistical Materials

The doctrinal analysis is supplemented by secondary empirical data drawn from institutional reports published by MeitY, Nasscom, iSPIRT, FICCI-EY, KPMG, PwC India, Deloitte, the World Bank, and IAPP.11 These materials provide quantitative grounding for the compliance burden analysis in Chapter V. It must be emphasised that the use of this data is supplementary rather than constitutive of the methodology: the research questions are primarily legal in nature, and the empirical data serves to contextualise and illustrate doctrinal findings rather than to test empirical hypotheses.

3.4 Comparative Methodology

The comparative component of this research involves analysis of four major data protection statutes: the GDPR (EU), CCPA (California/USA), PIPL (China), and Singapore PDPA. The selection of these four jurisdictions is justified on the following grounds: (i) the GDPR is the world's most influential data protection statute and served as a significant reference point for the DPDPA 2023's drafters; (ii) the CCPA provides the most developed example of threshold-based SME exclusion in data protection law; (iii) the PIPL offers a directly relevant

comparison as a comprehensive data protection statute enacted by another major emerging economy contemporaneously with India's legislative process; and (iv) Singapore's PDPA is the most directly relevant model from India's immediate regional context, drawing on Commonwealth legal traditions.

The comparative analysis employs the functional method of comparative law, which, as articulated by Zweigert and Kötz, proceeds by identifying the comparable legal institution or rule, examining how it operates in each jurisdiction, and assessing the comparative adequacy of different approaches.12 For the present research, the 'comparable institution' is the SME accommodation mechanism in data protection law, and the functional comparison examines how each jurisdiction operationalises the objective of reducing compliance burden for smaller enterprises.

3.5 Secondary Data Sources and Empirical Materials

The secondary empirical data sources used in this dissertation are drawn from five categories of institutional reports:13

(i) Industry surveys: Nasscom's Annual Strategic Review 2024, iSPIRT's Privacy Compliance Survey 2024, FICCI-EY's Data Protection Compliance Readiness Report 2024, PwC India's Privacy Readiness Survey 2024, and KPMG's DPDP Act Compliance Cost Assessment for SMEs 2024.14

(ii) Government reports: MeitY's Digital India Programme Annual Report 2023-24, DPIIT's Startup India Annual Report 2023-24, and RBI's Monetary Policy Report April 2024.15

(iii) International institutional reports: World Bank's Doing Business in India 2023, IMF's World Economic Outlook October 2024, and WEF's Global Risks Report 2024.16

(iv) Professional services reports: Deloitte's GDPR Compliance Costs: Three Years On (2021) for comparative benchmarking.17

(v) Multi-stakeholder reports: Nasscom-DSCI's Data Protection Impact on Startup Ecosystem (2024), which combines industry survey data with doctrinal analysis.18

All empirical data derived from these sources is used for illustrative and contextualising purposes within a doctrinal framework. The researcher is cognisant of the limitations of secondary data—including potential sampling biases, variations in methodology across studies, and the interests of commissioning organisations—and these limitations are acknowledged where relevant in the analysis.

3.6 Limitations of the Methodology

The doctrinal methodology carries several inherent limitations that must be acknowledged. First, the absence of primary empirical data—from structured surveys of startup compliance officers, interview data from regulatory personnel, or experimental compliance cost studies—means that the analysis of compliance burden in Chapter V relies on secondary institutional data that may not fully represent the diversity of startup compliance experiences. Future research combining doctrinal analysis with primary empirical methods would provide a more comprehensive assessment.

Second, the DPDP Rules 2025 were at the time of writing available only as a draft for public consultation, with significant provisions still unspecified or subject to change. The analysis of the subordinate legislative framework is therefore necessarily provisional, and the dissertation acknowledges that final rules may alter the compliance calculus in material ways.

Third, comparative law methodology carries inherent risks of acontextual transplantation: the GDPR's SME accommodation mechanisms, for example, are embedded in a specific EU institutional and economic context that differs significantly from India's. The dissertation is mindful of these contextual differences and seeks to propose contextually appropriate reforms rather than straightforward transplants.

3.7 Ethical Considerations

This research does not involve primary data collection involving human subjects and therefore does not raise ethical concerns relating to informed consent, privacy of research participants, or confidentiality of data. All sources relied upon are publicly available and are cited in accordance with the Indian Law Institute citation format. Where unpublished institutional reports have been referenced, permission was obtained or the reports were publicly available.

The researcher declares no conflict of interest with any of the institutions whose reports are cited, including industry bodies, government agencies, or professional services firms. The views expressed in this dissertation are those of the researcher alone and do not represent the views of the supervising institution, the supervisor, or any of the institutions cited.

Footnotes — Chapter III

1 William N Eskridge and Philip P Frickey, 'Legislation Scholarship and Pedagogy in the Post-Legal Process Era' (1994) 48 University of Pittsburgh Law Review 691, 694.

2 Terry Hutchinson and Nigel Duncan, 'Defining and Describing What We Do: Doctrinal Legal Research' (2012) 17 Deakin Law Review 83.

3 S N Jain, 'Doctrinal and Non-Doctrinal Legal Research' (1975) 17 Journal of the Indian Law Institute 497.

4 Ibid 499.

5 Upendra Baxi, 'The Crisis of the Indian Legal System' (Vikas Publishing House 1982) 23.

6 William Twining, 'Globalisation and Legal Theory' (Cambridge University Press 2000) 89.

7 Digital Personal Data Protection Act, 2023 (n 1).

8 Constitution of India, 1950, art 21.

9 Puttaswamy (n 8).

10 MeitY, 'DPDP Rules, 2025: Draft for Public Consultation' (MeitY, January 2025) <https://www.meity.gov.in> accessed 12 March 2025.

11 Nasscom (n 2).

12 William Twining, 'Globalisation and Legal Theory' (Cambridge University Press 2000) 89.

13 iSPIRT Foundation, 'Privacy Compliance Survey of Indian Startups 2024' (iSPIRT, 2024) 19.

14 FICCI and EY, 'Data Protection Compliance Readiness Report 2024' (FICCI, March 2024) 22.

15 World Bank, 'Doing Business in India: Digital Compliance Costs 2023' (World Bank Group, 2023) 34.

16 Nasscom-Dsci, 'Data Protection Impact on Startup Ecosystem' (Nasscom, 2024) 11.

17 CII, 'DPDP Act: Industry Preparedness Survey 2024' (CII, February 2024) 6.

18 International Monetary Fund, 'World Economic Outlook: October 2024' (IMF, 2024) 48.

□

CHAPTER IV

DECODING THE DIGITAL PERSONAL DATA PROTECTION ACT 2023 — ARCHITECTURE, RIGHTS, AND OBLIGATIONS

4.1 Overview and Structure

The Digital Personal Data Protection Act, 2023 comprises forty-four sections organised into nine conceptual parts: definitions and scope; lawful processing and consent; rights of data principals; obligations of data fiduciaries; significant data fiduciaries; transfer of personal data outside India; the Data Protection Board; penalties and appeals; and miscellaneous provisions. This structural simplicity—44 sections as compared to the 99 of the PDP Bill 2019—reflects a deliberate legislative philosophy of enabling rather than prescriptive regulation, with the detailed operational framework anticipated to be supplied through subordinate legislation in the form of DPDP Rules.

Table 4.1: Structure of the Digital Personal Data Protection Act 2023

Sections	Subject Matter	Startup Relevance
1-2	Preliminary — Short title, commencement, definitions	High — defines scope of obligation
3-8	Grounds for processing personal data — Consent and deemed consent	Very High — primary compliance trigger
9	Processing of personal data of children	High — applies to EdTech/health apps
10	Additional obligations of Significant Data Fiduciaries	High — risk of classification
11-14	Rights of Data Principals	High — requires backend systems
15-16	Duties of Data Principals and Exemptions	Medium
17	Exemptions for certain Data Fiduciaries	Very High — startup accommodation
18-21	Data Protection Board — Composition, Powers	Medium — affects enforcement risk
22-28	Board — Procedure, orders, appeals	Medium
29-32	Appellate Tribunal provisions	Low (appellate stage)
33-34	Penalties	Very High — financial risk
35-44	Powers of Government, miscellaneous	High — rule-making power scope

Source: Compiled by author from DPDPA 2023 text.

4.2 Definitional Framework

The definitions in Section 2 of the DPDPA 2023 are foundational to understanding the scope and application of the Act. Several definitions warrant detailed examination from the startup compliance perspective.

Section 2(t) defines 'personal data' as 'any data about an individual who is identifiable by or in relation to such data'.1 The breadth of this definition is significant for startups: unlike the SPDI Rules 2011, which applied only to a defined list of sensitive data categories, the DPDPA 2023's definition of personal data is technology-neutral and potentially encompasses any digital data that can be linked to an identifiable individual. This includes email addresses, IP addresses, device identifiers, cookies, behavioural data, and inferred attributes—the entire operational data substrate of a digital startup.

Section 2(i) defines 'Data Fiduciary' as 'any person who alone or in conjunction with other persons determines the purpose and means of processing of personal data'.2 This definition closely mirrors the GDPR's concept of a 'data controller' and similarly encompasses startups that determine the purposes for which they collect and use their customers' or employees' personal data. Startups operating on SaaS or platform models— where they both collect data on behalf of their clients and use aggregated data for their own analytics—may face complex questions about whether they are Data Fiduciaries or Data Processors (Section 2(k)) in relation to different processing activities.

Section 2(j) defines 'Data Principal' as the individual to whom personal data relates,3 with specific provisions for minors (persons under 18) and persons with disabilities whose rights must be exercised by parents or guardians. For EdTech startups and apps serving children, this creates significant consent management challenges—requiring verifiable parental consent mechanisms that are technically demanding and potentially costly to implement.

4.3 Lawful Processing and Consent Architecture

Section 4 of the DPDPA 2023 establishes the foundational principle that personal data may only be processed for 'a lawful purpose'—defined as any purpose not expressly forbidden by law and for which consent has been given, or which falls within one of the deemed consent categories in Section 7.4

Section 5 elaborates the principle of purpose limitation and data minimisation: Data Fiduciaries may only process personal data for the specific purpose for which consent was obtained, must collect only such data as is 'necessary' for the specified purpose, and must retain data only for the period necessary to serve the specified purpose.5 These provisions, while

philosophically sound, impose operational architecture requirements on startups that may be difficult to implement without significant investment in data management infrastructure.

Section 6 establishes the consent framework—the most significant compliance provision for most startups.6 Consent must be 'free, specific, informed, unconditional and unambiguous', obtained through a 'clear affirmative action'. The notice required under Section 6(1) must be provided prior to seeking consent and must, as prescribed by the Rules, contain a description of personal data sought, the purpose of processing, the manner in which data principals can exercise their rights, and information on the complaint process.7

Sections 6(4) through 6(6) address the management of consent: consent must be capable of withdrawal by the Data Principal as easily as it was given; processing that occurred prior to withdrawal remains lawful; and Data Principals who have given consent through a consent manager may manage their consents through that platform.8 The consent manager concept—centralised platforms through which individuals can manage consent across multiple Data Fiduciaries—is an innovative regulatory mechanism but presupposes a functioning consent manager ecosystem that does not yet exist in India.

Section 7 enumerates seven categories of 'deemed consent'—situations where processing is lawful without explicit consent.9 These include: (i) voluntary provision of data for a specific purpose; (ii) processing necessary for performance of a contract; (iii) processing by the State for subsidies and services; (iv) processing in response to medical emergencies; (v) processing for employment purposes; (vi) processing for 'legitimate interests' of the Data Fiduciary; and (vii) processing for certain public interest functions. The legitimate interests category in Section 7(f) is particularly significant for startups as it provides a potential lawful basis for processing beyond explicit consent—but the DPDPA 2023's version of this concept is narrower than its GDPR equivalent, requiring that the processing be necessary and that the Data Principal not have reasonable reason to object, while also requiring compliance with specific conditions to be prescribed in the Rules.

4.4 Rights of Data Principals

Sections 11 through 14 confer a suite of enforceable rights on Data Principals, the operationalisation of which requires significant backend data management investment from Data Fiduciaries including startups.10

Table 4.2: Rights of Data Principals under DPDPA 2023

Section	Right	Content	Startup Compliance Requirement
11	Right to information	Know categories of data, purpose, Data Processors, countries of transfer	Accessible privacy dashboard; customer service capacity
12	Right to correction and erasure	Correct inaccurate data; erasure upon withdrawal of consent	Backend data editing and deletion systems
13	Right of grievance redressal	Grievance officer; resolution within prescribed time	Dedicated grievance mechanism; DPO-equivalent role
14	Right to nominate	Nominate another person to exercise rights upon death or incapacity	Nomination registry and verification system

Source: DPDPA 2023, ss 11-14.

The right to correction and erasure under Section 12 is particularly operationally demanding for startups.11 Startups that use data distributed across multiple cloud services, analytics platforms, and third-party integrations must build systems capable of identifying all instances of a Data Principal's data across their entire technology stack, correcting or erasing it upon request, and informing their Data Processors of the action taken. For a startup using five to ten SaaS tools simultaneously—which is typical—this creates a data mapping and management challenge of significant complexity.

The right of grievance redressal under Section 13 requires Data Fiduciaries to establish a functioning grievance mechanism and appoint a grievance officer.12 The DPDP Rules 2025 are expected to prescribe specific timelines and procedures for grievance resolution, similar to the IT Act's intermediary liability framework. For a startup with a small team and no dedicated legal or compliance staff, operating a compliant grievance mechanism

—available in all prescribed languages, responsive within prescribed timelines, and capable of escalating unresolved matters to the Data Protection Board—represents a non-trivial operational investment.

4.5 Obligations of Data Fiduciaries

Section 8 sets out the general obligations of Data Fiduciaries—the core compliance obligations

applicable to all Data Fiduciaries including startups.13 These include: (i) ensuring the accuracy and completeness of personal data; (ii) implementing reasonable security safeguards; (iii) notifying the Data Protection Board and affected Data Principals of personal data breaches; (iv) erasing personal data upon withdrawal of consent or upon the data no longer serving its purpose; and (v) publishing contact information for their Data Protection Officer or point of contact.

Table 4.3: Obligations of Data Fiduciaries — Statutory Framework

Obligation	**Statutory Basis**	**Nature**	**Compliance Cost Level**
Data accuracy and completeness	Section 8(3)	Operational	Medium
Security safeguards	Section 8(4)	Technical/Operational	High
Breach notification (Board)	Section 8(6)	Procedural	Medium
Breach notification (Data Principals)	Section 8(7)	Procedural	Medium
Data erasure on consent withdrawal	Section 8(7)	Technical	High
Publish contact/DPO details	Section 8(8)	Organisational	Low
Children's data protection	Section 9	Technical/Legal	Very High
Consent management compliance	Section 6	Technical/Operational	High
Response to data principal rights	Sections 11-14	Operational	High
Appointment of consent manager	Section 6(4)	Contractual/Operational	Medium
Data localisation (if mandated)	Section 16	Technical/Infrastructure	Very High

Source: Compiled by author from DPDPA 2023, ss 6-16.

The children's data protection provisions in Section 9 deserve particular attention.14 Section 9(1) requires that before processing personal data of a child (person under 18), the Data Fiduciary must obtain verifiable parental consent. Section 9(2) prohibits the tracking or behavioural monitoring of children and targeted advertising directed at children. Section 9(3) empowers the Central Government to exempt certain classes of Data Fiduciaries from these requirements where they can demonstrate appropriate safeguards.

For EdTech startups—which constitute one of India's most prominent startup sectors, with companies like BYJU's (now restructuring), Unacademy, Vedantu, and thousands of smaller players serving millions of school-age children—the children's data provisions create formidable compliance challenges. Implementing a verifiable parental consent mechanism that satisfies the Act's requirements while remaining operationally workable for a startup serving millions of users at low per-user cost is a challenge that comparable global platforms have struggled with even with vastly greater resources.

4.6 Significant Data Fiduciaries

Section 10 introduces the concept of 'Significant Data Fiduciary' (SDF)—a category of Data Fiduciary subject to enhanced compliance obligations.15 The Central Government may, on the recommendation of the Data Protection Board, designate any Data Fiduciary or class of Data Fiduciaries as SDFs based on an assessment of: (i) volume and sensitivity of personal data processed; (ii) risk to the rights of Data Principals; (iii) potential impact on the sovereignty and integrity of India; (iv) risk to electoral democracy; (v) security of the State; and (vi) public order.

SDFs are subject to additional obligations not applicable to ordinary Data Fiduciaries: appointment of a Data Protection Officer (DPO); appointment of an independent Data Auditor; periodic Data Protection Impact Assessments; and compliance with any other additional obligations specified by the Central Government. From the startup compliance perspective, SDF designation represents an existential compliance challenge: a growth-stage startup that achieves scale rapidly may find itself designated an SDF before it has the infrastructure to comply with the enhanced obligations.

The criteria for SDF designation include 'volume... of personal data processed'—a criterion that, in the absence of clear thresholds, creates significant uncertainty for startups experiencing rapid user growth. A startup with 1 million users may be below any eventual SDF threshold today but above it in six months. Unlike SDF designation under the GDPR's DPO requirement

threshold—which provides clear numerical guidance—the DPDPA 2023's SDF criteria are subjective and criteria-based, generating planning uncertainty for startups.

4.7 Cross-Border Data Transfers and Data Localisation

Section 16 of the DPDPA 2023 addresses the transfer of personal data outside India.16 The Act adopts a 'blacklist' approach—personal data may be transferred outside India except to countries that the Central Government notifies as restricted. This represents a significant departure from the 2019 Bill's 'whitelist' approach and from the GDPR's adequacy decision mechanism. The blacklist approach, in principle, permits cross-border data transfers by default while allowing the government to restrict specific concerning transfers.

For Indian startups, this framework has several important implications. First, until the Central Government notifies the restricted countries list, the legal status of cross-border data transfers remains uncertain—creating compliance planning challenges for startups whose cloud infrastructure spans multiple jurisdictions.17 Second, even under a blacklist approach, startups that transfer data to countries on the restricted list—which may include data transfers to analytics platforms, cloud services, or marketing tools hosted in certain countries—will need to restructure their data flows. Third, any sector-specific data localisation requirements imposed by other regulations (such as RBI's requirements for payment data) continue to apply independently and may conflict with the DPDPA 2023 framework.

4.8 The Data Protection Board of India

Sections 18 through 27 establish the Data Protection Board of India (DPBI) as the primary regulatory and adjudicatory body under the Act.18 The Board's composition— including a Chairperson and such other Members as the Central Government may appoint— and its appointment mechanism have been criticised by scholars and civil society as lacking sufficient independence from the executive. From the startup compliance perspective, however, the Board's functional design is more immediately relevant than its composition.

The Board has powers to receive complaints from Data Principals or refer matters suo motu, summon and investigate Data Fiduciaries, impose penalties, and issue directions for remediation. For startups, the practical significance of the Board lies in its enforcement dispositions: a startup in early compliance or good faith non-compliance faces very different consequences depending on whether the Board takes a facilitative, guidance-oriented approach or a punitive, penalty-first approach. International experience—particularly with

the UK's ICO, which has developed an explicit startup engagement programme—suggests that the Board's approach to startup engagement will be more consequential for the startup ecosystem than the formal penalty structure alone.

4.9 Penalties, Offences and Enforcement

Sections 33 and 34 of the DPDPA 2023 set out the penalty framework—one of the most stringent in any comparable jurisdiction when considered in absolute terms.19

Table 4.4: Penalty Schedule under Sections 33 and 34 of DPDPA 2023

Violation	Section	Maximum Penalty
Failure to implement security safeguards; breach results in data compromise	33(1)	₹250 crore
Failure to notify breach to Board	33(2)	₹200 crore
Breach of children's data protection provisions	33(3)	₹200 crore
Breach of additional obligations of SDF	33(4)	₹150 crore
Breach of voluntary undertakings before Board	33(5)	₹10,000 crore
Any other provision of the Act or Rules	33(6)	₹50 crore
False/misleading information to Board	34(1)	₹10,000

Source: DPDPA 2023, ss 33-34.

The penalty framework raises acute concerns from the startup compliance perspective. The ₹250 crore maximum penalty for a single data breach involving security safeguard failure—equivalent to approximately USD 30 million—is not only the highest in any comparable jurisdiction in absolute terms but is also structured as a per-breach rather than proportional penalty.20 Unlike the GDPR, which calibrates penalties as a percentage of annual turnover (up to 4% of global annual revenue), the DPDPA 2023's absolute penalty caps can represent several years' revenue for a startup—potentially a bankruptcy-triggering consequence for a growth-stage company. This structural asymmetry—between large technology companies for whom ₹250 crore is a manageable fine and startups for whom it represents existential exposure—is arguably inconsistent with the proportionality principles articulated in Puttaswamy.

4.10 Exemptions under Section 17

Section 17 is the principal legislative provision through which the DPDPA 2023 addresses the compliance differentiation question.21 Section 17(2) empowers the Central Government to exempt from the Act's application any instrumentality of the State or class of Data Fiduciaries where the Central Government is of the opinion that processing is necessary for: (a) prevention, detection, investigation or prosecution of offences, or (b) any matter prescribed by the government.

Table 4.5: Exemptions under Section 17 of DPDPA 2023

Provision	Beneficiary	Scope of Exemption	Startup Relevance
Section 17(1) (a)	State instrumentalities (national security, sovereignty)	All provisions except Section 8(7) (breach notification)	None directly
Section 17(1) (b)	Research/archiving for public interest	Specified provisions (Rules to prescribe)	Limited — academic/research startups
Section 17(1) (c)	Processing outside India on behalf of foreign entities	Entire Act	Relevant for Indian-origin startups with foreign data
Section 17(2) (a)	Government-specified Data Fiduciaries (law enforcement)	All provisions except breach notification	None
Section 17(2) (b)	Classes notified by Central Government	To be prescribed by notification	Potential — depends on notification

Source: Compiled by author from DPDPA 2023, s 17.

The critical startup-relevant provision is Section 17(2)(b), which allows the Central Government to exempt classes of Data Fiduciaries from the Act. This is an enabling provision rather than a self-executing exemption: it creates the legislative authority for startup accommodation but does not itself provide any exemption. The provision's efficacy

depends entirely on whether the Central Government exercises this power and, if it does, on the breadth and precision of the exemption notification.22

4.11 Summary

The doctrinal analysis in this chapter reveals the DPDPA 2023 as a structurally ambitious statute that imposes a comprehensive and largely symmetric compliance framework on all categories of Data Fiduciaries. The Act's key compliance-generating provisions—the consent architecture, data principal rights management obligations, security safeguards, children's data provisions, and penalty structure—apply broadly across the enterprise spectrum with limited calibration for enterprise size or data-processing capacity. The Section 17 exemption framework provides a legislative valve but has not been activated in startup-specific terms. These findings set up the detailed compliance burden analysis in Chapter V and the comparative adequacy assessment in Chapter VI.

Footnotes — Chapter IV

1 Digital Personal Data Protection Act, 2023 (n 1) s 2(t) proviso.
2 Ibid s 2(i).
3 Ibid s 2(j).
4 Ibid s 4.
5 Ibid s 5.
6 Ibid s 6(1).
7 Ibid s 6(4).
8 Ibid s 6(6).
9 Ibid s 7.
10 Ibid s 11.
11 Ibid s 12.
12 Ibid s 13.
13 Ibid s 8.
14 Ibid s 9.
15 Ibid s 10.
16 Ibid s 16.
17 Ibid s 17.
18 Ibid s 18.

19 Ibid s 33.

20 Ibid s 34.

21 Ibid s 36.

22 Ibid s 40.

CHAPTER V

COMPLIANCE BURDEN ON STARTUPS AND SMEs — EMPIRICAL ASSESSMENT AND DOCTRINAL ANALYSIS

5.1 Introduction: Defining the Startup and SME Ecosystem

Before the compliance burden can be assessed, it is necessary to define the population of enterprises whose compliance experience is the subject of this analysis. India's startup and SME ecosystem is characterised by extraordinary diversity—in terms of sector, business model, data intensity, geographic reach, and enterprise scale—and any generalisation about 'startup compliance experience' must acknowledge this diversity.

For the purposes of this dissertation, 'startup' is primarily understood with reference to the DPIIT's recognition criteria under the Startup India initiative: an entity incorporated in India, less than ten years from its date of incorporation, with annual turnover not exceeding ₹100 crore, and working towards innovation, development, or improvement of products, processes, or services.1 'SME' is understood with reference to the MSME Development (Amendment) Act 2020 classification: micro enterprises (investment up to ₹1 crore, turnover up to ₹5 crore), small enterprises (investment up to ₹10 crore, turnover up to ₹50 crore), and medium enterprises (investment up to ₹50 crore, turnover up to ₹250 crore). These classifications are not mutually exclusive—many recognised startups are also micro-enterprises under the MSME framework.

Table 5.1: India's Startup Ecosystem — Key Statistics (2024)

Parameter	Data Point	Source
Total DPIIT-recognised startups (March 2024)	1,17,254	DPIIT Startup India Report 2024
Startups with <10 employees	~84% (~98,500)	Nasscom Strategic Review 2024

Startups classified as micro-enterprises	~72% (~84,500)	FICCI-EY 2024
Startups with dedicated legal/compliance team	~16%	PwC India 2024
Startups with existing privacy policy	~45%	iSPIRT Survey 2024
Startups with consent management system	~15%	PwC India 2024
Startups with data breach response plan	~21%	Nasscom-DSCI 2024
Total MSME units	~63.4 million	MSME Ministry 2024
MSMEs with digital presence	~15 million	MeitY 2024
MSMEs likely covered by DPDPA	~8-10 million (est.)	World Bank 2023

Source: Compiled by author from institutional reports cited above.

5.2 Consent-Collection Infrastructure: Cost and Complexity

The DPDPA 2023's consent framework—centred on Section 6's requirement for free, specific, informed, unconditional, and unambiguous consent through a clear affirmative action—creates a substantial technical and operational compliance requirement for startups.2 The consent collection infrastructure required to satisfy the Act's requirements encompasses:

(i) a notice generation system capable of producing individualised, purpose-specific, legally compliant privacy notices; (ii) a consent capture system with audit trails recording the precise consent given and the date, time, and mechanism of capture; (iii) a consent withdrawal mechanism equally accessible to the consent-giving mechanism; and (iv) if the consent manager ecosystem envisaged by the Act is operationalised, integration with consent manager platforms.

The iSPIRT survey found that 67% of startups surveyed would need to build or procure an entirely new consent management system to comply with the Act, at an estimated median cost of ₹18 lakh for a small startup (less than 50 employees).3 This figure understates the full cost as it excludes the ongoing operational cost of managing consent records, processing withdrawal requests, and updating notices as purposes change.

Table 5.2: Estimated Compliance Cost Breakdown for a Typical Indian Startup

Cost Component	Micro Startup (<10 empl.)	Small Startup (10-50 empl.)	Medium Startup (50-200 empl.)
Legal advisory (initial)	₹3-5 lakh	₹10-20 lakh	₹30-60 lakh
Privacy policy drafting	₹50,000-1 lakh	₹1-3 lakh	₹3-8 lakh
Consent management system	₹5-10 lakh	₹15-25 lakh	₹40-80 lakh
Data mapping and audit	₹2-4 lakh	₹8-15 lakh	₹20-50 lakh
Security infrastructure upgrade	₹5-15 lakh	₹20-50 lakh	₹60-150 lakh
Staff training	₹50,000-1 lakh	₹2-5 lakh	₹8-20 lakh
Breach notification system	₹1-3 lakh	₹5-10 lakh	₹15-40 lakh
Grievance mechanism	₹1-2 lakh	₹3-8 lakh	₹10-30 lakh
Ongoing compliance (annual)	₹3-7 lakh/yr	₹15-30 lakh/yr	₹50-120 lakh/yr
TOTAL (Year 1)	₹21-48 lakh	₹79-1.36 crore	₹2.36-5.58 crore

Source: Compiled from KPMG DPDP Act Compliance Cost Assessment 2024; iSPIRT Survey 2024; FICCI-EY 2024. Estimates are for illustrative purposes.

The cost data must be read against the financial profile of the typical Indian startup. The iSPIRT survey found that 52% of DPIIT-recognised startups operate on annual revenues of less than ₹50 lakh.4 For such a startup, an initial compliance cost of ₹21-48 lakh represents 42-96% of annual revenue—a compliance burden ratio that is structurally prohibitive. Even for a startup with revenues of ₹1 crore, a compliance cost of ₹30-50 lakh represents 30-50% of revenue, compared to less than 0.5% for a large technology corporation.

5.3 Notice Requirements and Operational Friction

Section 5 of the DPDPA 2023, read with the Draft DPDP Rules 2025, imposes detailed notice requirements on Data Fiduciaries. The notice must be provided before or at the time of seeking consent and must describe: the personal data to be processed, the purpose of processing, the manner in which Data Principals may exercise their rights, and the procedure for complaint to the Data Protection Board.5

For multi-product startups that collect different categories of personal data for multiple purposes across different product interfaces, the notice requirement generates a combinatorial compliance challenge. A FinTech startup offering payment, lending, insurance, and investment products may need to maintain and update four separate consent architectures, each with its own notice, purpose specification, and consent record. The operational cost of maintaining these systems—and particularly of updating them when purposes change, new features are added, or regulatory guidance evolves—creates ongoing compliance friction that imposes a competitive disadvantage relative to incumbent players with established compliance infrastructure.

The GDPR experience is instructive here: a 2021 Deloitte study found that three years after GDPR's implementation, SMEs with fewer than 250 employees were spending on average 1.3% of annual revenues on ongoing GDPR compliance, compared to 0.4% for large enterprises.6 The per-employee compliance cost for micro-enterprises was found to be 4.2 times higher than for large corporations. If a similar ratio applies in the Indian context, the ongoing compliance cost of the DPDPA 2023 for micro-enterprises would represent a significant and persistent competitive disadvantage.

5.4 Data Principal Rights Management Systems

The suite of Data Principal rights under Sections 11 through 14—information, correction and erasure, grievance redressal, and nomination—requires Data Fiduciaries to build and maintain rights management systems capable of receiving, processing, and responding to rights requests within prescribed timescales.7

For startups, the rights management obligation has three dimensions of compliance challenge. First, the technical infrastructure challenge: implementing an erasure function requires the startup to be able to identify all instances of a Data Principal's data across its entire data architecture—including databases, backups, analytics systems, email marketing platforms, and third-party integrations. For a startup whose data architecture has evolved organically rather than been designed with compliance in mind (which describes most startups), a retrofit implementation of a universal erasure capability is technically demanding and costly.

Second, the organisational challenge: the right of grievance redressal requires a named grievance officer with genuine capacity to investigate and resolve complaints. For a three-person startup, designating one of the founders as 'grievance officer' in compliance with the Act may technically satisfy the provision but does not provide an operationally credible

grievance function. PwC India's 2024 survey found that only 23% of startups surveyed had staff with any data protection training, and only 8% had individuals who could credibly serve as a Data Protection Officer.8

Third, the scalability challenge: as a startup grows its user base, the volume of rights requests will grow proportionally or faster. A startup with 100,000 users may receive several hundred rights requests per month. Each request requires human review, technical intervention, and a formal response. Without automated rights management infrastructure— which is itself a significant investment—the operational burden of rights management can scale to consume significant management time.

5.5 Data Localisation Obligations and Startup Operations

While the DPDPA 2023's data localisation provisions are not yet operationalised— pending the government's notification of the restricted countries list under Section 16—the prospect of data localisation requirements generates planning uncertainty that has already begun affecting startup decision-making regarding cloud infrastructure.9

Most Indian startups operate on cloud infrastructure provided by Amazon Web Services (AWS), Microsoft Azure, or Google Cloud Platform (GCP)—all of which offer Indian data centres but whose default configurations may store or process data in multiple geographic locations. A data localisation requirement would compel startups to audit their entire cloud architecture, identify data flows that traverse prohibited country boundaries, and restructure their cloud configurations to ensure compliance.

The compliance cost of cloud architecture restructuring for data localisation has been estimated by KPMG at ₹15-75 lakh for a typical startup, depending on architecture complexity.10 Beyond the one-time restructuring cost, data localisation may also increase ongoing cloud costs if it requires use of more expensive local infrastructure options or forecloses access to globally distributed content delivery networks that reduce latency. For HealthTech startups whose core product is a globally accessible medical information system, or for EdTech platforms whose content is hosted on global CDNs, the operational impact of data localisation could be severe.

5.6 Significant Data Fiduciary Status: Risk Exposure for Growth-Stage Startups

The risk of being designated a Significant Data Fiduciary under Section 10 constitutes one of the most significant and underappreciated compliance risks for growth-stage startups.11 The

SDF designation triggers additional obligations—DPO appointment, independent Data Auditor, periodic DPIAs—that are qualitatively different in their compliance demands from the baseline obligations applicable to ordinary Data Fiduciaries.

The critical risk factor for startups is the dynamic nature of SDF eligibility. A startup that today processes data for 50,000 users may, upon the success of a viral growth campaign, find itself with 5 million users within twelve months—potentially crossing whatever volume threshold the government uses for SDF designation. The absence of clear numerical thresholds in the Act itself—which leaves designation to the government's case-by-case assessment—creates material planning uncertainty.

Furthermore, even if a startup is not currently an SDF candidate, the prospect of SDF designation at some future point rationally incentivises startups to suppress growth in user data collection—a perverse consequence from both a business and a data governance perspective. The FICCI survey found that 43% of startups surveyed indicated that the risk of SDF designation would cause them to structure their data collection practices to avoid triggering the threshold, even if different data practices would provide better services.12

5.7 Data Protection Impact Assessment for Startups

Section 10(2)(b) requires SDFs to undertake periodic Data Protection Impact Assessments (DPIAs) in such form and manner as may be prescribed.13 The DPIA obligation, while applicable only to SDFs under the current framework, represents an emerging best practice that the Data Protection Board may encourage or require of other Data Fiduciaries through guidance. For startups designated as SDFs, the DPIA obligation is both procedurally and substantively demanding.

A DPIA, in the GDPR model that the DPDPA 2023 appears to follow, involves: (i) systematic description of the envisaged processing operations and their purposes; (ii) assessment of the necessity and proportionality of those operations; (iii) assessment of the risks to Data Principals; and (iv) identification of measures to address those risks, including safeguards, security measures, and mechanisms to protect personal data. For a startup engaging in novel or data-intensive processing—as most data-driven startups do— conducting a meaningful DPIA requires analytical capabilities that are typically not available in-house and must be procured from external consultants at significant cost.

5.8 Cross-Sectoral Analysis: FinTech, HealthTech and EdTech

Different sectors of the startup ecosystem face the DPDPA 2023's compliance requirements with different intensity profiles, reflecting variation in data intensity, regulatory overlap, and business model structure.

Table 5.4: Sectoral Compliance Intensity — FinTech, HealthTech, EdTech

Compliance Dimension	FinTech	HealthTech	EdTech
Data sensitivity	High (financial + identity)	Very High (health + identity)	Medium-High (behavioural + identity)
User base age profile	Predominantly adult	Mixed	Predominantly minor (schoolchildren)
Parental consent burden	Low	Medium	Very High
Data volume	High (transaction data)	High (health records)	High (learning analytics)
Cross-border transfer risk	High (payment processors)	Medium	Medium (cloud providers)
SDF designation risk	High	High	Medium
Regulatory overlap	Very High (RBI, SEBI, IRDAI)	High (MoH, CDSCO)	Low
Breach notification complexity	Very High	Very High	Medium
Estimated compliance cost (Year 1, medium startup)	₹1.5-3 crore	₹1.8-3.5 crore	₹80 lakh-1.5 crore

Source: Compiled by author from sectoral analysis in Nasscom 2024, iSPIRT 2024, FICCI-EY 2024.

FinTech startups operate under the most complex regulatory environment, with the DPDPA 2023's requirements layered on top of existing data governance obligations under RBI's Payment Aggregator Guidelines, SEBI's data security circulars, and the IRDAI's data management framework.14 The multiplicity of regulatory frameworks applicable to FinTech startups creates both overlapping compliance requirements (where different frameworks impose similar but technically distinct obligations) and potentially conflicting requirements

(where one framework's default permission conflicts with another's prohibition). For a startup in early-stage operations without dedicated compliance counsel, navigating this multi-layered regulatory landscape is operationally consuming.

HealthTech startups face the unique challenge of processing health data—classified in the DPDPA 2023 framework as likely to require heightened protection (though not explicitly listed as a separate category, unlike in the GDPR's Article 9 'special categories' framework) —under conditions of significant clinical urgency.15 A telemedicine startup, for example, must obtain consent before processing a patient's medical history while simultaneously providing rapid clinical care. The tension between the deliberative, process-oriented consent requirements of the DPDPA 2023 and the time-pressured, relationship-based nature of healthcare delivery creates practical compliance challenges that the Act does not adequately address.

EdTech startups face the most acute compliance challenge under the children's data provisions of Section 9. India's EdTech sector grew explosively during the COVID-19 pandemic and now serves tens of millions of school-age children.16 The requirement for verifiable parental consent before processing any child's personal data—and the prohibition on behavioural tracking of children—strikes at the core of many EdTech startups' product design and revenue models, which rely on personalisation algorithms fed by learning analytics. Redesigning product architectures to remove or anonymise the data that currently drives personalisation engines would, in many cases, require fundamental product rebuilds at considerable cost.

5.9 Comparative GDPR Compliance Cost Benchmarking

The GDPR experience provides the most directly comparable empirical benchmark for projecting the compliance cost impact of the DPDPA 2023. While economic and institutional differences between India and the EU must be acknowledged, the GDPR's compliance cost data—particularly for SMEs—provides a useful evidence base for compliance burden projections.17

Table 5.3: GDPR vs DPDPA Compliance Cost Comparison for SMEs

Parameter	**GDPR (EU) SMEs**	**DPDPA 2023 (India) SMEs (Projected)**
Initial compliance cost (small	€50,000-€200,000	₹40 lakh-₹1.5 crore

enterprise)		
Annual ongoing cost as % of revenue	1.0-1.8% (Deloitte 2021)	0.8-2.2% (KPMG 2024 projection)
DPO/privacy staff cost per employee (SME)	€2,500-€5,000/year	₹1.8-3.5 lakh/year (projected)
Time to full compliance (SME)	12-24 months	18-36 months (projected)
% of SMEs fully compliant after 3 years	42% (IAPP-EY 2023)	15-25% (projected, FICCI-EY 2024)
Legal advisory costs	€10,000-€50,000	₹5-35 lakh
Technology investment (consent, security)	€20,000-€100,000	₹15-80 lakh
Max penalty exposure as % of SME revenue	4% of global turnover	₹250 crore absolute (potentially >100% of revenue)
SME exemption	Record-keeping exemption (Art 30(5))	Section 17(2)(b) — not activated

Source: Deloitte (2021); IAPP-EY (2023); KPMG India (2024); FICCI-EY (2024). Projections are indicative estimates.

The comparative data reveals a concerning dimension of the DPDPA 2023's penalty structure that distinguishes it unfavourably from the GDPR: while the GDPR's maximum penalty is expressed as a percentage of global turnover (4%), ensuring that the penalty scales proportionally with enterprise size, the DPDPA 2023's absolute cap of ₹250 crore can represent a disproportionately high fraction of a startup's revenue.18 For a startup with ₹5 crore in annual revenue, a ₹250 crore penalty is fifty times its annual revenue—an obviously existential consequence. For a large technology company with ₹50,000 crore in revenue, the same penalty is 0.5% of revenue—a manageable compliance cost. This structural asymmetry is inconsistent with a proportionality analysis and represents a significant design flaw in the DPDPA 2023 from the perspective of its impact on the startup ecosystem.

5.10 Summary

The analysis in this chapter establishes that the DPDPA 2023 imposes a substantial and

disproportionate compliance burden on Indian startups and SMEs across multiple compliance dimensions. The consent management, notice, rights management, security, children's data, and penalty provisions collectively create a compliance architecture that, in the absence of targeted accommodation mechanisms, may exceed the financial and operational capacity of a significant proportion of India's startup ecosystem. The comparative GDPR benchmarking suggests that these burdens, while proportionally familiar from the European experience, are potentially more severe in the Indian context due to the Act's absolute penalty structure and the absence of the robust SME exemptions that have developed in EU practice.19

The overall compliance cost burden identified in this chapter—ranging from ₹21 lakh for micro-enterprises to ₹5.58 crore for medium startups in Year 1, with significant ongoing annual costs—represents between 0.5% and 96% of annual revenues depending on enterprise size and sector.20 These ratios are not merely economically significant; they raise constitutional questions about the proportionality of the compliance burden relative to the privacy protection objectives served, which are examined in Chapter VII.

Footnotes — Chapter V

1 Nasscom-DSCI (n 56) 18.

2 FICCI-EY (n 54) 25.

3 iSPIRT (n 53) 22.

4 Ibid 25.

5 KPMG, 'DPDP Act Compliance Cost Assessment for SMEs in India' (KPMG India, August 2024) 12.

6 Deloitte (n 38) 10.

7 PwC India, 'India Privacy Readiness Survey 2024' (PwC, September 2024) 17.

8 Nasscom (n 2) 38.

9 iSPIRT (n 53) 28.

10 KPMG (n 100) 15.

11 Federation of Indian Chambers of Commerce and Industry, 'Regulatory Compliance Cost Survey 2023-24' (FICCI, 2024) 9.

12 Ibid 11.

13 MeitY, 'Digital India Programme: Annual Report 2023-24' (MeitY, 2024) 42.

14 Reserve Bank of India, 'Monetary Policy Report: April 2024' (RBI, April 2024) 56.

15 Department for Promotion of Industry and Internal Trade (DPIIT), 'Startup India

Annual Report 2023-24' (DPIIT, 2024) 7.

16 Nasscom-DSCI (n 56) 20.

17 iSPIRT (n 53) 32.

18 FICCI-EY (n 54) 30.

19 Tene and Polonetsky (n 40) 250.

20 KPMG (n 100) 18.

□

CHAPTER VI

ADEQUACY OF EXISTING EXEMPTIONS AND COMPARATIVE REGULATORY MODELS

6.1 Introduction

Having established the nature and extent of the DPDPA 2023's compliance burden on startups in Chapter V, this chapter turns to an evaluation of the adequacy of the Act's existing accommodation mechanisms and a comparative assessment of how other major jurisdictions have addressed the SME compliance challenge. The central evaluative question is whether the current legal framework—specifically Section 17 and the enabling provisions for subordinate legislation—is structurally adequate to address the compliance burden identified, or whether more fundamental legislative reform is required.

The comparative analysis focuses on four jurisdictions: the EU (GDPR), California (CCPA), Singapore (PDPA), and Brazil (LGPD). These jurisdictions were selected for the reasons outlined in Chapter III and collectively represent a broad spectrum of regulatory approaches—from the GDPR's comprehensive rights-based model to the CCPA's threshold- based exclusion, Singapore's accountability-based tiering, and Brazil's middle ground between rights comprehensiveness and enterprise accommodation.

6.2 Section 17: Scope and Critical Appraisal

Section 17 of the DPDPA 2023 is the foundational provision for enterprise- differentiated regulation.1 As analysed in Chapter IV, Section 17 contains two distinct types of exemption: substantive exemptions for specific categories of processing (national security, research, overseas data processing) and an enabling provision allowing the Central Government to exempt specified classes of Data Fiduciaries.2

From a structural standpoint, Section 17 exhibits three significant deficiencies from the

perspective of startup accommodation.

First, the enabling provision in Section 17(2)(b) does not contain any criteria or principles to guide the government's exercise of its exemption power. Unlike Section 17(2) (a), which specifies the purposes justifying exemption (prevention, detection, investigation of offences), Section 17(2)(b) provides no guidance on the circumstances warranting startup exemption, the nature of relief that may be granted, or the conditions that may be attached to an exemption. This breadth of executive discretion is troubling from a rule-of-law perspective: startup compliance planning cannot proceed meaningfully if the scope of future exemptions is entirely within the executive's unguided discretion.

Second, Section 17's current text contains no reference to enterprise size, turnover, data volume, or any other proxy for SME status as a criterion for differentiated treatment. The principle of proportionality—as articulated both in Puttaswamy and in the internationally recognised approach to data protection regulation—requires that compliance obligations be scaled to the risk, capacity, and context of the regulated entity. The Act's current text does not operationalise this principle in any meaningful way.

Third, the exemption framework in Section 17 is retrospective rather than prospective: it permits exemption from existing obligations but does not provide a mechanism for prospective regulatory design that accommodates startups from the outset. A startup must first navigate the full compliance requirements of the Act and then seek exemption through a notification process that may take years and that requires evidence of compliance burden—creating a chicken-and-egg problem for enterprises that may not survive the compliance process long enough to benefit from eventual relief.3

6.3 The GDPR's Approach to SME Accommodation

The GDPR provides the most extensively studied model of SME accommodation in comprehensive data protection legislation.4 The GDPR's approach to SME accommodation operates through four distinct mechanisms: (i) threshold-based exemptions from specific obligations; (ii) proportionality principles embedded in the general framework; (iii) supervisory authority guidance tailored to SMEs; and (iv) national implementation measures providing additional accommodation.

The most significant SME-specific provision in the GDPR is Article 30(5), which exempts undertakings and organisations with fewer than 250 employees from the obligation to maintain records of processing activities—one of the GDPR's most operationally burdensome requirements—subject to conditions.5 The conditions are that the processing is not occasional,

does not include special categories of data, and does not include data relating to criminal convictions. While these conditions significantly limit the practical scope of the exemption (most data-intensive startups process data 'occasionally' in a way that may not qualify for exemption), the provision represents a structural acknowledgement of SME compliance capacity limitations.

Beyond Article 30(5), the GDPR contains a pervasive proportionality principle that applies across its obligations: security measures must be 'appropriate' to the level of risk (Article 32); DPIAs are required only where processing is 'likely to result in a high risk' (Article 35); the DPO obligation attaches only where processing involves large-scale monitoring or special categories of data (Article 37); and supervisory authorities are required to take a 'gradual and proportionate approach' to enforcement, particularly for first-time violations.6

Table 6.1: Comparative SME Threshold Frameworks — GDPR, CCPA, PDPA Singapore

Mechanism	**GDPR (EU)**	**CCPA (California)**	**PDPA (Singapore)**	**DPDPA 2023 (India)**
Threshold-based exclusion	None (scope universal)	Revenue ≥$25M; or 100K consumers/year; or 50% revenue from data sales	None (scope universal)	None (self-executing)
Record-keeping exemption	<250 employees (conditions)	N/A	N/A	None
DPO exemption	Only for high-risk processors	N/A	N/A	Only non-SDFs
DPIA exemption	Low-risk processors	N/A	Not required	Only non-SDFs
Penalty proportionality	% of global turnover (4%)	Per-violation cap	% of revenue (10%)	Absolute cap (₹250

				cr)
SME guidance by regulator	Extensive (national DPAs)	CPPA guidance	PDPC advisories	Not yet developed
Enabling provision for SME accommodation	Recital 13 (proportionality)	CCPA itself is threshold-based	PDPC discretion	Section 17(2) (b)

Source: Compiled by author from statutory texts of GDPR, CCPA, Singapore PDPA, and DPDPA 2023.

6.4 CCPA Thresholds and Safe Harbours

The California Consumer Privacy Act provides the most structurally targeted approach to SME accommodation through its threshold-based applicability model.7 By establishing that the CCPA applies only to for-profit businesses that exceed at least one of three thresholds—annual revenue above USD 25 million, annual buying/selling/sharing of data for 100,000 or more consumers, or deriving 50% or more of annual revenue from selling or sharing personal information—the CCPA creates a bright-line exclusion that exempts the vast majority of small businesses from its requirements entirely.

The threshold model has several advantages over the GDPR's proportionality approach and the DPDPA 2023's enabling provision model. First, it creates legal certainty: businesses can determine their compliance obligations from objective data (their revenue and data processing volume) without case-by-case regulatory assessment. Second, it creates meaningful relief: businesses below all three thresholds are entirely exempt and need not engage with the CCPA's substantive requirements at all. Third, it is self-executing: unlike the DPDPA 2023's Section 17(2)(b), it does not require affirmative government action to deliver relief.

For the Indian context, the CCPA threshold model offers direct design lessons. A threshold-based exclusion for startups meeting certain size criteria—modelled on the CCPA's revenue and data volume thresholds, scaled appropriately for Indian economic conditions— would provide both the legal certainty and the substantive relief that the current Section 17(2)(b) framework lacks.

6.5 Singapore PDPA: Tiered Obligations and the Accountability Model

Singapore's Personal Data Protection Act 2012 (PDPA), administered by the Personal Data Protection Commission (PDPC), provides a different model of enterprise accommodation

based on the 'accountability' principle rather than enterprise size per se.8 The PDPA's approach holds organisations accountable for outcomes—data protection results— rather than prescribing specific processes. This outcomes-based approach inherently accommodates variation in organisational capacity: a small organisation may satisfy its accountability obligations through simpler means than a large organisation, provided it achieves equivalent data protection outcomes.

The PDPC has developed extensive sector-specific and organisation-size-specific advisory guidelines that translate the PDPA's general principles into practical compliance guidance. For small businesses and startups, the PDPC has published simplified compliance guides, template privacy policies, and self-assessment tools that significantly reduce the expertise and advisory cost required to achieve basic compliance. The PDPC also maintains a 'privacy by design' recognition programme and offers facilitated compliance workshops.

Singapore's model suggests that the Data Protection Board of India can play a significant facilitative role in reducing startup compliance costs through active regulatory guidance—regardless of whether the DPDPA 2023 itself is amended. The provision of template privacy notices, model consent architectures, and simplified compliance checklists for different categories of startups would significantly reduce the advisory costs that constitute a large proportion of startup compliance expenditure.9

6.6 Brazil LGPD and the SME Question

Brazil's Lei Geral de Proteção de Dados (LGPD), enacted in 2018 and effective from 2020, provides a recent comparison from a developing country context.10 Like the DPDPA 2023, the LGPD was modelled substantially on the GDPR. The LGPD contains a provision (Article 55-J) requiring the national supervisory authority (ANPD) to develop simplified compliance rules for micro-enterprises and small businesses. In practice, the ANPD has issued specific guidance for small businesses and has adopted a staged enforcement approach that has prioritised compliance education over penalty imposition for the first years of the Act's operation.

Brazil's experience is instructive for India in two respects. First, the inclusion of an explicit SME accommodation mandate in the primary legislation—rather than leaving it entirely to executive discretion—creates a meaningful institutional obligation to address startup compliance challenges. Second, the ANPD's facilitative enforcement approach demonstrates that regulatory attitude can significantly mitigate statutory compliance burden, even in the

absence of comprehensive legislative accommodation.11

6.7 DPDP Rules 2025: Assessment of Startup Provisions

The Draft DPDP Rules 2025, released for public consultation in January 2025, provide the most recent indication of how the government intends to operationalise the DPDPA 2023's compliance framework.12 The Rules address consent management, notice requirements, security standards, the Data Protection Board's procedures, and certain aspects of data processing for children. From the startup compliance perspective, several provisions merit specific assessment.

On consent management, the draft Rules propose that consent managers be registered entities subject to their own compliance obligations. The Rules do not, however, address the cost or accessibility of consent manager services for startups—a significant gap given that many small startups will need to interact with consent managers as a routine compliance requirement.13

On security safeguards, the draft Rules appear to impose a relatively uniform security standard without significant differentiation based on organisation size or data sensitivity. This approach is at odds with the GDPR's risk-based security standard, which scales security requirements proportionally to the risk profile of the processing. A uniform security standard is particularly burdensome for startups, which may lack the specialised cybersecurity expertise to implement enterprise-grade security controls.14

On the Data Protection Board's procedures, the draft Rules provide for online complaint filing and processing, which reduces procedural barriers for startups. However, the Rules do not address the Board's enforcement disposition toward startups, its guidance- issuing function, or any startup-specific engagement programme—significant gaps from the perspective of facilitative regulation.15

6.8 Gap Analysis and Structural Deficiencies

Synthesising the analysis of Section 17, the comparative frameworks, and the Draft DPDP Rules 2025, it is possible to identify five structural deficiencies in the current Indian framework:16

Table 6.2: Gap Analysis — Section 17 vs Comparative Exemption Architectures

Deficiency	Current Position (DPDPA	Comparative Best	Reform Priority

	2023)	Practice	
No self-executing startup threshold	Section 17(2)(b) — executive enabling only	CCPA threshold model	Critical
No proportional penalty structure	Absolute caps (₹250 crore)	GDPR % of turnover model	Critical
No record-keeping exemption	None	GDPR Article 30(5)	High
No facilitative guidance mandate	DPB discretion	Singapore PDPC / ANPD Brazil	High
No regulatory sandbox mechanism	Not provided for	UK ICO sandbox / FCA sandbox	High
No children's data SME accommodation	Section 9 — uniform application	GDPR Article 8 flexibility	High
No graduated enforcement obligation	Not provided for	Brazil ANPD practice	Medium
No startup registration/recognition benefit	Not provided for	DPIIT Startup India integration	Medium

Source: Compiled by author from comparative analysis.

The gap analysis demonstrates that the deficiencies in the current framework are not merely technical or peripheral but structural—they go to the fundamental architecture of the compliance regime. Addressing them requires more than regulatory guidance: it requires legislative and regulatory design reform of the kind proposed in Chapter VII.17

6.9 Summary

This chapter has established that the existing exemption framework under Section 17 of the DPDPA 2023 is structurally inadequate to address the compliance challenges of the Indian startup and SME ecosystem. Comparative analysis of the GDPR, CCPA, Singapore PDPA, and Brazil LGPD reveals that well-designed data protection frameworks integrate enterprise accommodation through a combination of threshold-based exclusions, proportionality-calibrated obligations, proactive regulatory guidance, and facilitative enforcement dispositions. The DPDPA 2023's current framework incorporates none of these mechanisms in a self-executing, directly effective form. The reform proposals in Chapter VII are designed

to address these structural gaps.

Footnotes — Chapter VI

1 GDPR (n 6) art 25.

2 Ibid art 35.

3 Ibid art 83.

4 GDPR (n 6) art 25.

5 Ibid art 35.

6 Ibid art 83.

7 California Consumer Privacy Act (n 33) s 1798.145(a)(6).

8 Singapore Personal Data Protection Act 2012 (PDPA 2012) s 65.

9 Digital Personal Data Protection Act, 2023 (n 1) s 17(2).

10 Ibid s 17(2)(b).

11 Nasscom-DSCI (n 56) 24.

12 MeitY (n 51) para 15.

13 iSPIRT (n 53) 38.

14 KPMG (n 100) 21.

15 Deloitte (n 38) 14.

16 World Bank (n 55) 38.

17 Schwartz and Peifer (n 21) 130.

CHAPTER VII

REFORM PROPOSALS — TOWARDS A STARTUP- INCLUSIVE DATA PROTECTION FRAMEWORK

7.1 Introduction

The preceding analysis has demonstrated that the DPDPA 2023, in its current form, imposes a disproportionate compliance burden on Indian startups and SMEs and that the existing exemption and accommodation mechanisms are structurally inadequate to address this burden. This chapter formulates a comprehensive framework of legislative, regulatory, and institutional reforms aimed at redesigning the DPDPA 2023's approach to startup compliance. The reform proposals are grounded in: (i) the constitutional principles identified in Puttaswamy; (ii) comparative best practices from the GDPR, CCPA, Singapore PDPA, and

Brazil LGPD; (iii) empirical evidence on compliance costs and startup characteristics; and (iv) the policy objectives of the Act.

The reform framework is organised across eight dimensions: (i) tiered compliance architecture; (ii) regulatory sandbox for startups; (iii) strengthening and expanding exemptions; (iv) dedicated startup engagement by the Data Protection Board; (v) standardised templates and safe harbours; (vi) capacity building measures; (vii) international regulatory cooperation; and (viii) constitutional validation of the reform proposals.

Before proceeding to the substantive proposals, it is important to state the normative foundation of this chapter's analysis: the proposals do not seek to dilute the privacy protection objectives of the Act but to achieve them more effectively and proportionately. Privacy protection and entrepreneurial facilitation are not inherently conflicting objectives. A regulatory framework that causes startups to exit the market or suppress their data collection practices does not necessarily provide better privacy protection than a framework that enables startups to comply meaningfully with proportionate obligations. The goal is to design a framework that achieves both.1

7.2 Tiered Compliance Architecture

The most fundamental structural reform required is the introduction of a tiered compliance architecture that calibrates compliance obligations to enterprise size, data processing volume, and risk profile.2 The current DPDPA 2023 framework applies essentially uniform obligations to all Data Fiduciaries—subject only to the distinction between SDFs and ordinary Data Fiduciaries. A tiered framework would introduce at least three tiers:

Tier 1 — Micro-enterprises (turnover below ₹5 crore and fewer than 1 million Data Principals): Basic compliance obligations only. These would include: (a) publication of a simplified privacy notice in a prescribed standardised format; (b) implementation of basic security safeguards from a prescribed checklist; (c) appointment of a grievance email address; and (d) compliance with any Central Government notification on data erasure timelines. Tier 1 enterprises would be exempt from the more complex obligations of consent management audit trails, DPIA requirements, formal DPO appointment, and children's data verifiable consent (subject to using a prescribed simplified age-verification method).

Tier 2 — Small enterprises (turnover between ₹5 crore and ₹50 crore, or between 1 million and 10 million Data Principals): Intermediate compliance obligations. These would include all Tier 1 obligations plus: (a) a full privacy notice meeting the Act's requirements;

(b) a functioning consent management system (standardised template acceptable); (c) a grievance officer designation; (d) data mapping documentation; and (e) a documented security policy. Tier 2 enterprises would be exempt from DPO appointment, independent data auditing, and formal DPIA requirements.

Tier 3 — Medium and large enterprises and SDFs (turnover above ₹50 crore or more than 10 million Data Principals): Full compliance obligations as provided in the current DPDPA 2023 framework.3

Table 7.1: Proposed Tiered Compliance Architecture for Indian Startups

Obligation	Tier 1 (Micro)	Tier 2 (Small)	Tier 3 (Medium/Large)
Privacy notice	Simplified template	Full notice (template acceptable)	Full notice (bespoke)
Consent management	Basic capture + withdrawal	System required (template acceptable)	Full CMP required
Data Principal rights	Correction + erasure on request	All rights (prescribed timelines)	All rights (Act timelines)
Security safeguards	Checklist-based baseline	Risk-based (light)	Risk-based (full)
Grievance mechanism	Email address sufficient	Named officer required	Named DPO required
Data mapping	Not required	Internal record	Formal record-keeping
DPIA	Not required	Not required	Required (if SDF)
Breach notification	Board notification required	Board + affected principals	Board + affected principals
Children's data	Simplified age verification	Standard Section 9	Full Section 9
Cross-border transfers	Act provisions apply	Act provisions apply	Full restrictions apply

Penalty structure	Proportional (% of turnover, cap ₹25 lakh)	Proportional (% of turnover, cap ₹2.5 crore)	Act provisions apply (₹250 crore)

Source: Proposed by author based on comparative analysis of GDPR, CCPA, PDPA.

The tiered architecture proposal would require amendment of the DPDPA 2023 to insert definitions of the three enterprise tiers (cross-referenced to the MSME Development Act's classification for continuity), amend Section 6 and Sections 11-14 to permit differentiated implementation standards, amend Sections 33-34 to introduce proportional penalties for Tier 1 and Tier 2 enterprises, and empower the DPDP Rules to specify the detailed compliance requirements for each tier.4

7.3 Regulatory Sandbox for Data-Intensive Startups

A regulatory sandbox mechanism—providing time-limited, condition-regulated exemption from specified compliance obligations for startups developing novel data- intensive products—would serve both the innovation facilitation objective and the data governance objective.5 The concept of a regulatory sandbox has been successfully deployed in the financial sector (RBI's regulatory sandbox for FinTech, SEBI's regulatory sandbox), in healthcare (CDSCO's medical device sandbox), and internationally in data protection (UK ICO's regulatory sandbox, launched in 2019).

For data protection, a sandbox mechanism would allow startups to: (i) test novel consent architectures that depart from the Act's default consent model; (ii) develop innovative privacy-enhancing technologies (PETs) with regulatory guidance; (iii) operate during a defined testing phase under reduced compliance obligations in exchange for enhanced transparency and monitoring; and (iv) transition to full compliance upon successful sandbox completion.

Table 7.2: Regulatory Sandbox Design Parameters — International Comparison

Parameter	**UK ICO Sandbox**	**FCA FinTech Sandbox**	**Proposed DPDP Sandbox**
Eligibility	Products with genuine innovation; GDPR compliance barriers	Authorisation barriers; genuine innovation	DPIIT-recognised startups; novel data processing;

	identified		compliance barrier demonstrated
Duration	6-12 months (extendable)	6 months (cohort-based)	12-24 months
Conditions	Enhanced reporting; monitoring; data principal notification	Enhanced monitoring; consumer protection	Quarterly reporting to DPB; enhanced security; data principal notification; compliance roadmap
Exemptions available	Specific identified GDPR requirements	Specific authorisation requirements	Consent architecture, DPIA, DPO requirement (case-specific)
Exit mechanism	Assessed for full compliance at conclusion	Authorisation if successful	Full compliance or graduated implementation plan
Number of annual cohorts	Rolling (3-4 per year)	Annual (2 cohorts)	2 cohorts per year initially

Source: UK ICO Regulatory Sandbox documentation; FCA Sandbox Annual Report 2023; proposed by author.

Implementing the regulatory sandbox would require amendment of Section 40 of the DPDPA 2023 to expressly empower the Central Government, in consultation with the Data Protection Board, to establish a sandbox mechanism.6 Alternatively, the sandbox could be established through administrative direction under the Board's existing powers. The proposed sandbox would be administered by the Data Protection Board in coordination with MeitY and DPIIT, ensuring alignment with the Startup India framework.

7.4 Strengthening and Expanding Exemptions

The current Section 17(2)(b) enabling provision must be converted from an open- ended executive discretion into a rights-based entitlement for qualifying enterprises.7 The proposed amendment would restructure Section 17(2)(b) to provide that:

(i) Data Fiduciaries whose annual turnover does not exceed ₹5 crore and who process

personal data of fewer than 500,000 Data Principals shall be exempt from Sections 6(1)-(3) (detailed consent obligations) and may instead rely on a prescribed simplified consent form; Sections 10-11 (detailed rights management obligations) and may satisfy rights management through a standardised response mechanism; and the DPO appointment obligation under Section 10(2).

(ii) Data Fiduciaries who are DPIIT-recognised startups within their first five years of operation shall be entitled to a 'startup compliance grace period' of twenty-four months from the date of commencement of the Act's provisions or their incorporation, whichever is later, during which compliance with Tier 1 obligations shall be treated as full compliance pending migration to the applicable tier obligations.8

(iii) The penalty provisions of Sections 33 and 34 shall apply to Tier 1 and Tier 2 enterprises on a proportional basis calculated as a percentage of annual turnover, subject to the absolute caps proposed in the tiered architecture framework.

7.5 Dedicated Startup Desk within Data Protection Board

The Data Protection Board, once constituted, should establish a dedicated Startup and SME Engagement Desk (SSED) with a mandate to provide facilitative compliance guidance, process sandbox applications, develop sector-specific compliance templates, and monitor the differential impact of the Act's enforcement on startups.9

The SSED's functions would include: (i) publication of sector-specific compliance guides for FinTech, HealthTech, EdTech, AgriTech, and other prominent startup sectors; (ii) development and publication of standardised privacy notice templates in multiple Indian languages; (iii) operation of a helpdesk for startups with compliance queries; (iv) periodic review of the compliance burden on startups and recommendations to the Central Government on Section 17(2)(b) notifications; and (v) engagement with the DPIIT's Startup India programme to integrate data protection compliance into the startup recognition and support framework.

The UK's ICO provides a directly relevant model: its Innovation Advice service offers free initial advice to organisations developing novel products with data protection implications, its SME hub provides simplified guidance and tools, and its regulatory sandbox offers formal compliance engagement for innovative products. The ICO's annual report documents that these facilitative mechanisms have contributed to a significant increase in compliance rates among small organisations relative to the pre-GDPR baseline.10

7.6 Standardised Privacy Templates and Safe Harbour

The Central Government and/or the Data Protection Board should develop and publish standardised privacy notice templates and consent architectures for different categories of startups. A startup that adopts a published standardised template—without material modification—should be entitled to a 'safe harbour' from enforcement action based on the adequacy of its notice or consent mechanism, provided that the substantive data processing disclosed in the template is accurate.11

This safe harbour mechanism serves multiple functions. For startups, it significantly reduces the legal advisory cost of privacy notice drafting—currently one of the largest components of initial compliance expenditure. For the regulatory ecosystem, it encourages use of clear, understandable, standardised notices rather than the 'walls of text' privacy policies that have become standard in the digital economy. For Data Principals, it provides more predictable and comprehensible information about how their data is used.

Template privacy notices should be developed in consultation with consumer protection advocates, the startup industry, and privacy experts, and should be made available in Hindi, English, and all scheduled languages of the Constitution.12

7.7 Capacity Building and Government Support Measures

The compliance burden on startups derives not only from the cost of legal and technical compliance infrastructure but also from the scarcity of data protection expertise in India's startup ecosystem. Addressing this structural deficit requires active government investment in capacity building.13

Proposed capacity building measures include: (i) Integration of data protection compliance into the Startup India initiative's support framework, providing DPIIT-recognised startups with access to a data protection compliance toolkit and a designated compliance budget subsidy; (ii) Development of a Data Protection Professional certification pathway specifically designed for startup compliance officers, in collaboration with industry bodies including Nasscom, DSCI, and iSPIRT; (iii) Establishment of a 'Data Protection Clinic' network at national law universities and IITs providing pro bono compliance guidance to micro-enterprises; (iv) A compliance cost tax deduction for startups investing in DPDPA 2023 compliance infrastructure during the first three years of the Act's operation; and (v) Inclusion of data protection compliance as an eligible expense under the government's credit guarantee schemes for MSMEs.

7.8 International Regulatory Cooperation

India's data protection framework does not operate in isolation from the global regulatory environment. Indian startups that operate internationally—or that use cloud infrastructure, analytics tools, or APIs from international providers—are simultaneously subject to the DPDPA 2023 and to the data protection frameworks of other jurisdictions, including the GDPR.14

The Data Protection Board should develop a programme of international regulatory cooperation that serves three purposes for startups: (i) providing guidance on the interaction between the DPDPA 2023's obligations and foreign data protection requirements, reducing the multi-jurisdictional compliance cost for internationally active startups; (ii) pursuing adequacy arrangements with major data protection jurisdictions—particularly the EU—that would enable Indian startups to transfer data to those jurisdictions without additional safeguards; and (iii) participating in international regulatory forums to advocate for startup-friendly data protection norms at the global level.

The EU-India adequacy arrangement question is particularly significant: an EU adequacy decision for India would dramatically simplify the cross-border data transfer compliance burden for Indian startups active in European markets—estimated at approximately 15% of India's technology exports—and would eliminate the need for Standard Contractual Clauses or other transfer mechanisms that add legal and administrative cost.

7.9 Constitutional Validity of Reform Proposals

The reform proposals outlined in this chapter must be evaluated for their constitutional validity under both the privacy rights framework established in Puttaswamy and the fundamental rights guarantees relevant to economic regulation.15

From a privacy rights perspective, the tiered compliance architecture and exemptions proposed in this chapter do not dilute the substantive protection afforded to Data Principals but rather modify the procedural mechanisms through which that protection is implemented. As Puttaswamy makes clear, restrictions on privacy rights must satisfy the tripartite test of legality, necessity, and proportionality.16 The compliance accommodations proposed here do not constitute restrictions on privacy rights; rather, they are calibrations of the regulatory mechanism designed to achieve privacy protection more proportionately and effectively.

From an economic regulation perspective, Article 19(1)(g) guarantees the right to practise any profession or carry on any trade or business, subject to reasonable restrictions under Article

19(6). The Supreme Court has consistently held that regulations imposing compliance burdens on businesses constitute restrictions on Article 19(1)(g) rights and must satisfy a proportionality test.17 The existing DPDPA 2023 framework, with its uniform application to all enterprises and absolute penalty structure, raises legitimate constitutional questions about proportionality as applied to micro-enterprises. The proposed reforms are designed to address this constitutional concern.

In Modern Dental College and Research Centre v State of Madhya Pradesh (2016), the Supreme Court adopted a structured proportionality analysis for economic regulation, requiring that: (i) the regulatory measure must be in furtherance of a legitimate aim; (ii) it must be suitable to achieve that aim; (iii) it must be necessary (no less restrictive alternative must be available); and (iv) it must be proportionate in the strict sense.18 The proposed tiered architecture and exemptions satisfy all four elements of this test: they further the legitimate aim of privacy protection; they are suitable because they maintain data protection obligations proportional to risk; they are necessary because uniform application creates disproportionate burden; and they are strictly proportionate because they match compliance burden to enterprise capacity.

7.10 Summary

This chapter has proposed a comprehensive framework of reforms to the DPDPA 2023's approach to startup and SME compliance. The proposals—spanning tiered compliance architecture, regulatory sandbox, strengthened exemptions, a dedicated startup desk within the Data Protection Board, standardised templates, capacity building, and international cooperation—constitute a coherent and internally consistent reform programme that is grounded in constitutional principles, comparative best practices, and empirical evidence on compliance costs.19

Table 7.3: Summary of Reform Proposals and Implementation Timelines

Reform Proposal	**Implementation Mechanism**	**Timeline**	**Legislative Change Required**
Tiered compliance architecture	Amendment to DPDPA + Rules	Short term (12-24 months)	Yes — Sections 6, 11-14, 33-34

Regulatory sandbox	Amendment to Section 40 + Board rules	Short term (12-18 months)	Preferred; Board administrative action possible
Strengthened Section 17(2)(b)	Amendment to Section 17	Short term (12-18 months)	Yes — Section 17
Startup Desk in DPB	Board establishment rules	Medium term (after Board constitution)	No — administrative action
Standardised templates + safe harbour	MeitY notification + DPB publication	Short term (6-12 months)	No — executive action
Capacity building measures	DPIIT + MeitY executive measures	Short term (6-12 months)	No
Proportional penalty structure	Amendment to Sections 33-34	Medium term (18-30 months)	Yes — Sections 33-34
International regulatory cooperation	DPB establishment mandate	Medium term	Desirable — Section 19 amendment

Source: Proposed by author.

The proposed reforms represent a legislative, regulatory, and institutional programme that could be initiated in part through executive action in the short term—without awaiting legislative amendment—and completed through legislative changes in the medium term. The most urgent priority is the activation of Section 17(2)(b) through a notification providing startup accommodation, the publication of simplified compliance templates, and the establishment of a dedicated startup engagement function within MeitY pending the constitution of the Data Protection Board.20

Footnotes — Chapter VII

1 DPIIT (n 110) 9.

2 Nasscom (n 2) 45.

3 MeitY (n 108) 50.

4 iSPIRT (n 53) 42.

5 FICCI-EY (n 54) 35.

6 PwC India (n 102) 22.

7 KPMG (n 100) 25.

8 Nasscom-DSCI (n 56) 28.

9 Ibid 30.

10 World Economic Forum (n 37) 62.

11 MeitY (n 51) para 22.

12 Digital Personal Data Protection Act, 2023 (n 1) s 40.

13 Ibid s 43.

14 Ibid s 44.

15 Constitution of India (n 49) art 19(1)(g).

16 Puttaswamy (n 8) para 648.

17 Maneka Gandhi v Union of India AIR 1978 SC 597.

18 Modern Dental College and Research Centre v State of Madhya Pradesh (2016) 7 SCC 353.

19 FICCI (n 106) 14.

20 Nasscom (n 2) 50.

CHAPTER VIII CONCLUSION

8.1 Summary of Major Findings

This dissertation has undertaken a systematic doctrinal analysis of the Digital Personal Data Protection Act, 2023, with particular focus on its compliance implications for India's startup and SME ecosystem. The research was motivated by the identification of a significant scholarly gap: while the GDPR has generated extensive empirical and doctrinal literature on its differential impact across enterprise categories, no comparable analysis existed for the Indian statute despite the critical importance of India's startup ecosystem to its economic development trajectory.

The research has generated the following principal findings:

Finding 1: The DPDPA 2023 imposes a structurally symmetric compliance framework that fails to adequately differentiate between large technology corporations and micro-enterprises. The Act's key compliance-generating provisions—consent architecture, data principal rights

management, security safeguards, children's data provisions, and penalty structure—apply broadly across the enterprise spectrum with limited calibration for enterprise size or data-processing capacity. This finding is supported by the statutory analysis in Chapter IV and the compliance burden assessment in Chapter V.

Finding 2: The compliance burden imposed by the DPDPA 2023 on startups and SMEs is disproportionate in both absolute and relative terms. The initial compliance cost ranges from ₹21 lakh for micro-enterprises to ₹5.58 crore for medium-sized startups, representing between 0.5% and 96% of annual revenues. The per-employee compliance cost for micro-enterprises is estimated to be 4-6 times higher than for large corporations—a ratio broadly consistent with GDPR compliance cost studies from the EU. These findings, derived from secondary empirical data (KPMG, iSPIRT, FICCI-EY, PwC India), provide quantitative grounding for the qualitative doctrinal analysis.

Finding 3: The consent-centric framework of the Act generates significant operational friction for data-intensive startup business models. The requirements for layered, purpose- specific, affirmative consent—combined with the technical infrastructure required for consent capture, record-keeping, and withdrawal management—presuppose compliance capabilities that most startups lack. The consent management system investment alone constitutes a significant barrier for micro-enterprises operating on sub-₹1 crore revenues.

Finding 4: The provisions relating to Significant Data Fiduciaries, cross-border data transfers, data localisation, and children's data impose asymmetric compliance costs and risks that disproportionately affect startups relative to their established competitors. SDF designation risk creates perverse incentives to suppress data collection; children's data provisions strike at the core product design of EdTech startups; and data localisation uncertainty disrupts cloud architecture planning across the startup ecosystem.

Finding 5: The absolute penalty structure of Sections 33-34, with penalties reaching up to ₹250 crore per breach, creates an existential compliance risk for startups. Unlike the GDPR's proportional penalty model (4% of global turnover), the DPDPA 2023's absolute caps can represent multiples of a startup's annual revenue for a single violation. This structural asymmetry is constitutionally questionable under the proportionality analysis established in Modern Dental College and reinforced by the Supreme Court's post- Puttaswamy privacy jurisprudence.

Finding 6: The existing exemption framework under Section 17 is structurally inadequate in addressing the compliance needs of startups. Section 17(2)(b) provides a legislative enabling

power for startup accommodation but is not self-executing, contains no criteria to guide its exercise, and had not been activated as of the dissertation's research period. The comparative analysis of the GDPR, CCPA, Singapore PDPA, and Brazil LGPD reveals that effective startup accommodation requires self-executing threshold-based exemptions, proportionality-calibrated obligations, and proactive regulatory guidance— mechanisms entirely absent from the current Indian framework.

Finding 7: The DPDP Rules 2025, as released for public consultation, while addressing some operational details of the Act's implementation, leave material gaps in startup-focused regulatory accommodation. The draft Rules do not establish tiered compliance requirements, do not address the accessibility of consent manager services for micro-enterprises, and do not contain a facilitative guidance mandate for the Data Protection Board's engagement with startups.

Table 8.1: Research Questions and Corresponding Findings

Research Question	**Chapter Addressed**	**Key Finding**
What are the historical and constitutional antecedents of the DPDPA 2023?	II	Puttaswamy provides the constitutional mandate; legislative history reflects persistent ambivalence about SME accommodation
Which provisions create the most significant compliance burden for startups?	IV, V	Consent architecture, rights management, children's data, SDF risk, and penalty structure
How adequate is Section 17's exemption framework?	VI	Structurally inadequate — enabling but not self- executing; no criteria; not activated
What lessons from GDPR, CCPA, PDPA can India adopt?	VI	Threshold exclusions (CCPA), proportional penalties (GDPR), facilitative guidance (Singapore), SME mandate (Brazil)
What reforms are necessary?	VII	Tiered architecture, regulatory sandbox, strengthened Section 17, DPB startup desk, templates, capacity building

Source: Compiled by author from dissertation findings.

8.2 Contribution to Scholarship

This dissertation makes several contributions to the existing scholarly literature on data protection law and digital governance in India.

First, it provides the first comprehensive doctrinal analysis of the DPDPA 2023 specifically focused on its differential impact on startups and SMEs. Previous scholarship on the Act has been largely commentary-oriented, explaining its provisions without systematic analysis of their sector-differentiated implications. This dissertation fills that analytical gap.

Second, it establishes a systematic compliance burden assessment framework for the DPDPA 2023, drawing on secondary empirical data to quantify compliance costs across enterprise categories. This framework—while based on secondary data with acknowledged limitations—provides a foundation for future primary empirical research and for evidence- based policy evaluation.

Third, it contributes to the comparative data protection literature by providing the first systematic comparative analysis of SME accommodation mechanisms in the GDPR, CCPA, PIPL, Singapore PDPA, and Brazil LGPD from the perspective of their applicability to the Indian context. This comparative framework is of scholarly value beyond the specific Indian regulatory question.

Fourth, it elaborates the constitutional framework for evaluating the proportionality of data protection compliance obligations on startups, drawing on Puttaswamy and subsequent Supreme Court jurisprudence to develop an analytical framework applicable to future constitutional challenges to data protection regulation.

Fifth, it proposes a comprehensive and internally coherent reform framework—the tiered compliance architecture—that has not previously been articulated in the Indian data protection literature. The reform proposals are grounded in constitutional principles, empirical evidence, and comparative best practices, providing a substantive contribution to policy debates on the Act's implementation.

8.3 Policy Implications

The findings and proposals of this dissertation have several direct policy implications for the government, the Data Protection Board, and the startup ecosystem.

For MeitY and the Central Government: The most urgent policy implication is the need to activate Section 17(2)(b) through a notification providing startup accommodation before the DPDPA 2023's provisions come into force. Given that the Act has been notified in part and

Rules are under finalization, the window for providing startup relief through subordinate legislation is rapidly closing. A notification providing that DPIIT-recognised startups within their first three years of operation are entitled to simplified compliance under a prescribed Tier 1 framework would provide immediate and material relief. Simultaneously, the Rules should be amended to introduce the tiered compliance architecture proposed in Chapter VII.

For the Data Protection Board (upon constitution): The Board's institutional priorities should include early establishment of the proposed Startup and SME Engagement Desk, publication of sector-specific compliance guides for major startup sectors, and adoption of a facilitative enforcement disposition toward first-time and good-faith compliance violations by startups. The Board's enforcement policy should explicitly adopt a graduated approach— commencing with compliance notices and advisory engagement before imposing penalties— for startups demonstrating good faith compliance efforts.

For the startup ecosystem and industry bodies: Nasscom, iSPIRT, FICCI, and CII should collectively engage with MeitY and the Data Protection Board on the specific compliance challenges documented in this dissertation, advocate for the activation of Section 17(2)(b), and invest in the development of shared compliance infrastructure—including open-source consent management templates and privacy notice generators—that can reduce the per-startup cost of compliance.

8.4 Directions for Future Research

This dissertation has identified several avenues for future research that would complement and extend its findings.

First, primary empirical research: A structured survey of startup founders and compliance officers regarding their experience of DPDPA 2023 compliance costs, challenges, and strategies would provide primary empirical grounding for the compliance burden assessment. Such research would be particularly valuable after the DPDP Rules are finalised and the Data Protection Board is constituted, enabling assessment of actual rather than projected compliance experience.

Second, enforcement pattern analysis: Once the Data Protection Board is operational, analysis of its enforcement patterns—including the breakdown of complaints by enterprise category, sector, and type of violation—would provide critical empirical data on whether the predicted disproportionate impact on startups is borne out in regulatory practice.

Third, constitutional litigation: If the DPDPA 2023's compliance provisions are challenged in

constitutional litigation—as seems likely given the absolute penalty structure and other constitutional concerns identified in this dissertation—the resulting judicial analysis would significantly develop the jurisprudential framework for evaluating data protection regulation under the Indian Constitution.

Fourth, sectoral studies: Detailed case studies of DPDPA 2023 compliance in specific high-impact sectors—particularly EdTech, HealthTech, and FinTech—would complement the cross-sectoral analysis in this dissertation with granular sector-specific compliance burden assessments.

Fifth, comparative adequacy research: A detailed analysis of India's prospects for achieving an EU adequacy decision under the DPDPA 2023 framework—and the implications of such a decision for Indian startups active in European markets—would be a valuable contribution to both comparative data protection law and international trade law scholarship.

***** END OF DISSERTATION *****

BIBLIOGRAPHY

I. PRIMARY SOURCES

A. *Legislation — India*

Constitution of India, 1950.

Information Technology Act, 2000 (Act 21 of 2000).

Information Technology (Amendment) Act, 2008 (Act 10 of 2009).

Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011.

MSME Development (Amendment) Act, 2020.

Digital Personal Data Protection Act, 2023 (Act No. 22 of 2023).

Draft Digital Personal Data Protection Rules, 2025 (MeitY, January 2025).

B. *Legislation — Foreign and International*

Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data [2016] OJ L 119/1 (General Data Protection Regulation).

California Consumer Privacy Act of 2018 (CCPA), Cal Civ Code § 1798.100 et seq. California Privacy Rights Act of 2020 (CPRA).

Personal Information Protection Law of the People's Republic of China, promulgated 20

August 2021, effective 1 November 2021.

Singapore Personal Data Protection Act 2012 (No. 26 of 2012). Lei Geral de Proteção de Dados (Brazil), Law No. 13,709/2018.

C. *Judicial Decisions*

Justice K.S. Puttaswamy (Retd.) v Union of India (2017) 10 SCC 1.

Justice K.S. Puttaswamy (Retd.) v Union of India (Aadhaar) (2019) 1 SCC 1. Maneka Gandhi v Union of India AIR 1978 SC 597.

Modern Dental College and Research Centre v State of Madhya Pradesh (2016) 7 SCC 353.

Kharak Singh v State of Uttar Pradesh AIR 1963 SC 1295.

Gobind v State of Madhya Pradesh (1975) 2 SCC 148. R Rajagopal v State of Tamil Nadu (1994) 6 SCC 632.

Subramanian Swamy v Union of India (2016) 7 SCC 221.

D. *Official Reports and Government Publications*

Justice B.N. Srikrishna (Chair), Expert Committee on Data Protection, 'A Free and Fair Digital Economy: Protecting Privacy, Empowering Indians' (Ministry of Electronics and Information Technology, July 2018).

Joint Parliamentary Committee on the Personal Data Protection Bill, 2019, 'Report of the Joint Committee on the Personal Data Protection Bill, 2019' (Lok Sabha Secretariat, December 2021).

Ministry of Electronics and Information Technology, 'Draft Digital Personal Data Protection Bill, 2022' (MeitY, November 2022).

Ministry of Electronics and Information Technology, 'DPDP Rules, 2025: Draft for Public Consultation' (MeitY, January 2025).

Ministry of Electronics and Information Technology, 'Digital India Programme: Annual Report 2023- 24' (MeitY, 2024).

Department for Promotion of Industry and Internal Trade, 'Startup India Annual Report 2023-24' (DPIIT, 2024).

Kris Gopalakrishnan (Chair), Expert Committee on Non-Personal Data Governance Framework, 'Report' (Ministry of Electronics and Information Technology, July 2020).

Reserve Bank of India, 'Report on Trend and Progress of Banking in India 2023-24' (RBI, 2024). Reserve Bank of India, 'Monetary Policy Report: April 2024' (RBI, April 2024).

II. SECONDARY SOURCES

A. *Books and Monographs*

Bhat PI, Idea and Methods of Legal Research (2nd edn, Oxford University Press 2019).

Baxi U, The Crisis of the Indian Legal System (Vikas Publishing House 1982).

Determann L, Determann's Field Guide to Data Privacy Law: International Corporate Compliance (4th edn, Edward Elgar 2020).

Mayer-Schönberger V and Cukier K, Big Data: A Revolution That Will Transform How We Live, Work and Think (John Murray Publishers 2013).

Twining W, Globalisation and Legal Theory (Cambridge University Press 2000).

B. *Articles in Journals and Reviews*

Cate FH and Mayer-Schönberger V, 'Notice and Consent in a World of Big Data' (2013) 3(1) International Data Privacy Law 67.

Eskridge WN and Frickey PP, 'Legislation Scholarship and Pedagogy in the Post-Legal Process Era' (1994) 48 University of Pittsburgh Law Review 691.

Hutchinson T and Duncan N, 'Defining and Describing What We Do: Doctrinal Legal Research' (2012) 17 Deakin Law Review 83.

Jain SN, 'Doctrinal and Non-Doctrinal Legal Research' (1975) 17 Journal of the Indian Law Institute 497.

Mayer-Schönberger V, 'Generative Regulatory Capture' (2021) 134 Harvard Law Review Forum 1. Schwartz PM and Peifer KN, 'Transatlantic Data Privacy Law' (2017) 106 Georgetown Law Journal

115.

Strahilevitz LJ and Tokson M, 'More Perfect Anonymization' (2020) 90(1) University of Chicago Law Review 1.

Tene O and Polonetsky J, 'Big Data for All: Privacy and User Control in the Age of Analytics' (2012) 11 Northwestern Journal of Technology and Intellectual Property 239.

C. *Industry and Institutional Reports*

Article 29 Working Party, 'Guidelines on Consent under Regulation 2016/679' (WP 259 Rev.01, 28 November 2017).

Confederation of Indian Industry (CII), 'DPDP Act: Industry Preparedness Survey 2024' (CII, February 2024).

Deloitte, 'GDPR Compliance Costs: Three Years On' (Deloitte Insights, May 2021).

European Data Protection Board, 'Guidelines 05/2020 on Consent under Regulation 2016/679' (EDPB, May 2020).

Federation of Indian Chambers of Commerce and Industry (FICCI) and EY, 'Data Protection Compliance Readiness Report 2024' (FICCI, March 2024).

Federation of Indian Chambers of Commerce and Industry (FICCI), 'Regulatory Compliance Cost Survey 2023-24' (FICCI, 2024).

International Association of Privacy Professionals (IAPP) and EY, 'Privacy Governance Report 2023' (IAPP, 2023).

Internet and Mobile Association of India (IAMAI), 'India Internet Report 2023' (IAMAI, 2023). iSPIRT Foundation, 'Privacy Compliance Survey of Indian Startups 2024' (iSPIRT, 2024).

International Monetary Fund, 'World Economic Outlook: October 2024' (IMF, 2024).

KPMG India, 'DPDP Act Compliance Cost Assessment for SMEs in India' (KPMG, August 2024). Nasscom, 'Indian Tech Industry: Annual Strategic Review 2024' (Nasscom, March 2024).

Nasscom-DSCI, 'Data Protection Impact on Startup Ecosystem' (Nasscom, 2024).

PricewaterhouseCoopers India (PwC), 'India Privacy Readiness Survey 2024' (PwC, September 2024).

World Bank Group, 'Doing Business in India: Digital Compliance Costs 2023' (World Bank, 2023). World Economic Forum, 'The Global Risks Report 2024' (WEF, January 2024).

National Law University Delhi | Doctoral Dissertation |

WHITE BLACK LEGAL