



**SHRIDHAR INFOSEC**  
S O L U T I O N S



**DPDPA 2023**

# **From Regulatory Requirement to Operational Readiness**

An Engineering-Oriented DPDPA Compliance Framework for Indian MSMEs



# An Engineering-Oriented DPDPA Compliance Framework for Indian MSMEs

Research & Development Whitepaper

R&D Wing | Shridhar InfoSec Solutions (SIS)

Vadodara, Gujarat, India

Research Period: March to August 2026 | Publication: 2026

## Evidence classification used in this paper

- **Regulatory fact.**  
Statements drawn directly from the DPDPA, 2023 and the DPDP Rules, 2025, with section references.
- **External evidence.**  
Findings reported by third-party research, consulting, and legal sources, attributed inline.
- **SIS proposition.**  
Original analysis and framework design by the SIS R&D Wing. CCE, CCMM and DORI are internal research constructs, not certified standards or validated industry benchmarks.

This distinction is maintained throughout. Nothing in this document constitutes legal advice.



# Table of Contents

|                                                                            |           |
|----------------------------------------------------------------------------|-----------|
| <b>An Engineering-Oriented DPDPA Compliance Framework for Indian MSMEs</b> | <b>2</b>  |
| Evidence classification used in this paper                                 | 2         |
| Table of Contents                                                          | 3         |
| <b>Research at a Glance</b>                                                | <b>5</b>  |
| <b>Context and Purpose</b>                                                 | <b>6</b>  |
| <b>1. Executive Summary</b>                                                | <b>7</b>  |
| <b>2. Introduction</b>                                                     | <b>9</b>  |
| <b>3. Background: The DPDPA Regulatory Landscape</b>                       | <b>10</b> |
| 3.1 Consent, Notice and Withdrawal                                         | 10        |
| 3.2 Security Safeguards and Breach Notification                            | 11        |
| 3.3 Penalty Structure                                                      | 11        |
| 3.4 Applicability Beyond Customer Data: Internal Operations                | 12        |
| 3.5 Significant Data Fiduciary Status                                      | 12        |
| <b>4. Research Methodology</b>                                             | <b>13</b> |
| 4.1 Secondary research                                                     | 13        |
| 4.2 Practitioner observation                                               | 13        |
| 4.3 Treatment of evidence                                                  | 13        |
| <b>5. Key Findings, Industry Context</b>                                   | <b>14</b> |
| 5.1 Human risk is now an AI problem, not only an insider problem           | 14        |
| 5.2 Privacy-by-design is being driven by the same AI pressure              | 14        |
| 5.3 Governance responsibility is moving up the organisation                | 15        |
| 5.4 Data discovery, minimisation and vendor risk                           | 15        |
| 5.5 The MSME gap                                                           | 15        |
| <b>6. Key Findings, SIS Original Frameworks</b>                            | <b>17</b> |
| 6.1 Status of the frameworks                                               | 17        |
| 6.2 Continuous Compliance Engineering (CCE)                                | 18        |
| 6.3 Cybersecurity-to-Compliance Mapping Model (CCMM)                       | 19        |
| 6.4 DPDPA Operational Readiness Index (DORI)                               | 20        |



|                                    |           |
|------------------------------------|-----------|
| <b>7. Case Study</b>               | <b>22</b> |
| 7.1 Organisation profile           | 22        |
| 7.2 Readiness gaps identified      | 23        |
| 7.3 How the frameworks would apply | 23        |
| <b>8. Market Positioning</b>       | <b>24</b> |
| <b>9. Recommendations</b>          | <b>25</b> |
| 9.1 Operating principles           | 25        |
| 9.2 A phased 90-day roadmap        | 26        |
| <b>10. Limitations</b>             | <b>28</b> |
| <b>11. Conclusion</b>              | <b>29</b> |
| <b>About the SIS R&amp;D Wing</b>  | <b>30</b> |
| <b>References</b>                  | <b>31</b> |
| <b>Glossary of Terms</b>           | <b>33</b> |
| <b>Future Research Directions</b>  | <b>34</b> |

## How this paper is organised

- **Discover → Map**  
Inventory personal data, purposes, systems and vendors before any control claim.
- **Engineer**  
Translate each DPDPA duty into a capability, a control and a piece of evidence (CCMM).
- **Monitor → Improve**  
Treat readiness as a repeating CCE cycle, scored across the ten DORI domains.

SIS constructs in this paper - CCE, CCMM and DORI - are research models, not certified standards.

## Research at a Glance

| Parameter                         | Detail                                                                                                                                                                                      |
|-----------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Research focus                    | DPDPA operational readiness for Indian MSMEs                                                                                                                                                |
| Research period                   | March to August 2026                                                                                                                                                                        |
| Secondary source base             | Approximately 25-30 sources: primary legislation, Big Four analyses (EY, KPMG, Deloitte), legal commentary, industry surveys and sector reporting                                           |
| Practitioner input                | Structured discussions and gap-assessment conversations with 16 MSMEs across manufacturing, retail and e-commerce, professional services, healthcare and IT/ITeS in Gujarat and Maharashtra |
| Original frameworks proposed      | Three, CCE, CCMM and DORI                                                                                                                                                                   |
| DORI assessment domains           | Ten                                                                                                                                                                                         |
| Recommended implementation period | 90 days (phased)                                                                                                                                                                            |
| Core approach                     | Discover → Map → Engineer → Monitor → Improve                                                                                                                                               |

## Context and Purpose

India's Digital Personal Data Protection Act, 2023 marks a significant shift in how organisations are expected to collect, process, protect and govern personal data. Substantial guidance has emerged from regulators, law firms, consulting organisations, cybersecurity companies and industry bodies. Most of that material, however, concentrates on explaining legal requirements, interpreting policy, or supplying high-level compliance checklists.

For Micro, Small and Medium Enterprises, the challenge is different in kind.

The practical difficulty is not understanding what the DPDPA requires. It is translating those requirements into day-to-day operational controls across systems, employees, vendors, applications, communication channels and business processes, usually without a dedicated privacy or compliance function. An MSME may handle personal data through ERP systems, spreadsheets, email, messaging platforms, HR applications, accounting software and third-party services at the same time, producing a fragmented environment in which visibility and accountability are difficult to establish.

This whitepaper examines that gap from an engineering and operational perspective. Its objective is not to reproduce existing legal guidance, but to identify recurring operational failure patterns and convert them into practical, measurable approaches for organisations with limited resources.

A central finding of this research is that DPDPA readiness should not be treated as a one-time documentation exercise. It should function as a continuing organisational capability, supported by data discovery, control implementation, monitoring, measurement and improvement.

*The position of this paper is therefore straightforward: DPDPA compliance should be engineered, evidenced, measured and continuously improved, not treated as a one-time legal checklist.*

## SECTION 01

## Executive Summary

The Digital Personal Data Protection Act, 2023 applies in full to India's MSMEs. Most small manufacturers, retailers and service businesses, however, were never built with a legal or privacy function capable of meeting that obligation. Our research finds this gap to be structural rather than a matter of awareness or intent alone.

The available evidence is stark. One survey found that only 2.5% of surveyed MSMEs understand the DPDP Act. A separate EY survey of more than 150 professionals across sectors found close to 70% of respondents were not familiar with the Act and Rules at all, a gap extending into leadership teams, not merely frontline staff. Cost compounds the problem: one estimate places MSME compliance costs at roughly ₹5-25 lakh for a simpler business, rising beyond ₹50 lakh for data-heavy operations.

Meanwhile the enforcement environment is tightening. The Act carries penalties of up to ₹250 crore for failure to implement reasonable security safeguards, with the Data Protection Board able to double a penalty under Section 33(3) for repeat or grave contraventions. Full substantive compliance becomes mandatory by May 2027 under a phased implementation timeline.

**2.5%**

of surveyed MSMEs understand the DPDP Act

**~70%**

of professionals surveyed by EY are unfamiliar with the Act &amp; Rules

**₹250 Cr**

maximum penalty for failure to implement reasonable security safeguards

In response, the SIS R&D Wing has developed three original frameworks intended to move MSMEs from one-time compliance checklists toward continuous, evidence-based readiness measurement:

- **Continuous Compliance Engineering (CCE)**, a repeating lifecycle that embeds compliance into existing IT, cybersecurity and business processes rather than layering a separate programme on top.
- **Cybersecurity-to-Compliance Mapping Model (CCMM)**, a translation model linking each DPDPA obligation to a cybersecurity or operational capability, and then to the evidence demonstrating that capability actually operates.
- **DPDPA Operational Readiness Index (DORI)**, a maturity and readiness assessment model across ten domains, producing a prioritised, evidence-backed readiness output rather than a binary compliance claim.

These remain SIS research constructs and operational design proposals rather than validated industry standards, and this paper is explicit about that distinction throughout.

The core recommendation is a phased path rather than an all-at-once compliance overhaul: appoint a named accountable owner, build a minimum data and processing inventory, link each processing purpose to controls and evidence, implement proportionate safeguards, formalise vendor governance, and adopt periodic evidence-based readiness reviews. A practical 90-day sequence, Discover and Map, Engineer Core Controls, then Monitor, Measure and Improve, allows a resource-constrained MSME to reach a measurable and sustainable posture without a large dedicated privacy team.

## DORI: ten assessment domains, in sequence

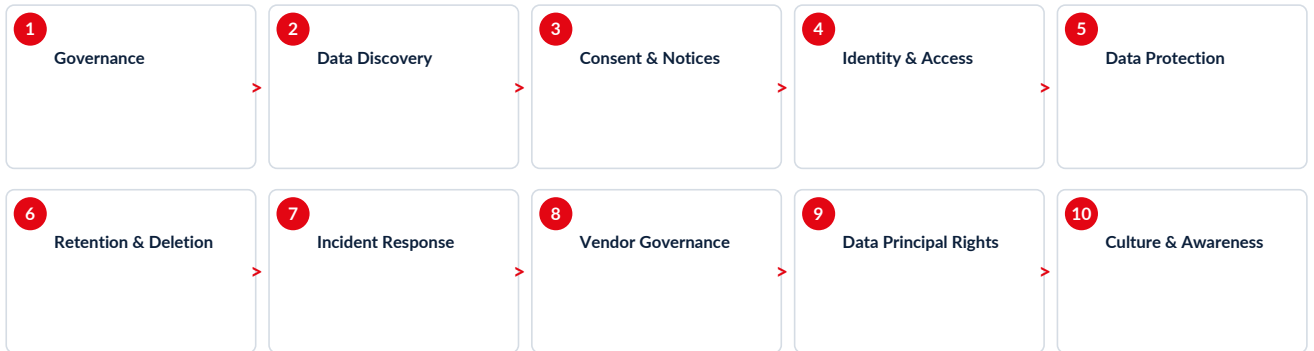


Figure 1. The compliance gap, the frameworks proposed to address it, and the intended outcome (preview of the DORI domains introduced in Section 6.4).

## SECTION 02

# Introduction

The Digital Personal Data Protection Act, 2023 is India's first comprehensive legislation governing the processing of digital personal data. Enacted on 11 August 2023, it establishes a framework balancing the individual's right to privacy against the legitimate need of organisations to process personal data for lawful purposes. Academic commentary describes it as a landmark instrument while also identifying interpretive and implementation uncertainties that remain unresolved.

The Digital Personal Data Protection Rules, 2025 operationalise parts of the Act, setting out detailed requirements on consent, notices, security safeguards, breach notification and Data Principal rights. The SIS baseline records the Rules as notified on 13 November 2025. Full substantive compliance becomes mandatory by May 2027 under a phased implementation timeline.

This paper investigates whether data discovery, governance, privacy engineering, cybersecurity controls, continuous monitoring and readiness measurement can together form a practicable operating path for such organisations.

For MSMEs, the Act creates an entirely new compliance obligation. Unlike large corporations that already maintain legal and privacy teams, most MSMEs process the personal data of customers, employees and vendors through informal or partially digitised systems, and typically lack dedicated privacy expertise, structured consent mechanisms or formal breach-response processes. Because the Act applies to virtually every entity determining the purpose and means of processing personal data, regardless of size, MSMEs now carry statutory duties with significant financial and operational consequences if left unaddressed.

The practical question is therefore not whether the law applies. It is whether a business with limited legal, privacy, security and technology personnel can identify its data, understand its purposes, configure its systems, control its vendors, respond to requests and incidents, and produce evidence of compliance without incurring disproportionate cost.

## SECTION 03

## Background: The DPDPA Regulatory Landscape

**NOTICE****CONSENT****WITHDRAWAL**

The following summary outlines the core regulatory requirements relevant to organisations, including MSMEs. Statements in this section are regulatory fact, referenced to the Act and Rules, with interpretive commentary attributed to its source.

### 3.1 Consent, Notice and Withdrawal

Consent must be free, specific, informed, unconditional and unambiguous, and must be obtained through a clear affirmative action. It is limited to the personal data necessary for the specified purpose, which rules out reliance on bundled or implied consent in practice.

Before or at the time of seeking consent, the Data Fiduciary must provide a notice in clear and plain language describing the personal data being collected, the purpose of processing, the rights available to the Data Principal, and the manner of withdrawing consent or complaining to the Data Protection Board. The notice and consent request must be available in English or any of the 22 languages specified in the Eighth Schedule to the Constitution, a requirement that materially raises the localisation burden for organisations operating across Indian states.

Withdrawal must be as easy as giving consent, a principle sometimes described as “easy in, easy out”. Once consent is withdrawn, the Data Fiduciary must cease processing, and cause its Data Processors to cease, within a reasonable time, unless continued processing is required or authorised by law. The DPDP Rules, 2025 explicitly prohibit dark patterns designed to make withdrawal harder than consent.

*Sources: DPDPA, 2023, Sections 5 and 6; DPDP Rules, 2025, Rules 3 and 8; EY India; DPDPA.com Section 6 interpretation.*

## 3.2 Security Safeguards and Breach Notification

Data Fiduciaries must implement reasonable security safeguards to prevent personal data breaches. The Act does not prescribe specific technical standards, leaving the standard to be assessed contextually against the nature and sensitivity of the data involved. Where applicable, safeguards include encryption, obfuscation or masking, appropriate access controls, logging and monitoring of access, resilience measures such as backups, and contractual obligations imposed on Data Processors.

On discovering a personal data breach, the Data Fiduciary must notify the Data Protection Board and affected Data Principals without delay, with a detailed report submitted to the Board within 72 hours of becoming aware. The clock runs from awareness rather than from the time of occurrence. There is no minimum harm threshold, every personal data breach is reportable.

A parallel and stricter obligation CERT-In Directions issued under the Information Technology Act require reporting of cybersecurity incidents within 6 hours of noticing them. This runs alongside the DPDPA timeline, not instead of it. Organisations must therefore operate a single detection and escalation process capable of satisfying both clocks. For most MSMEs this is the single most commonly overlooked interaction between the two regimes.

*Sources: DPDPA, 2023, Section 8; DPDP Rules, 2025, Rules 6 and 7; Cyril Amarchand Mangaldas FAQs; AMLEGALS DPDPA; EY analysis of the DPDP Rules, 2025.*



SAFEGUARDS

DETECT

NOTIFY

## 3.3 Penalty Structure

Enforcement under the DPDPA is civil and Schedule-based rather than formula-driven, with no imprisonment attached to non-compliance. The Data Protection Board determines the actual amount after weighing the statutory factors under Section 33(2), including the severity and duration of the breach, the sensitivity of the data involved, and whether the contravention was repeated.

| Contravention                                                                           | Maximum penalty |
|-----------------------------------------------------------------------------------------|-----------------|
| Failure to implement reasonable security safeguards resulting in a personal data breach | ₹250 crore      |
| Failure to notify the Board or affected Data Principals of a breach                     | ₹200 crore      |
| Non-compliance with obligations relating to children's data                             | ₹200 crore      |
| Breach of additional obligations by a Significant Data Fiduciary                        | ₹150 crore      |

| Contravention                            | Maximum penalty |
|------------------------------------------|-----------------|
| Other contraventions of the Act or Rules | ₹50 crore       |

Commentary further notes that Section 33(3) permits the Board to double a penalty for repeat or grave violations, which brings the effective ceiling to roughly ₹500 crore per contravention.

Sources: DPDPA, 2023, Section 33 and the Schedule; Motadata; SaralPrivacy.

### 3.4 Applicability Beyond Customer Data: Internal Operations

A common misconception is that the DPDPA governs only customer-facing data. In fact the Act governs the processing of digital personal data generally, and a wide range of internal activities constitute processing under the law, including those undertaken by HR, procurement, accounting and IT functions.

Employers may rely on the legitimate use provision under Section 7(1)(i) for core employment purposes without seeking fresh consent for routine functions. That exemption is not limitless. Organisations must still ask whether the data collected is genuinely necessary for the employment purpose or for protecting the business, and consent becomes necessary the moment data is used beyond core HR functions. The obligations of purpose limitation, data minimisation, security safeguards, breach notification and respect for Data Principal rights continue to apply across all internal functions.

The practical consequence for MSMEs is that exposure is not confined to whatever customer database or application the business operates. It extends to payroll systems, vendor onboarding records, recruitment files and everyday administrative data handling. Compliance is an organisation-wide responsibility rather than a single department's task.

Sources: DPDPA, 2023, Sections 4, 7 and 8; Anzen Technologies; Tsaaro.

### 3.5 Significant Data Fiduciary Status

Significant Data Fiduciary status is not automatic or self-declared. It is a classification conferred by the Central Government under Section 10(1), based on a risk-based assessment considering the volume and sensitivity of personal data processed, the risk of harm to Data Principals, potential impact on the sovereignty and integrity of India, risk to electoral democracy, security of the State, and public order.

Once designated, an SDF carries additional obligations: appointment of a Data Protection Officer based in India who reports directly to the board or governing body, engagement of an independent data auditor, and periodic Data Protection Impact Assessments and audits.

Large-scale processors are the primary target of the designation. Nasscom's public policy submissions nonetheless note that the SDF framework carries significant implications for governance and compliance design across India's digital economy, meaning MSMEs supplying services to, or operating within, large processing ecosystems should monitor whether their role or scale could eventually bring them into scope.

Sources: DPDPA, 2023, Section 10; DPDPA.com Section 10 interpretation; Nasscom public policy submissions.

Taken together, these requirements form the legal baseline against which the compliance readiness of organisations, and MSMEs in particular, must be assessed.

## SECTION 04

# Research Methodology

This whitepaper draws on a combination of secondary research and practitioner observation conducted by the SIS R&D Wing between March and August 2026.

## 4.1 Secondary research

The secondary base comprises approximately 25 to 30 sources: the Digital Personal Data Protection Act, 2023 and the Digital Personal Data Protection Rules, 2025; analyses from EY, KPMG and Deloitte; legal and consulting commentary from Indian firms; industry surveys including EY's survey of more than 150 professionals; threat research from Proofpoint and Google Cloud; and academic material on SSRN concerning privacy governance and the constitutional trajectory of data privacy in India.

## 4.2 Practitioner observation

Alongside the literature, the R&D Wing conducted structured discussions and gap-assessment conversations with 16 MSMEs across manufacturing, retail and e-commerce, professional services, healthcare and IT/ITeS sectors, primarily in Gujarat and Maharashtra. These were qualitative practitioner engagements intended to surface recurring operational failure patterns. They were not a statistically representative survey, and no quantitative claims in this paper rest on them.

## 4.3 Treatment of evidence

Throughout the paper, regulatory fact, external evidence and SIS proposition are distinguished explicitly. Where a source could not be verified, that is stated rather than concealed. Where a commonly cited source could not be located at all, the paper says so, for example, no single joint Deloitte-Google study devoted specifically to privacy-by-design was found, so related material from each firm is treated separately rather than presented as a unified publication.

## SECTION 05

## Key Findings, Industry Context

Industry research consistently shows that the DPDPA compliance gap is structural and widely recognised, and that it is most acute among organisations lacking dedicated privacy resources.

### 5.1 Human risk is now an AI problem, not only an insider problem

Proofpoint's 2026 AI and Human Risk Landscape report surveyed over 1,400 security professionals across 12 countries and found that 87% of organisations have pushed AI assistants past the pilot stage, while 42% have already experienced a suspicious or confirmed AI-related incident. In the Indian context, Proofpoint's 2025 Voice of the CISO research reported that 99% of Indian CISOs experienced a material loss of sensitive data in the preceding year, the highest rate globally, against a global average of 66%, with a significant share of incidents involving departing employees or careless handling.

**87%**

of organisations have pushed AI assistants past the pilot stage

**42%**

have experienced a suspicious or confirmed AI-related incident

**99%**

of Indian CISOs saw material loss of sensitive data (global avg. 66%)

More consequential than the headline numbers is the change in mechanics. Proofpoint's researchers describe an "invisible" insider threat in which the signals security teams historically relied upon, a file copied to a USB drive, a large attachment forwarded externally, simply no longer exist. An employee can type a single prompt into a copilot-style tool and receive a synthesised summary of confidential data in seconds, without any of the planning, collection and exfiltration steps that used to leave a trail.

For compliance purposes this matters directly. It undercuts the reasonable security safeguards standard discussed in Section 3.2: a control set designed around 2015-era data movement does not map cleanly onto how data actually leaks in 2026.

*Sources: Proofpoint, 2026 AI and Human Risk Landscape Report; Proofpoint, 2025 Voice of the CISO Report; Proofpoint insider risk research.*

### 5.2 Privacy-by-design is being driven by the same AI pressure

Google Cloud's Cybersecurity Forecast 2026 warns that shadow AI, employees feeding company or customer data into AI tools without security sign-off, is becoming an uncontrolled pipeline for data exposure and compliance violation, and argues that organisations need a discipline of AI data governance that embeds protection from the outset rather than bolting it on afterwards.

Deloitte's generative AI survey work supports this from the human side. In a poll of nearly 1,850 business and technology professionals, data privacy emerged as the leading ethical concern about generative AI, with roughly two in five respondents naming it their primary worry, close to double the share who said the same in 2023.

The direction of travel is consistent: privacy-by-design is shifting from an academic principle to a practical response to tools that make data far easier to move, combine and expose. Reactive approaches that rely on policy updates after systems are already live consistently prove insufficient.

*Sources: Google Cloud Cybersecurity Forecast 2026, via Kiteworks; Deloitte generative AI survey, via CIO Dive.*

### 5.3 Governance responsibility is moving up the organisation

Legal and academic commentary is broadly consistent on this point. Data governance is no longer a function that can be delegated to IT and forgotten. Accountability now sits with the executives who set policy rather than only the teams who administer systems, and boards are increasingly expected to treat data risk with the seriousness applied to a financial audit. A failure in this area reads not merely as a data breach but as a systemic governance failure, carrying personal liability exposure for leadership.

Whether Indian courts ultimately interpret DPDPA liability as GDPR enforcement has evolved remains open. The direction of the commentary, however, is unambiguous: this will not remain a back-office function.

*Sources: SJKP Law Firm LLP, data governance accountability commentary; Jain & Anand, SSRN, on the constitutional journey of data privacy in India.*

### 5.4 Data discovery, minimisation and vendor risk

EY, KPMG and Deloitte converge on a similar three-part message. KPMG's India commentary notes that the DPDPA has elevated personal data to a board-visible governance issue and demands strong vendor oversight, data minimisation, clear consent processes and rapid breach response as baseline expectations rather than stretch goals. EY's surveys of Indian organisations found that a large majority had not updated privacy governance frameworks or policies, and that third-party privacy risk assessment and contract remediation remain among the least mature activities.

Vendor risk deserves particular emphasis because it is routinely underestimated. Data Fiduciaries in India remain liable for personal data even where a third-party vendor performs the actual processing. Outsourcing a function does not outsource the legal exposure, a trap smaller organisations fall into when they assume that because a vendor handles the data, the vendor carries the risk.

On discovery and minimisation, the practical starting point is the same across every source: know what data you hold, why you hold it, where it lives and how long you keep it, before any claim to minimisation can be made meaningfully.

*Sources: KPMG India DPDP insights; EY India DPDP readiness surveys; Wattlecorp Cybersecurity Labs on third-party vendor risk.*

### 5.5 The MSME gap

This is where the research is most striking. The awareness figures are considerably worse than anticipated. One survey found that only 2.5% of surveyed MSMEs actually understand the DPDP Act. Separately, an EY survey of more than 150 professionals across sectors found close to 70% of respondents were not very familiar with the Act and Rules at all, a gap that extends into leadership teams and not merely frontline staff. That second figure is the one senior stakeholders should weigh most heavily: where leadership itself does not understand the obligation, no amount of downstream tooling compensates.

The cost picture is comparably difficult. One estimate places compliance costs for MSMEs at roughly ₹5-25 lakh for a simpler business, rising to ₹50 lakh or more for data-heavy operations, a range that can be existentially difficult for early-stage or resource-constrained businesses to absorb. Industry voices echo this operationally, noting that MSMEs typically lack both the budgets and the access to specialist consultants that larger enterprises can direct at compliance programmes.

The most useful reframe comes from sector reporting which argues that the barrier is not resistance or bad intent but an awareness and clarity gap. A large number of MSMEs already rely on cloud tools, digital payments and customer data day to day, which means the regulatory exposure exists whether or not the business recognises it. Compounding this, many are running on infrastructure never built with compliance in mind, basic ERP systems, Excel spreadsheets, or fragmented CRMs with no built-in consent tracking, automated deletion workflow or audit logging. That is not a policy gap; it is a tooling gap.

The disparity, illustrated One SME-focused legal commentary captures the imbalance concretely: a small e-commerce business using a foreign CRM cannot easily fulfil a customer's data deletion request, because large corporations can afford full privacy teams while SMEs face a disproportionate compliance burden without simplified mechanisms built for their scale. Because the DPDPA is largely size-neutral, these organisations carry the same baseline obligations as much larger entities with a fraction of the internal capacity to interpret the law, map data flows, implement technical safeguards or manage vendor contracts.

*Sources: SME Futures; EY India; The Frontier Manipur; Inc42; DPDPA.com, The DPDPA Conundrum for Indian SMEs.*

## SECTION 06

# Key Findings, SIS Original Frameworks

The research identified a clear structural gap: most existing guidance on the DPDPA is either purely legal or high-level advisory. MSMEs need practical, engineering-oriented models that translate regulatory obligations into measurable operational capabilities. In response, the R&D Wing developed three frameworks designed specifically for organisations with limited privacy resources.

## 6.1 Status of the frameworks

Please read this before the sections that follow CCE, CCMM and DORI are original SIS R&D proposals. They should be treated as hypotheses and operational design models, not as established standards, certifications or validated industry benchmarks. Their value depends on whether independent organisations can apply them consistently, whether they measurably reduce compliance effort, and whether their outputs correlate with improved control effectiveness. Validating those three questions is an active research objective, not a settled result.

## 6.2 Continuous Compliance Engineering (CCE)

CCE is proposed as a lifecycle for converting regulatory requirements into continuously maintained organisational and technical controls. It differs from a one-time assessment by treating compliance as a recurring operational capability.

At summary level, CCE runs as a five-stage repeating cycle: Discover → Map → Engineer → Monitor → Improve.



Expanded for implementation, that cycle decomposes into eight steps:

1. Interpret the applicable requirement.
2. Identify processing activities and data assets.
3. Assess risk and define control objectives.
4. Implement governance, privacy and security controls.
5. Collect evidence from systems and processes.
6. Monitor control operation and change.
7. Remediate deficiencies.
8. Reassess readiness periodically.

*The CCE proposition is that regulatory change, system change, vendor change, personnel change and incident learning should each trigger reassessment. This is SIS analysis based on recurring implementation difficulties identified in the research, not an established regulatory requirement.*

Table 1. CCE stage, core activity, expected output and evidence

| CCE stage        | Core activity                                             | Expected output               | Evidence                                   |
|------------------|-----------------------------------------------------------|-------------------------------|--------------------------------------------|
| <b>Interpret</b> | Convert legal requirements into operational obligations   | Requirement register          | Approved interpretation record             |
| <b>Discover</b>  | Identify data, systems, purposes, users and vendors       | Processing and data inventory | Discovery results and ownership record     |
| <b>Assess</b>    | Evaluate exposure, necessity, control maturity and impact | Risk and priority register    | Assessment rationale                       |
| <b>Design</b>    | Define governance, privacy and security controls          | Control plan                  | Control specifications                     |
| <b>Implement</b> | Configure processes and technologies                      | Operating controls            | Configuration and procedure evidence       |
| <b>Monitor</b>   | Track control operation, drift and change                 | Monitoring output and alerts  | Logs, access reviews, consent records      |
| <b>Improve</b>   | Remediate deficiencies and reassess                       | Updated control plan          | Remediation record and reassessment result |

The core principle is that compliance must be engineered into existing cybersecurity, IT and business processes rather than layered on top as a separate programme. This is what makes the approach sustainable for organisations that cannot maintain a dedicated privacy team.

### 6.3 Cybersecurity-to-Compliance Mapping Model (CCMM)

CCMM maps a regulatory requirement to a cybersecurity or operational capability, and then to the evidence demonstrating that the capability actually operates. Its purpose is translation, helping an organisation move from “the law requires safeguards” to “these capabilities must operate, and these records demonstrate that they do”.

Table 2. DPDPA requirement, required capability and typical MSME gap

| DPDPA requirement                                                 | Required capability                                                               | Typical MSME gap                                                                        | Control domain                |
|-------------------------------------------------------------------|-----------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------|-------------------------------|
| <b>Valid consent and clear notice (Sections 5 and 6)</b>          | Consent capture, purpose recording, multilingual notice delivery, easy withdrawal | Informal collection via WhatsApp or paper forms; no recorded purpose or withdrawal path | Consent and notice management |
| <b>Reasonable security safeguards (Section 8(5))</b>              | Encryption, access control, logging, backup, processor contracts                  | Basic or missing encryption; weak access control; no formal processor clauses           | Security safeguards           |
| <b>Breach notification (Section 8(6) and Rules)</b>               | Detection capability, 72-hour reporting process, affected-party communication     | No formal incident response playbook or notification workflow                           | Breach readiness              |
| <b>Data Principal rights (access, correction, erasure)</b>        | Request intake, verification, fulfilment tracking                                 | Ad hoc handling with no tracked process                                                 | Rights fulfilment             |
| <b>Purpose limitation and data minimisation</b>                   | Data inventory, retention schedules, deletion workflows                           | Over-collection and indefinite retention                                                | Data lifecycle management     |
| <b>Accountability for processors and vendors</b>                  | Vendor inventory, contractual flow-down, due diligence                            | Informal vendor relationships with no privacy clauses                                   | Vendor governance             |
| <b>Internal operations coverage (HR, procurement, accounting)</b> | Inclusion of employee, vendor and financial personal data in all of the above     | Only customer data treated as in scope                                                  | Scope completeness            |

Table 3. Requirement, cybersecurity capability and illustrative evidence

| DPDPA requirement             | Cybersecurity capability                | Illustrative evidence                                |
|-------------------------------|-----------------------------------------|------------------------------------------------------|
| <b>Consent and withdrawal</b> | Consent-management workflow or platform | Consent record, withdrawal record, suppression test  |
| <b>Identity verification</b>  | IAM and MFA                             | Authentication policy, access logs, review record    |
| <b>Access limitation</b>      | RBAC and privileged-access management   | Role matrix, privileged session record               |
| <b>Data protection</b>        | Encryption and tokenisation             | Key-management record, encryption configuration      |
| <b>Data discovery</b>         | Discovery and classification            | Inventory, classification rule, scan result          |
| <b>Retention and deletion</b> | Records lifecycle management            | Retention schedule, deletion job, exception register |
| <b>Breach detection</b>       | SIEM and monitoring                     | Alert log, triage record, detection rule             |
| <b>Incident response</b>      | SOAR and IR workflow                    | Incident log, containment record, notification draft |
| <b>Operational evidence</b>   | Audit logging and reporting             | System audit trail, access log, review sign-off      |

An important qualification The mapping does not assert that installing technology automatically establishes legal compliance. A tool is an enabler and an evidence generator, not a compliance guarantee. Nor does it imply that every MSME must purchase every named technology. A small organisation may satisfy a control objective through managed services, documented manual procedures, platform-native configuration, or compensating controls. CCMM requires a control-effectiveness test, not a product-presence test.

## 6.4 DPDPA Operational Readiness Index (DORI)

DORI is proposed as a maturity and readiness assessment model, designed to move an organisation beyond a binary yes/no compliance view toward evidence-backed operational measurement.



### Scoring principles

- Evidence reliance, self-declarations without supporting evidence should not receive maximum points.
- Non-linear scoring, critical vulnerabilities, such as unencrypted sensitive data in a public storage bucket, should cap or reduce the overall score regardless of governance scores.
- Action orientation, the output should identify priority remediation projects rather than produce a vanity score.

### Indicative readiness bands

Where an aggregate score is produced, the following interpretation bands are proposed as an indicative reading aid rather than a calibrated scale:

| Band  | Label      | Interpretation                                                   |
|-------|------------|------------------------------------------------------------------|
| 0-30  | Nascent    | Significant foundational gaps across multiple domains            |
| 31-55 | Developing | Basic controls present but incomplete or inconsistently operated |

| Band   | Label       | Interpretation                                                  |
|--------|-------------|-----------------------------------------------------------------|
| 56-75  | Established | Core obligations addressed with measurable, evidenced processes |
| 76-100 | Advanced    | Continuous monitoring and improvement demonstrably in place     |

Scope limits on DORI as published No DORI scoring formula is published in this paper. Weights, thresholds and aggregation rules have not been calibrated against a validation set, and it would be inappropriate to present invented values as settled methodology. The bands above are therefore an interpretation aid, not a certified maturity scale. A DORI-based self-assessment tool is currently under development by the R&D team. It should be understood as under development and not as an available or validated product.

A useful DORI output identifies domains with insufficient evidence, high-impact control gaps, dependencies between gaps, remediation priorities, accountable owners and reassessment status, rather than a superficial compliance percentage.

Together, CCE, CCMM and DORI constitute the original contribution of this whitepaper: a route from regulatory obligation, through operational capability, to measurable and evidenced readiness.

## SECTION 07

# Case Study

Note on this case study. The organisation below is anonymised and composite, drawn from the practitioner engagements described in Section 4.2. The readiness profile is illustrative of companies of this size and sector rather than the findings of a completed SIS audit engagement. No client assessment was conducted for this whitepaper, and no identifiable organisation is described.

## 7.1 Organisation profile

| Attribute          | Detail                                                                                                                                                                                                              |
|--------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Sector             | Industrial component manufacturing, supplying domestic and export customers                                                                                                                                         |
| Location           | Gujarat industrial corridor                                                                                                                                                                                         |
| Size               | Approximately 85 employees, squarely within the MSME bracket to which the DPDPA applies without exemption                                                                                                           |
| Personal data held | Customer data for order processing and invoicing; employee data for payroll, attendance and statutory compliance; vendor data for purchase orders and payments                                                      |
| Systems in use     | ERP software, Excel spreadsheets, WhatsApp Business and email                                                                                                                                                       |
| Why this profile   | Manufacturing appears consistently in readiness data as a sector with weaker DPDPA awareness, and the size and structure mirror the recurring pattern of a growing MSME with no dedicated legal or privacy function |

## 7.2 Readiness gaps identified

| Area                           | Gap observed                                                                                                                                                      | Why it is common at this scale                                                                                           |
|--------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------|
| Consent and notice             | No formal consent or notice process for customer or vendor data; information collected through informal channels without recorded purpose or withdrawal mechanism | Consent is typically an afterthought behind production and delivery priorities where no legal or privacy function exists |
| Data mapping                   | No documented data inventory; the organisation could not state what personal data it held, where it was stored, or how long it was retained                       | Matches the legacy ERP, spreadsheet and fragmented CRM pattern identified in Section 5.5                                 |
| Security safeguards            | Shared user credentials common, encryption inconsistently applied, no formal access control policy                                                                | Baseline IT security exists but was never designed against a data-protection control objective                           |
| Breach response                | No personal data breach response plan and no clarity on the 72-hour reporting obligation, nor on the parallel CERT-In 6-hour requirement                          | Most MSMEs have never had to treat breach reporting as a compliance obligation until now                                 |
| Vendor and client data sharing | No DPDPA-specific data processing clauses with vendors, despite regular exchange of technical and business data                                                   | Client-side Data Fiduciaries in regulated sectors will increasingly expect DPDPA-aligned contracts from suppliers        |

| Area                           | Gap observed                                                                                      | Why it is common at this scale                                                                                    |
|--------------------------------|---------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------|
| Internal data (HR and payroll) | Employee and vendor personal data not treated as in scope; only customer data considered relevant | Reflects the internal-operations misconception addressed in Section 3.4                                           |
| Rights fulfilment              | No structured process for handling access, correction or erasure requests                         | No intake channel exists, so requests are handled ad hoc if at all                                                |
| Governance ownership           | No named individual accountable for data protection compliance                                    | At this headcount the function is usually absorbed informally by operations or administration, or left unassigned |

Collectively these gaps place the organisation in the Nascent to early Developing range on the DORI bands.

### 7.3 How the frameworks would apply

Under CCE, the organisation would move from a reactive posture to a continuous cycle, beginning with a first-pass data map covering HR records, vendor contacts and customer correspondence, since none currently exists. Given a growth trajectory toward roughly 100 employees, drift detection matters particularly: as the company scales, adds vendors and onboards clients in regulated sectors, CCE would flag each new data relationship for a compliance check at the point it is created, rather than waiting for an annual review to catch it.

Applying CCMM would show a familiar pattern for a manufacturing MSME. Baseline IT security, network access controls, basic backup practice, probably exists and would map to covered or partial on the safeguards row. Consent management, rights-request handling and vendor data processing clauses would map to clear gaps, producing a prioritised and concrete list rather than a vague sense that compliance sits somewhere on the to-do list.

A baseline DORI assessment would produce a low-to-moderate composite result, weighted toward Governance and Data Discovery given the profile, with Vendor Governance elevated in importance because so much of the business involves handling data on behalf of larger and more scrutinised client organisations. The output gives ownership, even where informally held, a single board-presentable position to act on, and a baseline against which improvement can be measured.

Within a structured 90-day implementation, the organisation would be positioned to close the most critical gaps and move from the Nascent band into the Developing to Established range, establishing a sustainable foundation without a dedicated privacy team.

## SECTION 08

# Market Positioning



### CCE

### CCMM

### DORI

Most DPDPA service providers reviewed for this research, nationally and within Gujarat specifically, offer some combination of one-time gap assessments, generic maturity surveys, or implementation checklists. Several have built structured self-assessment tools, and at least one firm has developed a named evidence-readiness methodology.

What the review did not locate was a framework tying continuous, drift-triggered monitoring to a formal control-mapping matrix and a single weighted readiness score within one connected system, designed specifically for resource-constrained MSMEs. The combination of CCE, CCMM and DORI is built to do precisely that.

This is a claim about what a review of publicly available offerings surfaced, not an exhaustive market study, and it is stated on that basis. The distinctive position SIS occupies is the translation of DPDPA obligations into practical, measurable and sustainable operational capabilities, rather than treating compliance as a purely legal or one-time documentation exercise.

**SECTION 09**

# Recommendations

The recommendations below are set out in two layers: the operating principles an MSME should adopt, and a phased 90-day sequence for putting them in place.

## 9.1 Operating principles

### Establish accountability

Appoint an accountable owner for data protection activity, even where the role is combined with legal, IT, security, risk or operations responsibilities. Leadership should approve the scope, resources, escalation process and review cycle. Without a named owner, every subsequent step degrades into an unassigned intention.

### Build a minimum data and processing inventory

The first operational priority is to identify:

- what personal data is processed
- whose data it is
- why it is processed
- where it is stored
- who can access it
- which vendors receive it
- how long it is retained
- what happens when the purpose ends

### Link purposes to controls

Each processing purpose should be linked to a notice, a lawful basis, the data elements involved, a retention rule, an access group, the vendors concerned and an evidence source. This provides the practical bridge between legal analysis and technical implementation.

### Implement proportionate safeguards

Prioritise foundational controls: MFA for privileged and externally accessible accounts; least-privilege access; endpoint and cloud security; encryption where appropriate; secure backups; vulnerability and patch management; logging of material access and administrative activity; tested incident procedures; and employee reporting and awareness. The control set should reflect risk and feasibility. A control that is deployed but neither monitored nor tested should not be treated as fully effective.

### Formalise vendor governance

Vendor management should include a processor inventory, data-flow description, due diligence, contractual obligations, incident escalation, access review, audit or assurance evidence, subcontractor visibility, retention and deletion expectations, and exit planning.

### Use evidence-based readiness reviews

Assessments should record not only whether a policy exists but whether the control operates. Evidence may include system settings, logs, tickets, approvals, training records, test results, contracts, deletion reports and

incident exercises.

## 9.2 A phased 90-day roadmap



| MONTH 1                                                                                                 | MONTH 2                                                                                                | MONTH 3                                                                                             |
|---------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------|
| <b>MONTH 1</b><br>Discover & Map                                                                        | <b>MONTH 2</b><br>Engineer Core Controls                                                               | <b>MONTH 3</b><br>Monitor, Measure & Improve                                                        |
| Data discovery across customer, employee & vendor records; map processing to DPDPA obligations via CCMM | Notice-and-consent mechanism, baseline safeguards, processor contract clauses, breach response process | Baseline DORI assessment, ongoing monitoring of consent, access and incidents, continuous CCE cycle |

Figure 5. The recommended 90-day sequence from discovery to continuous improvement.

### Month 1, Discover and map

Conduct a basic data discovery exercise covering customer, employee and vendor personal data. Map each processing activity to the relevant DPDPA obligation using CCMM. Name the accountable owner and secure leadership sign-off on scope. Identify the highest-priority gaps, which are typically consent, security safeguards and breach readiness.

### Month 2, Engineer core controls

Implement the most critical controls: a simple notice-and-consent mechanism with a genuinely equivalent withdrawal path; baseline security safeguards covering access control, encryption where feasible, and processor contract clauses; and a lightweight personal data breach response process aligned to both the DPDPA 72-hour requirement and the CERT-In 6-hour incident reporting obligation.

### Month 3, Monitor, measure and improve

Run a baseline DORI assessment to obtain a readiness position and domain-level view. Establish simple monitoring covering consent records, access logs and incident indicators, and begin the continuous improvement cycle under CCE.

This sequence allows an MSME to move from the Nascent or early Developing stage into a measurable and sustainable compliance posture without a large dedicated privacy team.

Where external support helps For organisations that prefer external support, SIS offers a DPDPA Compliance Assessment based on the DORI model, providing a structured readiness report, prioritised gap analysis and a remediation roadmap tailored to the organisation's size and sector. The assessment is delivered as a consulting engagement. The DORI self-assessment tool referenced in Section 6.4 remains under development and is separate from this service.

## SECTION 10

# Limitations

---



---

**SCOPE**

A plain statement of scope is warranted.

This whitepaper draws on approximately 25 to 30 sources: Big Four reports, legal and consulting commentary, industry surveys and sector-specific reporting. That is a reasonable cross-section of what is publicly available and currently under discussion in the DPDPA space. It is not an exhaustive market study, and claims reported by secondary sources have not been independently verified beyond what those sources state.

The practitioner observations described in Section 4.2 involved 16 MSMEs across selected sectors in Gujarat and Maharashtra. These were qualitative engagements. Patterns observed within that group may not represent the diversity of MSMEs across all regions or industries in India, and no quantitative claim in this paper rests on them.

CCE, CCMM and DORI are SIS research proposals rather than validated standards. No scoring formula, weighting scheme or maturity calibration for DORI is published here, because none has been validated against an independent sample.

Where a source could not be located or verified, this paper says so rather than implying certainty it does not have. Several references carry that qualification explicitly.

Finally, nothing in this document is legal advice. DPDPA compliance carries real financial and legal consequences, and how the Act applies varies considerably with the business, the data handled and the way the organisation is structured. This paper is intended to build understanding and point toward practical next steps, not to substitute for a qualified lawyer or compliance professional reviewing an actual situation.

---

**EVIDENCE LIMITS**

## SECTION 11

# Conclusion

---



---

**GAP**

The compliance gap facing India's MSMEs is not a matter of bad intent or inattention. It is structural. Most small manufacturers, retailers and service businesses were never built with a legal or privacy function, and the DPDPA does not scale its expectations down for them. The distance between what the law requires and what most MSMEs currently have in place is real, widespread, and on the evidence assembled here, wider than is generally assumed.

**ENGINEER**

The frameworks proposed in this paper do not remove that gap. What they offer is a way to see it clearly and close it in sequence, with a measurable position and an evidence trail, rather than a general intention to address compliance at some future point.

**READINESS**

By translating legal obligations into engineering and operational capabilities, MSMEs can move from awareness to sustained readiness without disproportionate cost or complexity. That translation, tested and refined against real implementations, is the work this research programme continues to pursue.

## About the SIS R&D Wing

---



---

### APPLIED RESEARCH

Shridhar InfoSec Solutions (SIS) is a cybersecurity and information security practice based in Vadodara, Gujarat. The R&D Wing focuses on applied research that converts regulatory and threat developments into operational models usable by organisations that do not maintain large dedicated security or privacy teams.

This whitepaper is part of that programme. The frameworks proposed here, Continuous Compliance Engineering, the Cybersecurity-to-Compliance Mapping Model, and the DPDPA Operational Readiness Index, are internal research constructs under active development and validation.

Correspondence relating to this paper may be directed to the R&D Wing at Shridhar InfoSec Solutions, Vadodara, Gujarat, India. Further information is available at [www.shridharinfosec.com](http://www.shridharinfosec.com).

### OPERATIONAL MODELS

# References

## Primary legislation

Digital Personal Data Protection Act, 2023. Government of India.

Digital Personal Data Protection Rules, 2025. Government of India.

## Consulting and industry research

EY India. India's data privacy shift, steering the DPDP compliance and readiness.

[https://www.ey.com/en\\_in/insights/cybersecurity/india-s-data-privacy-shift-steering-the-dpdp-compliance-and-readiness](https://www.ey.com/en_in/insights/cybersecurity/india-s-data-privacy-shift-steering-the-dpdp-compliance-and-readiness)

KPMG India. Digital Personal Data Protection (DPDP).

<https://kpmg.com/in/en/insights/digital-personal-data-protection-dpdp.html>

Deloitte, via CIO Dive. Data privacy concerns swirl around generative AI adoption.

<https://www.ciodive.com/news/deloitte-generative-AI-survey/727792/>

Google Cloud / Mandiant, via Kiteworks. Google Cybersecurity Forecast 2026.

<https://www.kiteworks.com/cybersecurity-risk-management/google-cybersecurity-forecast-2026/>

Proofpoint. 2026 AI and Human Risk Landscape Report.

<https://www.proofpoint.com/us/resources/threat-reports/ai-human-risk-landscape-report>

Proofpoint. Insider Risk in 2026: AI Didn't Create Insider Risk, It Removed the Limits.

<https://www.proofpoint.com/us/blog/insider-threat-management/ai-insider-risk-no-limits>

Proofpoint. 2025 Voice of the CISO Report. Proofpoint, Inc.

## Industry bodies

Nasscom. Significant Data Fiduciary Designation under the DPDP Act: A Proportionate Approach for the Enterprise IT and ITES Industry.

<https://community.nasscom.in/communities/public-policy/significant-data-fiduciary-designation-under-dpdp-act-proportionate>

Nasscom. Feedback on the Draft Digital Personal Data Protection Rules, 2025.

<https://new.nasscom.in/communities/public-policy/nasscoms-feedback-draft-digital-personal-data-protection-rules-2025>

## Legal and regulatory commentary

AMLEGALS. DPDPA Ecosystem, Every Sector, One Law.

<https://amlegalsdpdpa.com/dpdpa-ecosystem>

DPDPA.com. Significant Data Fiduciary Under DPDPA: Complete Guide with Assessment Criteria.

[https://www.dpdpa.com/blogs/significant\\_data\\_fiduciary\\_sdf\\_dpdpa\\_guide.html](https://www.dpdpa.com/blogs/significant_data_fiduciary_sdf_dpdpa_guide.html)

DPDPA.com. The DPDPA Conundrum for Indian SMEs.

[https://www.dpdpa.com/blogs/The\\_DPDPA\\_Conundrum\\_for\\_Indian\\_SMEs.html](https://www.dpdpa.com/blogs/The_DPDPA_Conundrum_for_Indian_SMEs.html)

Wattlecorp Cybersecurity Labs. Why Does India Need Third-Party Vendor Risk Assessment DPDP?

<https://www.wattlecorp.com/third-party-vendor-risk-assessment-dpdp-india/>

Cyril Amarchand Mangaldas. FAQs on DPDPA security safeguards. [URL not separately captured, resource from the firm's publications page before publication.]

Motadata and SaralPrivacy. Penalty structure commentary.

Anzen Technologies. Internal operations and HR data commentary.

Tsaaro. Section 7(1)(i) legitimate use exemption commentary.

## Academic and governance literature

Jain, A. & Anand, A. Tracing the Constitutional Journey of Data Privacy in India: From Puttaswamy to the Draft DPDP Rules, 2025. SSRN.

[https://papers.ssrn.com/sol3/papers.cfm?abstract\\_id=5283949](https://papers.ssrn.com/sol3/papers.cfm?abstract_id=5283949)

SJKP Law Firm LLP. Data Governance Accountability: Legal Duties, Oversight, and Enforcement Risks.

<https://www.daeryunlaw.com/us/practices/detail/data-governance-accountability>

Klein, A., Manini, R. & Shi, Y. (2021). Across the Pond: How US Firms' Boards of Directors Adapted to the Passage of the GDPR. SSRN / Contemporary Accounting Research.

## MSME and sector data

SME Futures. India's MSME compliance problem is not resistance, it's awareness.

<https://smefutures.com/indias-msme-compliance-problem-is-not-resistance-its-awareness/>

The Frontier Manipur. DPDPA 2023 Series: Part III, Impact and Implementation Challenges.

<https://thefrontiermanipur.com/digital-personal-data-protection-act-dpdpa-2023-series-part-iii-impact-implementation-challenges/>

Inc42. DPDP Act Is Coming Fast But Indian Startups Are Moving At Different Speeds.

<https://inc42.com/features/dpdp-act-compliance-indian-startups-moving-at-different-speeds/>

## Market positioning research

Grant Thornton Bharat. DPDPA Readiness Assessment Tool.

<https://www.grantthornton.in/campaign/dpdpa-survey/>

Ampcus Cyber. Recruitment Firm Achieves Full DPDPA Readiness.

<https://www.ampcuscyber.com/blogs/how-ampcus-cyber-helped-recruitment-firm-achieve-full-dpdpa-readiness/>

## SIS

Shridhar InfoSec Solutions. <https://www.shridharinfosec.com/>

Shridhar InfoSec Solutions, R&D Wing. <https://www.shridharinfosec.com/rnd>

# Glossary of Terms

| Term                                    | Definition                                                                                                                                                                                                                |
|-----------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Data Fiduciary</b>                   | Any person who alone or in conjunction with other persons determines the purpose and means of processing of personal data.                                                                                                |
| <b>Data Principal</b>                   | The individual to whom the personal data relates.                                                                                                                                                                         |
| <b>Data Processor</b>                   | Any person who processes personal data on behalf of a Data Fiduciary.                                                                                                                                                     |
| <b>Significant Data Fiduciary (SDF)</b> | A Data Fiduciary designated by the Central Government under Section 10 on the basis of risk factors including volume and sensitivity of data.                                                                             |
| <b>Personal data breach</b>             | Any unauthorised processing of personal data or accidental disclosure, acquisition, sharing, use, alteration, destruction or loss of access to personal data that compromises confidentiality, integrity or availability. |
| <b>CCE</b>                              | Continuous Compliance Engineering, an SIS-proposed lifecycle for converting regulatory requirements into continuously maintained organisational and technical controls.                                                   |
| <b>CCMM</b>                             | Cybersecurity-to-Compliance Mapping Model, an SIS-proposed framework mapping each DPDPA requirement to a cybersecurity or operational capability and then to evidence.                                                    |
| <b>DORI</b>                             | DPDPA Operational Readiness Index, an SIS-proposed maturity and readiness assessment model across ten domains.                                                                                                            |
| <b>MSME</b>                             | Micro, Small and Medium Enterprise as classified under Indian law.                                                                                                                                                        |

## Future Research Directions

---

The R&D Wing treats this whitepaper as part of a continuing research programme rather than a completed exercise. Two workstreams are active.

First, a DORI-based self-assessment tool is under development, intended to let organisations generate a preliminary readiness position without requiring a full external engagement. No launch date is committed here, since the tool is still being built and tested. Validating the model, whether independent organisations apply it consistently, and whether its outputs correlate with improved control effectiveness, is the substantive research question attached to that work.

Second, and looking beyond the DPDPA specifically, OT and ICS security is planned as the Wing's next research focus. The intention is to extend the same structured, evidence-classified approach used here to the industrial control system and operational technology environments common across Gujarat's pharmaceutical, chemical and manufacturing base. Given how much of the region's industrial capacity depends on that infrastructure, and how rapidly IT and OT environments are converging, it is the natural next step for the Wing's research charter.

**Shridhar InfoSec Solutions, R&D Wing**

Vadodara, Gujarat, India | [www.shridharinfosec.com](http://www.shridharinfosec.com)

*This document is general guidance and does not constitute legal advice.*



**SHRIDHAR INFOSEC**  
S O L U T I O N S

DEFENDING YOUR DATA, SECURING YOUR SUCCESS



### Ready to take the next step?

Connect with our cybersecurity experts today.



+91 93286 67642



[info@shridharinfosec.com](mailto:info@shridharinfosec.com)



[www.shridharinfosec.com](http://www.shridharinfosec.com)