[recovered from the vector store — section8.html p.1]

Section 8 DPDPA

General obligations of Data Fiduciary. 8.(1) A Data Fiduciary shall, irrespective of any agreement to the contrary or failure of a Data Principal to carry out the duties provided under this Act, be responsible for complying with the provisions of this Act and the rules made thereunder in respect of any processing undertaken by it or on its behalf by a Data Processor. (2) A Data Fiduciary may engage, appoint, use or otherwise involve a Data Processor to process personal data on its behalf for any activity related to offering of goods or services to Data Principals only under a valid contract. (3) Where personal data processed by a Data Fiduciary is likely to be—

(a) used to make a decision that affects the Data Principal; or

(b) disclosed to another Data Fiduciary,

the Data Fiduciary processing such personal data shall ensure its completeness, accuracy and consistency. (4) A Data Fiduciary shall implement appropriate technical and organisational measures to ensure effective observance of the provisions of this Act and the rules made thereunder.
(5) A Data Fiduciary shall protect personal data in its possession or under its control, including in respect of any processing undertaken by it or on its behalf by a Data Processor, by taking reasonable security safeguards to prevent personal data breach. (6) In the event of a personal data breach, the Data Fiduciary shall give the Board and each affected Data Principal, intimation of such breach in such form and manner as may be prescribed. (7) A Data Fiduciary shall, unless retention is necessary for compliance with any law for the time being in force,—

(a) erase personal data, upon the Data Principal withdrawing her consent or as soon as it is reasonable to assume that the specified purpose is no longer being served, whichever is earlier; and

(b) cause its Data Processor to erase any personal data that was made

[recovered from the vector store — section8.html p.2]

available by the Data Fiduciary for processing to such Data Processor.

(I) X, an individual, registers herself on an online marketplace operated by Y, an e-commerce service provider. X gives her consent to Y for the processing of her personal data for selling her used car. The online marketplace helps conclude the sale. Y shall no longer retain her personal data.

(II X, an individual, decides to close her savings account with Y, a bank. Y is required by law applicable to banks to maintain the record of the identity of its clients for a period of ten years beyond closing of accounts. Since retention is necessary for compliance with law, Y shall retain X's personal data for the said period.

(8) The purpose referred to in clause (a) of sub-section (7) shall be deemed to no longer be served, if the Data Principal does not––

(a) approach the Data Fiduciary for the performance of the specified purpose;

(b) exercise any of her rights in relation to such processing,for such time period as may be prescribed, and different time periods may be prescribed for different classes of Data Fiduciaries and for different purposes.

(9) A Data Fiduciary shall publish, in such manner as may be prescribed, the business contact information of a Data Protection Officer, if applicable, or a person who is able to answer on behalf of the Data Fiduciary, the questions, if any, raised by the Data Principal about the processing of her personal data.

(10)A Data Fiduciary shall establish an effective mechanism to redress the grievances of Data Principals.

(11)For the purposes of this section, it is hereby clarified that a Data Principal shall be considered as not having approached the Data Fiduciary for the performance of the specified purpose, in any period during which she has not initiated contact with the Data Fiduciary for such performance, in person or by way of communication in electronic or physical

[recovered from the vector store — section8.html p.3]

form.

SCROLL DOWN for LEGAL INTERPRETATION

Applicable DPDP Rule 2025

Rule 6: Reasonable Security Safeguards

Rule 7: Intimation of Personal Data Breach

Rule 8: Time Period for Specified Purpose to be Deemed as No Longer Being Served

Rule 9: Contact Information of Person to Answer Questions About Processing

← Section 7 DPDPA

Section 9 DPDPA →

DPDPA
Table of contents

Report error

Your message
×

Please keep in mind that this form is only for feedback and suggestions for improvement. Unfortunately, questions will not be answered.

Do not fill this field

0 of 1000 max characters

Submit

Section 8: General Obligations of Data Fiduciary

Comprehensive Legal Interpretation & Corporate Compliance Framework

Digital Personal Data Protection Act, 2023 | Analyzed with DPDP Rules, 2025

By: Adv (Dr.) Prashant Mali | For: www.dpdpa.com

This interpretation draws upon GDPR jurisprudence, Indian constitutional law principles, comparative data protection frameworks, and practical corporate compliance experience across jurisdictions.

1. Section 8 in Statutory Context

1.1 Legislative History and Intent
Section 8 represents the legislative culmination of India's decade-long journey toward comprehensive data protection legislation. Its genesis can be traced through:

Justice B.N. Srikrishna Committee Report (2018): The Committee's draft Personal Data Protection Bill, 2018 proposed extensive obligations for Data Fiduciaries. Section 8 DPDPA synthesizes these recommendations while simplifying the compliance framework.

Constitutional Foundation - K.S. Puttaswamy v. Union of India (2017) 10 SCC 1: The Supreme Court's landmark recognition of privacy as a fundamental right under Article 21 necessitated a statutory framework to operationalize this right. Section 8 translates constitutional privacy protections into actionable corporate obligations.

IT Act, 2000 Section 43A (Now Omitted): The predecessor provision imposed liability for compensation for

neg

[recovered from the vector store — section8.html p.4]

ligent security practices. Section 8(5) builds upon this but creates a more comprehensive security framework with regulatory penalties rather than merely civil compensation.

Parliamentary Intent (2023): The Statement of Objects and Reasons accompanying DPDPA 2023 emphasized "recognising both the right of individuals to protect their personal data and the need to process such personal data for lawful purposes." Section 8 operationalizes this balance by imposing clear obligations while maintaining flexibility for business innovation.

1.2 Structural Position in the Act

Section 8 appears in Chapter II: Obligations of Data Fiduciary, which comprises Sections 4-10. This positioning is significant:

Section | Title | Relationship to Section 8

Section 4 | Grounds for processing personal data | Establishes when processing is lawful; Section 8 governs how to process lawfully

Section 5 | Notice | Section 8(9) operationalizes contact information requirement; both ensure transparency

Section 6 | Consent | Section 8(7) addresses erasure post-consent withdrawal; both protect Data Principal autonomy
Section 7 | Certain legitimate uses | Alternative lawful basis; Section 8 obligations apply regardless of basis (consent vs. legitimate use)

Section 8 | General obligations | Core operational requirements - the "how" of compliance

Section 9 | Processing of children's data | Specialized obligations; Section 8 provides baseline that applies to all processing including children's

Section 10 | Significant Data Fiduciaries | Enhanced obligations for SDFs; Section 8 applies to all Data Fiduciaries (baseline)

Critical Interpretive Principle: Section 8 as Baseline

Legal Effect: Section 8 establishes the minimum obligations applicable to ALL Data Fiduciaries. Other provisions may impose additional obligations (e.g., Section 9 for children's data, Section 10 for SDFs), but Section 8 represents the irreducible baseline.

Interpretive Canon: Apply expressio unius est exclusio alterius cautious

[recovered from the vector store — section8.html p.5]

ly. The enumeration of 11 obligations in Section 8 does not exclude other obligations found elsewhere in DPDPA. Rather, Section 8 must be read harmoniously with Sections 4-7, 9-10, and the Rules.

1.3 Non-Derogability Under Section 17(1)
Section 17(1) provides critical context for understanding Section 8's scope:

"The provisions of Chapter II, except sub-sections (1) and (5) of section 8, and those of Chapter III and section 16 shall not apply where [various exemptions listed]..."

Legal Significance: This carve-out means:

Absolute Application of §8(1): Even when processing personal data for judicial functions (§17(1)(b)), crime investigation (§17(1)(c)), or other exempted purposes, the Data Fiduciary CANNOT escape ultimate responsibility under §8(1). Universal Security Obligation §8(5): Similarly, the obligation to implement reasonable security safeguards applies WITHOUT EXCEPTION. The legislature determined that security is so fundamental that no exemption justifies weakening it. Penalty Implications: A government agency processing data under §17(1)(b) exemption cannot claim exemption from penalties for security failures under §8(5). This creates accountability even for sovereign functions. Comparative Analysis: This approach is stricter than GDPR, which allows more extensive exemptions for law enforcement processing (GDPR Article 23). India has chosen a more protective approach.
1.4 Interaction with IT Act, 2000

Section 44(2) of DPDPA amends the IT Act, 2000:

Section 43A Omitted: The previous regime of compensation for negligent security practices is replaced by DPDPA's more comprehensive framework. However, Section 43 (penalty for damage to computer systems) and Section 66 (computer-related offences) remain operative and may apply to data breaches involving unauthorized access.

Section 81 Amended: IT Act provisions do not override DPDPA. Where conflict exists, DPDPA prevails for personal data matters (per Section 38 DPDPA).

Practical Implication: Data

[recovered from the vector store — section8.html p.6]

breach scenarios may trigger BOTH DPDPA obligations (Section 8(6) notification, potential penalties under Schedule Item 1) AND IT Act consequences (Section 43 damages, Section 66 criminal liability for perpetrators).

2. Complete Statutory Text with Annotations
Section 8 - General Obligations of Data Fiduciary

(1) A Data Fiduciary shall, irrespective of any agreement to the contrary or failure of a Data Principal to carry out the duties provided under this Act, be responsible for complying with the provisions of this Act and the rules made thereunder in respect of any processing undertaken by it or on its behalf by a Data Processor. Annotation 8(1): Establishes absolute, non-delegable, vicarious liability. Four critical components: (a) contractual non-derogability, (b) immunity from Data Principal fault defense, (c) comprehensive compliance scope, (d) processor liability attribution. Comparable to GDPR Article 24(1) but stricter in non-contractibility. (2) A Data Fiduciary may engage, appoint, use or otherwise involve a Data Processor to process personal data on its behalf for any activity related to offering of goods or services to Data Principals only under a valid contract. Annotation 8(2): Mandatory pre-processing contract requirement. "Valid" imports Indian Contract Act, 1872 requirements. Broader scope than GDPR Article 28 - covers ALL forms of processor involvement. No retrospective cure possible.
(3) Where personal data processed by a Data Fiduciary is likely to be—

(a) used to make a decision that affects the Data Principal; or

(b) disclosed to another Data Fiduciary,

the Data Fiduciary processing such personal data shall ensure its completeness, accuracy and consistency. Annotation 8(3): Conditional data quality obligation triggered by: (a) decision-making impact or (b) disclosure. "Likely to be" creates anticipatory duty (lower threshold than "is"). Triad of quality: completeness (no material omissions), accuracy (factual correctness),

[recovered from the vector store — section8.html p.7]

consistency (uniformity across systems). Exempted for State under §17(4) where no decision affects Data Principal.

(4) A Data Fiduciary shall implement appropriate technical and organisational measures to ensure effective observance of the provisions of this Act and the rules made thereunder.

Annotation 8(4): "Appropriate" = context-specific, risk-based. "Effective observance" = not merely theoretical compliance but demonstrable operational adherence. Encompasses privacy by design and default. No specific implementing Rule, but overlaps with Rule 6.

(5) A Data Fiduciary shall protect personal data in its possession or under its control, including in respect of any processing undertaken by it or on its behalf by a Data Processor, by taking reasonable security safeguards to prevent personal data breach.

Annotation 8(5): Non-derogable security obligation (applies even under §17(1) exemptions). "Reasonable" = objective standard considering state of technology, costs, risks. Implemented comprehensively by Rule 6. Highest penalty: ₹250 crores (Schedule Item 1).
(6) In the event of a personal data breach, the Data Fiduciary shall give the Board and each affected Data Principal, intimation of such breach in such form and manner as may be prescribed.

Annotation 8(6): Dual notification obligation: Board + affected individuals. "Personal data breach" per §2(u) includes unauthorized processing or accidental disclosure/alteration/destruction compromising CIA triad. Detailed protocol in Rule 7. Penalty for non-notification: ₹200 crores (Schedule Item 2).

(7) A Data Fiduciary shall, unless retention is necessary for compliance with any law for the time being in force,—

(a) erase personal data, upon the Data Principal withdrawing her consent or as soon as it is reasonable to assume that the specified purpose is no longer being served, whichever is earlier; and

(b) cause its Data Processor to erase any personal data that was made available by the Data Fiduciary for

[recovered from the vector store — section8.html p.8]

Annotation 8(7): Erasure obligation with legal retention exception. Two triggers: (a) consent withdrawal OR (b) purpose no longer served (whichever earlier). Processor erasure is Data Fiduciary's responsibility ("cause its Data Processor"). Tension with Rule 6(1)(e) and Rule 8(3) minimum 1-year retention resolved by treating Rules as "law for the time being in force" under the exception clause.

(8) The purpose referred to in clause (a) of sub-section (7) shall be deemed to no longer be served, if the Data Principal does not––

(a) approach the Data Fiduciary for the performance of the specified purpose; and

(b) exercise any of her rights in relation to such processing,

for such time period as may be prescribed, and different time periods may be prescribed for different classes of Data Fiduciaries and for different purposes.

Annotation 8(8): Creates deemed cessation of purpose based on inactivity. Conjunctive test: BOTH no approach for purpose AND no rights exercise. Implemented by Rule 8(1) - Third Schedule specifies 3 years for e-commerce (≥2cr users), online gaming (≥50L users), social media (≥2cr users). Rationalized approach allowing different timelines by sector/purpose.

(9) A Data Fiduciary shall publish, in such manner as may be prescribed, the business contact information of a Data Protection Officer, if applicable, or a person who is able to answer on behalf of the Data Fiduciary, the questions, if any, raised by the Data Principal about the processing of her personal data.

Annotation 8(9): Transparency/accessibility obligation. DPO mandatory only for SDFs (§10(2)(a)); others must designate responsible person. "Publish" = make readily accessible. Rule 9 requires prominent publication on website/app.

(10) A Data Fiduciary shall establish an effective mechanism to redress the grievances of Data Principals.

Annotation 8(10): Mandatory internal grievance redressal. "Effective" = functional, accessible, respons

[recovered from the vector store — section8.html p.9]

ive. §13(3) makes exhausting this mechanism prerequisite to Board complaint (similar to GDPR's encourage-but-not-mandate approach to internal resolution). Rule 14(3) requires response within 90 days.

(11) For the purposes of this section, it is hereby clarified that a Data Principal shall be considered as not having approached the Data Fiduciary for the performance of the specified purpose, in any period during which she has not initiated contact with the Data Fiduciary for such performance, in person or by way of communication in electronic or physical form.

Annotation 8(11): Definitional clarification for §8(8). "Approach" = initiate contact (not mere passive receipt). Broad definition: in-person, electronic, or physical communication. Prevents Data Fiduciaries from claiming mere system-generated communications constitute "approach."

3. Constitutional & Legal Framework

3.1 Constitutional Moorings
Section 8's obligations must be interpreted against India's constitutional framework:

3.1.1 Right to Privacy (Article 21)

In Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 SCC 1, a nine-judge bench of the Supreme Court unanimously held that the right to privacy is a fundamental right protected under Article 21 (right to life and personal liberty) and Part III of the Constitution. Key holdings relevant to Section 8:

Justice D.Y. Chandrachud (for himself, CJI Khehar, Justices Agarwal and Nazeer):

"Privacy is the constitutional core of human dignity. Privacy has both a normative and descriptive function. At a normative level privacy subserves those eternal values upon which the guarantees of life, liberty and freedom are founded. At a descriptive level, privacy postulates a bundle of entitlements and interests which lie at the foundation of ordered liberty."

Application to Section 8: Section 8's obligations—particularly §8(5) (security), §8(7) (erasure), and §8(10) (grievance redressal)—operationalize the "bundle of entitlements" constituting privacy.

[recovered from the vector store — section8.html p.10]

These are not mere regulatory requirements but constitutional obligations flowing from Article 21.

"Right to privacy is protected as an intrinsic part of the right to life and personal liberty under Article 21 and as a part of the freedoms guaranteed by Part III of the Constitution."

Application to Section 8: The non-derogability of §8(1) and §8(5) even under Section 17(1) exemptions reflects this constitutional status. Privacy protections cannot be entirely suspended even for legitimate state functions.

3.1.2 Three-Fold Test for Privacy Infringement

The Puttaswamy judgment established that any infringement of privacy must satisfy a three-fold test:

Legality: Existence of law (satisfied by DPDPA itself)

Legitimate Goal: Law must serve a legitimate state aim (data-driven economy, consumer protection)

Proportionality: Rational nexus and least restrictive means
Interpretive Principle for Section 8: When interpreting ambiguities in Section 8 obligations (e.g., what constitutes "reasonable" safeguards under §8(5) or "appropriate" measures under §8(4)), courts should favor interpretations that satisfy proportionality. The least restrictive means necessary to achieve data protection goals should be preferred.

3.1.3 Reasonable Restrictions (Article 19)

Data processing activities often intersect with Article 19(1)(a) (freedom of speech and expression) and Article 19(1)(g) (right to practice any profession, trade, or business). Section 8's obligations must be "reasonable restrictions" under Article 19(2) and 19(6).

Judicial Review Standard: Courts will examine whether Section 8 obligations:

Serve public interest (data protection, privacy)

Implication for Corporates: If a Data Fiduciary challenges a penalty for §8 violation, the Board must demonstrate that the obligation serves data protection goals and is proportionate. However, given

[recovered from the vector store — section8.html p.11]

the deferential standard of review for economic legislation, challenges to validity of Section 8 itself are unlikely to succeed.

3.2 Statutory Interpretation Canons Applicable to Section 8

Per State of Himachal Pradesh v. Parent Hospital, (2021) 16 SCC 1: "The first and primary rule of construction is that the intention of the legislature must be found in the words used by the legislature itself."

Application: Section 8's text should be given its ordinary meaning unless leads to absurdity. Terms like "reasonable," "appropriate," "effective" should be interpreted according to common legal usage, not narrowly construed to minimize obligations.

Per Maneka Gandhi v. Union of India, (1978) 1 SCC 248: Constitutional provisions and rights-protecting statutes should be interpreted liberally to advance their purpose.

Application: Section 8, being a rights-protective provision implementing constitutional privacy guarantees, should be interpreted broadly in favor of Data Principals and narrowly against Data Fiduciaries seeking to limit obligations.
Per Commissioner of Income Tax v. Vegetable Products Ltd., (1973) 1 SCC 586: Provisions of an Act should be construed harmoniously to avoid contradiction.

Application: Apparent conflicts between Section 8(7) (erasure) and Rule 6(1)(e)/Rule 8(3) (1-year retention) must be harmonized. The Rules constitute "law for the time being in force" under §8(7)'s exception, thus mandatory retention prevails.

3.2.4 Strict Construction of Penal Provisions

Per State of Maharashtra v. Tapas D. Neogy, (1999) 7 SCC 685: Penal provisions should be strictly construed, but not so narrowly as to defeat legislative purpose.

Application: When Board imposes penalties for Section 8 violations, the breach must be clearly established. However, "strict construction" does not mean Data Fiduciaries escape liability through creative interpretation—the substance of vi

[recovered from the vector store — section8.html p.12]

Section 8(1)'s vicarious liability for Data Processor actions draws from established Indian tort and criminal law principles:

3.3.1 Master-Servant Liability

Per Pushpabai Purshottam Udeshi v. Ranjit Ginning & Pressing Co., AIR 1977 SC 1735:

"A master is liable for acts of his servant performed in the course of employment even if the master has not authorized or even forbidden such acts, provided they are not so alien to the authorized acts as to be outside the scope of employment."

Application to §8(1): Data Processor is analogous to servant; Data Fiduciary to master. Unlike traditional agency, §8(1) creates absolute liability—even acts "alien to authorized acts" (processor misconduct) don't excuse Data Fiduciary. This is stricter than common law vicarious liability. 3.3.2 Corporate Criminal Liability

Per Standard Chartered Bank v. Directorate of Enforcement, (2005) 4 SCC 530: Corporations can be held criminally liable for acts of employees under doctrine of "lifting the corporate veil."

Application: If a Data Processor's employee causes a breach, the chain of liability is: Employee → Data Processor (corporate liability) → Data Fiduciary (§8(1) vicarious liability).
Data Fiduciary cannot escape by pointing to rogue employee of its processor. 3.3.3 Non-Delegable Duties

Per Rylands v. Fletcher, (1868) LR 3 HL 330 (applied in India): Certain duties are non-delegable—liability persists regardless of delegation to contractors. Application to §8(1): DPDPA obligations are non-delegable duties. This is reinforced by "irrespective of any agreement to the contrary"—even contractual allocation of responsibility doesn't shift legal liability.

Section 8's obligations can be better understood by comparing with major international data protection frameworks:

4.1 European Union GDPR

DPDPA Section 8 Provision | GDPR Equivalent | Key Differences & Im

[recovered from the vector store — section8.html p.13]

plications
§8(1) - Absolute Responsibility | Article 24(1) - Controller responsibility Article 82(3) - Controller/processor liability | GDPR: Controllers "responsible for" compliance but can share liability with processors DPDPA: More absolute - "irrespective of any agreement to the contrary" prevents contractual liability-shifting Corporate Implication: Indian Data Fiduciaries cannot rely on GDPR-style joint liability defenses; must bear full responsibility
§8(2) - Valid Contract Requirement | Article 28(3) - Processor contracts | GDPR: Specifies minimum contract clauses in detail (Art.
28(3)(a)-(h)) DPDPA: Simpler - requires "valid contract" without prescribing specific clauses (though Rule 6(1)(f) adds security requirement) Corporate Implication: More flexibility in contract drafting but still must include security provisions per Rule 6
§8(3) - Data Quality | Article 5(1)(d) - Accuracy principle | GDPR: Unconditional obligation - accuracy always required DPDPA: Conditional - only when data "likely to be" used for decisions or disclosed Corporate Implication: Indian approach more flexible for non-critical data but requires careful determination of when trigger conditions met
§8(5) - Security Safeguards | Article 32 - Security of processing | GDPR: "Appropriate technical and organisational measures" DPDPA: "Reasonable security safeguards" Practical Effect: Similar standard; both risk-based. DPDPA's "reasonable" may be slightly less demanding than GDPR's "appropriate" but Rule 6 details are comprehensive
§8(6) - Breach Notification | Articles 33-34 - Breach notification | GDPR: Authority notification within 72 hours (Art. 33); individual notification "without undue delay" when high risk (Art. 34) DPDPA: "Without delay" to Board (Rule 7(2)(a));
72 hours for detailed report (Rule 7(2)(b)); individual notification also required but no specific timeline in Act Corporate Implication: Similar timelines; DPDPA simpler (all breaches notifiable, not just "high risk" to indiv

[recovered from the vector store — section8.html p.14]

iduals)
§8(7) - Erasure | Article 17 - Right to erasure ("right to be forgotten") | GDPR: Right-based (Data Subject requests erasure) with 6 grounds DPDPA: Obligation-based (Data Fiduciary must erase) triggered by consent withdrawal or purpose cessation Corporate Implication: DPDPA creates proactive duty, not just reactive right; potentially more burdensome
§8(8) - Purpose Cessation Timeline | Article 5(1)(e) - Storage limitation principle | GDPR: No specific inactivity timeline; case-by-case determination DPDPA: Prescribed timelines (3 years for major platforms per Rule 8(1) & Third Schedule) Corporate Implication: Indian approach provides more certainty; easier to operationalize than GDPR's vague standard
§8(10) - Grievance Redressal | No direct equivalent (GDPR encourages but doesn't mandate) | GDPR: Data Subjects can directly approach supervisory authority DPDPA: Internal grievance redressal mandatory; must exhaust before Board complaint (§13(3)) Corporate Implication: Indian approach reduces regulator burden but increases corporate compliance costs (must build grievance systems)

Key Insight: DPDPA as "GDPR-Lite" with Indian Characteristics
Similarities: Core principles (accountability, security, breach notification, erasure) mirror GDPR, facilitating compliance for global companies

Stronger absolute liability (§8(1) non-contractibility)

Conditional data quality (§8(3) trigger-based)

Specific inactivity timelines (§8(8) + Rules)

Mandatory internal grievance redressal (§8(10))

Corporate Strategy: Companies with existing GDPR programs can leverage much of that infrastructure for DPDPA but must adapt for India-specific requirements (grievance systems, specific retention timelines, absolute processor liability).

Aspect | DPDPA §8 | California CPRA
Philosophical Approach | Fiduciary obligations-centric (duties imposed on Data Fiduciaries) | Consumer rights-centric (rights granted to consumers)
Security

[recovered from the vector store — section8.html p.15]

Requirements | Mandatory "reasonable security safeguards" (§8(5)); detailed in Rule 6 | Must implement "reasonable security procedures" (§1798.150(c)); less detailed
Data Retention | Proactive erasure upon consent withdrawal/purpose cessation (§8(7)); specific timelines (§8(8)) | Retention limitations but reactive (must honor deletion requests); no proactive duty
Processor Liability | Data Fiduciary vicariously liable for all processor actions (§8(1)) | Service Providers have independent obligations; shared liability model
Private Right of Action | No private right of action; enforcement through Board only | Private right of action for data breaches (§1798.150); statutory damages $100-$750 per consumer per incident
Penalties | Administrative penalties only; up to ₹250 crores (~$30M) for security breaches | Administrative penalties ($2,500-$7,500 per violation) PLUS private litigation exposure

Critical Corporate Consideration: Litigation Risk Profile

CPRA: High litigation risk due to private right of action; class action lawsuits common for data breaches

DPDPA: Lower litigation risk (no private right of action); regulatory risk primary concern
Strategic Implication: Indian companies should focus on Board compliance rather than preparing for shareholder/class action lawsuits. However, reputational risk remains significant.

4.3 Singapore Personal Data Protection Act (PDPA)

Singapore's PDPA shares India's common law heritage and pragmatic approach:

Feature | DPDPA §8 | Singapore PDPA
Accountability | §8(1) absolute responsibility | Section 11 - Accountability obligation; similar but less explicitly non-contractible
Data Accuracy | §8(3) conditional (when used for decisions/disclosed) | Section 12 - Unconditional accuracy obligation
Data Protection Officer | §8(9) + §10(2)(a) - Mandatory for SDFs; others must designate contact person | Mandatory for all organizations; DPO must be Singapore-based
Breach Notification | §8(6) + Rule 7 - Mandatory notification to Boa

[recovered from the vector store — section8.html p.16]

rd and affected individuals | Section 26D - Similar dual notification; 3-day timeline to PDPC for significant breaches
Penalties | Up to ₹250 crores (~$30M USD) for serious violations | Up to SGD 1 million (~$750K USD) or 10% of annual turnover

Convergence Observation: Singapore and India follow similar philosophical approaches (accountability-based, pragmatic, business-friendly while protecting privacy). However, DPDPA's penalty regime is significantly more severe, reflecting India's determination to ensure robust compliance from the outset.
4.4 Brazil LGPD (Lei Geral de Proteção de Dados)

Brazil's LGPD, enacted in 2018 and effective 2020, provides useful comparison as another major emerging economy implementing comprehensive data protection:

Similarities with DPDPA §8:

Security Obligation (LGPD Art. 46): Similar to §8(5), requires technical and administrative measures to protect data

Data Quality (LGPD Art. 6, III-IV): Principles of adequacy, relevance, accuracy

Purpose Limitation (LGPD Art. 16): Data must be eliminated when purpose achieved, similar to §8(7)

LGPD Innovations Not in DPDPA:

Data Protection Impact Assessment (Art.
38): Detailed DPIA requirements for high-risk processing (DPDPA only requires this for SDFs under §10(2)(c)(i))

Data Protection Officer (Art. 41): Mandatory for all controllers (DPDPA only for SDFs)

Corporate Implication: Companies operating in both Brazil and India face heavier compliance burden in Brazil (mandatory DPO, DPIA for all) but heavier penalties in India (up to ₹250cr vs. Brazil's 2% revenue cap of ~R$50M).

5. Section 8(1): Absolute, Non-Delegable Responsibility - Deep Dive

Statutory Text

"A Data Fiduciary shall, irrespective of any agreement to the contrary or failure of a Data Principal to carry out the duties provided under this Act, be responsible for complying with the provisions of this Act and the rules made thereunder in respect of any processing undertaken by it or on its behalf by a Data Processor."

5.1

[recovered from the vector store — section8.html p.17]

Legal Doctrine: Non-Derogable Obligations

The phrase "irrespective of any agreement to the contrary" invokes the principle of jus cogens or peremptory norms in contract law. Analysis:

5.1.1 Contract Law Foundation (Indian Contract Act, 1872)
Section 23 ICA: "The consideration or object of an agreement is lawful, unless... it is forbidden by law... or... is of such a nature that, if permitted, it would defeat the provisions of any law; or is fraudulent; or involves or implies injury to the person or property of another; or the Court regards it as immoral, or opposed to public policy."

Application: Any contract term attempting to transfer Data Fiduciary responsibility under §8(1) "defeats the provisions" of DPDPA and is thus void under Section 23 ICA. This is not merely voidable (subject to party challenge) but void ab initio (void from inception).
⚠️ Critical Corporate Compliance Point

Invalid Clauses (Void Under Section 23 ICA + §8(1)):

"The Data Processor shall be solely responsible for all data protection compliance under DPDPA 2023."

"Data Fiduciary's liability under DPDPA shall not exceed ₹1 crore."

"Data Processor indemnifies Data Fiduciary for all penalties imposed by Data Protection Board."

"Each party shall be responsible only for its own DPDPA compliance."

"Data Fiduciary is not liable for Data Processor's security failures."

Why These Are Void: Each attempts to limit, transfer, or cap the absolute responsibility imposed by §8(1). While indemnification agreements are valid commercially (Data Fiduciary can seek reimbursement from Data Processor), they DO NOT affect Data Fiduciary's liability to Data Principals or the Board.
Correct Approach: "Data Fiduciary acknowledges its continuing responsibility under DPDPA 2023, including for processing by Data Processor. Data Processor shall [security obligations]. If Data Fiduciary incurs losses, penalties, or liabilities due to Data Processor's breach of this Agreement, Data Processor shall indemnify Da

[recovered from the vector store — section8.html p.18]

ta Fiduciary for such losses."

5.1.2 Comparative Analysis: GDPR Article 82(3)

GDPR Article 82(3) states: "A controller or processor shall be exempt from liability... if it proves that it is not in any way responsible for the event giving rise to the damage."

DPDPA §8(1) is Stricter: Unlike GDPR, which allows a controller to potentially "prove" lack of responsibility for a processor's actions, DPDPA §8(1)'s "irrespective of any agreement" language suggests NO such defense. The Data Fiduciary IS responsible, period.

Corporate Implication: European case law (e.g., Fashion ID, C-40/17, CJEU) allowing controllers to argue they weren't responsible for specific processing stages is INAPPLICABLE in India. Under DPDPA, "irrespective" means the Data Fiduciary can't escape liability by showing the processor acted independently or wrongfully.

5.2 "Failure of a Data Principal to Carry Out the Duties" - No Contributory Negligence Defense
Section 15 DPDPA lists Data Principal duties:

Comply with applicable laws (§15(a))

Not impersonate another person (§15(b))

Not suppress material information for government IDs (§15(c))

Not register false/frivolous grievances or complaints (§15(d))

Furnish only verifiably authentic information (§15(e))

Section 8(1) makes clear: Data Principal's breach of these duties does NOT reduce or eliminate Data Fiduciary's obligations.

5.2.1 Comparison with Tort Law

Tort Law Principle | DPDPA §8(1) Approach
Contributory Negligence If plaintiff's negligence contributed to harm, damages reduced proportionally Example: If plaintiff 30% at fault, damages reduced by 30% | No Reduction for Data Principal Fault Even if Data Principal violated §15 duties, Data Fiduciary's obligations remain 100% Example: If Data Principal provided false info (§15(e)) but breach occurred due to poor security (§8(5)), Data Fiduciary still fully liable
Defense of Inevitable Accident Defendant not liable if harm was unforeseeable and unavoidable despite reasonable care | N

[recovered from the vector store — section8.html p.19]

o "Inevitable Accident" Defense Even sophisticated cyberattacks (e.g., zero-day exploits) don't eliminate liability if "reasonable security safeguards" (§8(5)) weren't implemented Note: May affect quantum of penalty but not liability itself
Plaintiff's Assumption of Risk If plaintiff voluntarily assumed known risk, defendant may avoid liability | No "Assumption of Risk" Defense Even if Data Principal consented to risky processing, Data Fiduciary must comply with §8 obligations Example: User clicks "I accept the risk" for weak password - Data Fiduciary still must implement reasonable security (MFA, encryption, etc.)

5.2.2 Policy Rationale: Why No Contributory Negligence Defense?

Three Rationales for Absolute Liability:

1. Information Asymmetry: Data Fiduciaries are sophisticated entities with technical expertise and resources. Data Principals are typically individuals without technical knowledge. Allowing Data Fiduciary to blame Data Principal would reverse the power dynamic DPDPA seeks to correct.
2. Professional Responsibility: Data Fiduciaries are in the business of data processing. Part of that professional responsibility is implementing safeguards that don't depend on Data Principal perfection. Analogy: A doctor can't avoid malpractice liability by arguing patient didn't follow post-op instructions if the surgical error itself was negligent.

3. Incentive Alignment: If Data Fiduciaries could reduce liability by pointing to Data Principal faults, they'd have perverse incentive to implement lax verification and blame users. Absolute liability incentivizes robust systems that work even with imperfect user behavior.

5.2.3 Practical Scenario Analysis

Case Study: The False Identity Document Scenario

Facts:

Priya opens a fintech account using fabricated Aadhaar card and PAN card

Fintech platform FinFast relies on these documents without verification

Data breach later exposes Priya's account data (including the false IDs)

FinFast argues: "Priya violated §15(c

[recovered from the vector store — section8.html p.20]

) by suppressing material information, so we're not liable"

Priya's Liability: She violated §15(c). Schedule Item 5 penalty: up to ₹10,000. She may also face fraud charges under IPC.

FinFast's Liability: §8(1) states liability is "irrespective of... failure of Data Principal to carry out duties." FinFast remains fully liable for:

Breach notification failure (§8(6)) - Schedule Item 2: up to ₹200 crores

Inadequate security safeguards (§8(5)) - Schedule Item 1: up to ₹250 crores

Failure to implement appropriate measures (§8(4)) - Schedule Item 7: up to ₹50 crores

Board's Determination: The Board will consider FinFast's argument regarding Priya's fraud when determining penalty quantum under §33(2)(a)-(g), but CANNOT excuse the violation entirely. Factors §33(2) requires Board to consider:

Type and nature of personal data affected

Proportionality and effectiveness of penalty

Priya's fraud goes to factor (a) - "nature... of breach" - Data Fiduciary was misled. This may reduce penalty from maximum, but doesn't eliminate it.

Implement DigiLocker integration for digital verification of government IDs

Use Aadhaar-based e-KYC or Video KYC per RBI guidelines
Deploy document authentication technologies (UV feature detection, etc.)

Maintain audit trails of verification attempts

Risk-based additional verification for high-value accounts

Corporate Takeaway: §8(1) means Data Fiduciaries must implement verification systems robust enough to detect fraudulent documents. "The user lied" is not a defense - you must build systems that don't simply trust user submissions.

5.3 "Responsible for Complying" - Scope of Liability

The phrase "responsible for complying with the provisions of this Act and the rules made thereunder" creates comprehensive liability spanning:

[recovered from the vector store — section8.html p.21]

al Scope

Pre-Collection: Responsibility begins BEFORE data collection (must have valid contract with processors per §8(2), must plan security per §8(5), must prepare notice per §5)

During Processing: Ongoing obligations (maintain security, ensure quality, respond to rights requests)

Post-Processing: Even after active processing ends, obligations persist (breach notification if later discovered, retention per Rules, erasure when required)

Post-Erasure: Certain obligations survive (1-year retention of logs per Rule 8(3), potential Board inquiries)

Corporate Implication: Data protection compliance is a lifecycle obligation, not a one-time checkpoint. Companies must budget for ongoing compliance, not treat it as a one-time project. 5.3.2 Substantive Scope

DPDPA Obligation Category | §8(1) Responsibility Implications
Lawful Basis (§§4-7) | Data Fiduciary responsible for ensuring valid consent (§6) or legitimate use basis (§7) exists BEFORE processing. If processor begins processing without valid basis at Fiduciary's direction, Fiduciary liable. Notice & Transparency (§5) | Data Fiduciary must ensure notice provided to Data Principals.
If processor collects data without providing Fiduciary's notice, Fiduciary responsible.

Section 8 Obligations (self-referential) | Fiduciary responsible for own AND processor's compliance with ALL §8 obligations. Creates recursive liability - responsible for ensuring processors are responsible.
Children's Data (§9) | If processor processes children's data without parental consent, Fiduciary liable. No defense: "We told processor not to collect children's data."
SDF Obligations (§10) | If Fiduciary is SDF, responsible for conducting DPIA, audit, appointing DPO. Cannot delegate these responsibilities (though can hire consultants to assist).
Data Principal Rights (§§11-14) | Fiduciary must ensure processors cooperate in fulfilling rights requests (access, correction, erasure, grievance redressal, nomination).
Cross-Border Transfers (§16

[recovered from the vector store — section8.html p.22]

) | If processor transfers data outside India in violation of §16 restrictions, Fiduciary liable even if transfer unauthorized.
Rules Made Under Act | Responsibility extends to ALL rules (current DPDP Rules 2025 and any future rules). Fiduciary must monitor for new rules and ensure compliance.

5.3.3 Geographic Scope
Section 3 DPDPA establishes extraterritorial application. Combined with §8(1):

Indian Fiduciary, Indian Processor: Clear application

Indian Fiduciary, Foreign Processor: Indian Fiduciary liable for foreign processor's actions

Foreign Fiduciary, Indian Data Principals: Foreign Fiduciary liable if offering goods/services to Indians (§3(b))

Foreign Fiduciary, Foreign Processor, Indian Data Principals: Foreign Fiduciary liable for foreign processor when processing data of Indians

Enforcement Challenge: Board's ability to enforce penalties against foreign entities depends on:

Presence of assets in India

International cooperation agreements

Voluntary compliance (reputational pressure)

Corporate Strategy: Foreign Data Fiduciaries should either: (a) appoint Indian representative/agent, (b) maintain escrow account in India for potential penalties, or (c) obtain liability insurance covering Indian regulatory penalties. 5.4 "Any Processing Undertaken...
on its Behalf by a Data Processor" - Vicarious Liability Deep Dive

5.4.1 What Constitutes "On Behalf Of" Processing?

§2(k) defines Data Processor as "any person who processes personal data on behalf of a Data Fiduciary." But what makes processing "on behalf of" rather than independent processing?

GDPR Guidance (Applicable by Analogy):

CJEU in Wirtschaftsakademie Schleswig-Holstein, C-210/16:

"The administrator of a Facebook fanpage... determines, at least in part, the purposes and means of the processing of personal data relating to visitors of that fanpage... must be regarded as taking part, by its use of a fanpage, in the determination of the purposes and means of the processing..."

Key Test: Who

[recovered from the vector store — section8.html p.23]

Data Fiduciary: Determines WHY (purpose) and HOW (means) to process

Data Processor: Processes according to Fiduciary's instructions; doesn't determine purpose, limited discretion on means

Grey Area - Joint Controllers: If two entities jointly determine purpose and means, BOTH are Data Fiduciaries (joint controllers). §8(1) would apply to each.

5.4.2 Processor Sub-Contracting: Chain Liability

Company A (Indian E-Commerce Company) = Data Fiduciary

Company B (Cloud Storage Provider) = Data Processor for A

Company C (Data Center Operator) = Sub-Processor for B

Company D (Hardware Maintenance) = Sub-Sub-Processor for C

Breach Occurs: Company D's employee steals hard drive containing Company A's customer data.

Company A (Data Fiduciary): Fully liable to Data Principals and Board under §8(1). No defense: "We didn't know about Company D" or "We only contracted with Company B."

Company B (Data Processor): May have independent liability under §8(1) if it also acts as Fiduciary for its own purposes OR under contractual obligation to Company A. Could also face penalties as processor (Schedule Item 6: voluntary undertaking breach).
Company C & D: Similar to Company B - potential liability in processor capacity.

Pay penalty to Board (no choice under §8(1))

Sue Company B for breach of Data Processing Agreement

Company B sues Company C for sub-processor breach

Company C sues Company D for sub-sub-processor breach

Company A may sue Company D directly if tort law permits (likely yes under Indian law)

With Company B: "Company B shall not engage sub-processors without prior written approval of Company A. Company B remains liable for all acts of sub-processors. Company B shall flow down all data protection obligations to sub-processors."

[recovered from the vector store — section8.html p.24]

Evidence of sub-processor contractual obligations

Liability insurance covering data breaches (minimum ₹100 crores)

Right for Company A to audit any sub-processor

Indemnification: "Company B shall indemnify Company A for all penalties, damages, costs, and expenses arising from sub-processor failures, including legal fees and Board penalties."

Critical Point: These contractual protections provide Company A with recourse against Company B, but DO NOT reduce Company A's liability under §8(1). Company A must pay the Board's penalty first, then seek reimbursement from Company B.

Under the Companies Act, 2013 and corporate governance best practices, Board of Directors has fiduciary duty to ensure company complies with law. §8(1)'s absolute liability means:

Personal Liability Risk: While DPDPA doesn't create personal director liability (penalties on Data Fiduciary entity), directors may face:

Companies Act, 2013 §166: Duty to act in good faith, with due care and diligence. Failure to ensure DPDPA compliance could breach this duty.
Shareholder Derivative Suits: If penalty causes significant financial loss, shareholders may sue directors for breach of fiduciary duty (especially if directors ignored clear compliance risks).

D&O Insurance Claims: Directors & Officers insurance may exclude coverage if directors were grossly negligent in overseeing data protection.

Reputational Risk: Directors of companies facing major DPDPA penalties may find difficulty securing future board positions.

Establish Board-Level Committee: Data Protection & Privacy Committee (or add to Audit Committee charter)

Regular Reporting: Quarterly reports to Board on:

Data Processor relationships and due diligence

[recovered from the vector store — section8.html p.25]

Annual Resolution: Board should annually approve:

Data Protection Impact Assessment (for SDFs)

Expert Advice: Board should engage external legal counsel for annual DPDPA compliance opinion (similar to tax or financial audit opinions).

Insurance: Ensure D&O policy and general liability policy cover regulatory penalties (noting many insurers exclude fines/penalties, so special cyber/privacy insurance needed).

Whistleblower Mechanism: Enable employees to report compliance concerns directly to Board/Audit Committee without management filtering.

5.5.2 Chief Privacy Officer / Data Protection Officer

While §10(2)(a) mandates DPO only for Significant Data Fiduciaries, §8(1)'s absolute liability means ALL Data Fiduciaries should seriously consider appointing a Chief Privacy Officer (CPO) or equivalent, reporting to Board/CEO.

Overall accountability for DPDPA compliance (subject to Board oversight)

Oversight of Data Processor relationships

Internal compliance audits and monitoring

Regulatory intelligence and updates to Board

Report to CTO/CISO: Pros - Technical alignment. Cons - Privacy may be subordinated to technology priorities.
Report to General Counsel: Pros - Legal expertise, independence. Cons - May be seen as purely legal/compliance function rather than business enabler.

Report to CEO (Best Practice): Pros - High visibility, cross-functional authority, clear business accountability. Cons - CEO attention bandwidth limited.

Report to Board Committee: Pros - Maximum independence. Cons - May lack day-to-day operational engagement.

Recommendation: CPO/DPO should have dual reporting: administratively to CEO (for operational matters) and functionally to Board Audit/Risk Comm

[recovered from the vector store — section8.html p.26]

ittee (for compliance oversight). This mirrors Chief Audit Executive structures in many companies.

End of Excerpt - Full Document Continues

This comprehensive legal interpretation continues with detailed analysis of:

 Sections 8(2) through 8(11) - Complete subsection analysis

 Rules 6-9 - Detailed rule-by-rule breakdown

 Penalty framework and enforcement strategies

 100+ practical scenarios and case studies