jsa
advocates & solicitors

JSA Prism

Privacy and Data Protection

Digital Personal Data Protection Act

Edition VIII

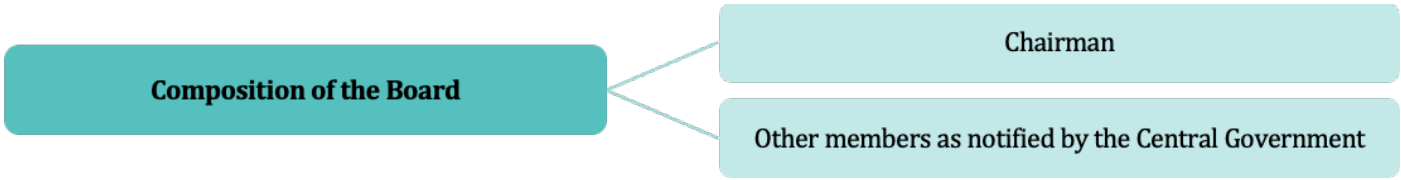
November 2024

Enforcement and penalties under the Digital Personal Data Protection Act, 2023

The Digital Personal Data Protection Act, 2023 ("**DPDPA**") establishes a multi-tier oversight mechanism and a penalty framework to enforce accountability among data fiduciaries. In the eighth edition of the Prism series, we delve into the enforcement mechanisms and penalties for non-compliance under DPDPA. DPDPA requires that the data principal must first exhaust the grievance redressal mechanism provided by the data fiduciary or consent manager and then approach the Data Protection Board of India ("**Board**"), if not resolved by the data fiduciary/consent manager. We analyse the powers and functions of the Board, its complaints resolution procedure and factors for imposing penalties. In the latter section of the Prism, we compare enforcement and penalty provisions across major data protection laws, such as the General Data Protection Regulation ("**GDPR**"), California Consumer Protection Act ("**CCPA**") and Singapore's Personal Data Protection Act ("**PDPA**").

Data Protection Board of India

The Board under DPDPA, will be an independent corporate entity empowered to enforce the DPDPA, adjudicate on complaints related to data protection violations, impose penalties, and provide guidance on the implementation of data protection laws.



The Board members serve renewable 2 (two) year terms, and post-tenure employment with any data fiduciaries previously overseen is restricted to avoid conflicts of interest. The chairperson holds administrative authority, including assigning responsibilities, managing administrative matters, and delegating functions among members. In the chairperson's absence, the senior-most member assumes these duties.

The members, officers, and employees of the Board are classified as public servants under the Bharatiya Nyaya Sanhita, 2023, which subjects them to specific accountability standards while discharging their regulatory duties. Its core responsibilities include:

1. **Response to personal data breaches:** remedial and mitigation measures: On receiving notification of a personal data breach, the Board is empowered to direct urgent remedial or mitigation measures to address the breach immediately. Following this, the Board may conduct an inquiry into the breach and, if warranted, impose penalties.
2. **Handling complaints and references:**
    a) Data principal complaints: If a data principal submits a complaint about a personal data breach, or a failure by a data fiduciary to meet its obligations, the Board is authorised to conduct an inquiry and, where appropriate, impose penalties.
    b) Consent manager complaints: The Board may also inquire into and penalise any breach by a consent manager regarding its obligations towards a data principal's personal data.
    c) Breach of registration conditions: In the event of a breach of any registration condition by a consent manager, the Board has the authority to investigate and impose penalties as it is vested with the powers of a civil court.
    d) Intermediary breaches: The Board may investigate breaches of Section 37 (2) (*Power of Central Government to issue directions*) by an intermediary based on a reference from the Central Government and impose penalties as stipulated in DPDPA.
3. **Issuance and modification of directions; directive powers:** For effective enforcement, the Board may issue directions necessary for compliance. These directions are binding, and the Board must provide an opportunity for the concerned party to be heard, along with documented reasons for the directive.

    Upon receiving a representation from an affected party or a referral from the Central Government, the Board holds the power to modify, suspend, withdraw, or cancel issued directions. In doing so, the Board can impose conditions it deems appropriate, specifying the terms under which the modification or cancellation is effective.

This consolidated framework establishes the Board as a pivotal entity in the enforcement of data protection compliance, enabling prompt responses to breaches, robust oversight of obligations, and clear mechanisms for modifying and enforcing compliance directives.

Complaints and Resolution

The procedural framework of the Board is structured to allow for systematic handling of data breaches and complaints. Below is a step-by-step breakdown:

Complaint and reference review

Upon receiving a complaint, government reference, or court directive, the Board examines its validity. If grounds are determined insufficient, the case may be closed with reasons recorded in writing.

Grounds for inquiry determination

When grounds are sufficient, the Board decides whether an inquiry is warranted. The Board is empowered to examine the activities of any entity suspected of violating DPDPA provisions.

Issuance of interim orders

If immediate action is necessary, the Board can issue interim orders to prevent or mitigate further breaches, following a fair hearing for the affected party.

Final decision and documentation

Upon concluding the inquiry, the Board may either close the case or impose penalties and sanctions as outlined in DPDPA, ensuring that all decisions are substantiated with written documentation.

Appeals to Appelate Tribunal

Individuals aggrieved by an order from the Board may appeal to the Appellate Tribunal within 60 (sixty) days of receiving the order. The Appellate Tribunal can allow late appeals for valid reasons. After reviewing the case and hearing from all the parties, it can confirm, modify, or overturn the Board's order. If any party is not satisfied with the decision of the Appellate Tribunal, they may futher appeal to the Supreme Court.

Additional factors:

1. The Board functions as a digital office, managing the receipt, hearing, and resolution of complaints entirely online, implementing techno-legal measures as necessary.
2. During the inquiry, the Board abides by principles of natural justice, meticulously documenting each action taken to ensure transparency.
3. To effectively discharge its responsibilities, the Board is vested with the powers of a civil court**.** Additionally, the Board has the authority to inspect relevant documents and records.
4. The Board avoids impeding daily business activities, refraining from seizing premises or equipment essential for operations during inquiries.
5. The Board may request assistance from police or government officers to carry out its investigations, and such officers are legally obliged to comply.
6. To discourage abuse of the complaint process, the Board may issue warnings or impose costs on complainants if a complaint is deemed false or frivolous.
7. “Appellate Tribunal” means the Telecom Disputes Settlement and Appellate Tribunal established under Section 14 of the Telecom Regulatory Authority of India Act, 1997.

Alternative Mechanisms

1. **Mediation:** The Board may recommend mediation if it believes a complaint can be resolved amicably. Parties are encouraged to engage with mutually agreed mediators or follow relevant Indian mediation laws, promoting collaborative solutions to disputes.

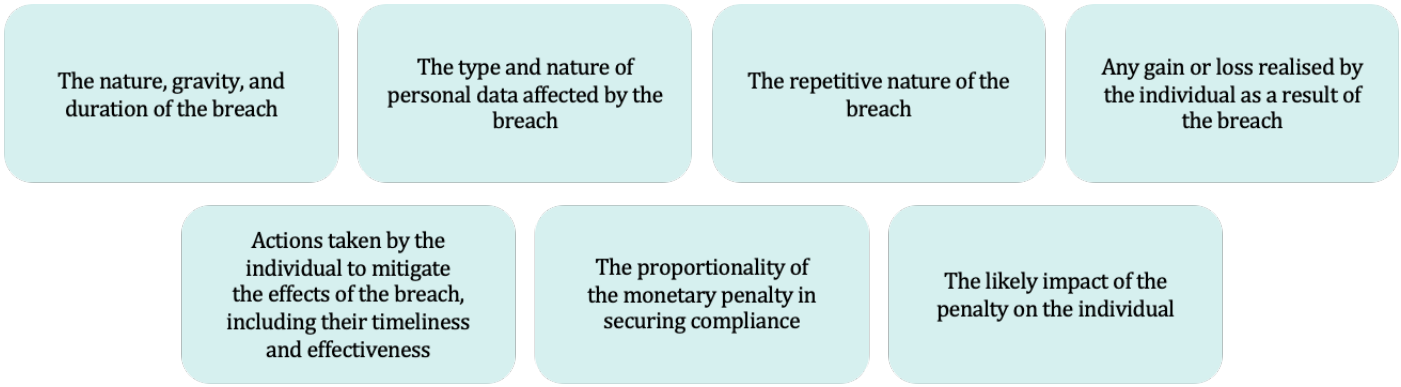
Mediation is an alternative dispute resolution process where a neutral third party, known as a mediator, assists the disputing parties in reaching a mutually acceptable agreement. The mediator does not make a decision but facilitates communication, helping parties find common ground and solutions voluntarily. The Code of Civil Procedure, 1908 allow courts to refer cases for mediation when they see the potential for an amicable settlement. Since the Board is vested with powers similar to that of civil courts, the Board may also refer cases to mediation where it deems fit.

2. **Voluntary Undertakings:** The Board can accept voluntary undertakings from individuals to ensure compliance with the DPDPA at any stage of a proceeding. These undertakings may include commitments to take specific actions or refrain from certain behaviours. The Board can modify the terms with mutual consent. While a voluntary undertaking can halt further proceedings on the related issues, failure to comply is treated as a breach of DPDPA, allowing the Board to initiate enforcement actions after giving the individual a chance to be heard. This process fosters compliance and accountability among stakeholders.

Penalties under DPDPA

Under the DPDPA, if the Board determines that a significant breach of DPDPA or its rules has occurred, it may impose a monetary penalty after providing the individual with an opportunity to be heard. In assessing the appropriate penalty, the Board considers several factors to ensure that penalties are proportional and effective in deterring future violations.

These factors include:



The penalties for specific breaches are as follows:

Breach of provisions of the DPDPA or rules made thereunder	Penalty
Breach of security safeguards under Section 8(5)	Up to INR 250,00,00,000
Failure to notify the Board or affected data principal of a breach under Section 8(6)	Up to INR 200,00,00,000
Breach of obligations concerning children under Section 9	Up to INR 200,00,00,000

Breach of provisions of the DPDPA or rules made thereunder	Penalty
Breach of obligations for significant data fiduciaries under Section 10	Up to INR 150,00,00,000
Breach of duties of data principal under Section 15	Up to INR 10,000
Breach of voluntary undertakings accepted by the Board under Section 32	Penalties vary based on the breach
Any other violations of the DPDPA or its rules	Up to INR 50,00,00,000

Under Section 37 of the DPDPA, the Central Government is empowered to block public access to information held by a Data Fiduciary that has been subject to monetary penalties for violations of data protection regulations, in 2 (two) or more instances. This action is initiated upon a formal recommendation from the Board. Importantly, the data fiduciary is afforded an opportunity to respond before any blocking order is issued, ensuring a degree of procedural fairness. Compliance with such directives is mandatory for intermediaries, with terms clearly defined in alignment with the Information Technology Act, 2000, highlighting the intersection of data protection and regulatory enforcement.

All sums collected as penalties will be credited to the Consolidated Fund of India.

The Consolidated Fund of India is the main fund of the Indian Government, where all revenues received (like taxes), loans raised, and money received in repayment of loans are deposited. It's essentially the government's primary financial reservoir, set up under Article 266(1) of the Indian Constitution.

Comparison with Global Data Protection Laws

The table below compares enforcement and penalty provisions across the DPDPA, GDPR, CCPA, and PDPA, highlighting key differences in penalty scope, criteria for fines, appeal mechanisms, and revenue allocation.

CONCEPT	DPDPA	GDPR	CCPA	PDPA
Enforcement body	Data Protection Board of India	Data Protection Authorities in each European Union member State (supervisory authorities)	Direct CCPA/ (California Consumer Privacy Act) issues will be referred to the California Privacy Protection Agency as the main enforcement authority. The California Attorney General's office is involved mainly in data breach consumer suits or significant oversight cases	Personal Data Protection Commission
Maximum penalty amount	Up to INR 250,00,00,000 for security breaches, unauthorised processing, and non-	Up to Euro 20,000,000 or 4% of global annual turnover, whichever is higher	Fines up to USD 7,500 per intentional violation and USD 2,500 per	Up to SGD1,000,000 for each breach

CONCEPT	DPDPA	GDPR	CCPA	PDPA
	compliance (per the DPDPA's Schedule)		unintentional violation	
Appeal process	Appeals against Board's decisions can be made to the Appellate Tribunal, with further appeal options under the Telecom Regulatory Authority of India Act, 1997 for unresolved cases	Right to judicial appeal against penalties before national courts	No specific provision mentioning the appeal process.	Appeals against penalties may be submitted to the Data Protection Appeal Committee
Alternate dispute resolution	The Board may recommend mediation for complaints that may be resolved without further litigation	Alternative dispute resolution ("**ADR**") mechanisms available at the discretion of national supervisory authorities	Does not specify ADR mechanisms directly within its provisions	No specific ADR; enforcement handled by the Personal Data Protection Commission

Infotech Practice (Privacy and Data Protection)

Our team understands the importance of data privacy in today's digitally interconnected world. We have dedicated our practice to ensuring that your and your customers' personal and business data remains secure, compliant, and respects the sovereignty of individuals and jurisdictions globally.

We prioritise creating bespoke solutions tailored to your business needs. We recognise that every business has unique data privacy challenges, and we use our deep understanding of international and domestic regulations to provide you with the most effective and robust legal strategies. JSA provides advice on highly sophisticated data management, data security and privacy issues. Our depth of experience gives our clients the crucial advantage of consistent and comprehensive, yet practical advice. Our Technology Law Practice group has successfully worked with several multinational organisations for the structuring and roll-out of privacy and information-security programs. We have carried out audit and risk assessments, customised global privacy and information management policies, helped create international data transfer strategies, structure and negotiate complex international data transfer agreements.

This Prism has been prepared by:

Akshaya Suresh
Partner

Drishya A. Kamath
Associate

18 Practices and
25 Ranked Lawyers

7 Ranked Practices,
16 Ranked Lawyers

Elite – Band 1 -
Corporate/ M&A Practice
---
3 Band 1 Practices
---
4 Band 1 Lawyers,1 Eminent Practitioner

12 Practices and
42 Ranked Partners
IFLR1000 APAC Rankings 2023

Banking & Finance Team of the Year

Fintech Team of the Year

Restructuring & Insolvency Team of the Year

14 Practices and
38 Ranked Lawyers

20 Practices and
22 Ranked Lawyers

Ranked Among Top 5 Law Firms in India for ESG Practice

Recognised in World's 100 best competition practices of 2024

Among Top 7 Best Overall Law Firms in India and
11 Ranked Practices
---
11 winning Deals in IBLJ Deals of the Year
---
12 A List Lawyers in IBLJ Top 100 Lawyer List

Asia M&A Ranking 2024 – Tier 1

Employer of Choice 2024

Energy and Resources Law Firm of the Year 2024

Litigation Law Firm of the Year 2024

Energy - Law Firm of the Year (APAC)

7 Practices and
3 Ranked Lawyers

For more details, please contact km@jsalaw.com

jsa
advocates & solicitors

Ahmedabad | Bengaluru | Chennai | Gurugram | Hyderabad | Mumbai | New Delhi