

Section 27 DPDPA

Powers and functions of Board. 27.(1) The Board shall exercise and perform the following powers and functions, namely:—

(a) on receipt of an intimation of personal data breach under sub-section (6) of section 8, to direct any urgent remedial or mitigation measures in the event of a personal data breach, and to inquire into such personal data breach and impose penalty as provided in this Act; (b) on a complaint made by a Data Principal in respect of a personal data breach or a breach in observance by a Data Fiduciary of its obligations in relation to her personal data or the exercise of her rights under the provisions of this Act, or on a reference made to it by the Central Government or a State Government, or in compliance of the directions of any court, to inquire into such breach and impose penalty as provided in this Act; (c) on a complaint made by a Data Principal in respect of a breach in observance by a Consent Manager of its obligations in relation to her personal data, to inquire into such breach and impose penalty as provided in this Act; (d) on receipt of an intimation of breach of any condition of registration of a Consent Manager, to inquire into such breach and impose penalty as provided in this Act; and

(e) on a reference made by the Central Government in respect of the breach in observance of the provisions of sub-section (2) of section 37 by an intermediary, to inquire into such breach and impose penalty as provided in this Act. (2) The Board may, for the effective discharge of its functions under the provisions of this Act, after giving the person concerned an opportunity of being heard and after recording reasons in writing, issue such directions as it may consider necessary to such person, who shall be bound to comply with the same. (3) The Board may, on a representation made to it by a person affected by a direction issued under sub-section (1) or sub-section

[recovered from the vector store — section27.html p.2]

(2), or on a reference made by the Central Government, modify, suspend, withdraw or cancel such direction and, while doing so, impose such conditions as it may deem fit, subject to which the modification, suspension, withdrawal or cancellation shall have effect.

Applicable DPDP Rule 2025

Rule 19: Functioning of Board as Digital Office

← Section 26 DPDPA

Section 28 DPDPA →

DPDPA

Table of contents

Report error

Your message

x

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

Legal Interpretation of the

Section 27 of the Digital Personal Data Protection Act, 2023 (DPDPA)

Statutory Provision and Purpose

Provision: Section 27 of the Digital Personal Data Protection Act, 2023 states:

"Powers and functions of Board."

While the section title is concise, its implications are significant within the framework of the DPDPA 2023. This provision delineates the comprehensive powers and functions vested in the Data Protection Board (hereinafter referred to as "the Board"). By outlining these powers and functions, the Act ensures that the Board possesses the necessary authority to effectively oversee, enforce, and promote data protection standards across various sectors. Purpose:

The primary objective of Section 27 is to empower the Board with the requisite authority to perform its duties efficiently and effectively. By defining the Board's powers and functions, the Act aims to:

Ensure Compliance: Monitor and enforce adherence to data protection laws among data fiduciaries.

Facilitate Enforcement: Implement corrective measures and impose penalties for non-compliance. Promote

Best Practices: Advocate for robust data protection measures and standards.

[recovered from the vector store — section27.html p.3]

ild confidence among individuals that their personal data is being safeguarded effectively.

Legal Interpretation

1. Nature of the Provision

- Regulatory Authority: Section 27 establishes the Board as a powerful regulatory body with broad authority to oversee and enforce data protection norms.

- Comprehensive Powers: The provision ensures that the Board is not limited to advisory roles but is also empowered to take decisive actions against violations.

2. Core Powers of the Board

Investigative Powers:

Authority to summon witnesses, request documents, and conduct on-site inspections.

Ability to gather and analyze evidence related to data protection breaches.

Advisory Functions:

Provide guidance and recommendations to data fiduciaries on implementing effective data protection measures.

Develop and disseminate best practice frameworks for data management and security.

Enforcement Powers:

Impose penalties, fines, and sanctions on data fiduciaries found in violation of the Act.

Mandate corrective actions to rectify data protection lapses.

Policy Formulation:

Participate in the creation and revision of data protection policies and regulations.

Adapt policies to keep pace with technological advancements and emerging data privacy challenges.

Public Awareness and Education:

Conduct campaigns to educate the public and data fiduciaries about data protection rights and obligations.

Promote awareness of data privacy issues and the importance of safeguarding personal information.

3. Functions of the Board

Monitoring Compliance:

Regularly assess the compliance of data fiduciaries with the provisions of the DPDPA 2023.

Conduct audits and reviews to ensure adherence to data protection standards.

Handling Complaints:

Receive and investigate complaints from data principals regarding data protection violations.

Facilitate a fair and impartial hearing process for all parties involved.

Enforcing Penalties:

Impose fines and sanctions on

[recovered from the vector store — section27.html p.4]

entities that fail to comply with data protection requirements.

Ensure that penalties are proportionate to the severity of the violation.

Advising Stakeholders:

Offer expert advice to organizations on enhancing their data protection frameworks.

Assist in the development of privacy policies and data management practices.

Developing Guidelines:

Create and update guidelines to help data fiduciaries implement effective data protection measures.

Ensure that guidelines reflect current technological trends and data privacy challenges.

4. Enforcement Mechanisms

Penalties and Fines:

Monetary fines proportional to the nature and extent of the data protection violation.

Additional penalties for repeated or severe breaches.

Corrective Actions:

Mandate organizations to rectify data protection deficiencies.

Require the implementation of specific measures to prevent future violations.

Public Directives:

Issue directives to cease unauthorized data processing activities.

Order organizations to notify affected individuals about data breaches.

5. Oversight and Accountability

Internal Oversight:

The Board conducts regular internal audits to assess its own compliance and effectiveness.

Implements policies to ensure accountability within its operations.

External Oversight:

Subject to judicial review to ensure adherence to legal and constitutional standards.

Reports and findings may be reviewed by parliamentary committees to ensure transparency and accountability.

6. Integration with Other Provisions

Consistency with the Act:

Ensures that the Board's powers and functions align with other sections of the DPDPA 2023.

Supports the overarching objectives of data protection and privacy as stipulated in the Act.

Collaboration with Other Agencies:

Works in tandem with law enforcement agencies for cases involving criminal data breaches.

Partners with international data protection authorities to address cross-border data privacy issues.

[recovered from the vector store — section27.html p.5]

Equips the Board with sufficient powers to enforce compliance without overstepping its regulatory mandate.

Ensures that the Board's actions are proportionate and justified.

Implements checks and balances to prevent misuse of the Board's powers.

Establishes clear guidelines and protocols for the exercise of authority.

Maintains transparency in the Board's operations to foster public trust.

Ensures that the Board's actions are perceived as fair and just by all stakeholders.

Illustration 1: Enforcing Compliance Through Investigations

Scenario: **FinSecure Ltd.**, a financial services company, is suspected of mishandling customer data by failing to implement adequate security measures, leading to unauthorized access.

Affected customers file complaints with the Data Protection Board regarding data breaches.

The Board, exercising its investigative powers, summons FinSecure's Chief Data Officer and requests relevant documentation on data security protocols.

During the hearing, experts testify on the deficiencies in FinSecure's data protection measures. The Board deliberates and concludes that FinSecure violated data protection standards by not implementing adequate encryption and access controls.

The Board orders FinSecure to enhance its data security systems within six months and imposes a penalty of ₹4 lakhs.

FinSecure is also directed to notify all affected customers about the data breach.

The Board schedules follow-up audits to ensure that FinSecure complies with the directives.

FinSecure appeals the penalty, arguing that the breach was due to unforeseen technical issues, and seeks a reduction of the fine from the Appellate Tribunal as per Section 29.

[recovered from the vector store — section27.html p.6]

Scenario: ****HealthCarePlus****, a hospital chain, seeks guidance on improving its data protection policies to better safeguard patient information in light of increasing cyber threats.

HealthCarePlus submits a request to the Board for advice on enhancing data protection measures.

The Board conducts a thorough assessment of HealthCarePlus's existing data protection policies.

Experts within the Board recommend the implementation of advanced encryption techniques, regular security audits, and comprehensive employee training programs.

The Board formalizes its recommendations in a detailed advisory report and shares it with HealthCarePlus.

HealthCarePlus implements the recommended measures and informs the Board of the changes.

The Board monitors the implementation through periodic reviews to ensure adherence to the best practices.

With enhanced data protection measures, HealthCarePlus significantly reduces the risk of data breaches, thereby improving patient trust and compliance with the DPDPA 2023.

Illustration 3: Policy Formulation in Response to Emerging Technologies

Scenario: The rise of blockchain technology presents new challenges for data protection. The Board is tasked with formulating guidelines to address data privacy concerns related to blockchain applications.

The Board recognizes that existing data protection policies may not adequately cover the nuances of blockchain technology.

Experts within the Board research the implications of blockchain on data privacy, focusing on immutability, decentralization, and data transparency.

The Board holds consultations with blockchain developers, data security experts, legal professionals, and consumer rights groups to gather

[recovered from the vector store — section27.html p.7]

diverse perspectives. Drafting Guidelines:

Based on the research and consultations, the Board drafts comprehensive guidelines that address data minimization, consent mechanisms, and data anonymization in blockchain applications. Policy Approval and Publication:

The Board reviews and approves the drafted guidelines, which are then published for public reference and implementation by relevant stakeholders. Monitoring Implementation:

The Board monitors how blockchain applications adhere to the new guidelines, conducting audits and providing further advisory support as needed. Continuous Review:

As blockchain technology evolves, the Board periodically reviews and updates the guidelines to ensure they remain relevant and effective. Illustration 4: Public Awareness Campaigns

Scenario: To combat increasing data privacy concerns, the Board initiates a public awareness campaign aimed at educating individuals and organizations about data protection rights and obligations.

Application of Section 27:

Planning the Campaign:

The Board outlines the objectives, target audience, and key messages for the awareness campaign.

Developing Educational Materials:

Creation of brochures, infographics, webinars, and online resources that explain data protection principles and best practices. Launching the Campaign:

The Board partners with media outlets, educational institutions, and industry associations to disseminate the educational materials. Engaging the Public:

Organizing workshops and seminars to engage with the public and answer questions related to data privacy. Evaluating Impact:

The Board conducts surveys and feedback sessions to assess the effectiveness of the campaign and identify areas for improvement. Continuous Education:

Maintaining an ongoing education initiative to keep the public informed about new data protection developments and emerging privacy concerns. Conclusion

Section 27 of the Digital Personal Data Protection Act, 2023 grants the Data Prot

[recovered from the vector store — section27.html p.8]

ection Board comprehensive powers and defines its multifaceted functions to ensure effective oversight and enforcement of data protection norms. By empowering the Board with investigative, advisory, enforcement, and policy-formulation capabilities, the Act ensures that data protection standards are upheld across various sectors, fostering a secure and trustworthy digital environment.

Comprehensive Authority: The Board is equipped with broad powers to investigate, enforce, and guide data protection practices, ensuring robust oversight.

Enforcement and Corrective Actions: Empowering the Board to impose penalties and mandate corrective measures enhances compliance among data fiduciaries.

Advisory and Policy Formulation: The Board's role in advising organizations and shaping data protection policies ensures that best practices are continuously promoted and updated.

Transparency and Accountability: Structured procedures and transparent operations foster public trust and ensure the Board's accountability in its regulatory functions.

Public Engagement: Initiatives like public hearings and awareness campaigns engage stakeholders and the general public, promoting a culture of data privacy and protection.

Integration with Broader Framework: Aligning the Board's powers and functions with other provisions of the DPDPA creates a cohesive and effective data protection ecosystem.

Through the meticulous implementation of the powers and functions outlined in Section 27, the Data Protection Board can effectively safeguard personal data, address violations with due diligence, and adapt to the evolving landscape of data privacy challenges, thereby ensuring that the principles and objectives of the DPDPA 2023 are upheld consistently and effectively.