[recovered from the vector store — section28.html p.1]

Section 28 DPDPA

Procedure to be followed by Board. 28.(1) The Board shall function as an independent body and shall, as far as practicable, function as a digital office, with the receipt of complaints and the allocation, hearing and pronouncement of decisions in respect of the same being digital by design, and adopt such techno-legal measures as may be prescribed. (2) The Board may, on receipt of an intimation or complaint or reference or directions as referred to in sub-section (1) of section 27, take action in accordance with the provisions of this Act and the rules made thereunder. (3) The Board shall determine whether there are sufficient grounds to proceed with an inquiry. (4) In case the Board determines that there are insufficient grounds, it may, for reasons to be recorded in writing, close the proceedings. (5) In case the Board determines that there are sufficient grounds to proceed with inquiry, it may, for reasons to be recorded in writing, inquire into the affairs of any person for ascertaining whether such person is complying with or has complied with the provisions of this Act. (6) The Board shall conduct such inquiry following the principles of natural justice and shall record reasons for its actions during the course of such inquiry. (7) For the purposes of discharging its functions under this Act, the Board shall have the same powers as are vested in a civil court under the Code of Civil Procedure, 1908, in respect of matters relating to—

(a) summoning and enforcing the attendance of any person and examining her on oath; (b) receiving evidence of affidavit requiring the discovery and production of documents; (c) inspecting any data, book, document, register, books of account or any other document; and

(d) such other matters as may be prescribed. (8) The Board or its officers shall not prevent access to any premises or take into custody any eq

[recovered from the vector store — section28.html p.2]

uipment or any item that may adversely affect the day-to-day functioning of a person.

(9) The Board may require the services of any police officer or any officer of the Central Government or a State Government to assist it for the purposes of this section and it shall be the duty of every such officer to comply with such requisition.

(10) During the course of the inquiry, if the Board considers it necessary, it may for reasons to be recorded in writing, issue interim orders after giving the person concerned an opportunity of being heard.

(11) On completion of the inquiry and after giving the person concerned an opportunity of being heard, the Board may for reasons to be recorded in writing, either close the proceedings or proceed in accordance with section 33.

(12) At any stage after receipt of a complaint, if the Board is of the opinion that the complaint is false or frivolous, it may issue a warning or impose costs on the complainant.

Applicable DPDP Rule 2025

Rule 19: Functioning of Board as Digital Office

← Section 27 DPDPA
Section 29 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

Legal Interpretation of the

Section 28 of the Digital Personal Data Protection Act, 2023 (DPDPA)

Statutory Provision and Purpose

Provision: Section 28 of the Digital Personal Data Protection Act, 2023 states:

"Procedure to be followed by Board."

While the section title is succinct, its implications are substantial within the framework of the DPDPA 2023. This provision outlines the specific procedures and protocols that the Data Protection Board (hereinafter referred to as "the Board") must adhere to when performing its functions. These functions may include handling complaints, conducting investigations

[recovered from the vector store — section28.html p.3]

, issuing directives, and imposing penalties related to data protection violations.

Purpose:

The primary objective of Section 28 is to ensure that the Board operates in a structured, transparent, and accountable manner. By delineating clear procedures, the Act aims to:

Promote Consistency: Ensure uniformity in the Board's decision-making processes.

Enhance Transparency: Provide clear guidelines on how the Board conducts its duties, thereby fostering public trust.

Ensure Accountability: Establish mechanisms for the Board to be accountable in its actions and decisions.

Facilitate Efficiency: Streamline processes to enable the Board to address data protection issues promptly and effectively.

Protect Rights: Safeguard the rights of data principals (individuals whose data is being processed) and data fiduciaries (entities processing data) by ensuring fair and just procedures.

Legal Interpretation
1. Nature of the Provision

- Operational Framework: Section 28 serves as an operational blueprint for the Board, detailing the procedural aspects that govern its activities.

- Regulatory Compliance: It ensures that the Board's actions are in compliance with the overarching principles and objectives of the DPDPA 2023.

2. Scope of Procedures

The procedures outlined in Section 28 likely encompass the following areas:

Complaint Handling:

Intake Process: Steps for receiving and acknowledging complaints from data principals or data fiduciaries.

Initial Assessment: Criteria for determining the validity and urgency of complaints.

Investigation Protocols:

Evidence Gathering: Methods for collecting and preserving evidence related to data protection violations.

Interviews and Hearings: Procedures for conducting interviews with involved parties and holding hearings.

Decision-Making Processes:

Deliberation Mechanisms: Guidelines for how the Board deliberates on cases, including quorum requirements and voting procedures.

Issuance o

[recovered from the vector store — section28.html p.4]

f Orders: Steps for drafting, reviewing, and issuing binding orders or directives.

Imposition of Penalties:

Penalty Assessment: Criteria and scales for determining appropriate penalties based on the severity of violations.

Appeal Processes: Procedures for parties to appeal Board decisions, ensuring fairness and due process.

Record-Keeping and Reporting:

Documentation Standards: Requirements for maintaining accurate and comprehensive records of all proceedings and decisions.

Public Reporting: Guidelines for reporting statistics, trends, and outcomes to the public to ensure transparency.

3. Authority and Powers of the Board

Investigative Powers: Authority to summon witnesses, demand documents, and conduct on-site inspections.

Advisory Role: Providing recommendations to data fiduciaries on best practices for data protection.

Enforcement Actions: Ability to enforce compliance through directives, penalties, and other remedial measures.

4. Procedural Fairness and Due Process

Right to be Heard: Ensuring that both data principals and fiduciaries have the opportunity to present their cases.

Impartiality: Procedures to prevent conflicts of interest and ensure that Board members act without bias.

Timeliness: Establishing timelines for each stage of the procedure to prevent undue delays.

5. Checks and Balances

Internal Oversight: Mechanisms within the Board to review and audit its own processes for compliance and effectiveness.

External Oversight: Possible avenues for judicial review or parliamentary scrutiny to ensure the Board operates within its statutory mandate.

6. Integration with Other Provisions

Consistency with Other Sections: Ensuring that the procedures align with other sections of the DPDPA 2023, such as those outlining the Board's composition, powers, and responsibilities.

Interagency Coordination: Guidelines for collaborating with other regulatory bodies or law enforcement agencies when handling complex data protection cases.

[recovered from the vector store — section28.html p.5]

- Flexibility vs. Rigidity: Balancing the need for structured procedures with the flexibility to adapt to unique or evolving data protection challenges.

- Preventing Misuse: Establishing safeguards to prevent the Board from overstepping its authority or being used as a tool for harassment or undue penalties.

- Public Trust: Ensuring that procedural guidelines enhance public confidence in the Board's ability to protect data rights effectively.

Illustration 1: Handling a Complaint from a Data Principal

Scenario: Ms. Anjali, a citizen, discovers that RetailStoreX, an e-commerce platform, has been sharing her personal data with third-party marketers without her explicit consent. Feeling aggrieved, she decides to file a complaint with the Data Protection Board.

Ms. Anjali submits her complaint through the Board's official portal.

The Board acknowledges receipt of the complaint within three business days.

The Board reviews the complaint to determine its validity and the urgency of the matter.

Given the nature of the violation, the Board prioritizes the case for immediate investigation.
The Board assigns an investigator to gather evidence, including consent forms, data sharing agreements, and correspondence between RetailStoreX and third-party marketers.

Interviews are conducted with RetailStoreX's data protection officer and the third-party marketers involved.

The Board convenes a meeting with a quorum of at least three members to deliberate on the findings.

After reviewing the evidence, the Board concludes that RetailStoreX violated data protection norms by sharing Ms. Anjali's data without consent.

The Board orders RetailStoreX to cease unauthorized data sharing practices and imposes a penalty of ₹2 lakhs for the violation.

[recovered from the vector store — section28.html p.6]

ed to inform all affected customers about the data sharing breach.

RetailStoreX, believing the penalty to be excessive, decides to appeal the Board's decision to the Appellate Tribunal as per Section 29.

Illustration 2: Board's Investigation into a Data Breach Incident

Scenario: HealthCarePlus, a hospital chain, experiences a data breach resulting in unauthorized access to patient records. The incident raises concerns about the hospital's data security measures.

Several patients report unauthorized access to their medical records to the Board.

The Board aggregates these reports and initiates an investigation.

The Board deploys a team to conduct a thorough investigation, including technical assessments of HealthCarePlus's data security infrastructure.

Experts examine logs, security protocols, and employee access controls to identify the breach's cause.

Findings indicate that HealthCarePlus failed to implement adequate encryption measures, leading to the data breach.

The Board discusses the severity of the negligence and its impact on patient privacy.

The Board mandates HealthCarePlus to upgrade its data encryption systems within three months.
A penalty of ₹5 lakhs is imposed for the breach and failure to protect sensitive personal data.

HealthCarePlus is required to submit monthly progress reports to the Board, detailing the implementation of the prescribed encryption measures.

The Board conducts periodic audits to ensure compliance.

HealthCarePlus disputes the penalty, arguing that the breach was due to unforeseen technical failures and not negligence.

The company appeals to the Appellate Tribunal under Section 29 for a reassessment of the penalty.

Illustration 3: Issuing Directives for Data Protection Policy Enhancement

Scenario: EduLearn, an online education platform, is observed

[recovered from the vector store — section28.html p.7]

by the Board to have outdated data protection policies that do not fully comply with the latest DPDPA standards.

The Board conducts routine audits and identifies discrepancies in EduLearn's data protection policies.

A formal notice is sent to EduLearn highlighting the areas of non-compliance.

EduLearn acknowledges the shortcomings and expresses willingness to enhance its data protection measures.

The Board evaluates EduLearn's commitment and the feasibility of the proposed enhancements.

A directive is formulated to guide EduLearn in updating its policies.

EduLearn is instructed to revise its data protection policies to incorporate robust consent mechanisms, data minimization principles, and regular employee training on data protection.

A timeline of six months is set for the implementation of these policies.

EduLearn must submit a comprehensive report detailing the updates made to its data protection policies.

The Board schedules a follow-up audit to verify compliance.

If EduLearn faces challenges in implementing the directives, it can seek an extension or modifications by appealing to the Appellate Tribunal.
Illustration 4: Enforcing Compliance with Data Localization Requirements

Scenario: GlobalTech, an international data fiduciary, processes personal data of Indian citizens but stores it on servers located outside India, potentially violating data localization mandates under the DPDPA.

The Board receives complaints from data principals about their data being stored overseas without proper safeguards.

An investigation is initiated to assess compliance with data localization requirements.

The Board reviews GlobalTech's data storage practices, data transfer agreements, and security measures implemented overseas.

[recovered from the vector store — section28.html p.8]

on-compliance with the specified data localization norms.

Decision-Making:

The Board deliberates on the extent of non-compliance and its implications for data privacy.

Considerations include the sensitivity of the data involved and the potential risks to data principals.

Issuance of Order:

GlobalTech is ordered to establish data storage facilities within India or ensure equivalent data protection standards overseas as specified by the DPDPA.

A penalty of ₹7 lakhs is imposed for the violation.

Monitoring and Reporting:

GlobalTech must provide bi-monthly updates on the progress of establishing compliant data storage solutions.

The Board conducts periodic checks to verify adherence to the order.

Appeal Process:

GlobalTech disputes the necessity of the penalty and the feasibility of immediate compliance.

The company appeals to the Appellate Tribunal seeking a revision of the order and penalty.

Conclusion
Section 28 of the Digital Personal Data Protection Act, 2023 establishes a critical procedural framework for the Data Protection Board, ensuring that its operations are systematic, transparent, and accountable. By delineating clear procedures for handling complaints, conducting investigations, making decisions, and enforcing orders, this provision enhances the efficacy and credibility of the Board's role in safeguarding data protection norms.

Key Highlights:

Structured Processes: The provision ensures that the Board follows a consistent and fair approach in addressing data protection issues.

Transparency and Accountability: Clear procedural guidelines promote transparency in the Board's actions and hold it accountable to the public and stakeholders.

Efficiency in Redressal: Streamlined procedures enable the Board to address complaints and enforce compliance promptly, reducing delays and enhancing trust in the data protection framework.

Protection of Rights: By ensuring fair and just procedures, Section 28 safeguards the rights of both data princi

[recovered from the vector store — section28.html p.9]

pals and fiduciaries, fostering a balanced and equitable data protection environment.

Integration with Broader Mechanisms: The procedural framework complements other provisions of the DPDPA, such as appeal mechanisms and voluntary undertakings, creating a holistic and robust data protection ecosystem.

Through the meticulous implementation of the procedures outlined in Section 28, the Data Protection Board can effectively uphold the principles and objectives of the DPDPA 2023, ensuring that data protection standards are maintained and that violations are addressed with due diligence and fairness.