

[recovered from the vector store — section36.html p.1]

Section 36 DPDPA

Power to call for information.

36. The Central Government may, for the purposes of this Act, require the Board and any Data Fiduciary or intermediary to furnish such information as it may call for.

Applicable DPDP Rule 2025

Rule 22: Calling for Information from Data Fiduciary or Intermediary

← Section 35 DPDPA

Section 37 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 36 of the Digital Personal Data Protection Act, 2023 (DPDPA)

Introduction

Section 36 of the Digital Personal Data Protection Act, 2023 (India) empowers the Data Protection Board to request and obtain information necessary for performing its duties. This provision ensures that the Board can access relevant data, documents, or explanations from Data Fiduciaries, Data Processors, or other concerned parties to evaluate compliance, investigate potential violations, and enforce the Act effectively.

Key Elements of Section 36

Section 36 grants the Data Protection Board the statutory right to demand information related to the processing of personal data. This can include technical documents, security protocols, policies, audit reports, or any other data necessary to assess compliance with the Act's provisions.

2. Scope of Information Requests

The Board's requests are not limited to Data Fiduciaries alone. Any entity involved in personal data handling—Data Processors, third parties, or others holding relevant details—may be required to furnish the requested information. This broad scope ensures no critical data remains inaccessible during an investigation or compliance check.

3. Purpose of the Information

The collected information aids the Board in:

[recovered from the vector store — section36.html p.2]

checks: Verifying adherence to data protection obligations (e.g., security measures, consent mechanisms).

Enforcement and Investigations: Gathering evidence in cases of suspected non-compliance, data breaches, or other violations.

Policy and Regulatory Oversight: Understanding industry practices, identifying systemic issues, and informing future guidance or regulations.

4. Legal Weight and Obligations to Comply

Once the Board issues a notice or request, the recipient is legally obliged to respond. Refusal, undue delay, or providing misleading information can lead to enforcement actions, including penalties. This legal enforceability ensures the Board's investigative powers are not undermined by non-cooperation.

5. Ensuring Due Process and Fairness

While Section 36 provides broad powers, the Board must exercise these powers lawfully and reasonably. The Act's procedural safeguards, including opportunities for representation, help prevent arbitrary or excessive demands.

Illustrations

1. Compliance Verification of a Social Media Platform

Scenario:

The Board receives complaints that a social media platform is not properly protecting user data or honoring erasure requests.

Application:

The Board issues a formal request for information about the platform's data retention policies, encryption standards, and records of how user deletion requests are handled. This information determines whether the platform complies with the Act's mandates.

2. Investigating a Suspected Data Breach at a Bank

Scenario:

A bank reports a suspected data breach involving customer account details.

Application:

The Board requests security audit reports, incident response plans, system access logs, and vendor contracts to assess if the bank failed to implement reasonable security safeguards.

3. Examining Industry-Wide Practices

Scenario:

The Board wants to understand how EdTech companies handle children's personal data.

Application:

It requests

[recovered from the vector store — section36.html p.3]

information from multiple EdTech providers about their age verification, parental consent methods, and targeted advertising policies. The Board can then identify common shortcomings and issue sector-wide guidance.

Legal Interpretation and Impact

Empowering the Board's Oversight Role:

Section 36 reinforces the Board's capability as an effective regulator. It can uncover hidden lapses and maintain accountability without relying solely on complaints or voluntary disclosures.

Deterrent Against Non-Compliance:

Knowing that the Board can scrutinize internal practices at any time encourages organizations to maintain stronger compliance measures proactively.

Facilitating Transparency and Trust:

Access to information ensures regulators can act transparently and effectively, boosting trust among consumers, businesses, and international stakeholders.

Conclusion

Section 36 of the DPDP Act, 2023 is a fundamental enforcement tool empowering the Data Protection Board to access crucial information needed for oversight. By compelling cooperation from Data Fiduciaries, Data Processors, and others, this provision enhances the Board's ability to detect non-compliance, foster accountability, and support a trustworthy digital ecosystem.

© 2024 Advocate (Dr.) Prashant Mali