

[recovered from the vector store — section37.html p.1]

Section 37 DPDPA

Power of Central Government to issue directions. 37. (1) The Central Government or any of its officers specially authorised by it in this behalf may, upon receipt of a reference in writing from the Board that—

a) intimates the imposition of monetary penalty by the Board on a Data Fiduciary in two or more instances; and
b) advises, in the interests of the general public, the blocking for access by the public to any information generated, transmitted, received, stored or hosted, in any computer resource that enables such Data Fiduciary to carry on any activity relating to offering of goods or services to Data Principals within the territory of India,

after giving an opportunity of being heard to that Data Fiduciary, on being satisfied that it is necessary or expedient so to do, in the interests of the general public, for reasons to be recorded in writing, by order, direct any agency of the Central Government or any intermediary to block for access by the public or cause to be blocked for access by the public any such information.

(2) Every intermediary who receives a direction issued under sub-section (1) shall be bound to comply with the same. (3) For the purposes of this section, the expressions “computer resource”, “information” and “intermediary” shall have the meanings respectively assigned to them in the Information Technology Act, 2000. ← Section 36 DPDPA

Section 38 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 37 of the Digital Personal Data Protection Act, 2023 (DPDPA)

Introduction

Section 37 of the Digital Personal Data Protection Act, 2023 (India) grants the Central Government the authority to issue directions to the Dat

[recovered from the vector store — section37.html p.2]

a Protection Board and other concerned parties. This provision ensures that the highest executive authority can guide the implementation of data protection laws, aligning enforcement and policy with broader national objectives, public interest, and good governance.

Key Elements of Section 37

1. Power to Issue Directions

The Central Government can issue directions to the Data Protection Board or any other entities tasked with executing the Act's provisions. These directions help ensure proper implementation, reinforce compliance, and clarify ambiguities that may arise during enforcement.

2. Binding Nature of Directions

When directions are issued, recipients must comply. The statutory backing of these directions ensures they carry legal weight, preventing interpretational disputes and promoting a consistent approach to data protection enforcement.

3. Alignment with Public Policy and National Interest

Section 37 acknowledges that data protection must consider national security, sovereignty, public order, and economic interests. By empowering the Central Government, the Act ensures data protection efforts remain harmonized with the country's overarching policy framework.

4. Scope of Directions

The directions may cover various matters, including:

Guidelines for handling sensitive personal data.

Prioritization of enforcement actions against systemic non-compliance.

Steps to harmonize DPDP Act enforcement with other laws or international norms.

Responses to emerging threats like large-scale cyber-attacks or global data breaches.

These directions are generally intended to serve the Act's objectives and the public interest.

5. Checks and Balances

While granting the government significant power, Section 37 does not allow it to override fundamental rights or the Act's core protective principles. Directions must remain lawful, and if they appear to conflict with constitutional provisions or the Act's spirit, they could face judicial scrutiny.

Illus

[recovered from the vector store — section37.html p.3]

1. Responding to a Major Data Breach Trend

Scenario:

A surge in cybersecurity breaches impacts multiple industries, endangering vast amounts of personal data.

Application:

The Central Government may direct the Data Protection Board to prioritize investigations into organizations with repeated breaches and adopt stricter technical standards. These directions ensure a unified, robust response to systemic threats.

2. Addressing Cross-Border Data Flows

Scenario:

Changes in global data transfer frameworks necessitate adjustments in India's approach.

Application:

The government could instruct the Board to issue guidelines for approving cross-border data transfers, ensuring they meet DPDP Act standards while considering trade partnerships and diplomatic relations.

3. Clarifying Interpretation of Certain Provisions

Scenario:

The Board faces uncertainty interpreting a specific provision regarding children's data.

Application:

The Central Government might clarify the approach to be adopted, ensuring uniform interpretation that protects children's interests and aligns with broader child welfare policies.

Legal Interpretation and Impact

Ensuring Cohesion and National Alignment:

Section 37 ensures data protection enforcement aligns with larger governance objectives. It fosters coherence and reduces enforcement fragmentation.

Preventing Enforcement Fragmentation:

Without this power, different enforcement bodies might diverge. Central government directions promote consistency, clarity, and predictability.

Limited by the Rule of Law:

Although broad, the government's power is not absolute. Unjustified or unconstitutional directions can be challenged in court.

Conclusion

Section 37 of the DPDP Act, 2023 is a crucial tool for guiding India's data protection ecosystem, allowing the Central Government to issue directions that shape enforcement priorities and interpretive stances. By balancing individual privacy with national interests, this p