[recovered from the vector store — section40.html p.1]

Section 40 DPDPA

Power to make rules. 40.1) The Central Government may, by notification, and subject to the condition of previous publication, make rules not inconsistent with the provisions of this Act, to carry out the purposes of this Act. (2) In particular and without prejudice to the generality of the foregoing power, such rules may provide for all or any of the following matters, namely:—

(a)the manner in which the notice given by the Data Fiduciary to a Data Principal shall inform her, under sub-section (1) of section 5; (b) the manner in which the notice given by the Data Fiduciary to a Data Principal shall inform her, under sub-section (2) of section 5; (c) the manner of accountability and the obligations of Consent Manager under sub-section (8) of section 6; (d) the manner of registration of Consent Manager and the conditions relating thereto, under sub-section (9) of section 6; (e) the subsidy, benefit, service, certificate, licence or permit for the provision or issuance of which, personal data may be processed under clause (b) of section 7; (f) the form and manner of intimation of personal data breach to the Board under sub-section (6) of section 8;
(g) the time period for the specified purpose to be deemed as no longer being served, under sub-section (8) of section 8; (h) the manner of publishing the business contact information of a Data Protection Officer under sub-section (9) of section 8; (i) the manner of obtaining verifiable consent under sub-section (1) of section 9; (j) the classes of Data Fiduciaries, the purposes of processing of personal data of a child and the conditions relating thereto, under sub-section (4) of section 9; (k) the other matters comprising the process of Data Protection Impact Assessment under sub-clause (i) of clause (c) of sub-section (2) of section 10; (l) the other measures that the Si

[recovered from the vector store — section40.html p.2]

gnificant Data Fiduciary shall undertake under sub-clause (iii) of clause (c) of sub-section (2) of section 10; (m) the manner in which a Data Principal shall make a request to the Data Fiduciary to obtain information and any other information related to the personal data of such Data Principal and its processing, under sub-section (1) of section 11; (n) the manner in which a Data Principal shall make a request to the Data Fiduciary for erasure of her personal data under sub-section (3) of section 12; (o) the period within which the Data Fiduciary shall respond to any grievances under sub-section (2) of section 13; (p) the manner of nomination of any other individual by the Data Principal under sub-section (1) of section 14; (q) the standards for processing the personal data for exemption under clause (b) of sub-section (2) of section 17; (r) the manner of appointment of the Chairperson and other Members of the Board under sub-section (2) of section 19; (s) the salary, allowances and other terms and conditions of services of the Chairperson and other Members of the Board under sub-section (1) of section 20;
(t) the manner of authentication of orders, directions and instruments under sub-section (1) of section 23; (u) the terms and conditions of appointment and service of officers and employees of the Board under section 24; (v) the techno-legal measures to be adopted by the Board under sub-section (1) of section 28; (w) the other matters under clause (d) of sub-section (7) of section 28; (x) the form, manner and fee for filing an appeal under sub-section (2) of section 29; (y) the procedure for dealing an appeal under sub-section (8) of section 29; (z) any other matter which is to be or may be prescribed or in respect of which provision is to be, or may be, made by rules. ← Section 39 DPDPA

[recovered from the vector store — section40.html p.3]

f 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 40 of the Digital Personal Data Protection Act, 2023 (DPDPA)

Introduction

Section 40 of the Digital Personal Data Protection Act, 2023 (India) grants the Central Government the authority to make rules to give effect to the Act's provisions. This power is a common legislative tool allowing the executive branch to detail procedures, standards, and requirements not explicitly defined in the Act. By enabling subordinate legislation,

Section 40 ensures that the regulatory framework can adapt over time, remaining responsive to technological changes, industry practices, and evolving data protection needs.

Key Elements of Section 40

1. Rule-Making by the Central Government
Section 40 authorizes the Central Government to formulate rules consistent with the Act's objectives. These rules serve as secondary legislation, providing operational details that elaborate on the Act's broad principles—ranging from technical security standards to procedures for handling complaints and enforcing compliance.

2. Consistency with the Act's Objectives

Any rules made under Section 40 must align with the DPDP Act's core principles and purposes. They cannot override or contradict the Act; instead, they must work within its framework, helping implement its provisions more effectively.

3. Flexibility and Responsiveness

The power to make rules allows the government to respond dynamically to new developments. As data protection challenges evolve—emerging cyber threats, new data processing technologies, shifting international standards—the government can update rules without passing new primary legislation. This ensures the regime stays current, practical, and effective.

[recovered from the vector store — section40.html p.4]

d Public Consultation

While Section 40 does not explicitly mandate consultation, it's common practice to invite stakeholder feedback on draft rules. Input from industry, civil society, and the public can help refine these rules, enhancing their legitimacy, clarity, and acceptance.

5. Scope of the Rules

The scope of rule-making is broad. Possible areas include:

Specifications for obtaining and recording consent.

Technical standards for reasonable security safeguards.

Timeframes and formats for breach notifications.

Criteria for classifying Significant Data Fiduciaries and extra duties for them.

Guidelines for protecting children's data.

Mechanisms ensuring compliant cross-border data transfers.

By placing these operational details in rules rather than in the Act, the law balances legislative certainty with administrative agility.

Illustrations
1. Defining Security Standards

Scenario:

The Act requires Data Fiduciaries to maintain "reasonable security safeguards" but does not specify details.

Application:

Under Section 40, the government might issue rules detailing acceptable encryption protocols, access control systems, audit frequencies, and vulnerability assessments. These rules give Data Fiduciaries clear benchmarks to meet.

2. Setting Breach Notification Timelines

Scenario:

The Act mandates timely breach notifications but does not specify exact deadlines.

Application:

Rules made under Section 40 could require Data Fiduciaries to notify the Board and affected individuals within 72 hours of discovering a breach. Such specificity ensures consistency and fairness.

3. Children's Data Protection Guidelines

Scenario:

The Act provides stronger protections for children's data but leaves practical details unspecified.

Application:

The government could frame rules defining methods for age verification, obtaining

verifiable parental consent, and implementing content moderation, ensuring a uniform and effective approach.

Legal Interpretat

[recovered from the vector store — section40.html p.5]

ion and Impact

Democratic Oversight and Accountability:

While the government has broad discretion, rules typically undergo parliamentary scrutiny and can be challenged in courts if they exceed the Act's scope or violate constitutional principles.

Ensuring Adaptability and Specialization:

Separating broad statutory principles from detailed mechanics ensures the law remains stable while rules adapt to evolving circumstances. This acknowledges that technology and best practices change rapidly.

Enhancing Compliance and Clarity:

Detailed rules help stakeholders understand their obligations. Clear guidelines reduce uncertainty, improve compliance, and foster trust in the data protection ecosystem.

Conclusion

Section 40 of the DPDP Act, 2023 empowers the Central Government to create detailed, responsive rules that operationalize the Act's data protection principles. By filling in the gaps left by the statute, these rules provide clarity, adaptability, and practical direction. This ensures effective implementation, strengthens data protection governance, and maintains a robust, future-ready regulatory environment.