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

Sl. No. | Breach of provisions of this Act or rules made thereunder | Penalty
1. | Breach in observing the obligation of Data Fiduciary to take reasonable security safeguards to prevent personal data breach under sub-section (5) of section 8. | May extend to two hundred and fifty crore rupees.
2. | Breach in observing the obligation to give the Board or affected Data Principal notice of a personal data breach under sub-section (6) of section 8. | May extend to two hundred crore rupees.
3. | Breach in observance of additional obligations in relation to children under section 9. | May extend to two hundred crore rupees.
4. | Breach in observance of additional obligations of Significant Data Fiduciary under section 10. | May extend to one hundred and fifty crore rupees.
5. | Breach in observance of the duties under section 15. | May extend to ten thousand rupees.
6. | Breach of any term of voluntary undertaking accepted by the Board under section 32. | Up to the extent applicable for the breach in respect of which the proceedings under section 28 were instituted.
7. | Breach of any other provision of this Act or the rules made thereunder. | May extend to fifty crore rupees.
Please keep in mind that this form is only for feedback and suggestions for improvement. Unfortunately, questions will not be answered.

Penalties in the Digital Personal Data Protection Act, 2023 (DPDPA)

The Schedule appended to the Digital Personal Data Protection Act, 2023 (India) outlines a structured penalty framework for different categories of non-compliance with the Act's provisions. Referenced under Section 33(1), it sets forth maximum penalties that may be imposed by the Data Protection Board for various types of breaches. By clearly delineating dis

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

tinct violations and their corresponding financial consequences, the Schedule provides transparency, deterrence, and guidance for Data Fiduciaries, Data Processors, and, in a limited instance, Data Principals.

Key Features of the Schedule

Tiered Penalty Structure: Specific categories of breaches each have a maximum monetary penalty cap, reflecting the severity and potential impact on individuals' data protection rights.

Focus on Data Fiduciaries: High penalties primarily target Data Fiduciaries to incentivize robust data protection measures, especially regarding children's data and breach notifications.

High Caps on Penalties: Some violations carry penalty limits in the hundreds of crores of rupees, illustrating the seriousness with which the law views data protection failures.

Breakdown of the Schedule's Provisions
1. Breach of Security Safeguards (Sub-section (5) of Section 8)

Obligation: Data Fiduciaries must implement reasonable safeguards to prevent personal data breaches.

Potential Penalty: Up to 250 crore rupees.

Interpretation: This highest-tier penalty underscores the importance of cybersecurity. Lax security that leads to breaches can result in extremely high fines, urging organizations to maintain rigorous security standards.

2. Failure to Notify Data Breaches (Sub-section (6) of Section 8)

Obligation: Data Fiduciaries must notify the Board and affected Data Principals of any personal data breach.

Potential Penalty: Up to 200 crore rupees.

Interpretation: Prompt and transparent breach reporting is crucial. Delays or secrecy can harm individuals and erode trust, hence the significant penalty ceiling.

3. Non-Compliance with Children's Data Obligations (Section 9)

Obligation: Strict additional obligations apply when processing children's personal data.

Potential Penalty: Up to 200 crore rupees.

Interpretation: Children are considered vulnerable data subjects. Heavy penalties sig

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

nal that their data must be handled with utmost care and responsibility.

4. Breach by a Significant Data Fiduciary (Section 10)

Obligation: Significant Data Fiduciaries must meet additional compliance measures (e.g., audits, risk assessments).

Potential Penalty: Up to 150 crore rupees.

Interpretation: Entities designated as Significant Data Fiduciaries play a systemic role in the data ecosystem. Large penalties reflect their heightened responsibility and the potential widespread impact of their non-compliance.

5. Breach of Duties under Section 15 (Duties of Data Principal)

Obligation: Data Principals must not misuse their rights or provide false information.

Potential Penalty: Up to 10,000 rupees.

Interpretation: Although less severe than corporate penalties, this ensures individuals also adhere to fair and honest behavior, maintaining integrity in the data ecosystem.

6. Breach of a Voluntary Undertaking (Section 32)

Obligation: If a Data Fiduciary fails to honor a voluntary undertaking, they face penalties corresponding to the original breach severity.

Potential Penalty: Up to the extent applicable for the underlying breach.

Interpretation: This encourages organizations to keep their promises to rectify issues. Breaking a voluntary undertaking can reinstate penalties similar to the initial violation.

7. Breach of Any Other Provision of the Act or Rules

Potential Penalty: Up to 50 crore rupees.

Interpretation: A catch-all category ensures no loopholes. Violations not specifically listed still carry meaningful penalties, maintaining overall compliance integrity.

Illustrations

1. Poor Cybersecurity Measures

An online payment firm fails to encrypt user financial data, leading to a breach. The penalty could approach 250 crore rupees, emphasizing robust data protection.

2. Delayed Breach Reporting

A social media platform discovers a hack but waits too long to inform users and the Board. It risks a penalty of up to 200 crore rupees, reinf

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

3. Mishandling Children’s Data

An EdTech company uses children’s data for targeted marketing, violating Section 9. It could face a penalty of up to 200 crore rupees, protecting minors from exploitation.

4. Neglect by Significant Data Fiduciary

A large tech company designated as Significant Data Fiduciary fails mandatory audits. Penalties up to 150 crore rupees highlight the gravity of non-compliance for high-impact organizations.
5. Data Principal Misconduct

An individual repeatedly submits false data to cheat a rewards system. A fine up to 10,000 rupees ensures even Data Principals follow rules.

Legal Interpretation and Impact

Enforcement and Deterrence: Large penalty caps strongly deter non-compliance, encouraging better security, compliance programs, and accountability.

Global Comparisons and Confidence: High penalties align India’s standards with global data protection regimes, reassuring foreign investors and stakeholders.

Flexibility for the Data Protection Board: Maximum limits allow the Board to adjust penalties based on breach severity, harm caused, and mitigating factors.

Conclusion

The Schedule under the DPDP Act, 2023 is a pivotal enforcement tool, aligning compliance expectations with strong deterrents. By associating each violation with a distinct penalty cap, it guides entities and individuals to uphold the highest standards of data protection. As India’s digital ecosystem evolves, these structured penalties ensure all parties remain alert and accountable, ultimately safeguarding Data Principals’ rights and interests.

© 2024 Advocate (Dr.) Prashant Mali