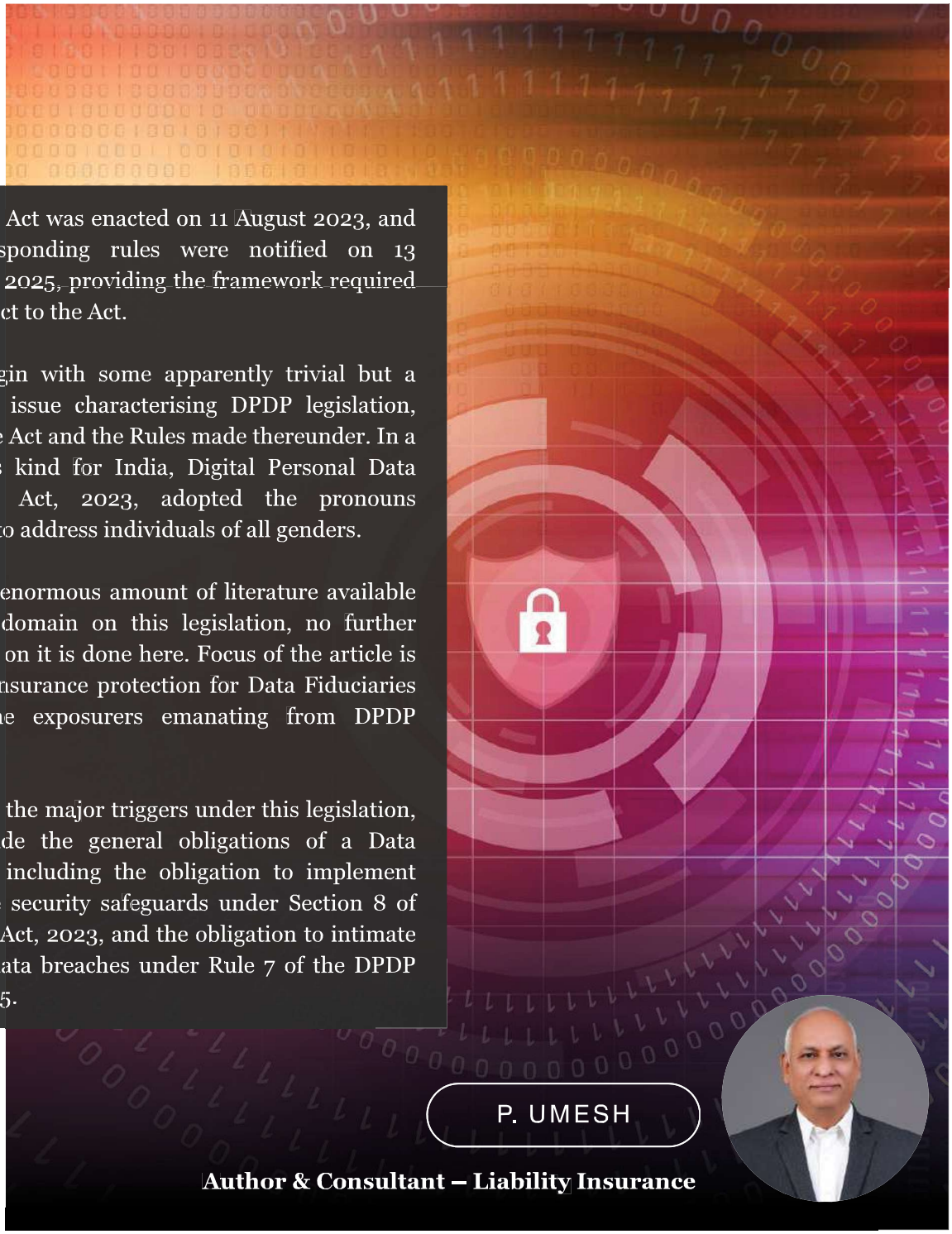
INDIA: DIGITAL PERSONAL DATA PROTECTION (DPDP) ACT / RULES - CYBER INSURANCE COVERAGE



The DPDP Act was enacted on 11 August 2023, and the corresponding rules were notified on 13 November 2025, providing the framework required to give effect to the Act.

Let us begin with some apparently trivial but a significant issue characterising DPDP legislation, namely the Act and the Rules made thereunder. In a first of its kind for India, Digital Personal Data Protection Act, 2023, adopted the pronouns "she/her" to address individuals of all genders.

Given the enormous amount of literature available in public domain on this legislation, no further discussion on it is done here. Focus of the article is on cyber insurance protection for Data Fiduciaries against the exposurers emanating from DPDP legislation

As regards the major triggers under this legislation, they include the general obligations of a Data Fiduciary, including the obligation to implement reasonable security safeguards under Section 8 of the DPDP Act, 2023, and the obligation to intimate personal data breaches under Rule 7 of the DPDP Rules, 2025.

P. UMESH

Author & Consultant – Liability Insurance

Data Breaches – Consequences and Costs

Cost of Forensic study
It depends upon many factors like incident size, complexity, regulatory scrutiny, sensitivity of data breached, and the technology environment in which the organisation is working, etc. As a ballpark figure, a small or contained incident may cost around ₹5 lakh at the low end of the spectrum; while large breaches can run into crores.

Cost of Data Breach
The average cost of a data breach for Indian organizations is estimated to be around ₹22 crore. Data breach entails forensic study of the problems for detection and its resolution and many other costs.

Ransom Demands
Data breaches may also result in ransom demands. As per Sophos "The State of Ransomware in India 2025 Report" the median ransom payment is around US$481,636 in India.

Penalties
Section 33 of the DPDPA, 2023 deals with the imposition of penalties for any violation of its provisions. These are listed in the schedule to the Act. They vary depending upon the nature of breach. The maximum penalty of up to ₹ 250 Cr. is for Breach in observing the obligation of Data Fiduciary to take reasonable security safeguards to prevent personal data breach.

Risk Mitigation Measures – Cyber Insurance

To mitigate risk, organisations must combine robust contracting practices and rigorous Information Technology (IT) security with comprehensive insurance for financial resilience.

A comprehensive cyber insurance program, complemented by other necessary coverages, helps withstand losses resulting from DPDP exposures. Cyber insurance policy is designed to help protect businesses from the financial impact of wide range of costs and liabilities resulting from cyber incidents.

It may be noted that unlike other similar legislations like General Data Protection Regulation (GDPR), there is no provision under DPDP legislation for payment of compensation to data principals whose personal data has been breached, even though there was a recommendation (Recommendation no. 73) by the Joint Parliamentary Committee on this subject. However, alternative remedies under Consumer Protection Act, 2019 and Information Technology Act, 2000 and civil suits for negligence continue to be available. So, the risk of claims for compensation remains.

The key takeaway is that while exposure to claims for compensation may not be significant, other consequences—such as breach notification costs, forensic expenses, substantial penalties, and potential business interruption—remain consequential.

Cyber insurance coverage in the context of DPDP legislation is expected to include, at a minimum, the following:

Forensic costs, Legal costs, Incidence response/ Notification/PR costs, and others for breaches including improper data collection, consent failure, misuse, wrongful disclosure, or theft of data and credit monitoring costs etc.
Regulatory interventions – Inquiry, Fines and Penalties
Ransomware, extortion, system, and data restoration costs etc.
Liability - Awards and Settlements including defence costs

For cyber insurance providers, penalties would be a matter of concern if they have covered penalties and those are admissible. For now, liability for compensation resulting from breach of personal data does not appear to pose any major challenge. The other exposures remain though. Another important aspect is that implementing Reasonable Security Safeguards is both a regulatory requirement and an insurance policy condition. For insurers, this is a favourable feature that is likely to reduce unfavourable claim ratios.

Cyber Insurance – Some Focus Areas

Insurance policy holders must meticulously review every detail of their insurance coverage. While not exhaustive, the following points deserve extra attention.

- **Broad Coverage:** There is no escape for Data Fiduciary from facing consequences for breaches irrespective of their causation. Responsibility of Data Fiduciary is absolute. It is therefore necessary to have the broadest attainable coverage for all cyber-attacks, and operational failures with limited conduct exclusions. In a way it needs to be on the lines of all risks cover with specified exclusions. Coverage needs to be extended for third party failures also. All of this is necessary to effectively align the insurance coverage with the Data Fiduciary's absolute responsibility.

- **Fines and Penalties:** It is vital to seek explicit coverage instead leaving it for interpretations to a future date. Some insurers are beginning to offer coverage for data breach related to lawfully insurable fines and penalties.

- **Failure to Maintain Safeguards:** Insurers require adherence to agreed-upon safeguards and standards to manage risk effectively. However, these requirements should not become absolute conditions precedent for claim settlements. To prevent coverage from becoming illusory, any exclusion based on a breach of safeguards, procedures, or representations should ideally be limited to instances involving a material change in risk or a direct causal link to the loss, ensuring that claims are not unfairly denied over technicalities or unrelated lapses.

- **Wrongful Collection of Data:** It is preferable to have explicit coverage for claims attributable to the allegation of wrongful collection of data.

- **Artificial Intelligence (AI) Exclusions:** AI being ubiquitous, it is necessary to ensure that there is no exclusion for AI exposures including chatbots

- **Absolute Exclusions:** These are designed to eliminate coverage entirely regardless of the circumstances, causation, or who was at fault. Ideally, all absolute exclusions are to be avoided.

- **Emergency Defence Costs:** Insurance policies generally require defence costs to be incurred with the prior approval of the insurer. Emergency defence cost provisions recognise the practical realities of a cyber event by allowing insureds to act swiftly as intimation of personal data breach has to be done without delay. This provides flexibility to incur the costs for which approval can be obtained post facto.

- **Cross-Border Data Transfer:** Coverage for exposures emanating from breach of provisions relating to transfer of personal data outside the territory of India needs to be explicitly built in.

- **Non-Cancellation Clause:** This eliminates the risk of midterm cancellation guaranteeing coverage till the end of policy period.

DPDP legislation has enhanced relevance of cyber insurance. However, it is important to recognize that the DPDP legislation is only one among several sources of exposures. The scope and purchase of cyber insurance should therefore be guided by a complete assessment of all relevant risks, not by a singular focus on data protection legislation.

Cyber insurance is just one of the many policies an organisation requires. Coverage under various insurance policies should be suitably structured based on a comprehensive risk assessment, so that, taken together, they meaningfully address the full spectrum of exposures effectively eliminating coverage gaps.