

ANTICIPATING COMPLIANCE WITH THE DIGITAL PERSONAL DATA PROTECTION ACT, 2023 ON DATA BREACHES IN INDIA

DECEMBER 2024

AUTHORED BY
RAKESH MAHESHWARI
DEDIPYAMAN SHUKLA



Executive Summary

Anticipating Compliance with the Digital Personal Data Protection Act, 2023 on Data Breaches in India

In August 2023, the Digital Personal Data Protection Act was passed into law, marking a paradigm shift in India's data protection and privacy standards. One of the key aspects of this legislation is the attempt to minimize the risks stemming from personal data breaches. The following two-part report examines compliance with cyber security incident reporting, specifically personal data breaches under the present Information Technology Act, 2000 to identify expectations for breach intimation under the newly introduced Digital Personal Data Protection Act, 2023. The report seeks to fulfil the following objectives:

- Analyse the record of data fiduciary breach reporting in India till date,
- Provide expectations for the degree of personal data breach reporting compliance under the Digital Personal Data Protection Act,
- Identify systemic gaps in both compliance and regulatory capacity with respect to the new data protection law's reporting framework,
- Make legislative and administrative recommendations to ensure the Data Protection Board is sufficiently empowered to enforce personal data breach reporting requirements and protect Indian data principals.

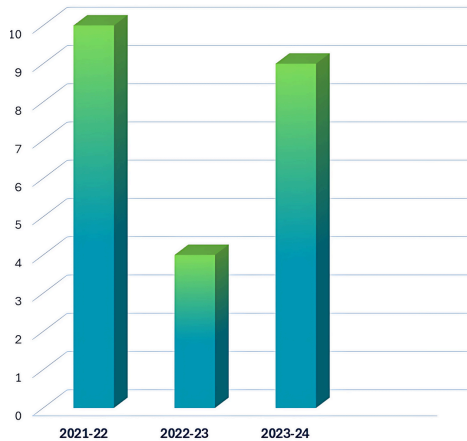
Part I of this report focuses on the existing compliance landscape and empirically analyses past trends in data fiduciary behaviour, while highlighting issues in regulation and compliance. **Part II** of this report assesses the new Digital Personal Data Protection Act's specific implementation challenges, in light of findings under Part I, and recommends measures for effective breach management from a regulatory capacity standpoint.

Findings

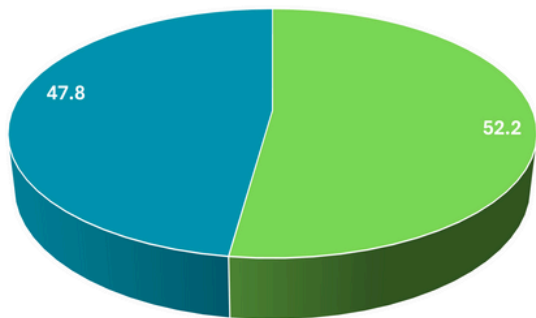
As per the findings in Part I of this report, India's incident reporting framework for data breaches, largely guided by the Information Technology Act and rules, appears to have been inconsistently applied, with limited accountability for body corporates in respect of their personal data handling oversight. Other key findings are listed below:

- Only 23 publicly disclosed instances of domestic data breaches were identified within the 3-year period studied (2021-24), where an excess of 1,00,000 personal data records were impacted.
- This averages out to approximately 7.67 substantial breaches each year. However, CERT-In reporting indicated an average of 37.8 such incidents per year for the 5 year period ending in March 2023.

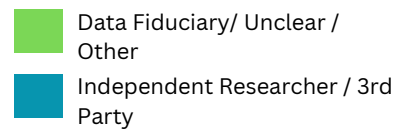
- Independent researchers were often found to reveal the existence of personal data breaches before data fiduciaries disclosed them (in at least 47.8% of studied cases), indicating a low rate of voluntary disclosure and poor levels of internal monitoring.
- Of the data fiduciaries (impacted by data breaches) that did publish privacy policies, only in 3 instances was the data of last modification to the applicable Indian privacy policy specified. Informing users about updates to the privacy policy may be considered a best practice and is also a legal requirement in some jurisdictions.



Chronological representation of the number of significant Indian personal data breaches identified for this report (by year)

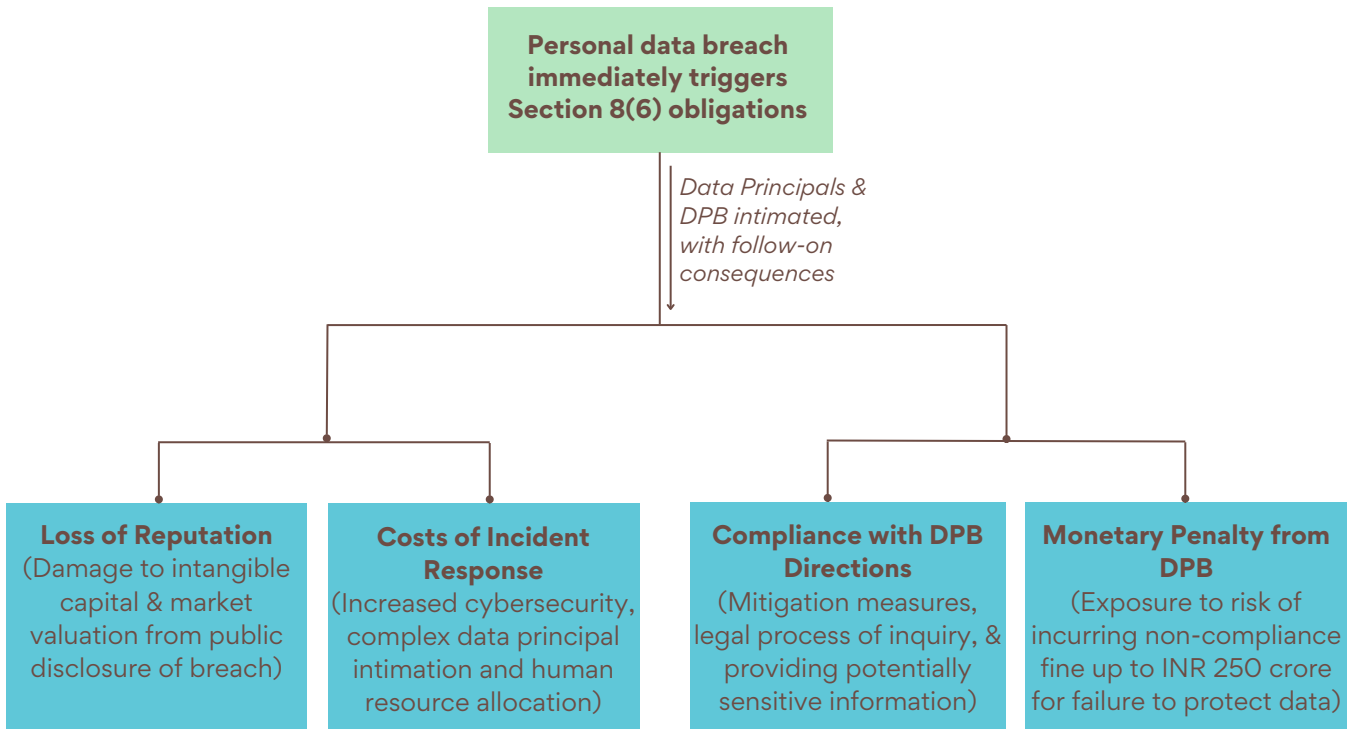


Proportion of personal data breaches identified by 3rd parties / independent researchers



- Repeated breaches were a common occurrence in 26.1% of studied instances (i.e. where the breach suffered by the data fiduciary was not an isolated incident).
- Findings also indicate that public sector data fiduciaries are more likely to face repeated instances of data breach as compared to private sector data fiduciaries (71.4% of public sector entities, as compared to 6.3% of private sector entities).
- Personal data breach disclosures from Indian entities did not provide any information on how the affected data principals may be placed at risk from the unauthorized access to their information.

Part I of this report also identifies multiple potential factors contributing to the low levels of personal data breach disclosure and reporting during the studied period, including strong regulatory and economic disincentive structures which discourage timely breach disclosures, and high-costs associated with remedial action, which larger entities, especially publicly listed companies, may find financially and reputationally risky. It is evident that personal data breaches have significant costs attached, which continue to rise each year. However, the analysis indicates that the disincentives against timely breach reporting by fiduciaries would be enhanced with the new Digital Personal Data Protection Act. This law includes a monetary penalty of up to INR 250 crore for the failure to take reasonable security safeguards to prevent personal data breaches.



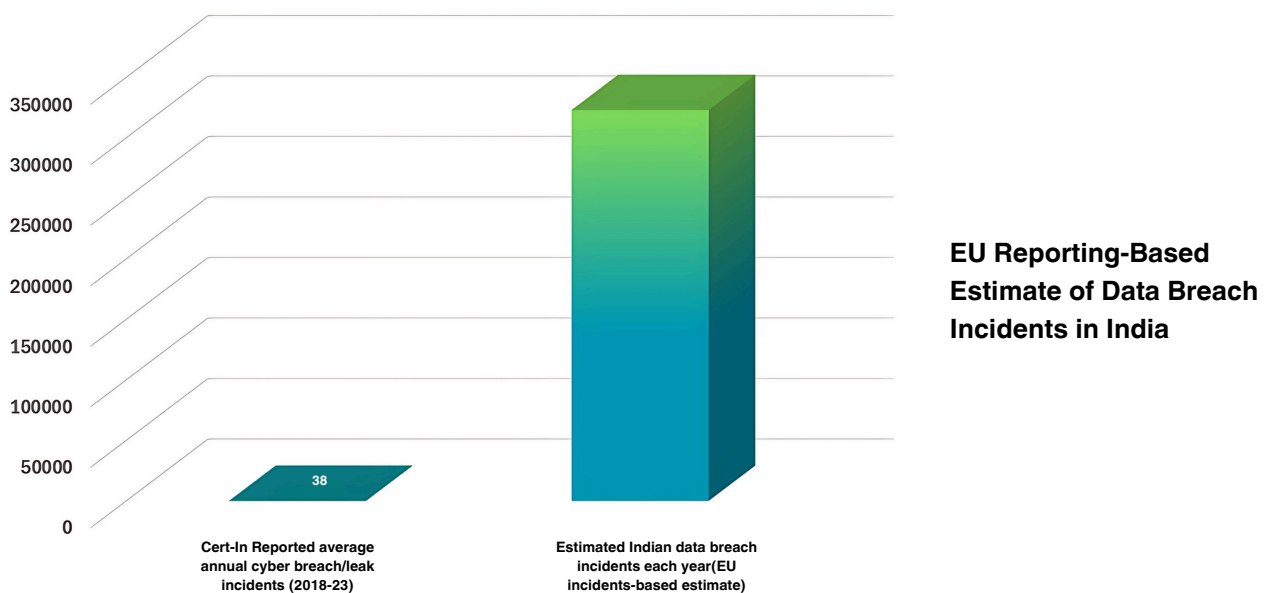
Disincentives & factors associated with triggering of notice/intimation DPDP Act obligations by Data Fiduciaries

The following key concerns are specifically noted:

- Limited availability of breach response information from fiduciaries in India,
- Inadequate compliance with current data protection standards,
- Independent third parties have played a crucial role in monitoring domestic personal data breaches,
- Operationalising breach reporting under DPDP Act presents several significant challenges for data fiduciaries, and
- There is need for data fiduciaries to prepare for the breach reporting compliances under the Act.


While the Digital Personal Data Protection Act seeks to address these gaps by mandating that all personal data breaches be reported to a new body, the Data Protection Board, as well as to affected data principals, this ambitious scope can potentially overwhelm both fiduciaries and regulators due to its broad definitions and low thresholds for reporting.

Further, while the difference in actual data breach reporting between the European Region and India is significant, the legal conditions for breach intimation in India actually encompass a larger range of situations requiring an intimation. Overcoming these challenges will also involve resolving any overlap of the Data Protection Board with existing government regulators and agencies. For example, such personal data breaches are also considered a cyber security incident.



The Data Protection Board will inherit significant regulatory responsibilities, particularly for mitigating breaches and enforcing compliance across diverse sectors. To improve levels of compliance with the new personal data breach reporting framework and rectify clearly identified regulatory gaps, Part II of the report elaborates on the need for specific structural and operational recommendations, including:

- **Mitigating Regulatory Overlaps of the Board** with the mandates of other regulators.
- **Developing Incentives for Breach Reporting** to counteract the observed reluctance of data fiduciaries in personal data breach reporting.
- **Augmenting the Board’s Capacity** with an initial staffing threshold of at least 250 qualified professionals.
- **Strengthening Breach Monitoring and Suo-Moto Powers** for the Board to support robust oversight (which may require an amendment in the law).
- **Potential Modifications to the Incident Reporting Format of CERT-In** to seek information on personal data breach reported to the Board.
- **Adopting a Tiered or Conditional Reporting System** to allow fiduciaries to report breaches based on their impact on data principals, reserving mandatory notifications for high-risk incidents (which may require an amendment in the law).



WHAT IS IGAP ?

The Indian Governance And Policy Project (IGAP) is an emerging think tank focused on driving growth, innovation, and development in India's digital landscape. Specializing in areas like AI, Data Protection, FinTech, and Sustainability, IGAP promotes evidence-based policymaking through interdisciplinary research. By working closely with industry bodies in the digital sector, IGAP provides valuable insights and supports informed decision-making. Core work streams include policy monitoring, knowledge dissemination, capacity development, dialogue and collaboration.

For more details visit: www.igap.in