

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

PART II

DECEMBER 2024

**AUTHORED BY**  
**RAKESH MAHESHWARI**  
**DEDIPYAMAN SHUKLA**



# INDEX

<b>I. Background</b>	<b>02</b>
<b>II. Legal Requirements and Mandate of DPB</b>	<b>04</b>
<b>III. Institutional Requirements for DPB in Relation to Data Breaches</b>	<b>06</b>
(a) Overcoming the large scope of personal data breaches under DPDP	06
(b) Lack of exceptions for intimation of DPB in case of personal data breach	09
(c) Resolving overlap with existing government regulators and agencies	11
(d) Size and capacity requirements for data protection regulators	14
<b>IV. Concluding Remarks and Suggestions</b>	<b>17</b>

# I. Background

---

The Digital Data Protection Act, 2023 (**DPDP Act**), enacted in August last year, is a watershed legislation in the history of data protection and citizen privacy protection for India. In Part I of this report, we delved into the kinds of additional responsibilities which the DPDP Act placed on data fiduciaries in the event of personal data breaches. Using recent data on entity breach response patterns, the authors were able to piece together a framework of data fiduciary behavior and breach reporting compliance expectations. Through this exercise some findings and compliance concerns were made clear. These are re-iterated briefly below.

(a) By the standards of the existing data privacy framework under the Information Technology Act, 2000 (**IT Act**) and the Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules, 2011 (**RSPDI Rules**), the data breach reporting framework envisioned under the DPDP Act is ambitious, and requires a large variety of incidents classified as ‘personal data breach’ under Section 2(u) to be intimated to the Data Protection Board (**DPB**), and each affected data principal. Ultimate responsibility for this compliance is placed on the data fiduciary.

(b) The breach reporting and response framework that is subsequently triggered exposes the targeted data fiduciary to a large number of regulatory and financial risks. These factors may potentially disincentivize the data fiduciary from timely reporting breaches to the DPB, which is otherwise necessary for compliance with the DPDP Act.

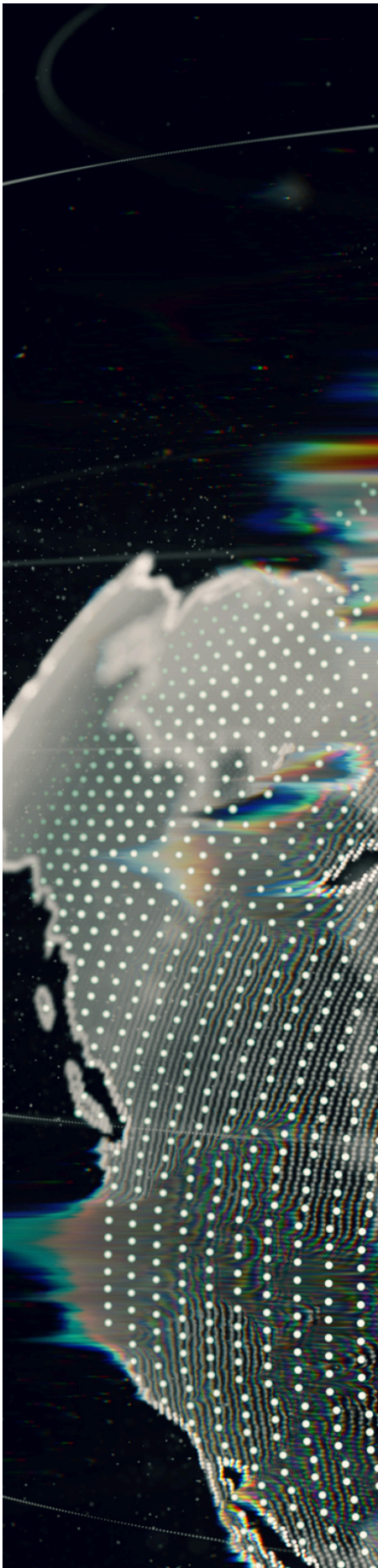
(c) These concerns were supported by the compliance related findings on data breaches under the IT Act regime, with a large proportion of personal data breaches being discovered and reported by independent researchers, as opposed to the relevant data fiduciary.

(d) The disincentives against reporting of a personal data breach are particularly significant for larger and publicly-listed entities which may see a considerable impact to their intangible capital and market valuations as a consequence of the reporting of a breach. This, coupled with largescale deployment of breach incident response resources by a fiduciary, and potential penalty up to INR 250 crore for the failure take reasonable security safeguards (INR 200 crore for not reporting breaches), may significantly add to the cost of breaches for entities under the DPDP Act. As of 2023, the average cost of a data breach in India was estimated at USD 2.18 million (approximately INR 18 crore).<sup>1</sup>

(e) Further, findings indicated that the evidence of remedial action being taken by private sector data fiduciaries was lesser, as compared to their public sector data counterparts, raising questions on the need for accountability mechanisms.

---

1. Cost of a Data Breach Report 2023, IBM Security, available at <https://www.ibm.com/reports/data-breach>



In the absence of any substantial breach detection capacity with individual data principals, it is apparent that enforcement of privacy rights of individuals in the context of breach related harms will remain a high-priority incumbent responsibility for the DPB. Consequently, the anticipated regulatory burden on the DPB upon the enforcement of the DPDP Act may be quite substantial by the historical standards for Indian regulatory institutions. Curbing errant data fiduciary behaviour will necessitate strict monitoring and active engagement from the DPB as the nodal body for privacy protection in India. While some aspects of breach incident monitoring may continue to be handled by Indian Computer Emergency Response Team (**CERT-In**), as discussed in Part I of this report, it retains a broader mandate to provide response to a host of other kinds of cyber incidents as well.<sup>2</sup> CERT-In's role across these incident types is also limited to information collection, monitoring and coordinating emergency measures, whereas the DPB is required to specifically enforce data protection standards and penalize entities failing to protect the privacy of data principals, after conducting inquiries and investigating personal data breaches.

Accounting for this legal mandate and the existing state of data protection measures in India, the following sections of Part II of this report delves into important considerations that may be taken into account by government administrators as well as the DPB, while formulating the administrative and regulatory structures necessary to carry out the mandate under the DPB.

# II. Legal Requirements and Mandate of DPB

---

## (a) Structure for DPB under the DPDP Act

Section 18 of the DPDP Act provides for the establishment of the DPB by the Central Government as a body corporate. The DPB is to have a Chairperson and Members who may hold office for a term of 2 years with the possibility of re-appointment. As for the expertise of the board, the DPDP Act requires that they possess special knowledge or practical experience in fields including:

- data governance,
- administration or implementation of laws related to social or consumer protection,
- dispute resolution,
- information and communication technology,
- digital economy, and
- law, regulation or techno-regulation.

However, the DPDP Act does not specify the size of the board or number of Members. This decision has been left to the Central Government to determine. To some degree, the size of the DPB will be a factor deciding in the administrative capacity of the DPB for discharge of its functions. In addition to the appointment Members, the DPB has been empowered to appoint such officers and employees as it may deem necessary for the efficient discharge of its functions under the provisions of this Act. Hence, a secretariat appointed through these powers is anticipated to handle the administrative and operational tasks to ensure the Board's functions are carried out effectively and efficiently.

Regarding the powers of the DPB to conduct an inquiry under Section 28 of the DPDP Act, the DPB is also empowered to requisition the services of any<sup>5</sup> police officer or any officer of the Central Government or a State Government for assistance. This, to some degree, may lessen the operational challenges for the DPB.

---

3. Section 20(2), DPDP Act

4. Section 24, DPDP Act

5. Section 28(9), DPDP Act



## (b) Operational challenges for DPB in relation to breach reporting based on previous trends

In light of our findings in Part I of this report, the Members and secretariat of the DPB will need to solve the following practical obstacles in the context of data breaches to make the implementation of the DPDP Act a successful endeavor:

- Lack of incentives to intimate data breaches under the DPDP Act, beyond merely avoiding final penalties,
- Difficulty of large-scale monitoring of 'personal data breaches' which have been broadly defined,
- Relatively high rates of data breach incidents within India with the potential for future increase,
- Lack of remedial action undertaken by fiduciaries post-detection, and
- Low compliance under the existing light-touch RSPDI Rules and IT Act framework for data privacy and cyber incident reporting

Addressing these challenges will require a thoughtfully structured and well-functioning DPB with an adequately staffed secretariat. As noted above, the operational structure for such a DPB is left open-ended by the DPDP Act. This provides the Central Government with the legal scope and flexibility build a DPB that responds to the unique requirements and challenges of personal data handling practices within India.

# III. Institutional Requirements for DPB in Relation to Data Breaches

---

## (a) Overcoming the large scope of personal data breaches under DPDP

The DPDP Act requires that all personal data breaches, regardless of their size be made subject to notice and intimation requirements. Even the disclosure of a single data principal's personal information qualifies under the breach definition as an incident requiring intimation.<sup>6</sup> This dramatically increases the scope of incidents requiring intervention from the DPB. Accurate incident numbers in the Indian context for data breaches would be difficult estimate.

Further, the definition of a data fiduciary under the DPDP Act should also be noted as including 'any person who ... determines the purpose and means of processing of personal data'.<sup>7</sup> This wide definition does not include any thresholds regarding the scale of personal data that is handled or processed by the entity. It is also evident that a wide and increasing range of activities involve digital personal data collection and processing within the country (such as e-commerce sales, health records processing, loan approvals, credit scoring, customer relationship management, welfare scheme implementation, ticket bookings, customer profiling etc.). As per this definition, many thousands, and potentially millions of entities may potentially qualify as data fiduciaries under the DPB's purview.

While it may be difficult to provide an accurate assessment of the precise number of potential breaches or fiduciaries, it cannot be doubted that the volume of entities and incidents requiring DPB involvement is extremely high due to the broad terminology employed for both breaches, as well as fiduciaries. Government disclosures on such incidents may shed further light on the existing monitoring infrastructure in place for such breaches.

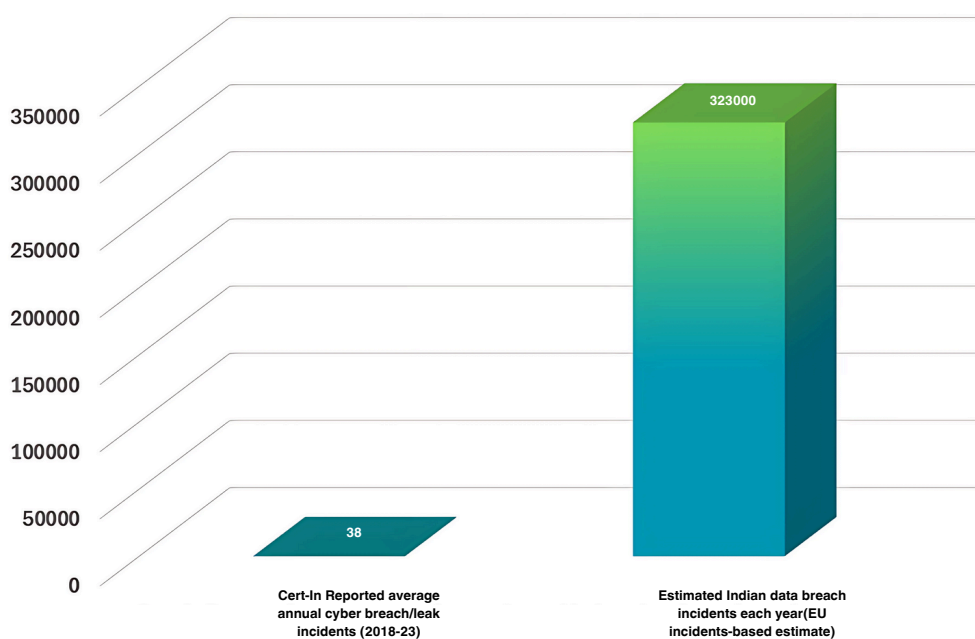
---

6. Under Section 2(u), a personal data breach means 'any unauthorised processing of personal data or accidental disclosure, acquisition, sharing, use, alteration, destruction or loss of access to personal data, that compromises the confidentiality, integrity or availability of personal data;'

7. Section 2(i), DPDP Act

As per publicly available information provided by the union Ministry of Electronics and Information Technology (**MEITY**) in 2023, a total of 189 cyber leak/breach incidents were reported to CERT-In. This results in an average of roughly 38 such incidents brought to the notice of CERT-In every year.<sup>8</sup> The disclosed information also included 22 government organization data leaks (approximately 7 per year) reported to CERT-In in the 3-year period from 2020 to the end of 2022.<sup>9</sup> However, regularly updated data regarding such incidents is not publicly distributed.

However, data such as this does not paint an accurate picture of the true extent of the issue within the country. In the United States, a country of 330 million citizens, more than 3,000 ‘data compromise’ incidents alone are estimated to have taken place.<sup>10</sup> In the European region, where the General Data Protection Regulation (**GDPR**) is in operation, more than an estimated 1,20,000 personal data breach notifications took place in 2023-24 approximately 500 million population, as per a recent report by DLA Piper. Based on these rough estimations, personal data breach incidents in India within the confines of its population may exceed 323,000 incidents each year, as illustrated below.



**Figure 1: EU Reporting-Based Estimate of Data Breach Incidents in India**

8. Unstarred Question No. 2418, Answered on 15 March 2023 (AU2418), available on Lok Sabha portal at <https://sansad.in/ls/questions/questions-and-answers>

9. Ibid

10. Annual number of data compromises and individuals impacted in the United States from 2005 to 2023, Statista, available at <https://www.statista.com/statistics/273550/data-breaches-recorded-in-the-united-states-by-number-of-breaches-and-records-exposed/>

11. DLA Piper GDPR fines and data breach survey: January 2024, available at <https://inform-new.dlapiper.com/125/9494/uploads/dla-piper-fines-and-data-breach-survey-2024.pdf?intlaContactId=xaFXI7DcEUOPIDUihE2MwA%3d%3d&intExternalSystemId=1>



For context, it should be noted that under the GDPR, a 'personal data breach' is defined as a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored or otherwise processed.<sup>12</sup> While this is not an exact parallel of the concept of personal data breach in India, GDPR's definition remains significantly broad and encompasses a wide range of data related incidents. Controllers under the GDPR are required to notify the supervisory authority of a breach where there is a likely risk to the rights and freedoms of natural persons.<sup>13</sup> While this reporting data provides extremely rough estimates and a high potential variance in actual data breach incidents, it also indicates the difference between cyber incident information available with CERT-In and the actual reality of data security in India. These estimates also support the finding of a high degree of non-compliance with incident reporting norms within the country. Assuming an increase compliance with the implementation of the DPDP Act, the number of reported incidents based on the Indian definition of breaches may increase substantially.

Further, it is anticipated that compliance struggles will be exacerbated by the lack of experience which entities may have with data protection processes. According to a recent survey conducted within India, 54% of data fiduciaries, even ones with larger user bases, do not have previous experience in implementing data protection laws in other countries.<sup>14</sup> While compliance preparedness may increase in the months following up enforcement, skill, awareness and organizational capacity issues endemic to the domestic economy will continue to pose a formidable challenge for implementing breach reporting obligations.

As compared to CERT-In, the DPB will have a far more significant role to play in the event of personal data breaches, broadly defined. Acknowledging the impact of these combined factors, robust monitoring and reporting options should be made available for adequate oversight in relation to data breaches.

---

12. Article 4(12), General Data Protection Regulation

13. Article 33(1), General Data Protection Regulation

14. Meghna Bal, An Empirical Evaluation of the Implementation Challenges of the Digital Personal Data Protection Act, 2023: Insights and Recommendations for the Way Forward. January 2024, Esya Centre, available at <https://www.esyacentre.org/documents/2024/1/17/an-empirical-evaluation-of-the-implementation-challenges-of-the-digital-personal-data-protection-act-2023-insights-and-recommendations-for-the-way-forward>



However, under the present DPDP Act, the DPB is provided with limited mechanisms to identify and act upon personal data breach incidents, i.e.

- Intimation by Data Fiduciary
- Complaint by Data Principals
- Reference from Government
- Directions from Court

In Part I of the report, the significant limitations of these mechanisms are elaborated. In brief, most of these potential reporting entities and individuals, other than the data fiduciary, suffer from information asymmetry preventing effective breach monitoring and awareness. Further, strong disincentives to the reporting of breaches plague data fiduciary entities themselves. Additionally, no suo-moto powers are provided to the DPB to inquire into reports of data breaches emanating from unaffected third-parties. The DPB is entirely reliant on the legally valid methods of intimation / reference / complaint mentioned above to exercise its powers under the DPDP Act. To improve the robustness of DPB oversight over data-breaches, it will be beneficial enable the DPB to take cognizance of alleged breaches on the basis of credible third-party reports from individuals or organizations which may otherwise not be linked with the breach incident.

Separately, the DPB should also be augmented with an in-house personal data breach monitoring capability. Due to the sensitive nature and potential non-disclosure of breaches, over-reliance on breach reporting may not be a suitable mechanism for the DPB to gauge compliance levels across fiduciaries or estimate the number of breaches taking place within India. Such monitoring capability would go a long way towards resolving data breach-related information asymmetries. Precedence for such monitoring and analysis of trends can be seen among data privacy regulators in other jurisdictions. For instance, the Information Commissioner's Office in the United Kingdom maintains and publishes 'data security incidents' on the periodical basis, which include individual details of incidents, as well as aggregated trends.<sup>15</sup> The DPB may also seek reliance on information collection from other government entities with similar capacities, as discussed subsequently.

## **(b) Lack of exceptions for intimation of DPB in case of personal data breach**

Interestingly, 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 from the data fiduciary once the DPDP Act is under enforcement.

---

15. Data security incident trends, UK Information Commissioner's Office, available at <https://ico.org.uk/action-weve-taken/data-security-incident-trends/>

The nuances of breach intimation processes in different jurisdictions with sophisticated IT infrastructure are illustrated in the table provided below.

**Table 1: Comparison of Breach Intimation Requirements Across Countries/Regions<sup>16</sup>**

	<b>Intimation to authority in event of a personal data breach</b>	<b>Intimation to each data principal in event of a personal data breach</b>
<b>India</b> (post-DPDP Act enforcement)	Mandatory	Mandatory
<b>European Union</b>	Conditional (Risk to rights and freedoms)	Conditional (High risk to rights and freedoms)
<b>United States</b>	Conditional (Dependent on category of breached information and State)	Conditional (Dependent on category of breached information and State)
<b>Singapore</b>	Conditional (Breach must be a 'notifiable breach')	Conditional (Breach must be a 'notifiable breach' and likely to result in significant harm to the individual)
<b>Japan</b>	Conditional (Breach could harm the rights and interests of individuals)	Conditional (Breach could harm the rights and interests of individuals)

As the above table indicates, a number of countries with sophisticated and well-developed IT-systems, as well as data protection regimes, provide for exceptions to the notification of personal data breaches on the grounds of significance to individuals. This raises multiple concerns in the context of the DPB under the DPDP Act, where no exceptions to intimation, of any kind are provided. In Part I, the significant cost and resource burden on data fiduciaries resulting from the stringent intimation requirements to data principals were noted. Apart from this issue, the lack of exceptions to DPB breach intimation are an equally concerning aspect worth noting. Based on the domestic breach estimations calculated above, the DPB would be at risk of inundation with many hundred-thousand breach intimations from fiduciaries, assuming a higher level of compliance with the law. Even where compliance remains relatively low, thousands of Indian breach instances may nonetheless be intimated to the DPB. This carries the potential to cripple the administrative resources available with the DPB in responding to each individual intimation. Further, resources of the DPB would be occupied with low-impact data breaches with limited consequences, in addition to those breaches warranting greater attention.

16. Table based on data collected from country specific laws, as well as the DLA Piper Data Protection Laws of the World database, available at <https://www.dlapiperdataprotection.com/>

## (c) Resolving overlap with existing government regulators and agencies

The establishment of the DPB under the DPDP Act introduces a specialized regulatory body for data protection in India. This creates a significant overlap with other sectoral regulators and statutory agencies, which include CERT-In, Reserve Bank of India (**RBI**), Securities and Exchange Board of India (**SEBI**), and the Department of Telecommunications (**DoT**), which also handle similar incident-types within their domains, among their other duties. While the DPB will focus exclusively on personal data breaches, sectoral regulators may often deal with personal data breaches as part of their broader regulatory mandates. The challenge lies in coordinating responses to breaches to avoid duplication of efforts and ensure comprehensive protection.

### CERT-In:

In Part I of this report, the regulatory overlaps between CERT-In and the DPB are discussed in detail. CERT-In's mandate extends to 'cyber security incidents' and 'cyber incidents' generally, which may also include personal data breaches. However, significant differences in mandate were also outlined, which included the responsibility of CERT-In to coordinate emergency measures, response activities and provide forecasts or alerts.

While the DPB does not replace the role of CERT-In, existing provisions result in a duplication of responsibilities on the part of data fiduciaries. Certain kinds of cyber security incidents, which include unauthorized access to data, breaches and leaks in the nature of a personal data breach, need to be mandatorily reported by service providers, body corporates, intermediaries and data centers affected by the incident to CERT-In for action to be taken.<sup>17</sup> Similarly, in the event of a personal data breach, the data fiduciary required to provide intimation of this breach to the DPB, and also to each data principal that is affected by the breach.<sup>18</sup> As both laws continue to be in force, it will be incumbent on entities to fulfill both reporting requirements immediately following a breach incident, bringing an additional angle to breach reporting compliance. This would also require the fiduciary to rapidly assess the nature of the cyber incident and potential involvement of personal data in a short timeframe to abide by legal obligations. A failure to do so would carry risks of a potential fine up to INR 200 crore under the DPDP Act or criminal sanctions under the IT Act.

It may be advantageous for regulators to consider streamlining of the personal data incident response framework. As personal data breaches form a component of the larger set of cyber incidents, some level of coordination on cyber incidents between the two organizations could drastically improve data breach monitoring. For instance, CERT-In may consider revising its incident reporting format to seek information on whether an incident, which is also a personal data breach, has been reported to DPB as per requisite timelines.

17. Rule 12(1)(a), CERT-In Rules; CERT-In Directions, available at [https://www.cert-in.org.in/PDF/CERT-In\\_Directions\\_70B\\_28.04.2022.pdf](https://www.cert-in.org.in/PDF/CERT-In_Directions_70B_28.04.2022.pdf)

18. Section 8(6), DPDP Act, 2023

## RBI:

The RBI is the central bank of India, established under the Reserve Bank of India Act, 1934 (**RBI Act**). Since its establishment, the RBI has become the principal regulator for various kinds of entities operating in the financial sector including banks, payment aggregators, non-banking financial companies etc. Financial institutions handle large amounts of sensitive personal and financial information as a part of their business operations. These include the bank account details and transaction histories of clients. As the sectoral regulator for these entities, the RBI retains certain powers relevant in the context of data security. This includes the power to seek information from financial institutions information relevant to their operations, and potentially, information regarding data security practices.<sup>19</sup> RBI's intervention in the aftermath of a data breach was observed in one of the studied instances of this report (i.e. Mobikwik data breach)<sup>20</sup>, where a forensic audit report was submitted to the regulator by the digital banking platform affected by the data breach. The RBI (Information Technology Governance, Risk, Controls and Assurance Practices) Directions, 2023<sup>21</sup> (**RBI Cyber Directions**) require regulated entities to have a robust IT governance framework including business continuity/ disaster recovery management, vulnerability assessment processes and information system audits. Further, the paragraph 27(d) of the RBI Cyber Directions requires regulated entities to proactively notify the RBI in addition to CERT-In regarding incidents, further increasing incident reporting compliances for some categories of fiduciaries.

Beyond this, the RBI has also integrated data protection obligations into its directions to regulated entities, which may overlap with provisions under the new DPDP Act. For instance, the RBI's Guidelines on Digital Lending 2022 require regulated entities to ensure that data collection via digital lending applications is 'need-based and with prior and explicit consent of the borrower' after providing notice of purpose.<sup>22</sup> Due to the wide definition of data fiduciaries under the DPDP Act, RBI regulated entities may also be subject to the notice and consent requirements under this law. This demonstrates that the regulatory overlaps between the RBI and DPB may extend beyond mere incident reporting to other aspects of data protection as well.

19. Section 45L, Reserve Bank of India Act, 1934 empowers the RBI to seek information from financial institutions relating to the conduct of their business.

20. The Hindu Businessline Report, 24 October 2021, available at <https://www.thehindubusinessline.com/money-and-banking/ipo-bound-unicorn-mobikwik-under-rbi-scanner-for-data-breach/article37153558.ece>

21. Master Direction on Information Technology Governance, Risk, Controls and Assurance Practices, 7 November 2023, available at [https://www.rbi.org.in/Scripts/BS\\_ViewMasDirections.aspx?id=12562#30](https://www.rbi.org.in/Scripts/BS_ViewMasDirections.aspx?id=12562#30)

22. Technology and Data Requirement, RBI Guidelines on Digital Lending, 2 September 2022, available at <https://www.rbi.org.in/Scripts/NotificationUser.aspx?Id=12382&Mode=0>

## SEBI:

The SEBI was established in 1988 and was given statutory powers through the Securities and Exchange Board of India Act, 1992. This provided SEBI with the necessary authority to regulate the securities market in India and protect the interests of investors. Information disclosure forms a key aspect of SEBI's regulatory mandate. SEBI's Cyber Security and Cyber Resilience framework of Stock Exchanges, Clearing Corporations and Depositories<sup>23</sup> require the reporting of cyber incidents to CERT-In, as well as the National Critical Information Infrastructure Protection Centre (an organization under the IT Act, 2000). Further, cyber-attacks, threats, incidents and breaches (which may entail personal data breach) experienced by some entities SEBI regulates, for instance Qualified Registrars to an Issue and Share Transfer Agents, are also to be reported to SEBI within 6 hours of detection, apart from incident reporting to CERT-In.<sup>24</sup>

Other aspects of SEBI's mandate are significant in terms of notifying the public of data breaches. The Securities and Exchange Board of India (Listing Obligations and Disclosure Requirements) Regulations, 2015 (**LODR 2015**) require publicly listed companies to make disclosures of any events or information which, in the opinion of the board of directors of the listed company, is material.<sup>25</sup> Material information would likely include disruptions of operations of the entity and events likely to affect conduct of business. Hence, personal data breaches may potentially breach this threshold of materiality.

## DoT:

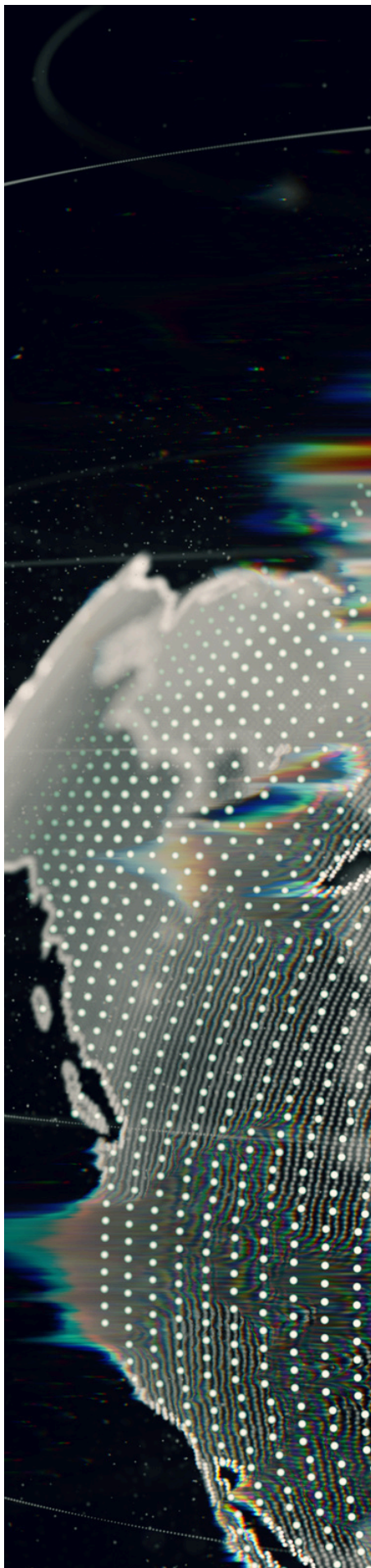
A department under the Ministry of Communications, the DoT oversees a range of functions including the licensing of telecommunication resources to service providers. Licenses in this regard are granted under a strict set of conditions relating to finance, technical operations and service area under what is referred to as the 'Unified License'.<sup>26</sup> However, the conditions under the Unified License also prescribe data and information security measures to be implemented by licensee service providers. This includes the introduction of network elements in line with contemporary Indian or International Security Standards (IT and IT related elements against ISO/IEC 15408 standards, Information Security Management System against ISO 27000 series Standards etc.), and creation of mechanisms for monitoring of all intrusions, attacks and frauds on technical facilities. Under these conditions, the licensee is also required to provide reports of all cyber intrusions to DoT. However, the recent Telecommunications Act, 2023 introduces a new framework of 'authorisation' for telecommunication services. This is yet to be fully implemented.

23. Cyber Security and Cyber Resilience framework of Stock Exchanges, Clearing Corporations and Depositories, Circular No.: CIR/MRD/CSC/148/2018, 7 December 2018, available at [https://www.sebi.gov.in/legal/circulars/dec-2018/cyber-security-and-cyber-resilience-framework-of-stock-exchanges-clearing-corporations-and-depositories\\_41244.html](https://www.sebi.gov.in/legal/circulars/dec-2018/cyber-security-and-cyber-resilience-framework-of-stock-exchanges-clearing-corporations-and-depositories_41244.html)

24. SEBI Circular No.: SEBI/HO/MIRSD/TPD/P/CIR/2022/96, 6 July 2022, available at <https://www.sebi.gov.in/legal/circulars/jul-2022/modification-in-cyber-security-and-cyber-resilience-framework-of-qualified-registrars-to-an-issue-and-share-transfer-agents-qrta-60605.html>

25. Regulation 30, LODR 2015, available at <https://www.sebi.gov.in/legal/regulations/sep-2023/securities-and-exchange-board-of-india-listing-obligations-and-disclosure-requirements-regulations-2015-last-amended-on-september-20-2023-77239.html>

26. License Agreement For Unified License updated 31 March 2024, available at <https://dot.gov.in/sites/default/files/Compendium-UL-AGREEMENT%20updated%20up%20to%2031032024.pdf?download=1>



A penalty up to INR 50 crore per occasion may be levied for any security breach (which may include a personal data breach) caused due to inadvertent inadequacies in precautions prescribed under the Unified License. The conditions of the Unified License clearly demonstrate an overlap in function with the DPB, and the potential awareness within the DoT of reported personal data breaches.

The regulatory bodies discussed above do not comprise a comprehensive list of authorities with overlapping functions on data protection. A survey of Central and State entities with potential regulatory overlap powers in relation to data protection, and specifically data breaches would be necessary to comprehensively identify all relevant bodies. However, the examples of the above specified large, central authorities indicate a complex regulatory environment for data fiduciaries aiming for full compliance with data protection norms.

Therefore, it is evident that collaboration mechanisms and a clear delineation of responsibilities at the operational level may be required to harmonize the activities of the DPB and other regulators, thus providing a cohesive framework for addressing data breaches across different sectors. This coordination can be facilitated through several mechanisms and need not be entirely dependent on legislative measures. Firstly, the DPB can establish formal agreements or Memoranda of Understanding (**MoUs**) with other regulatory bodies including the RBI, SEBI, and DoT to define roles, responsibilities, and protocols for data breach management, to coordinate an effective executive-level regulatory response. The degree of coordination should factor in the individual responsibilities and specific priorities of respective regulatory entities, while not adversely affected the rights of data principals, or the existing liabilities of data fiduciaries.

#### **(d) Size and capacity requirements for data protection regulators**

It is crucial for the capacity, size and structure of the DPB secretariat to also be informed by the existing structure of similarly placed organizations

A small secretariat may struggle to handle high volumes of breach reports, leading to delays in acknowledging and addressing incidents. Limited resources can also hinder thorough investigations, reducing the effectiveness of enforcement actions. Inadequate monitoring of data fiduciaries may result in lower compliance rates and overlooking of critical breaches. These concerns are crucial to consider in light of the broad definition for breaches and low notification threshold under the DPDP Act. Various statutory boards established for regulatory purposes have been established in India on previous occasions under other legislation. Relevant details of these entities are discussed below.

SEBI was established initially as an administrative body and was later given statutory powers through the SEBI Act in 1992. This provided SEBI with the necessary authority to regulate the securities market in India and protect the interests of investors in the country. Being a regulator of national economic significance, SEBI maintains physical offices in 6 primary locations throughout the country.<sup>27</sup> Additionally, the publicly available organizational structure of SEBI lists over 980 employees in addition to the Chairperson and whole-time members across multiple verticals.<sup>28</sup>

Similar to SEBI, the DPB also possesses certain quasi-executive and quasi-judicial powers, although its quasi-legislative powers are relatively limited in the context of the DPDP Act. SEBI enforces compliance among a large number of entities. It is, in many respects, functionally similar to DPB. SEBI also focuses on regulatory oversight and enforcement, ensuring adherence to standards and safeguarding public interest. Both regulators emphasize transparency, accountability, and protection - SEBI in the financial markets and the DPB in personal data protection.

Another Indian regulator with similarities to the DPB is the Insurance Regulatory and Development Authority of India (**IRDAI**), which is the nodal regulator for insurance products and service providers in the country. IRDAI regulates the insurance industry to protect policyholder interests, ensure financial soundness of insurers, and promote market efficiency. It oversees compliance with laws, regulates insurance companies, and educates consumers about insurance products. As per public information, IRDAI lists over 200 employees across its main and 2 regional offices.<sup>29</sup> In the context of this comparison, considering the secretarial size of regulators such as the RBI and TRAI may not be relevant due to the large difference in kinds of regulatory mandates and regulated number of entities of these bodies.

It is equally, if not more important, to also consider the size of data protection regulators in other countries with a matured privacy landscape. In this respect, the large-population countries implementing the GDPR, Europe's seminal data protection regulation, provide us with some useful insights.

---

27. Economic Times, 29 June 2023, available at <https://economictimes.indiatimes.com/markets/stocks/news/sebi-to-close-down-16-smaller-offices/articleshow/101321934.cms?from=mdr>

28. Employee Profile in SEBI, available at <https://www.sebi.gov.in/departments/human-resources-department-37/employee-profile-in-sebi.html>

29. IRDAI Directory of Employees, available at <https://irdai.gov.in/directory-of-employees>



The United Kingdom’s Information Commissioner’s Office (**ICO**), which is responsible for upholding information rights and data privacy in the country was initially established as a small organization of 10 people, headed by a Data Protection Registrar in 1984. As per the official website, the ICO more than 500 staff based and 4 regional offices.<sup>30</sup>

The Commission Nationale Informatique & Libertés (**CNIL**), the French Data Protection Agency has an 18 member college and 288 agents as per their recent report on the status of the body’s composition.<sup>31</sup> It should be noted that the DPB would oversee the privacy of over 20 times the number of data principals as European regulators, and data fiduciaries potentially larger by an order of magnitude. Hence, sufficient resources must be dedicated to the secretarial staff to ensure the requisite functions are executed. The data specified here indicates a size of more than 200 employees and multiple regional offices is a common threshold for similarly placed regulators.

**Table 2: Comparison of Regulator Secretarial Size**

Regulator	Secretariat Size (Number of Employees)
SEBI	980
IRDA	Over 200
Data Protection Authorities	
ICO (United Kingdom)	Over 500
CNIL (France)	288
Autoriteit Persoonsgegevens (Netherlands)	Approximately 250 <sup>32</sup>
Australian Information Commissioner (Australia)	Approximately 120 <sup>33</sup>

30. History of the ICO, available at <https://ico.org.uk/about-the-ico/our-information/history-of-the-ico/>

31. CNIL Status & Composition, 5 April 2024, available at <https://www.cnil.fr/en/cnil/status-composition>

32. Approximate employee count data available at 31. CNIL Status & Composition, 5 April 2024, available at <https://www.cnil.fr/en/cnil/status-composition>

33. Approximate employee count data available at <https://lead4j.com/c/office-of-the-australian-information-commissioner/5a1d9cc62300005b008c8fb1>

# IV. Concluding Remarks and Suggestions

---

The details of this study outline a series of significant challenges for data fiduciaries, the DPB, and the entire Indian digital ecosystem to overcome for effectively implementing the breach compliances under the DPDP Act. Among these issues, the following observations are particularly concerning from the point of view of a regulator.

## **(a) Addressing Regulatory Overlap:**

The regulatory overlap between sectoral regulators and the DPB in relation to personal data breaches are not insignificant. This increases the complexity of breach incident compliance for data fiduciaries in India. However, an opportunity is presented to provide procedures to streamline compliances and enhance executive-level coordination among regulators and the DPB.

## **(b) Improving Poor Breach Intimation Compliance:**

The data on surveyed Indian data breaches and information disclosed by CERT-In indicates a general failure among body corporates and data fiduciaries in India to dutifully notify data breaches in a timely manner to relevant authorities at present. In contrast to this observation, the DPDP Act breach intimation requirements are far more stringent than the existing obligations, which may result in a drastic increase of reported data breaches to the DPB. However, the lack suo-moto powers to investigate breaches, coupled with no breach monitoring capability would make it difficult for the DPB to estimate intimation compliance among fiduciaries, or punish deviant entities.

## **(c) Low Intimation Thresholds Under DPDP Act**

It is evident that India's thresholds for intimating data breaches under the DPDP Act (both to data fiduciaries and principals) are relatively low compared to other jurisdictions. This theoretically results in a larger volume of incidents requiring intimation, even if compliance with this requirement is low, post-enforcement of the law. Due to the vast scale of estimated non-reported breaches taking place in India, scope remains for a substantial increase in breach reporting post-implementation of the DPDP Act, which may carry the potential to inundate the DPB's oversight capacity and prevent its effective functioning. In any case, it may be necessary for the DPB to devise mechanisms to identify and segregate the high-risk breaches intimated to it, while responding promptly to all intimated cases.

## (d) Ensuring Adequate Regulatory Capacity of DPB:

The functional capacity of the DPB for administering the law would be largely dependent on its available human resource pool. The experience of other regulators and data protection authorities demonstrates the need for a large secretarial size (often in excess of 200 personnel). While the exact resource requirements for India's DPB are not clear, the country's sheer size (more than any other studied jurisdiction) and large number of estimated breaches point to significant personnel requirements for effective functioning of the DPB. However, the DPDP Act does not clarify specific aspects of the DPB beyond the appointment of a chairperson and members of the board.

On the basis of the findings in Part I of this report, and the insights discussed above in Part II, the following inputs are also suggested for the consideration of the Central Government, MEITY and the DPB for an effective data breach reporting framework under the DPDP Act:

### (a) Legislative action suggested via DPDP Act and rules:

- **Positive Incentives for Timely Reporting:** The introduction of incentives and encouragement for data fiduciaries to intimate personal data breaches in a timely manner will be crucial for improving the poor levels of existing data protection compliance. Mechanisms such as mitigation of penalties applicable to data fiduciaries for quick reporting and demonstrating proactive remediation efforts may encourage greater breach intimation compliance.
- **Enhance Legal Mechanisms for Breach Monitoring:** The data analyzed in this report indicates the possibility that the vast majority of Indian personal data breaches continue to be undetected by authorities or the public. In order to assess the levels of personal data breach incidents under DPDP Act, and the degree intimation compliance within the Indian digital eco-system, it may be necessary enable the DPB or other agencies to undertake general monitoring of data breach incidents. Such monitoring would supplement the inadequate existing mechanisms under the DPDP Act or CERT-In.
- **Tweaking the CERT-In Incident Reporting Formats:** The incident reporting format of CERT-In may also be revised to seek information on whether an incident, which is also a personal data breach, has been reported to DPB as per requisite timelines, to improve monitoring and coordination.

- **Suo-Moto Cognizance of Data Breaches by DPB:** Providing the DPB with suo-moto investigative powers would be equally essential for addressing the lack of effective data breach intimation options. As discussed in Part I of the Report, third party disclosures of data breaches continue to play a vital role in alerting Indian citizens of privacy risks, even where data fiduciaries fail to do so. The DPB should be empowered to act on such public disclosures by credible third-party reports (which can include reports from cyber-security firms, researchers, and non-governmental organizations) to safeguard the privacy of Indians. However, this will require an amendment to the DPDP Act.


- **Refining Breach Reporting Requirements with a Tiered / Conditional System:** The Central Government may also consider the implementation of a tiered or conditional reporting system to the DPB, akin to that present under the GDPR or other jurisdictions highlighted above. This enables discretion to the data fiduciary to intimate authorities only where there is a risk to data principals. Further, the complex, expensive and difficult intimation of each affected individual can also be conditional on a 'high-risk' to their rights and freedoms, similar to the GDPR threshold. This would simultaneously ease intimation compliances for fiduciaries while also avoiding inundation of the DPB with high volumes of low-risk breach intimations. Such a system also has the potential to improve intimation compliance in India generally.

## **(b) Executive and organizational recommendations for DPB:**

- **Provide Adequate Staffing:** The DPB secretariat should be adequately staffed with professionals possessing expertise in data protection, information technology, law, and governance. A target of at least 250 employees initially, expanding as necessary, would be advisable based on the population size and expected regulatory load.

- **Develop In-house Monitoring Capabilities:** In-house capabilities for continuous monitoring and analysis of data breach trends may also enhance the administrative capacity of the DPB. This could include developing an incident reporting and tracking system. Regular publishing of aggregated data on reported breaches and compliance may also inform stakeholders about the data protection landscape in India.

- **Formal Agreements with regulators:** Establishing agreements or other mechanisms to coordinate with other overlapping regulators (RBI, SEBI, DoT etc.) will help to define roles, responsibilities, and protocols for data breach management and response at the government and data fiduciary levels.



## 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](http://www.igap.in)