

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

PART I

DECEMBER 2024

AUTHORED BY
RAKESH MAHESHWARI
DEDIPYAMAN SHUKLA



INDEX

Executive Summary	02
I. Background	06
II. Relevant Legal & Regulatory Provisions	08
III. Methodology and Scope of Breaches Analyzed in the Report	12
IV. Concept of personal data breaches	14
CASE STUDY 1 : ICMR Data Breach	16
V. Findings	17
VI. Insights Into Domestic Data Fiduciary Behaviour	25
CASE STUDY 2 : Bookchor Data Breach	31
CASE STUDY 3 : AIIMS Delhi Data Breach	35
VII. Outlined Concerns from Analysis of Breaches and DPDP Act Obligations	39

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 (**DPDP 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 major personal data breach as reported in the media, in India till date,
- Provide expectations for the degree of personal data breach reporting compliance under the DPDP Act,
- Identify systemic gaps in both compliance and regulatory capacity with respect to the DPDP Act's reporting framework,
- Make administrative (and, if necessary, legislative) recommendations to ensure the Data Protection Board is sufficiently empowered to enforce personal data breach reporting requirements and protect Indian data principals.

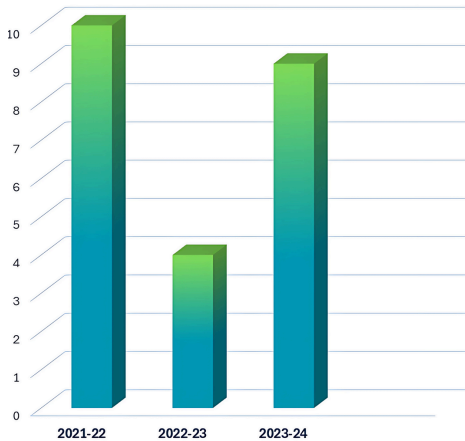
Part I of this report focuses on the existing compliance landscape and empirically analyses past trends in data fiduciary behaviour, while highlighting issues in regulation and compliance. **Part II** of this report assesses the DPDP Act's specific implementation challenges, in light of the findings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

Findings

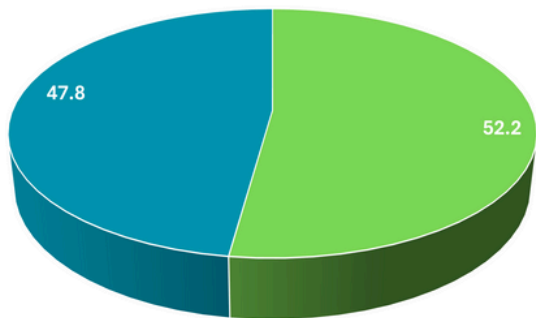
As per the findings in Part I of this report, India's incident reporting framework for data breaches, largely guided by the Information Technology Act and rules, appears to have been inconsistently applied, with limited accountability for body corporates in respect of their personal data handling oversight.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

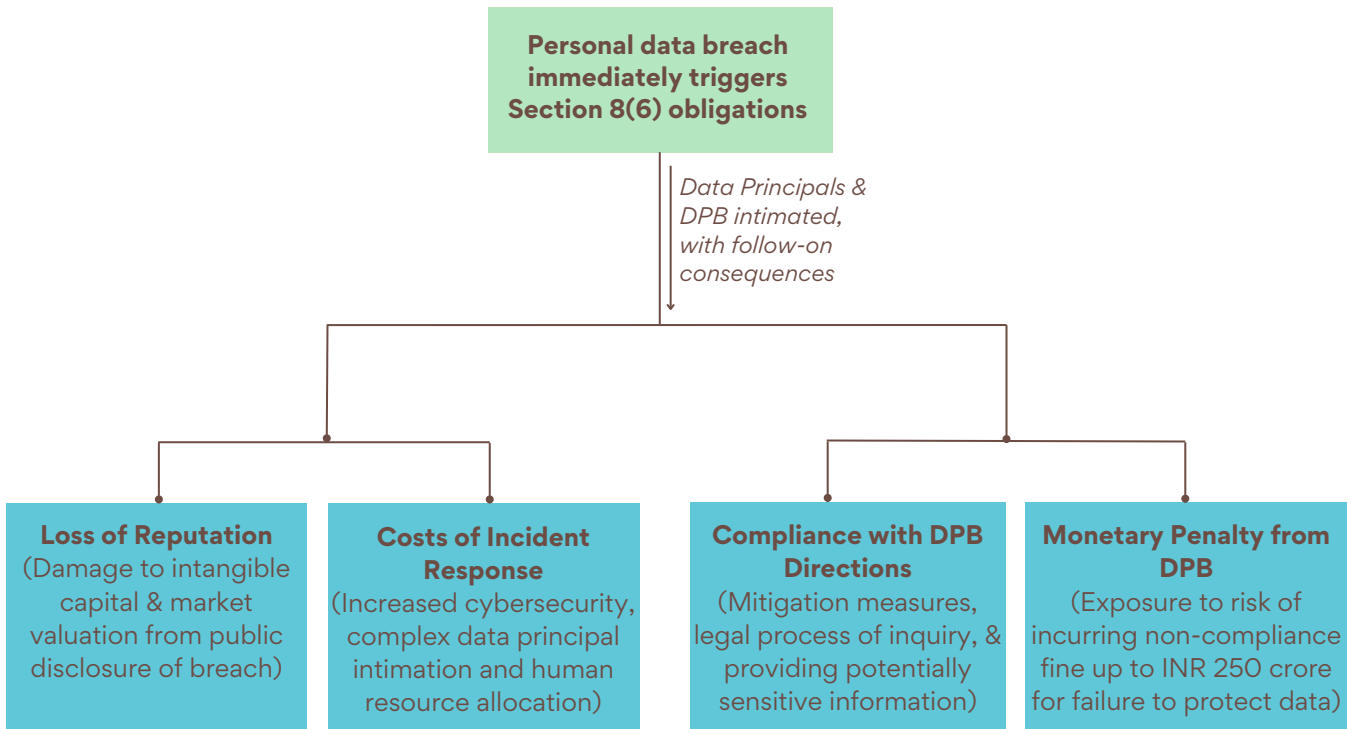


Proportion of personal data breaches identified by 3rd parties / independent researchers

- Data Fiduciary / Unclear / Other
- Independent Researcher / 3rd Party

- 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.



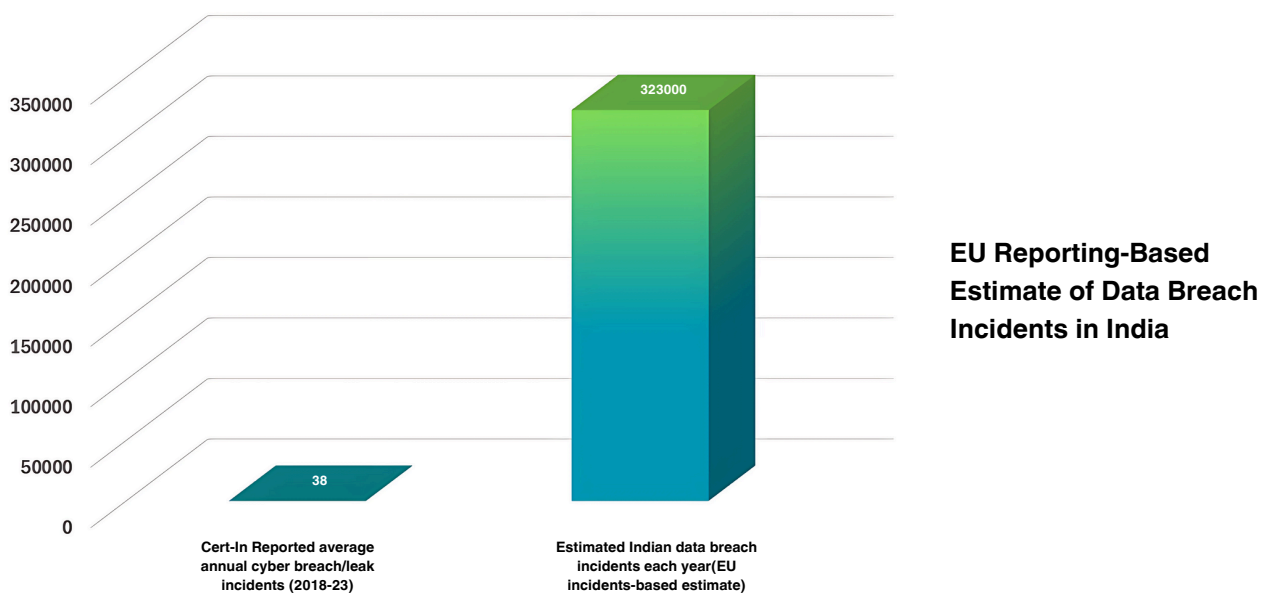
Disincentives & factors associated with triggering of notice/intimation DPDP Act obligations by Data Fiduciaries

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).

I. Background

In August 2023, the Parliament of India passed into law the Digital Personal Data Protection Act, 2023¹ (**DPDP Act**). The mandate for this framework was envisioned by the Hon'ble Supreme Court in *KS Puttaswamy v. Union of India* (2017)², where the court ruled on the existence of an implicit right to privacy, as a fundamental right, in relation to the right to life under Article 21 of the Constitution of India, 1950. In this context, the DPDP Act was enacted with a scope relating to all processing of digital personal data including automated and partially automated processing of personal data in digital space, in recognition of the specific need for privacy safeguards in this domain.³

In 2024, compliance with the DPDP Act has become a key focus point for the multitude of entities that operate within, or provide services, in India. As of late 2024, the Central Government is expected to notify subordinate rules to give effect to the law, and bring it into force.⁴ In fact, the notification of substantive rules is essential to give meaningful effect to the provisions of the DPDP Act, as the law does not by itself provide sufficient guidance to effectively regulate digital privacy. The enforcement of the DPDP Act, along with its rules, may be carried out in phases, with some provisions coming into effect earlier than others.

However, it is essential for data fiduciaries, processors, and the Central Government to recognize, in advance, the operational bottlenecks that may arise during the implementation phase of this law. Among other requirements, several working details regarding data breaches in India must be properly understood to plan for implementation challenges under the DPDP Act, as one of the core aspects covered by the law is the handling of data breaches.

The threat to the personal data of Indian citizens arising from data breaches continues to grow on a real-time basis. According to some estimates, 9,478 public data breach incidents have already been reported globally in 2024.⁵

However, an accurate assessment of the risks to Indian personal data is difficult to obtain, as few data breaches are reported publicly. More details on this aspect of breach reporting is provided subsequently in this report. Nonetheless, it is evident that use of data breaches, as a form of cyber-attack, remains an effective tool at the disposal of cyber criminals to gain leverage over data fiduciaries for financial gain, or to cause wrongful loss to unsuspecting data principals.

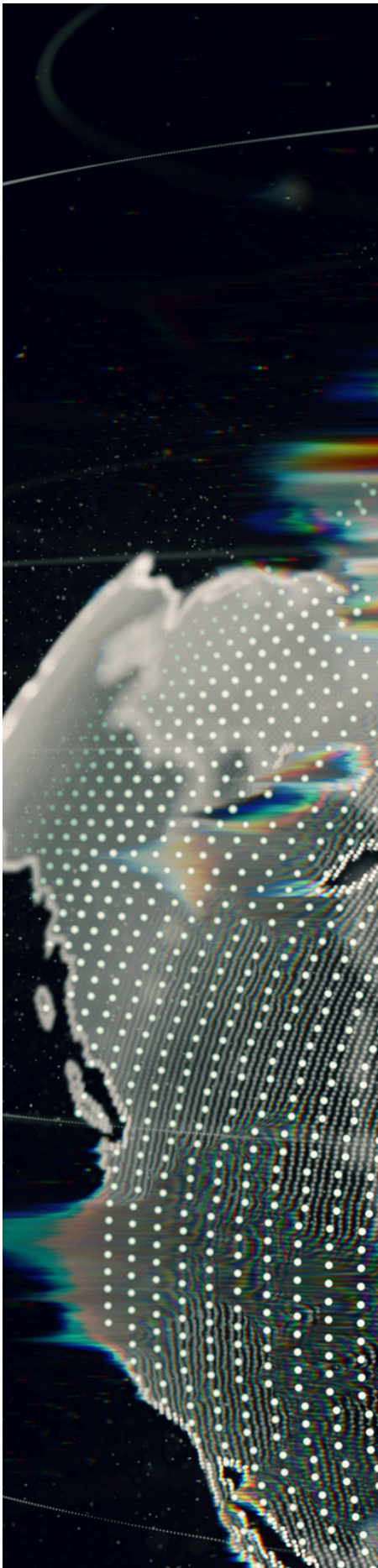
1. Digital Personal Data Protection Act, 2023 (DPDP Act), available at <https://www.meity.gov.in/writereaddata/files/Digital%20Personal%20Data%20Protection%20Act%202023.pdf>

2. *KS Puttaswamy v. Union of India*, (2017) 10 SCC 1

3. Section 2(b), DPDP Act

4. Subjects for rulemaking under the law include consent, standards for processing data and classes of data fiduciaries. Section 40(2), DPDP Act. Entities may be given a year's time to comply with DPDP Act: Government, *The Hindu Businessline*, 20 September 2023, available at <https://www.thehindubusinessline.com/news/national/entities-may-be-given-a-years-time-to-comply-with-dpdp-act-government/article67325518.ece>

5. Data Breach Dashboard for 2024 and 2023, IT Governance UK, available at <https://www.itgovernance.co.uk/blog/global-data-breaches-and-cyber-attacks-in-2024#top-stats> and <https://www.itgovernance.co.uk/blog/list-of-data-breaches-and-cyber-attacks-in-2023#top-data-breach-stats>



The following report highlights key findings relating to the existing practices and protections afforded by data fiduciaries in the event of data breaches, in order to map critical points of failure in the enforcement framework under the DPDP Act (i.e. potential situations of non-compliance by the data fiduciaries / processors). This report also seeks to illustrate concerns regarding circumstances in which a data breach may be reported, as any remedial action under the law is entirely contingent upon the initial detection and reporting of incidents to relevant authorities, as well as to the concerned members of the public.

II. Relevant Legal & Regulatory Provisions

(a) Personal Data Breaches and Fiduciary Responsibilities under the DPDP Act

The DPDP Act, under Section 2(u) defines a personal data breach as ‘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’. This definition is notably wide, and therefore likely to yield a large number of ‘technical data breaches’ in practice once implemented. The occurrence of a breach is a trigger point for many subsequent actions under the DPDP Act. In the event of a personal data breach, the concerned data fiduciary is required to provide intimation of this breach to the Data Protection Board (**DPB**), and also to each data principal that is affected by the breach. It should be noted that no option is provided under the act to merely intimate the DPB, and avoid intimating the affected principal of the breach.⁶

Once the DPB is intimated of the personal data breach, it may direct urgent remedial or mitigatory measures to be undertaken by the fiduciary. Power is also provided to the DPB to make inquiries into the breach and impose penalties on errant parties for identified violations of the DPDP Act.⁷ Apart from the direct intimation of breach by the data fiduciary, there are additional mechanisms provided by which the DPB may be notified of a breach for the purpose of conducting inquiry,⁸ namely:

- Complaint made by a data principal,
- Reference made by the Central/State Government, or
- Directions from a court of law

While carrying out its intended responsibilities, the DPB is expected to function as an independent body and only proceed with an inquiry after it has determined the existence of sufficient grounds for doing so.⁹ Otherwise, the DPB may choose to close proceedings, while recording its reasons in writing. For this purpose, it has been vested with the powers of a civil court, and is required to apply the principles of natural justice in its process of inquiry.

6. Section 6(6), DPDP Act

7. Section 27(1)(a), DPDP Act

8. Section 27(1)(b), DPDP Act

9. Section 28, DPDP Act



Upon the completion of an inquiry, the DPB may again choose to close the process on the basis of its findings. Alternatively, a wide range of monetary penalties may be imposed on the errant entity or individuals if the DPB unearths credible evidence of a violation.¹⁰ The extent of penalties will depend on a range of factors, which include the gravity of the breach, type of affected data, repetition in incidents, gain to the liable individual, mitigation activity, and financial status. The penalty amount may extend up to INR 250 crore post the evaluation of relevant factors. This highest penalty under the DPDP Act (i.e. INR 250 crore) may be imposed specifically for a failure to take reasonable safeguards in preventing a personal data breach. This indicates the high priority that the DPDP Act accords to the prevention of data breaches and securing the personal information of Indian citizens.¹¹

For greater clarity, it should be noted that the term ‘data fiduciary’ has been used within this report even when referring to breach instances affecting body corporates prior to the enactment of the new data protection law in August 2023. The term ‘data fiduciary’, in this context, carries the same meaning as provided under the DPDP Act¹² and such entities would likely qualify as data fiduciaries post the enactment of the law.

(b) Privacy and reporting obligations under the Information Technology Act, 2000

While the DPDP Act introduces the first stand-alone law for privacy breach, the broader category of cyber-security breach was already under the reporting framework of the Information Technology Act, 2000 (**IT Act**). The relevant details of this framework are equally significant, as personal data breaches, for the larger part of India’s digital history, have not been treated as a distinct kind of incident from a regulatory point of view.

10. Section 33(1), DPDP Act

11. The Schedule, DPDP Act

12. Under Section 2(i) of the DPDP Act, a data fiduciary is defined as ‘any person who alone or in conjunction with other persons determines the purpose and means of processing of personal data’.

The IT Act was enacted to create a legal framework for all electronic communication and data interchange in India. Under it, a statutory body called the 'Indian Computer Emergency Response Team' (**CERT-In**) was created to serve as the national agency for cyber incident response. 'Cyber security' was defined under the law to include protection of information from unauthorized access or disclosure.¹³ While 'cyber security incidents' were not defined under the IT Act, a definition was provided under the Information Technology (The Indian Computer Emergency Response Team and Manner of Performing Functions and Duties) Rules, 2013 (**CERT-In Rules**) which includes unauthorized access to a computer resource, data or information.¹⁴ CERT-In, vide its directions in April 2022, further increased the scope of cyber security incidents and defined strict reporting timelines for incidents to CERT-In.¹⁵ This definition would evidently cover a personal data breach. Data breaches and leaks are also covered as a sub-category of incident-type under the Incident Reporting Form provided by CERT-In.¹⁶

Among other tasks, CERT-In was allocated the following crucial functions:¹⁷

- Collect, analyze and disseminate information on cyber incidents,
- Provide forecasts or alerts,
- Coordinate response activities and emergency measures, and
- Issue guidelines, advisories, and papers on information security practices, procedures, prevention, response and reporting of cyber incidents.

Further, the CERT-In Rules, and associated directions, require that certain kinds of cyber security incidents, which include unauthorized access to data, breaches and leaks, among others, need to be mandatorily reported by service providers, body corporates, intermediaries and data centers affected by the incident to CERT-In, within a reasonable time, in order to leave scope for action to be taken.¹⁸

The IT Act also provided for a light-touch privacy framework. This framework was devised under Section 43A of the IT Act, which specified the liability of body corporates possessing, dealing or handling any sensitive personal data or information¹⁹ stored in a computer resource. Additionally, the Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules, 2011 (**RSPDI Rules**) were notified to guide the information security and data handling processes undertaken by body corporates.

13. Section 2(1)(nb), IT Act

14. Rule 2(h) of the CERT-In Rules defines a 'cyber security incident' as any real or suspected adverse event in relation to cyber security that violates an explicitly or implicitly applicable security policy resulting in unauthorized access, denial of service or disruption, unauthorized use of a computer resource for processing or storage of information or changes to data, information without authorization. is likely to cause or causes an offence or contravention, harm to critical functions and services across the public and private sectors by impairing the confidentiality, integrity, or availability of electronic information, systems, services or networks resulting in unauthorized access, denial of service or disruption, unauthorized use of a computer resource, changes to data or information without authorization; or threatens public safety, undermines public confidence, have a negative effect on the national economy, or diminishes the security posture of the nation.

15. CERT-In directions under Section 70B(6), dated 28 April 2022, available at https://www.cert-in.org.in/PDF/CERT-In_Directions_70B_28.04.2022.pdf

16. CERT-In Incident Reporting Form, available at <https://www.cert-in.org.in/PDF/certinirform.pdf>

17. Section 70B(4), IT Act

18. 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

19. Section 43A of the IT Act reads "Where a body corporate, possessing, dealing or handling any sensitive personal data or information in a computer resource which it owns, controls or operates, is negligent in implementing and maintaining reasonable security practices and procedures and thereby causes wrongful loss or wrongful gain to any person, such body corporate shall be liable to pay damages by way of compensation to the person so affected."

The RSDPI Rules mandated that all body corporates comply with reasonable security practices and procedures on the lines of the International Standard IS/ISO/IEC 27001 on 'Information Technology - Security Techniques - Information Security Management System – Requirements'.²⁰ It was also necessary for body corporates to demonstrate, when required, that they implemented security control measures in the event of an information security breach. This framework continues to be in force till such time the as the DPDP Act formally gets operationalized. Perhaps the most significant difference between the older framework of the IT Act and the newer DPDP Act is the quantum of penalties applicable. A breach of privacy by non-consensual disclosure of personal information of another person under lawful contract is punishable under the IT Act with a fine of INR 25,00,000.²¹ However, a failure to protect personal data through reasonable safeguards is merely punishable with payment of compensation to the affected person under Section 43A. Further, a penalty of INR 1,00,000 could be imposed for violating any rules, regulations or directions made under the IT Act.²² The quantum of penalties appears quite limited in comparison to those specified under the DPDP Act. Despite this distinction, the IT Act provisions clearly demonstrate that a framework was previously in place to guide entities through the management and mitigation of personal data breaches within India.



20. Rule 8, RSPDI Rules

21. Section 72A, IT Act, as amended in 2023

22. Section 45, IT Act, as amended in 2023

III. Methodology and Scope of Breaches Analyzed in the Report

This report, divided into two distinct parts, has been prepared by utilizing publicly available data and reports relating to personal data breaches taking place in India during the studied period. This data has been used, in combination with legal analysis of existing data protection laws, to extrapolate on the 'data breach'-preparedness of entities in India, as well as the relevant government authorities. The data collection, necessary for this report, was carried out directly by the authors using publicly accessible sources of information. As data breach incidents are often treated as a sensitive subject, publicly available information surrounding such breaches can be somewhat limited.

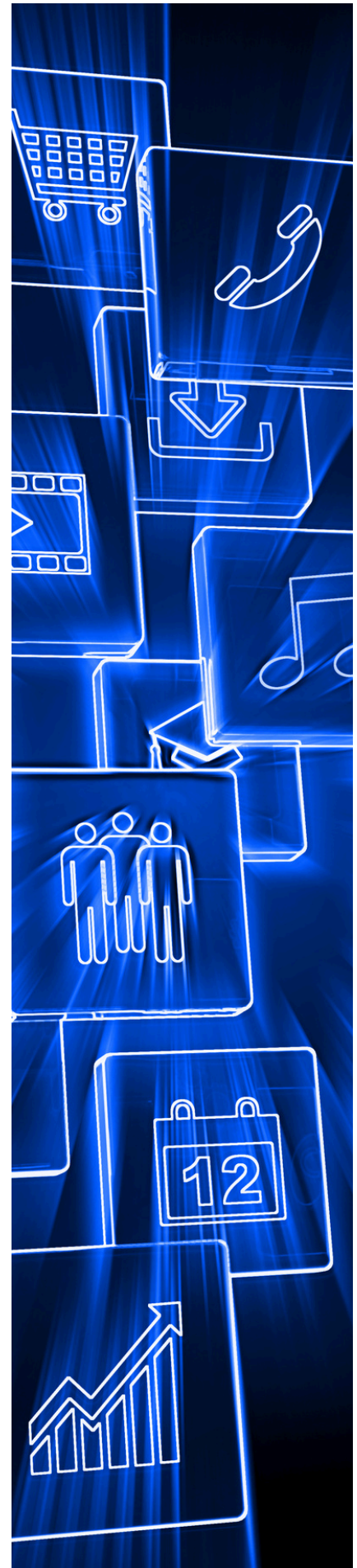
To compound this difficulty, different entities (i.e. data fiduciaries, independent researchers, and government agencies) were found to occasionally provide conflicting accounts, or denials relating to the same breach incident. To best ensure the reliability of data collected, priority was placed on reports of data breaches by authoritative media and news sources. Additionally, only incidents that could be corroborated by at least two separate sources were included within the scope of this report.

- During the course of this study, a total of 29 significant personal data breaches were identified as per the outlined thresholds, from 2021 till August 2024. Details of these breaches have been specified in the Annexure to this report.
- However, to ensure the relevance of data breach response behaviours studied, the analysis of data has been limited to only those Indian personal data breach incidents (23 incidents) taking place within the previous 3 years (i.e. January, 2021 to January, 2024).
- Additionally, focus was also placed on more significant data breaches taking place in India, which would be likely to attract greater sanction from regulators, or the Data Protection Board in the future. Hence, the insights provided below are only drawn from a sample space containing data breaches where more a threshold minimum of 1,00,000 principals or electronic records of personal data were impacted. In this respect, independent third-party monitoring platforms such as 'Mozilla Monitor'²³ were found to be of specific utility in identifying breach instances that met the requirements formulated under this study.

23. Mozilla Monitor, available at <https://monitor.mozilla.org/breaches>

The following limitations of the study should also be noted:

- The verification of all reported information regarding data breaches incidents by the authors themselves was not within the purview of this exercise.
- While some breach disclosures were available on public sources, these disclosures may not be concurrent with the timeline of the actual personal data breach incidents, as the emergence of verifiable information on these breaches may have been delayed in multiple instances. Hence, the precise day of occurrence of each data breach studied under this report is difficult to estimate.
- As the CERT-In data mentioned in this report implies, a large number of data breaches are not made public or disclosed. Such information could not be incorporated into the ambit of the report due to the limited information access available to the authors. Further, breaches with limited information disclosure that could not be verified from at least 2 independent sources have also been excluded from the analysis in this report.
- This report does not comment on the quality and adequateness of information and data security standards currently implemented in India by data fiduciaries suffering data breaches. Such information is not generally available publicly. However, the authors acknowledge this forms a crucial aspect of data privacy regulation and compliance.



IV. Concept of personal data breaches

As noted above, the concept of a personal data breach under the DPDP Act encompasses a wide range of incident types as captured by the legal definition, and includes any unauthorized processing of personal data or accidental disclosure, acquisition, sharing, use, alteration, destruction or loss of access to personal data. The practical effects and characteristics of common kinds of personal data breaches are detailed below:

1. Data theft:

Traditional data theft refers to the stealing of personal information that is digitally stored on electronic devices. This may commonly include categories such as passwords, date of birth, bank account information or government identity data. Data theft is typically carried out by malicious actors hoping to derive a benefit from the stolen data.²⁴ Stolen personal data can enable 'phishing attacks' to extract more information or financial gain from the data principal, among other harms. Alternatively, such information may be aggregated and sold to other entities which may derive utility from it.

2. Accidental disclosure/ data leak:

In a large proportion of instances,²⁵ a personal data breach may not be malicious, and may be the result of human error. For instance, the personal information of one individual may accidentally be disclosed to another person or entity which should not have access to it. This may take place due to the lack of access restrictions, misconfigured information systems, or employee errors.

3. Destruction of personal data:

Destruction of the personal data stored by an entity at the end of its lifecycle, where planned, can be a part of a data fiduciary's normal operations to limit legal liability and rationalize data handling processes. However, unauthorized and premature destruction of personal data can be a serious breach and have negative ramifications. This can impact decision-making, disrupt business practices and complicate regulatory compliances for the entity.

24. What is data theft and how to prevent it, AO Kaspersky Lab, available at <https://www.kaspersky.com/resource-center/threats/data-theft>

25. Business Standard report on human error breach dated 21 March 2024, available at https://www.business-standard.com/finance/personal-finance/ransomware-attack-top-threat-in-india-human-error-leading-cause-of-breaches-124032100449_1.html

4. Unauthorized personal data alteration:

This involves the modification of personal data without the consent of the data principal, or without the proper authorization from the data fiduciary responsible for managing the data. Such an incident may commonly include information falsification, which can compromise the accuracy, integrity, and reliability of the data. Harms resulting from such a breach may involve incorrect decision-making, financial loss, or damage to individual reputation.

5. Ransomware attacks:

While not an explicit category of breach, it is important to note the characteristics of ransomware attacks, which have become increasingly common in recent years. A ransomware attack is a type of cybercrime where malicious software, or ransomware, is used to encrypt a victim's files or lock them out of their system, essentially causing a loss of access to personal data. The attacker would then demand a ransom, often in a difficult to trace format like cryptocurrency, in exchange for a decryption key or data access. Ransomware can spread through phishing emails, malicious file downloads, or exploiting vulnerabilities in a system. The impact of such attacks on large databases can be devastating, leading to significant financial loss, disruptions, and reputational damage to the data fiduciary. Paying the ransom may not guarantee the recovery of the data, and may further encourage criminal activity. Some of the incidents studied for this report demonstrate characteristics of this kind of attack.

6. Intentional data sharing:

This includes instances where data is shared in violation of contractual obligations or without a lawful basis, as well as situations where data sharing has been authorized but the data principal is inadequately aware of the extent or purpose of data usage. Such practices can compromise the privacy and autonomy of individuals, leading to potential harms such as identity theft, financial loss, or reputational damage.

In respect of the various kinds of personal data breaches, it should be noted that additional breach types, causes, impacts and other nuances may be prevalent. Further, a personal data incident may involve more than one kind of breach in some instances.

CASE STUDY 1

ICMR Data Breach

Perpetrators of data breaches can be notoriously difficult to identify or trace. In 2023, the Indian Council of Medical Research (ICMR), one of India's most prominent medical research organizations, experienced a significant data breach where personal data from its database was made available for sale on the dark-web. This breach highlighted the vulnerabilities in data protection practices within even the most reputable institutions and underscored the importance of robust cybersecurity measures. The breach was initially detected by an American cybersecurity agency which found the unprotected database of over 80 crore Indian citizens available online, and not by ICMR itself. Detection by third parties of breached personal data is a common characteristic of multiple instances in India. By the time the breach was acknowledged, and acted upon by authorities, the database had already been accessed multiple times by unknown entities. Most concerning was the fact that the breached personal information contained user Aadhaar and passport information apart from names, phone number and addresses. Such information is closely tied with public services, financial transactions and other activities of an individual. It is one of the most sensitive aspects of a person's personal identification information within India. A breach of Aadhaar information has the potential to result in identity theft, fraud, unauthorized tracking, misuse of welfare schemes and erosion of trust in public institutions. This breach, like several others, was reported to CERT-In, which was able to verify the authenticity of the leaked data from the sample provided by the hackers. In this instance typical of many Indian data breaches, the relevant data fiduciary was not the discovering entity for the breach. ICMR, an entity under the Union Government, was also not prompt to address the allegations of the breach, which resulted in public speculations on the incident. However, public attention towards this high-profile breach incident did result in some legal action. Approximately two months after the initial detection of the breach, the cyber unit of the Delhi Police made 4 arrests after taking suo-moto cognizance in the case. However, arrests and convictions in personal data breach cases are extremely rare, and the present status of this instance of arrest is unclear from public information. Additional details regarding this incident are available in the report's Annexure.

V. Findings

The DPDP Act is expected to bring about an overhaul of the privacy practices and procedures currently implemented in India, once it is brought into effect. This is contingent on effective compliance with the provisions of the law by domestic data fiduciaries and processors, as well as a well-functioning DPB. One of the purposes of the data analysis exercise in this report was to understand whether these expectations would be met, taking into consideration the preceding record of data fiduciary compliance under the IT Act provisions, rules and regulations.

Some broad trends from this study, based on publicly available sources, is provided below:

(a) Number of Substantial Breaches

The information collected for the purpose of this report was restricted to only those Indian personal data breach incidents which took place within the previous 3 years (i.e. January 2021 to January 2024), and were substantial in size (i.e. where an estimated 1,00,000 principals or electronic records of personal data were impacted by the incident). Within these parameters, 23 publicly disclosed instances of domestic personal data breaches were identified, at an average of approximately 7.67 substantial breaches each year. However, it is necessary to view this data in light of information placed before Parliament by CERT-In.

As per information provided by the Ministry of Electronics and Information Technology (**MEITY**) in March 2023, 47 incidents of data leak and 142 incidents of data breach (189 incidents in total) were reported to CERT-In in the previous 5 years²⁶, averaging to 37.8 such incidents per year. However, this number would include breaches below the minimum threshold for this study (i.e. less than 1,00,000 records) and breaches not otherwise disclosed to the public. Crucially, 22 government organization 'data leaks' were reported CERT-In in the 3-year period from 2020 to the end of 2022, although the gravity of these leaks is not clear from MEITY's statements.²⁷ Also relevant in this context is CERT-In's Annual Report 2023 which notes the handling of 15.9 lakh incidents by the authority in the previous year.²⁸ However, this report does not provide clear data on the proportion of personal data breaches handled among the other incident types.

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

27. Ibid

28. Indian Computer Emergency Response Team (CERT-In) Annual Report 2023, Ministry of Electronics & Information Technology (MeitY), Government of India, at page 8

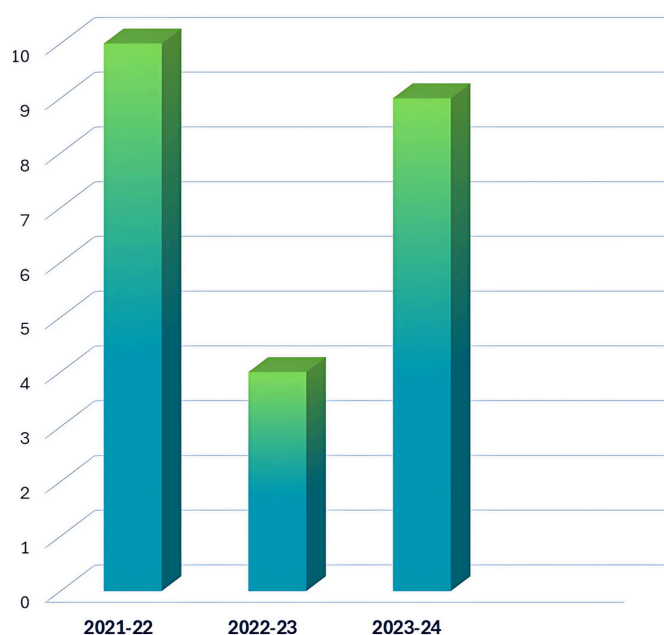


Figure 1: Chronological representation of the number of significant Indian breaches identified for this report (by year)

(b) Types of personal data affected in Indian data breaches

The DPDP Act defines personal data as ‘any data about an individual who is identifiable by or in relation to such data.’²⁹ This broad principle-based definition implies that a wide range of data-types may be classified as personal data.³⁰ This is at least as broad as the definition of ‘personal information’ under the older RSPDI Rules. An analysis of affected data types in breaches, in the documented publicly disclosed instances over the studied period, indicates that the following types of personal data, in descending order, (apart from personal names) are most likely to be affected in a personal data breach: phone number, email address, physical address, and date of birth.³¹ These types of personal data form core aspects of personal identity authentication and verification processes implemented by data fiduciaries and carry the potential to be used in criminal activities like phishing and identity theft.

Type of personal data	% of breach instances affecting the data-type
Phone Number	78.2 %
Email Address	65.2 %
Physical Address	56.5 %
Date of Birth	39.1 %

Table 1: Types of personal data affected by data breach in the largest proportion of cases³²

29. Section 2(t), DPDP Act

30. Rule 2(1)(i), RSPDI Rules. The definition under the RSPDI Rules is somewhat limited in applicability to body corporates, unlike the DPDP Act.

31. Based on the author’s independent calculations of studied breaches. Further details of instances are available in the Annexure.

32. Based on the author’s independent calculations of studied breaches.

It should also be noted that in at least 34.7% of instances, data from an Indian government issued identification was reported to be breached (such as Aadhaar, PAN and passports). This highlights the specific challenge of protecting authentic identity information, processing of which is often made necessary by data fiduciaries for accessing online services. More details about compromised data types in the study are available under the Annexure.

(c) Size of Breaches

While a minimum threshold of 1,00,000 breached records/users was applied for the purpose of identifying breaches in this study, the exact size of the personal data breach incidents captured in this analysis varies widely from a few hundred thousand to over 1 billion affected records. The breach size exceeded 100 million users (an extremely large number of records) in almost a third of studied instances.³³

(d) Target of Data Breaches

It is also crucial to note the ostensible target of privacy breaches in India. During the studied period, only a few personal data breaches were found to emanate at the premises of the data processor. Most breaches reportedly took place regarding data under the control of the data fiduciaries themselves, although information about the exact location of breach was limited in the majority of instances. Disclosure of the primary source or exact location of the breach was not common practice, either in the statements of data fiduciaries, or in third party news reports.

(e) Intimation of Breaches

One of the pivotal aspects of handling and responding to breaches is the process of reporting and intimation. Taking appropriate and timely action can mitigate the negative impact of a data breach. Further, making data principals aware of a breach involving their personal data provides them the opportunity to exercise abundant caution and take appropriate actions individually. However, the RSPDI Rules discussed above, which were in operation for the duration of this study (2021-23) did not have any specific requirement to intimate the instance of a data breach to the concerned data principals or provide public disclosure of the details of the data breach. In the absence of a mandated responsibility to disclose information on breaches, breached entities often chose to deny or make limited disclosures regarding instances.

In many of the studied instances, the fact of the breach was discovered by independent researchers or third parties not associated with either the data fiduciary, government or law enforcement agencies.

33. Based on the author's independent calculations of studied breaches.

This was reported to be the case in 47.8 % of breaches studied, highlighting the crucial role played by civil society in uncovering breaches of privacy and holding data fiduciaries responsible for the protection of data under their control.³⁴ However, this number may potentially be even greater as the discovering entity was not made clear in several instances, as per the public reports of breaches.

Entity Discovering Data Breach (in % terms)

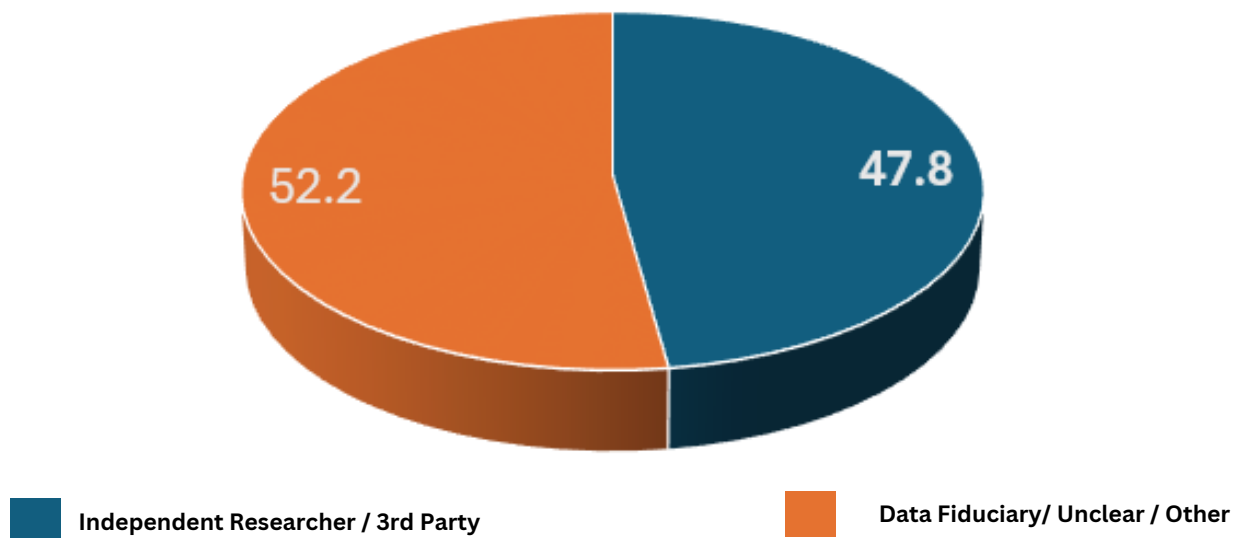


Figure 2: Proportion of personal data breaches identified by third parties / independent researchers

As mentioned above, a requirement is placed on body corporates, service providers, intermediaries, and data centers to report the occurrence of cyber security incidents (including data breaches) to CERT-In for monitoring and remedial action within a short timeframe. Among the breach instances studied, strong compliance with this requirement was not evident. Responses to breaches varied from outright denial and non-disclosure, to total security overhauls in some cases. However, the fact of intimation of the breach incident by the concerned data fiduciary to CERT-In was verifiable by public disclosure in only 36.4 % of cases.³⁵

(f) General RSPDI Rules Compliance

Irrespective of whether a body corporate suffered a personal data breach, it is necessary for such body to adhere to the requirements of the IT Act and RSPDI Rules if personal information and sensitive personal information is processed or collected from users. However, insights from a study of the organizations affected by the data breaches were revealing on the extent of compliance with these rules, despite the relatively light-touch and minimal compliances involved.

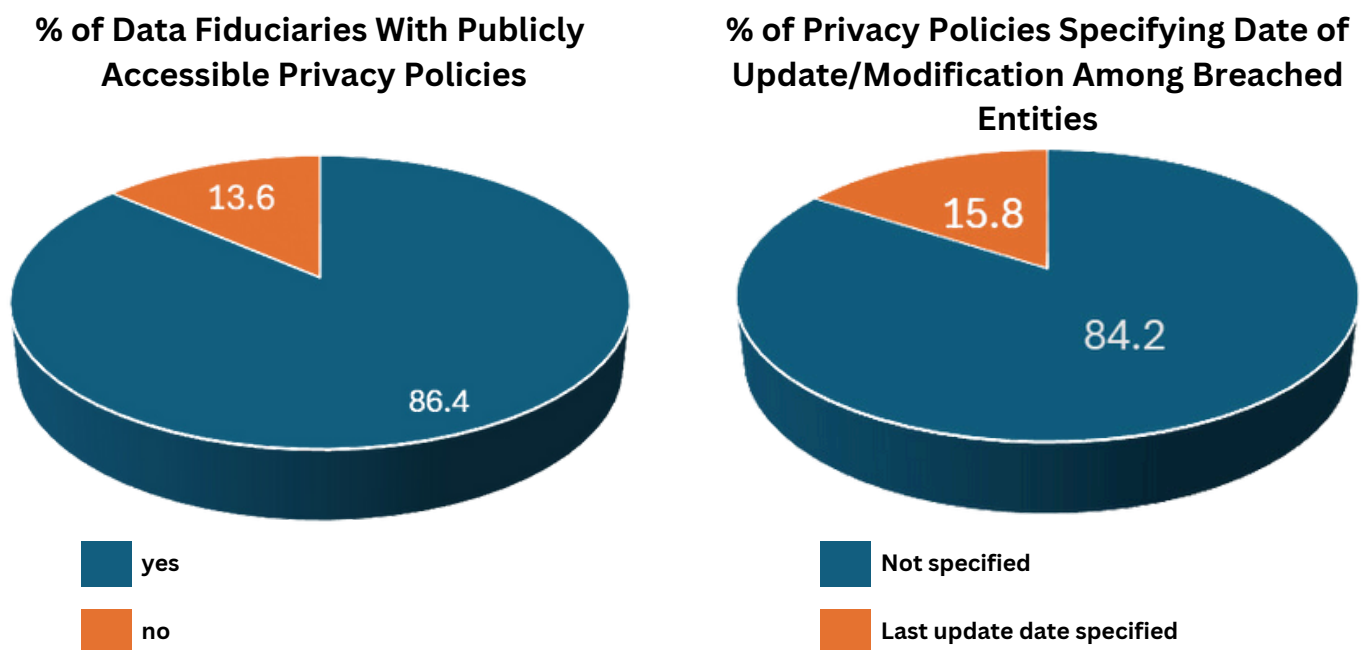
34. Based on the author's independent calculations of studied breaches. Further details of instances are available in the Annexure.

35. Based on the author's independent calculations of studied breaches.

For instance, Rule 4 of the RSPDI Rules require that:

'body corporate or any person who on behalf of body corporate collects, receives, possess, stores, deals or handle information of provider of information, shall provide a privacy policy for handling of or dealing in personal information...'

The data below indicates that not all fiduciaries were in compliance with this legal requirement. It may also be relevant to note the degree to which organisations that do maintain privacy policies keep them updated. Informing users about updates and changes to the privacy policy may be considered a best practice, and is also a legal requirement in some jurisdictions.³⁶ Of the data fiduciaries that did publish privacy policies, only in 3 instances was the data of last modification to the applicable Indian privacy policy specified (i.e. Air India, IndiaMART, Jubilant FoodWorks).³⁷



Figures 3&4: Availability of privacy policies & updation disclosure as observed in breach affected data fiduciaries

(g) Repeated Breach of Data Fiduciaries

One concerning aspect of the study of information on Indian breaches was the common occurrence of repeated breaches (i.e. where the breach suffered by the data fiduciary was not an isolated incident). Such systematic occurrence of personal data breaches indicates greater vulnerability of the data principals associated with that fiduciary, as well as the failure of the data fiduciary to adequately improve information security practices and procedures in the face of a clear threat to their data.

36. Under the Children's Online Privacy Protection Act, 1998 in United States, specifying changes or updates to privacy policy is a legal requirement.

37. Based on the author's independent calculations.

In a substantial proportion of instances, data breaches were found to not be an isolated incident. Such breaches, if associated with a compliance failure by the fiduciary, would likely attract a higher monetary penalty from the DPB under the DPDP Act.³⁸

% of Fiduciaries Facing Repeated Breaches

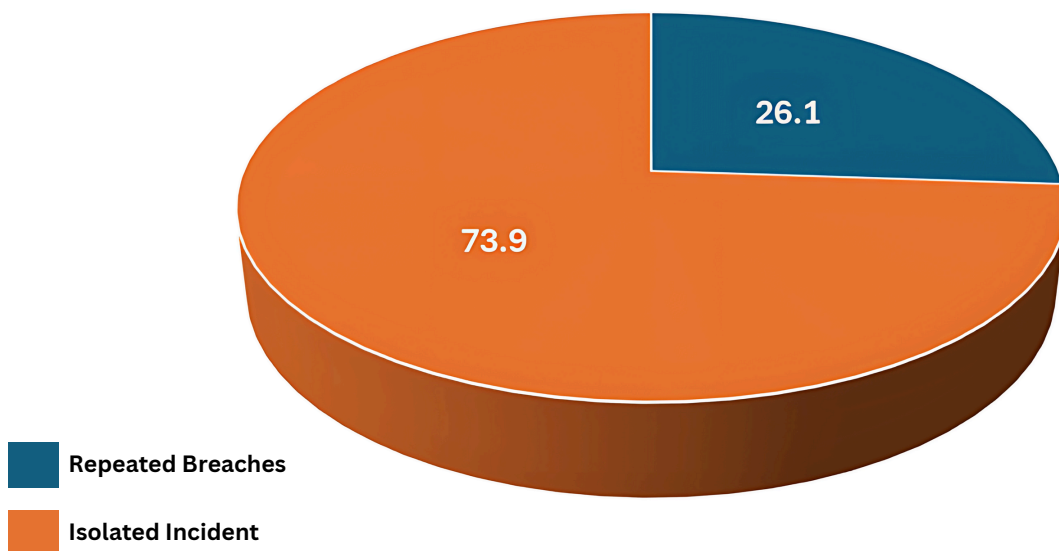


Figure 5: Proportion of data breaches that were a repeated occurrence

(h) Remedial Actions Post-Breach

While reporting of a breach incident to CERT-In is essential to comply with the legal mandate of the IT Act, RSPDI Rules and CERT-In Rules, it is not sufficient action to ensure that the harm to data principals is mitigated and future incidents of this nature are deterred. In the context of the studied breach instances, independent remedial actions taken by data fiduciaries fall into three broad categories:

- **Registration of FIR and criminal action against perpetrators:**

While the registration of an FIR, whether by the data fiduciary or other entity post-breach was a common occurrence, instances of any substantive legal action against perpetrators were limited. These were largely restricted to arrests made during the criminal investigation into serious cyber-attacks. Identification of responsible individuals in a data breach can be notoriously difficult, and this was reflected in the findings of the report.

38. Under Section 33(2) of DPDP Act, the DPB may consider the repetitive nature of the breach as an extenuating factor while calculating the penalty.

- **Internal investigation into cause of breach:**

In a number of instances, data fiduciaries were found to engage external specialists and forensic auditors to scrutinize the internal data-related practices of the organizations and identify issues that may have contributed to the data breach, or may contribute to future breaches. However, details of the findings of these investigations, vulnerability assessments and audits were generally not disclosed making it difficult to gauge the extent of rectifications undertaken by Indian data fiduciaries after suffering a breach.

- **Precautionary upgrade of information security systems and communication of risks to affected principals:**

In some instances, data fiduciaries were found to disclose various precautionary and mitigatory measures in the immediate aftermath of disclosing a personal data breach. Such measures included: *new standard operating procedures for handling breaches, upgradation of network architecture, encryption of stored data, introduction of multifactor authentication, reset of user passwords, review of third-party plugins/software interacting with the fiduciary's platform, taking platform offline, ringfencing of networks, tightening information security protocols and access controls etc.*³⁹

(i) Lack of Information on Consequent Harm to Data Principals

One limitation observed in publicly available information on personal data breaches was the scarcity of information on how the data principals may be affected or placed at risk from the unauthorized access to their information. Information of this nature is crucial for the assessment of penalties to be imposed in case of a breach under the DPDP Act.⁴⁰ Though clear cases of direct harm to the data principal were difficult to identify, potential harms from these breaches were outlined in statements made by fiduciaries or public reports on the relevant breaches. A compilation of these is specified below:

- Targeted phishing, card duplication and other financial frauds
- Blackmail and extortion using personal details
- Forgery of documents
- Disclosure of sensitive information regarding high-profile individuals / damage to reputation
- Impersonation of government employees / espionage
- Identity theft

39. Measures are identified from authors own analysis of collected information.

40. Factors such as 'nature' and 'gravity' of breach are factors to be taken into account by the DPB while determining monetary penalty under Section 33(2) of the DPDP Act.

As the list indicates, the breach of personal information can, in theory, yield harms having wide ranging ramifications extending past the individual person. In some cases, national security may also be impacted by the personal information compromised in a data breach.

However, linking actual consequences to data principals from specific data breaches remains difficult. Resultantly, many real-world harms suffered due to the studied data breaches may not be documented or correlated publicly.



VI. Insights Into Domestic Data Fiduciary Behaviour

(a) Typical Approach of Data Fiduciaries Towards Domestic Personal Data Breaches:

As implied by the figures above, the compliance with the RSPDI Rules and the IT Act on privacy has been imperfect among Indian data fiduciaries and processors. While ensuring adequacy of data security and handling practices to prevent targeted cyber-attacks can be a complex technical challenge, some fiduciaries did not even meet the simpler requirements, such as maintenance of an accessible privacy policy. Further, a significant portion (26.1 %) of the studied breach instances were found to be one in a series of repeated breaches occurring within the same fiduciary.

These identified trends point to important regulatory concerns and forewarn of the specific difficulties that the DPB may face in ensuring robust compliance with the ambitiously drafted breach reporting requirements of the DPDP Act. Simultaneously, the gaps highlighted also present a critical opportunity for the DPB and Central Government to refine the regulatory approach to data privacy in India.

Reporting/Notice of Breach to Authorities

The reporting of data breaches, despite the directions of CERT-In remain an area of concern for Indian data fiduciaries, with at least 47.8 % of personal data breaches during the concerned period discovered by independent persons separate from the data fiduciary. In many of the studied breaches, the fact of the breach was often published on social and traditional media platforms by these independent sources before a response was elicited from the concerned fiduciary and government authorities. In such cases, the affected personal data was usually put on sale or made available online on the darknet, enabling external persons to detect and verify the breach by examining the data. The existence of breaches



The failure of Indian data fiduciaries to detect such breaches at the first instance (before third party detection) points to systematic challenges in the processing of data in India. At the same time, the frequent discovery of such breaches by external researchers also raises the question of potential disincentives in the legal framework which prevent the timely reporting and disclosure by fiduciaries themselves.

Under the RSPDI Rules, in the event of an information security breach, the relevant entity would be required to demonstrate that they have implemented security control measures as per their documented program and information security policies, if called upon by CERT-In.⁴¹ Further, the CERT-In Rules enabled the agency to collect information relating to cyber security incidents to better discharge its multitude of functions.⁴² Inviting the scrutiny from a government agency of internal information and practices may appear a daunting proposition for data fiduciaries, however, CERT-In is mandated by law to maintain strict confidentiality in regard to such information, save for a limited set of circumstances relating to national security or incitement of cognizable offences. Further, CERT-In has been tasked with the responsibility to assist the incident-affected entities and take timely action for mitigation. Consequently, it would be in a data fiduciary's best interest to report a personal data breach or leak incident to CERT-In in a timely manner. Hence, the legal disincentives against breach reporting under the IT Act framework appear relatively limited.

This may be an indication that the largest disincentives currently operating on fiduciaries do not emanate from any tangible legal compliances. A 2021 academic paper studying the reputational damage associated with data breaches came to a related conclusion. Based on firm-level data for the period between 2002 to 2018, it found the largest and most salient breaches were associated with a 5-9% decrease in intangible capital (i.e. brand power and familiarity) for the concerned organization. However, the impact was not as significant for smaller breaches.⁴³ This evidence may explain, to some degree, the reluctance among fiduciaries to report large breaches in a timely manner. It should also be noted that a number of breached entities surveyed emanated from private sector entities and even listed companies. Such entities may also face significant impact on their market valuations as a consequence of reputational harm.

A second operational disincentive to take into consideration is the additional cost and resources that a data fiduciary must deploy as an incident response imperative. As the sophistication of cyber-attacks has continued to increase, so has the need for additional human capital to handle the fiduciary's response. A recent study into this aspect found entities suffering a breach to significantly increase their cyber security human capital in the subsequent quarter after suffering a breach, to bolster their incidence response capacity.⁴⁴

41. Rule 8, RSPDI Rules

42. Rule 13, CERT-In Rules

43. Makridis, Do Data Breaches Damage Reputation? Evidence from 43 Companies Between 2002 and 2018 (May 9, 2020) available at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3596933

44 Bana, Brynjolfsson, Erik, Wang, Sebastian and Wang, Human Capital Acquisition in Response to Data Breaches (June 30, 2023), available at <https://ssrn.com/abstract=3806060>



Apart from cybersecurity experts, the post-incident hiring patterns also emphasized the role of public-relations (**PR**) personnel, indicating importance of reputation management for the entity. In terms of absolute costs, IBM Security's Cost of a Data Breach Report⁴⁵ estimates the global average total cost of a breach to be USD 4.45 million (approximately INR 36.7 crore) in 2023, with this cost being the highest for the healthcare and financial sectors. However, the report also notes that the average cost of data breach in India is significantly lower at USD 2.18 million (approximately INR 18 crore).⁴⁶ While some components of this cost may be fixed at the instance of breach, others such as PR resource deployment would only become applicable after a breach is detected, acknowledged, and reported.

It is also essential to also consider what disincentives to reporting of breaches may potentially apply in the context of DPDP Act, once operational. Under the new law, a breach triggers many new responsibilities and potential legal liabilities for the data fiduciary. The data fiduciary must provide intimation of this breach to not only the DPB, but also to each data principal that is affected by the breach.⁴⁷ This exercise may become resource intensive as it would require identification of affected data principals on a real-time basis. This may also be beyond the capacity of the standard grievance redressal resources which a fiduciary may have in place for interacting with data principals, depending on the volume of records affected by a breach.

Immense complications can arise in the context of informing each affected data principal in a country like India which has achieved partial digitization. For instance, internet penetration in India has exceeded 821 million persons.⁴⁸ This includes data principals who would be able to take advantage of online intimation of breaches.

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

46. Ibid

47. Section 8(6), DPDP Act

48. Kantar Report, Internet in India 2023, IAMA, available at https://uat.indiadigitalsummit.in/sites/default/files/thought-leadership/pdf/Kantar_iamai_Report_20_Page_V3_FINAL_web_0.pdf

However, the figure still excludes a large proportion of individuals (up to 600 million) of India's 1.4 billion population, whose personal data may be collected in physical form, subsequently digitized and impacted by a data breach. Robust mechanisms for notifying such individuals would be difficult, if not impossible to develop. While Section 8(6) of the DPDP Act empowers the Central Government to specify the 'form and manner' of breach intimation, it is not clear if these complex aspects of intimating data principals will be addressed by subordinate legislation.

It also is important to note the lack of a carve-out or exception clause within the DPDP Act reporting obligation in India for data principals, as compared to other jurisdictions. It is not unusual practice for data fiduciaries in other regions to be exempt from the obligation to notify data principals regarding a personal data breach. For examples, the General Data Protection Regulation (**GDPR**) in Europe governs the breach response of fiduciaries under Article 33 and 34.⁴⁹ In the event of a personal data breach where there is a high risk to the rights and freedoms of natural persons, the 'controller' (fiduciary) must inform the data subject of the breach without undue delay. Information provided to the subject should include the likely consequences and measures taken by the controller to mitigate the effects. This provision enables does enable the controller to avoid this responsibility in the event that a personal data breach would not carry a 'high-risk' to the rights and freedoms of the data subject. The GDPR also accounts for the complexity and difficulty of this notice process. Hence, another exception is provided to controllers where communication would involve disproportionate effort. In such situations, 'a public communication or similar measure whereby the data subjects are informed' would suffice the requirements of the law.⁵⁰

It may be argued that the GDPR places too much discretion in the hands of the controller, while notifying a breach to the public. In this respect, oversight is also maintained by data protection authorities under the GDPR as any personal data breach resulting in a risk to rights and freedoms of natural persons will be intimated to the authority in any case.⁵¹ The supervisory authority, if it deems necessary, may still direct the controller to intimate the data subjects.⁵²

Further, in respect of the DPDP Act, the DPB, once notified of the breach by the fiduciary, may choose to inquire into the incident, and is vested with the powers of a civil court for this purpose. Data fiduciaries would therefore have to contend with the additional time and resources required during the quasi-legal inquiry process undertaken by the DPB.

49. Article 34, GDPR, available at <https://gdpr-text.com/read/article-34/>

50. Article 34(3)(c), GDPR

51. Article 33(1), GDPR, available at <https://gdpr-info.eu/art-33-gdpr/>

52. Article 34(4), GDPR

As a consequence of this process, the data fiduciary would face the potential outcome of a monetary penalty of up to INR 250 crore for the failure take reasonable security safeguards to prevent personal data breach, among other lapses, on the conclusion of the DPB’s inquiry.

Unlike the reporting of cyber incidents to CERT-In, which merely assists the reporting entity manage the incident, the intimation under the DPDP Act invites additional responsibilities, liabilities, and costs on the data fiduciary suffering on account of the personal data breach. The additional economic disincentives associated with reputational damage and the deployment more personnel towards breach handling, as noted above, would also continue to operate in such cases. A diagram illustrating the cumulative factors which data fiduciaries would have to take into consideration when regulated under the DPDP Act are compiled in the diagram below:

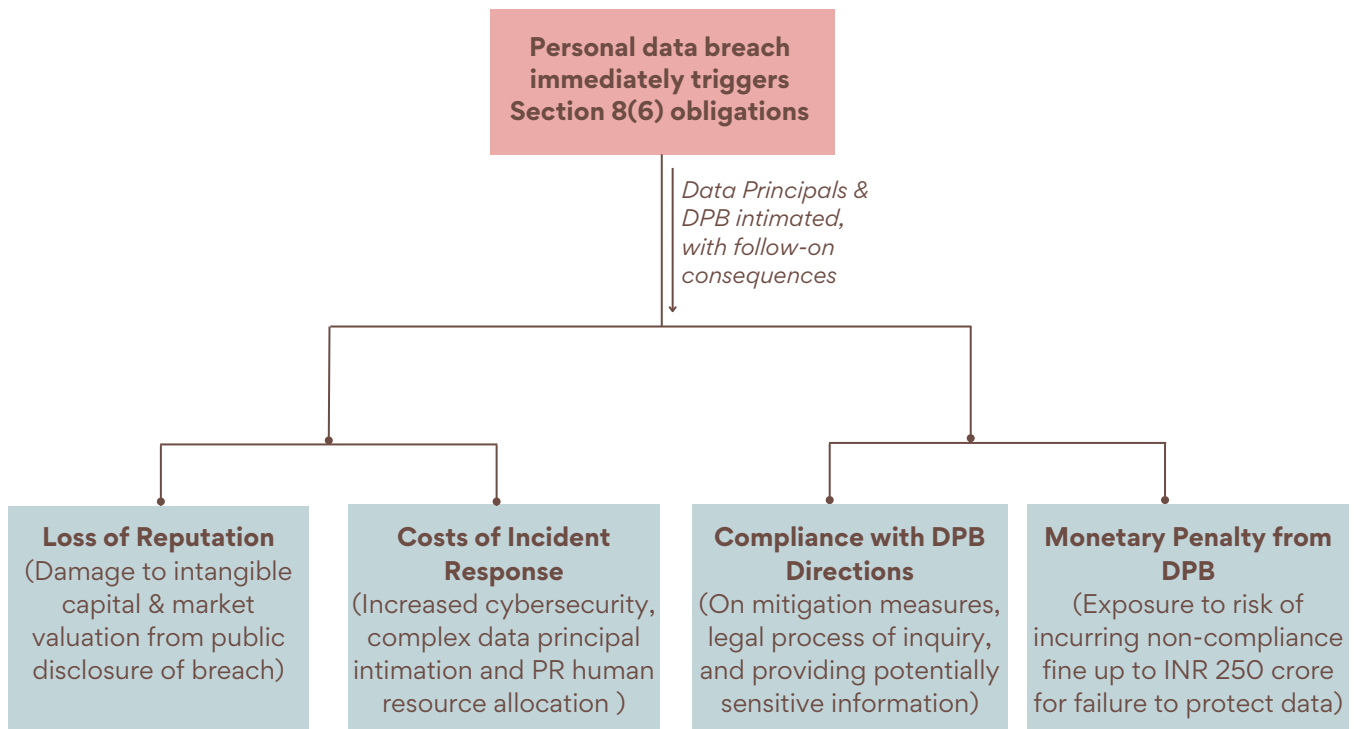


Figure 6: Disincentives & factors associated with triggering of notice/intimation DPDP Act obligations by data fiduciaries



Accountability of Data Fiduciaries

As illustrated above, the intimation obligations under Section 8(6) of the DPDP Act serve as a trigger for a host of liabilities, responsibilities and legal risks for a data fiduciary which may seek to disincentivize compliance to a greater degree than the reporting requirements under the current IT Act presently do. Likewise, it will be incumbent upon fiduciaries to anticipate and plan for the impact of these factors, as part of their DPDP Act compliance preparedness.

An examination of mechanisms within the DPDP Act to ensure the accountability of data fiduciaries on these aspects is also warranted. Under Section 8(1), a data fiduciary is explicitly responsible for complying with the act in respect of any processing of data by it, or on its behalf, regardless of the behavior or failures of a data principal. The provision also prohibits the fiduciary from contractually shifting this liability to another entity. To meet the prescribed standards, the fiduciary is also required to adopt technical and organizational capability, if it is lacking.⁵³ Further, the data fiduciary is required to protect personal data in its possession or under its control by taking 'reasonable security safeguards to prevent personal data breach'.⁵⁴

53. Section 8(4), DPDP Act

54. Section 8(5), DPDP Act

CASE STUDY 2

Bookchor Data Breach

In March 2021, an Indian online e-commerce platform Bookchor.com was reported to be breached by hackers resulting the exposure of the information of over 5 lakh users. Bookchor was an innovative digital platform developed by Indian entrepreneurs to facilitate the sale of pre-owned books at reasonable prices by users within the country. The breached information was placed by an anonymous user on a database sharing marketplace, which included names, email addresses, phone numbers, date of birth, physical addresses and MD5 hashed passwords. While the files were reportedly deleted from public access eventually, an unknown number of persons would have accessed and exploited the information contained in the leaked database up till that point. Once a database is breached, a data fiduciary is no longer in control of access or use of the exposed personal information. This can create severe risks for affected data principals such as fraud, phishing attacks, blackmail, and identity theft. Hence, alerting the impacted data principals of any high risks stemming from a breach is a crucial aspect of the DPDP Act. However, these obligations were not in existence in India at the time of the Bookchor breach, and are still pending enforcement. In the aftermath of this data breach, the founders were not responsive to the reported allegations and did not issue a public statement. It is not clear if any action was taken in response to the incident by the company or if authorities were alerted. Affected users of the platform were left with little recourse and no clear mechanism for seeking accountability from the unresponsive company. Many may not have been aware of the breach or the impact on their personal information. Such incidents are not uncommon where low compliance with breach reporting obligations and best practices in data protection is observed. Further details regarding this incident are available in the Annexure.

Essentially, accountability of a data fiduciary in the event of a breach would be assessed by the DPB on three parameters: (i) intimation to DPB and data principals in prescribed form and timeframe; (ii) adoption of technical and organizational standards for the data that are reasonable (including security safeguards); and (iii) non-contravention of any ancillary provision, or rule under the DPDP Act.⁵⁵ In each of these parameters, a potential fine of INR 250, 200 and 50 crore respectively may be attracted for non-compliance. While such fines (maximum of 250 crores or approximately USD 33 million) may not compare with those levied by Europe's GDPR⁵⁶ authorities, they far exceed the existing average cost of data breaches in India, valued at approximately INR 18 crore in 2023.

In the typical case of a significant domestic data breach incident, personal data stolen during the breach would be made available on the darknet.⁵⁷ In some of these cases the release of the data was a consequence of the failure of the fiduciary to pay a 'ransom' to the perpetrators.⁵⁸ In other cases, the explanation for the disclosure was less clear, or it was done for some financial gain. Where a 'ransom' is sought from a data fiduciary, it may be presumed that the fiduciary is aware of the breach, however, where the data is directly uploaded to the darknet, such awareness cannot be presumed. In these typical breach cases, the fact of the breach is detected only when the personal data is uploaded and identified (often by independent researchers), sometimes long after the breach has actually taken place. However, the obligations under Section 8(1) and 8(6) are categorical that fiduciary shall remain ultimately remain responsible for compliance, including for timely intimation of the personal data breach.

On a plain reading of the provision, the duty to intimate the DPB and data principals is triggered from the time of the actual breach. The DPDP Act does not clarify what amount of delay in providing notice would amount to a breach of obligations by the fiduciary and invite a penalty up to INR 200 crore. In the hypothetical instance of a typical data breach, where a fiduciary was otherwise compliant with security and technical requirements, the potential levy of a penalty would hinge on an assessment of the failure to provide notice of the breach. Factors such as the date / time of breach, date / time of detection by fiduciary, and date / time of disclosure of data would be relevant to making such an assessment.

55. The details of responsibilities placed on fiduciaries are awaited, as rules under the DPDP Act are yet to promulgated, at the time of writing this report.

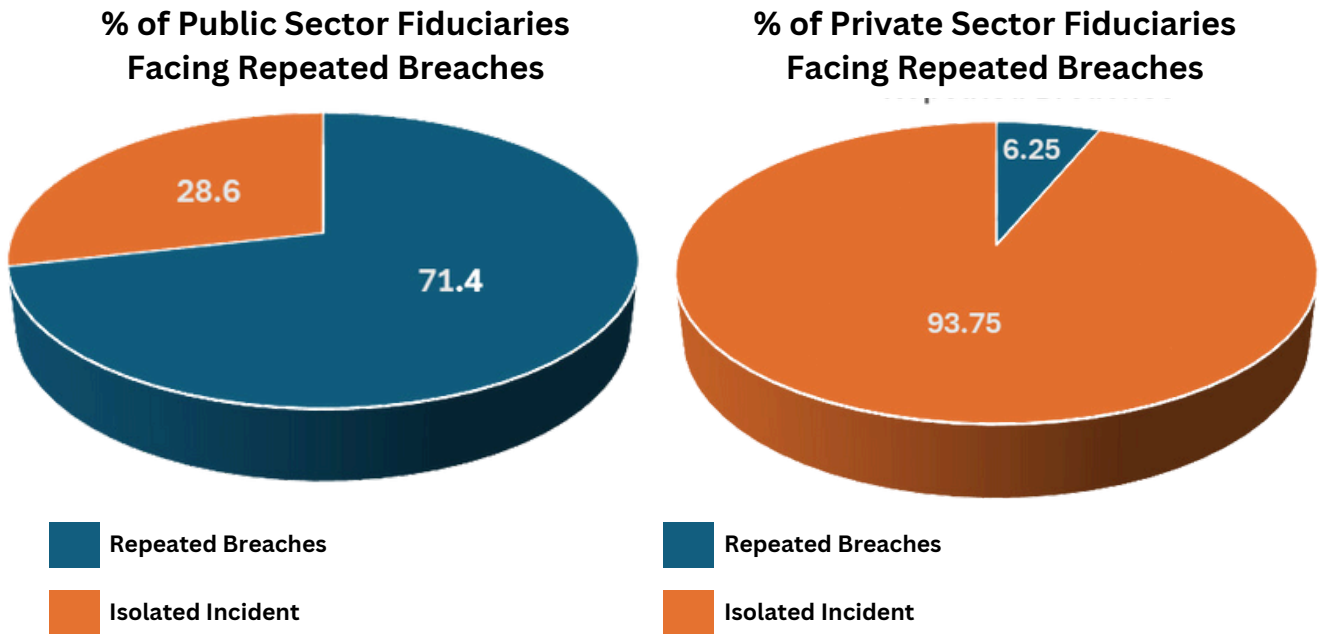
56. In the past GDPR authorities have levied fines in past instances ranging from a tens of million (available at [https://www.huntonprivacyblog.com/2020/10/30/ico-fines-marriott-international-18-4-million-for-security-breach/#:~:text=On%20October%2030%2C%202020%2C%20the,Regulation%20\(%E2%80%9C%20GDPR%E2%80%9D\).](https://www.huntonprivacyblog.com/2020/10/30/ico-fines-marriott-international-18-4-million-for-security-breach/#:~:text=On%20October%2030%2C%202020%2C%20the,Regulation%20(%E2%80%9C%20GDPR%E2%80%9D).)) to hundreds of million USD (available at <https://www.forbes.com/sites/kateoflahertyuk/2022/11/29/facebook-owner-meta-fined-275-million-by-irish-regulator/?sh=7b565ac91a37>)

57. Examples of some 'ransomware' attacks are the IHCL breach, available at <https://timesofindia.indiatimes.com/gadgets-news/taj-hotel-data-breach-what-the-company-has-to-say-ransom-demanded-conditions-set-by-hackers/articleshow/105461155.cms>; and Tata Power breach, available at <https://www.infosecurity-magazine.com/news/hive-ransomware-leaking-data/>

58. Examples include the ABFRL breach, available at <https://www.thehindubusinessline.com/companies/abfirl/article64895452.ece>; and Upstox breach, available at <https://timesofindia.indiatimes.com/business/india-business/upstox-face-data-breach-co-says-ramped-up-security/articleshow/82021166.cms>

(b) Private versus Public Sector Approach to Breaches

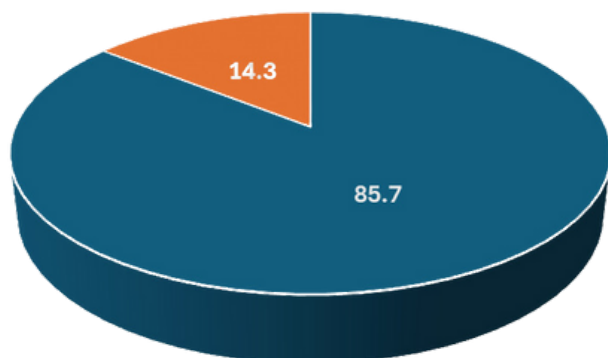
Another noteworthy insight from the study is the contrast in the handling of significant data breaches by public sector and private sector entities. The compiled data categorically indicates that public sector data fiduciaries are far more likely to face repeated instances of data breach, as compared to private sector fiduciaries. However, this data does not identify the precise cause of this variation. Difference in data security standards, a higher threat perception from nefarious actors, and greater access to citizen personal data may be some of the many potential factors at play for public sector entities.



Figures 7&8: Comparison of repeated breach instances among public & private sector fiduciaries

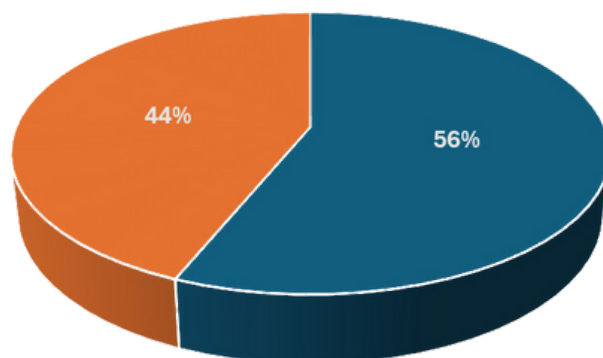
Further, it should be noted that public and private sector data fiduciaries also differ in terms of the transparency they provide in a post-breach context. Based on the review of news reports and available facts in the aftermath of studied data breaches, greater transparency was observed in the organizational response to the breach of Indian citizen data from public sector or government entities (examples include Air India, IRCTC, and AIIMS data breaches). This is evident regarding the kinds of remedial actions taken by the organization, with the details of such actions being disclosed to the public in most instances of public sector breaches. This information would often take the form of press releases and responses to parliamentary questions and indicates a greater array of institutional mechanisms of accountability available to citizens for public sector data fiduciaries. While some private sector fiduciaries may also have responded proactively to personal data breaches, public disclosure of the kinds of action taken was not provided to the same degree. It is also plausible that the higher levels of transparency may also have contributed to more reports of repeated breaches among public sector entities.

% of Public Sector Fiduciaries Taking Post- Breach Overt Remedial Action



■ Action Taken
■ Not Taken

% of Private Sector Fiduciaries Taking Post- Breach Overt Remedial Action



■ Action Taken
■ Not Taken

Figures 9&10: Comparison of overt remedial action taken by public & private sector fiduciaries

Lastly, consideration should be given to criminal legal action taken against the perpetrators of personal data breaches. The unauthorized access of personal data may result in criminal charges against the accused person under the IT Act and the Bharatiya Nyaya Sanhita, 2023 (earlier the Indian Penal Code). Among the breaches documented in this report, some form of criminal action (i.e. arrest of suspects) was taken against the perpetrators in public sector data breaches in 3 instances. In stark contrast, no clear evidence of arrest was found for any of the surveyed private sector data breaches.

This contrast may be indicative of greater stringency in the approach of law enforcement towards public sector breaches. However, the contrast may also be the result of a lack of reporting on the part of the private sector, as compared to active reporting on public sector breaches.

CASE STUDY 3

AIIMS Delhi Data Breach

In November 2022, the All India Institute of Medical Sciences (**AIIMS**) in New Delhi, one of India's premier healthcare institutions, experienced an unprecedented data breach. AIIMS regularly handled large volumes of patient health data, which can be of an extremely sensitive nature, and is classified as 'sensitive personal data or information' under the RSPDI Rules. The alleged ransomware attack crippled the hospital's digital infrastructure, and led to significant concerns about the misuse of sensitive personal, financial and medical information of about 40 million patients, including high-profile individuals. The attackers (allegedly of Chinese origin) reportedly infiltrated the hospital's servers, encrypting sensitive data and demanding a ransom for its release. The breach disrupted the hospital's operations, forcing the institution to revert to manual processes for several days. This placed immense pressure on the hospital while also impacting the quality of services provided to patients. Due to the high profile and sensitive nature of the information affected, as well as the status of AIIMS as a premiere central government establishment, CERT-In, Intelligence Fusion & Strategic Operations (**IFSO**) of Delhi Police, and the National Informatics Centre were roped in to coordinate a response to the breach. Due to the availability of greater resources with the Central Government, National Investigation Agency, Central Bureau of Investigation, and other agencies were also reported to be involved. It was later reported that the data in the 5 affected servers was eventually retrieved from a backup server. Further, servers used at AIIMS, Delhi were replaced with ones with newer configurations to enhance data security. Based on the recommendations of government agencies, security features like endpoint hardening, strong firewall policies, network segmentation, network access controls, endpoint detection and recovery solution etc. were implemented at AIIMS. The Central Government also directed security audits to be conducted at all AIIMS locations based on the inputs of CERT-In. The AIIMS breach sparked a debate in the Indian Parliament on the need for a comprehensive data protection law, stringent cybersecurity standards for institutions handling sensitive data, and timely breach notifications. The AIIMS personal data breach is exemplary of the greater resource availability, and demands for transparency and accountability that accompany public sector data breaches. These factors contributed to a prompt institutional response and security enhancements. Consequently, more visible response actions were typically observed, as compared to breaches occurring in the private sector. However, even the breach response of public sector breaches like AIIMS, Delhi do not address all crucial concerns, including mitigation of harms to data principals from the breach, and transparent intimation to affected patients. Further details regarding this incident are available in the Annexure.



(c) Identified Regulatory Gaps in Breach Compliance:

The insights elaborated above indicate some key concerns to ensure that data fiduciaries from both the public and private sector ably comply with the DPDP Act and meaningfully protect the privacy of Indian citizens. While some fundamental differences in public and private sector entity behavior can be demonstrated, these relate largely to activities and processes taking place after a breach is reported.

However, once a breach is detected by a fiduciary, the first step in the chain reaction, is the providing of notice to the DPB and data principals. This notice serves as the linchpin triggering subsequent action from the DPB and Data Principal. As recognized previously, the breach discovering entity in a number of instances tended to be a member of civil society or independent researcher and not the targeted data fiduciary itself. Further, only in a minority of studied cases could the mandatory reporting to CERT-In be verified. These observations raise questions over the willingness of domestic data fiduciaries to report breaches on their discovery. This report has noted that strong disincentives operate against such reporting. Further, these disincentives were heightened by the rigorous DPDP Act obligations operating on a data fiduciary after a breach.

These observations cumulatively highlight a potential point of failure in the reporting requirements for breaches under the DPDP Act. Under Section 27 of the DPDP Act, four trigger mechanisms for DPB involvement in a breach are provided:

- **Intimation by Data Fiduciary:**

The law places the burden of protection of personal data including reasonable security safeguards on the data fiduciary possessing / controlling such user personal data. It accordingly requires the data fiduciary to not only intimate the DPB of each personal data breach, but also the affected data principals. However, in the event this mechanism fails (as may be in the case of a generally non-compliant and disincentivized fiduciary), the DPB must rely on one of the other mechanisms.

- **Complaint by Data Principals:**

A data principal may complain to the DPB in respect of a personal data breach, as an exercise of their rights under the DPDP Act. However, detection of a data breach by a data principal would be unlikely due to their limited awareness and capacity. Further, attribution of the original source of a data breach can be a significant challenge in the case of personal data that is made available in an unauthorized manner, when discovered by a data principal. No resources are available at the disposal of most data principals to assist with this. Data principals would, in effect, be largely dependent on the data fiduciaries themselves for intimation of breaches. Additionally, it should be noted that the DPDP Act also does not provide strong incentives to enable complaints from data principals. The DPDP Act does not provide an effective method of compensation to data principals who successfully report breaches of their personal data. All sums realized by way of penalties under the act, are to be credited to the Consolidated Fund of India.⁵⁹ Further, if the DPB finds a complaint to be false or frivolous, it may go as far as to impose costs on the complainant.⁶⁰ Such provisions may actively discourage proactive data principals from filing genuine complaints, due to the difficulties in identifying the responsible data fiduciary, with multiple fiduciaries potentially storing similar kinds of personal data.

- **Reference from Government:**

Inquiry of breaches by the DPB can also take place upon a reference made by the Central or State Government. However, Governments may also be vulnerable to similar reporting disincentives as discussed for other data fiduciaries, in case of affected public sector entities (loss of reputation, cost of incident response, DPB inquiry and potential monetary penalty). As noted above, a number of personal data breaches pertained to public sector entities, and these were often repetitive in nature. This points to major privacy compliance concerns existing within government organization as well. Further, it would be unlikely for Central or State Government authorities to have an updated awareness of personal data breaches pertaining to the private sector, where a large number of breaches also take place.

- **Directions from Court:**

The final mechanism the DPB may rely on relate to court directions to inquire into a data breach. However, the utility of this mechanism may be limited. Generally, Indian judicial courts lack any specialized expertise for identification of personal data breaches. Here, it is relevant to also note Section 39 of the DPDP Act prohibits any civil court from having the jurisdiction to entertain any suits or proceeding in respect of any matter for which the DPB is empowered under this act. This further diminishes the role courts are likely to play in relation to data protection after the DPDP Act is implemented.

59. Section 34, DPDP Act

60. Section 28(12), DPDP Act



Presently suo-moto powers are not available 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. The shortcomings of these mechanisms of notice to the DPB are apparent from the explanation provided above. The findings of this report indicate that third-party reports form a decisive factor in preservation of privacy. The incorporation of suo-moto powers to inquire into breach reports, coupled with the necessary breach surveillance capability would make the DPB a more effective regulator for ensuring a higher percentage of personal data breaches is intimated in a timely manner and acted upon.

VII. Outlined Concerns from Analysis of Breaches and DPDP Act Obligations

By analyzing the unique characteristics of personal data breaches, entity-level responses and India's regulatory infrastructure, key concerns associated with DPDP Act-related data fiduciary compliance are noted below:

(a) Limited availability of breach response information of fiduciaries in India:

As indicated by the instances analyzed in this report, publicly available details about the entity-level responses of data fiduciaries in India, after a personal data breach were limited. This included information regarding enhancements in data security and the outcomes of investigation processes or arrests. The extent of available information also varied between public and private sector entities affected by breaches, with greater transparency, prompt remedial actions, and accountability observed in public sector data breaches. However, public sector entities were also found to be at a higher risk of repeated personal data breaches.

(b) Unsatisfactory levels of existence data protection compliance in India:

The data above illustrates that compliance with breach intimation and reporting requirements of CERT-In are not presently adequately adhered to. This is evident from the common observation of third parties alerting the public and authorities to numerous data breaches occurring within the country.

(c) Crucial role of independent third parties in breach monitoring:

In the absence of strong reporting compliance, the vital role played by independent researchers and cybersecurity firms in timely monitoring of personal data breach incidents cannot be overstated. The actions of these entities plays a crucial role in increasing data fiduciary accountability and highlighting to Indian citizens any specific threats to their individual data.

(d) Considerable difficulties in operationalizing breach reporting:

The analysis of data fiduciary responsibilities in the event of a breach paint a daunting picture of the compliance-heavy activity that impacts the intangible value of data fiduciaries, introduces massive resource and expense requirements, and exposes the entity to future legally liabilities. Of particular concern is the DPDP Act's obligation to intimate each affected data principal of the personal data breach under Section 8(6) of the DPDP Act. Coupled with a broad definition of 'personal data breach' and no exceptions to the intimation requirement, this obligation is far more stringent and challenging than those under established counterparts like the GDPR (further details provided in Part II of this Report). While considerable data breach intimation challenges may also provide a potential business opportunity for regulatory solutions providers and professionals,⁶¹ a drastic increase in the cost of breach compliance may be unavoidable for data fiduciaries in India.

(e) Disincentives to timely breach intimation:

As noted above, strong disincentives plague timely or reasonable personal data breach intimation to the data principals and authorities under Section 8(6) of the DPDP Act. These include the risks of high penalties, damage to reputation, massive resource undertaking and complexity of public intimation, and massive incident response costs. The DPDP Act's ability to protect the privacy of Indian citizens will be largely contingent on improving intimation compliance to enable the DPB to take prompt action in high-risk breaches. As will be discussed in Part II of the Report, CERT-In's public statements indicate that the majority of personal data breaches taking place in India are still undetected.


(f) Course of action in case of data breach denial:

In some of the surveyed personal data breach instances, the concerned data fiduciary was found to outright deny allegations of a breach in their database. In such an instance, the recourse to the data principals under the DPDP Act remains unclear, without the facts of breach accessible to concerned data principals, government or courts. This is due to the lack of suo-moto powers and breach monitoring capability provided to the DPB under the DPDP Act. Consequently, data principals are likely to continue to be reliant on third parties, and largely non-compliance data fiduciaries to be made aware of data breaches affecting them.

61. See exemplar Privacy & Cyber Response Solutions by EY, available at https://www.ey.com/en_in/services/assurance/privacy-cyber-response#:~:text=EY%20teams%20combine%20cybersecurity%20and,facts%20pertaining%20to%20a%20breach

(g) Need for significant preparations for DPDP Act reporting compliances by fiduciaries:

The findings of this report point to the considerable challenge before data fiduciaries in implementing compliance with intimation requirements, and the broader DPDP Act obligations, once the law is enforced. It is necessary for fiduciaries to overcome intimation hurdles and disincentives by making advanced preparations. This includes aspects such as creating an incident response plan, best practices in data storage, access and management, and significant resource allocations towards personal data breach incident management.



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