DSCI
PROMOTING DATA PROTECTION
A nasscom Initiative

The Future of Data Protection in India

A Roadmap for Regulators

PART 1

First edition: 2023

The Future of Data Protection in India

Published by:

DSCI
PROMOTING DATA PROTECTION
A nasscom Initiative

4th Floor, NASSCOM Campus
Plot No. 7-10, Sector 126, Noida
Uttar Pradesh 201303, India

The Future of
Data Protection in India

A Roadmap for Regulators

PART 1

Contents

Background

The history of data protection & privacy framework can be traced back to the Information Technology Act, 2000[1] (hereinafter referred to as IT Act, 2000) & the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011[2] (hereinafter referred to as SPDI rules). The IT Act, 2000 & the SPDI rules marked the brief advent of data protection & privacy framework in India. Organizations are required to adhere to the regulations outlined in the IT Act of 2000 and the SPDI rules, which necessitate the implementation of reasonable security practices and procedures to safeguard sensitive data.

In addition to the IT Act, 2000 & SPDI rules, Personal Data Protection Bill, 2019 (hereinafter referred to as PDPB 2019), was introduced in the Indian Parliament in December 2019.[3] PDPB 2019 was construed as a steppingstone acknowledging the need to have an exhaustive framework governing data protection & privacy. PDPB 2019 aimed to regulate the collection, storage, processing, and transfer of personal data of individuals in India. Furthermore, PDPB 2019 provided for the establishment of a Data Protection Authority (DPA) to oversee the implementation and enforcement of the law.[4]

However, in August 2022, PDPB (2019) was withdrawn[5], and the Central Government rolled out a new draft Digital Personal Data Protection Bill in November 2022[6] for public consultation. Finally, in August 2023, a revised version of the same was introduced and passed before the Parliament of India. The notified Digital Personal Data Protection Act 2023 ('DPDPA')[7] was devised with the intention to provide for the processing of digital personal data in a manner that recognizes the right of individuals to protect their personal data, the need to process personal data for lawful purposes and for other incidental purposes.[8]

In furtherance to a data protection regime being developed by the Centre, sectoral regulators in the country have released guidelines and advisories related to personal data protection. The objective of these guidelines and advisories is to ensure that organizations comply with best practices for managing personal data and have adequate safeguards in place to prevent unauthorized access, use, or disclosure. This paper seeks to examine these guidelines and advisories in detail to identify similarities and differences in the approaches taken by various sectors to address data privacy concerns.

Further, it is noteworthy that the DPDPA has introduced a comprehensive framework to tackle data privacy concerns. The purpose of this report, however, is to identify and examine the potential concerns arising from the Act while substantiating it with research from global data protection statutes and best practices. The report focuses on three main areas of concern, which will be discussed in detail. These concerns will be supported by evidence and analysis to provide a comprehensive understanding of the issues at hand. By identifying and addressing these concerns, it is expected that the DPDPA can be refined and improved to provide a more effective and robust framework for data protection in India. There are three thematic areas that have been identified in defining the scope of Part I of this report:

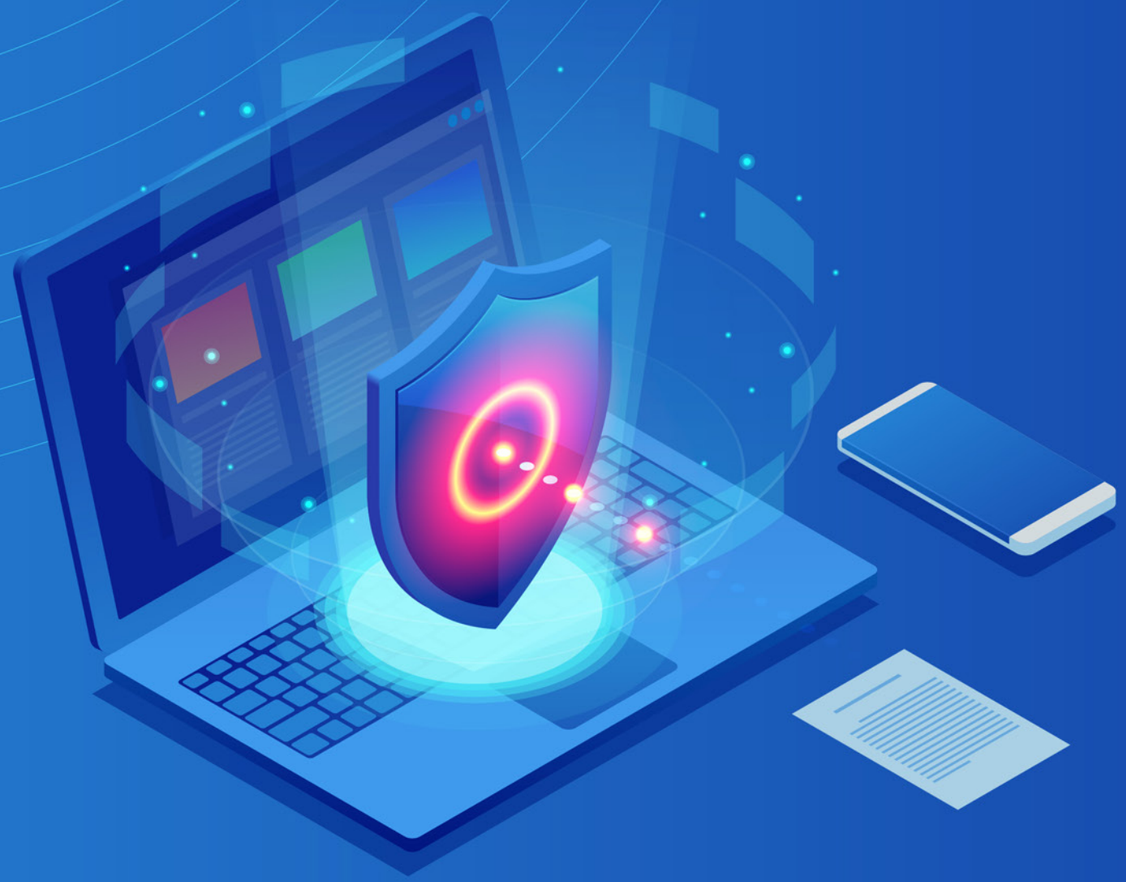
1. **Data Breaches:** The DPDPA defines a personal data breach and delineates the legal obligations on data fiduciaries and regulatory mechanisms for reporting data breaches. This section seeks to identify and address potential issues posed by the current definition and the framework for breach reporting requirements. The section examines the current definition of personal data breach as well as the obligations imposed on data fiduciaries. Through a robust analysis of the provisions proposed in the Act and a corresponding study of requirements globally, this section makes recommendations about changes that may be required in the provisions of the Act, as well as the guidelines that may be required in the future. The goal of these recommendations is to ultimately establish a more robust framework for regulation of personal data breaches in India.

2. **Consent managers:** Consent manager has been defined as a person that facilitates an accessible, transparent, and interoperable platform for individuals to give, manage, review, and withdraw their consent. The second section of this report highlights that there is a lack of comprehensive commentary and guidance surrounding consent managers, which has resulted in confusion and uncertainty regarding their roles and responsibilities. The suggestions also emphasize the need for the development of detailed guidelines that outline the best practices for consent managers, address concerns surrounding their use, and provide additional safeguards to protect data.

3. **Cross Border Data Transfers:** Under the DPDPA, transfers of personal data outside India are permitted except to jurisdictions which are notified as being restricted. This section of the report seeks to identify the challenges and issues posed by the current legal framework and provides recommendations for the addressal of these potential challenges. It also highlights that addressing these challenges / issues will create a more robust framework and will ease the compliance burden on the data fiduciaries.

Part 1 of this report delves into three key areas pertaining to data protection regulation in India: Data Breaches, Consent Managers, and Cross Border Data Transfers.

Overall, while India's data protection framework is still evolving, the Digital Personal Data Protection Act, 2023, along with other laws and guidelines, exhibits a comprehensive framework for regulating data breaches and protecting the privacy and security of personal data in India. This report aims to provide recommendations for future guidelines that can simplify the compliance obligations imposed by the current Act and strike a balance between being strict and easy to comply with. The purpose is to identify the challenges faced by data fiduciaries under the current Act and suggest practical solutions to streamline compliance. By analyzing the global best practices and examining the current legal framework in India, this report intends to propose measures that can facilitate the creation of a more efficient and effective framework for the implementation of provisions related to data breaches, consent managers and cross border data transfers.



Section 1

Navigating Data Breaches and Breach Reporting Mechanisms

Executive Summary

This section will examine and explore the regulatory practices revolving around personal data breaches globally. Taking reference from the global practices across jurisdictions, it examines the existing framework for personal data breaches proposed under the Digital Personal Data Protection Act ('DPDPA') 2023. The aim to put forth recommendations for regulatory changes that may be required to implement the legal requirements effectively and efficiently around data breach mitigation, reporting, and notification.

The first chapter puts forth a comprehensive outline of what personal data breaches are, the distinction between security incidents, data breaches, and personal data breaches, and their impact on organizations and individuals. Following this, it expands on the understanding of what constitutes a personal data breach by looking into the definition of a personal data breach as proposed under the DPDPA and examines the distinction between data breaches and unauthorized processing. The ultimate purpose is to review the definition and outline any challenges that may arise from the conflation of incidents of unauthorized processing with breach incidents.

After outlining the conceptual notions of a personal data breach, the succeeding chapter delves into the regulatory requirements in other jurisdictions. The review focuses on regulations in the APAC region (Singapore, South Korea, Japan, and Australia), references to the obligations under GDPR in the European Union and derives insights on the regulatory trends regarding personal data breaches from the regulations in Brazil. This chapter looks at eight key parameters which define legal obligations surrounding personal data breaches:

i. prescribed time for breach reporting and the supervisory authority to which the breach is to be reported,
ii. scope of a personal data breach,
iii. criteria for reporting a breach to the supervisory authority,
iv. criteria for notifying a breach to data principals,
v. responsibility for reporting a breach,
vi. contents of a breach report to the supervisory authority,
vii. contents of a breach notification to the data principals, and
viii. the consequences of non-compliance with these obligations.

Analyzing these parameters reveals common practices, trends, and legal requirements across jurisdictions, informing effective data protection regulations. This chapter further explores guidance from Data Protection Authorities, providing a comprehensive review of breach implications, obligations, and organizational responsibilities.

The third chapter examines sectoral requirements regarding data breaches across the banking & finance, insurance, healthcare, and telecom sectors. This portion of the report sheds light on the current legal landscape surrounding breach reporting and highlights the challenges associated with multiplicity of obligations.

To understand the regulatory approaches in harmonizing sectoral requirements with national data protection laws, it highlights the prevailing data breach regime in various jurisdictions such as Singapore, Brazil, India, etc.

The final chapter provides recommendations derived from overall research and analysis. These recommendations are intended for regulatory authorities and policymakers to consider, catering to the needs of industry stakeholders and data principals.

1

Understanding Personal Data Breaches

1.1 How do personal data breaches occur?

A data breach refers to the deliberate or accidental exposure of confidential information to unauthorized individuals. In today's digital age, data holds immense importance for enterprises, making data leakage a grave concern. Such incidents pose severe threats to organizations, leading to substantial reputational harm and financial setbacks. Further, data breaches can jeopardize an organization's long-term stability. These breaches may result from internal or external sources, whether intentional, such as data theft by intruders or insider sabotage, or inadvertent, like accidental disclosure of sensitive information by employees or partners.[9]

Data breaches can occur because of stolen information, deployment of ransomware, recording of keystrokes, phishing attacks, etc.[10]

At this stage, it would be important to understand the conceptual contours of what constitutes a ''data breach', more specifically, a 'personal data breach'.

While a personal data breach is a type of security incident, not all security incidents are considered personal data breaches. It is crucial to delineate these concepts, as this understanding would form the basis for defining personal data breaches in the country's data protection law. The succeeding paragraphs therefore, aim to explore the intersection between personal data breaches and security incidents.

1.2 Personal data breaches as security incidents

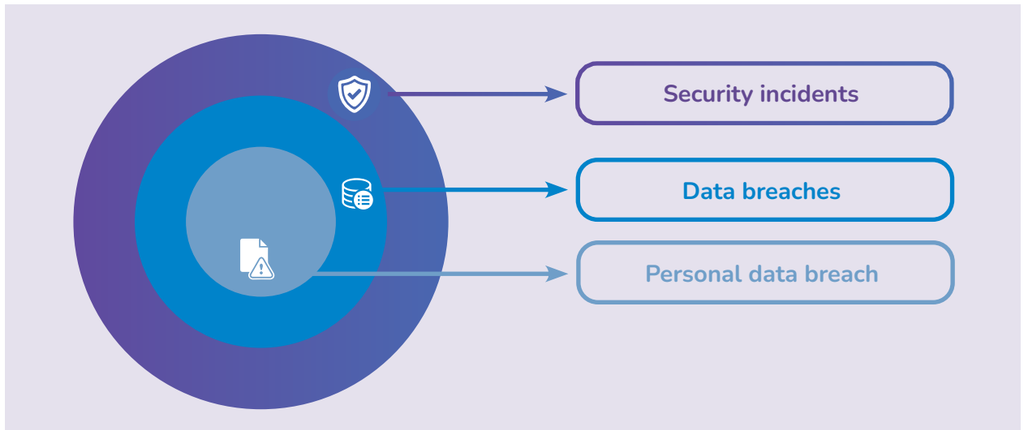
'Personal data breach' means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored or otherwise processed[11] This includes breaches that are the result of both accidental and deliberate causes.[12] A personal data breach can broadly be defined as a security incident that has affected the confidentiality, integrity or availability of personal data.[13] In short, a personal data breach occurs whenever any personal data is accidentally lost, destroyed, corrupted or disclosed; if someone accesses the data or passes it on without proper authorization; or if the data is made unavailable and this unavailability has a significant negative effect on individuals.[14]

According to Peter Carey, a personal data breach is "any incident in which personal data is accidentally or unlawfully destroyed, lost, altered, disclosed, or accessed". He notes that a personal data breach can result from a variety of causes, including human error, technical failures, and deliberate attacks.[15]

From the above definitions, personal data breach may be generally understood to be a security incident that involves the exposure, loss, theft, destruction, or alteration of personal information — either intentional or accidental.[16]

A security incident, however, is defined as "An occurrence that actually or potentially jeopardizes the confidentiality, integrity, or availability of an information system or the information the system processes, stores, or transmits or that constitutes a violation or imminent threat of violation of security policies, security procedures, or acceptable use policies."

There exists a distinction between the conceptual notions of a security incident, a data breach, and a personal data breach. To understand the scope of this document, it is pertinent to clarify these distinctions at this juncture.



The above illustration explains that security incidents constitute the wider ambit of scenarios which impact an organization's systems, including changes to software or hardware without the consent of the organization, mala fide disruption of services[17], and violations of internal security policies by legitimate individuals.[18]

Additionally, data breaches also constitute some part of the larger bucket of security incidents. It is therefore accurate to state that, 'all data breaches are security incidents but not all security incidents are categorized as data breaches'.[19] Finally, not all data breaches amount to personal data breaches and be governed by personal data protection laws.

The below illustrations further illuminate this distinction-

i. **Security incidents vis-a-vis data breaches:** As highlighted above, malicious, coordinated disruption of an organization's services amounts to a security incident. For instance, if the website of an airline company is faced with a distributed denial-of-service (DDoS) attack, this would amount to a security incident as it would lead to overwhelming the airline's website and its network traffic, making it impossible for users to access and use the website. While this is a security incident, it does not necessarily amount to a data breach as long as the confidentiality, integrity, and availability of any data is not affected.

ii. **Data breaches vis-a-vis personal data breaches:** It is also important to highlight that not all data breaches would amount to a personal data breach. For instance, if the proprietary information of an IT company is stolen from its servers, such an incident would qualify as a data breach but not as a personal data breach. Therefore, if the data in question does not contain any personally identifiable information, it does not amount to a personal data breach.

In conclusion, personal data breaches

are recognized as security incidents in both academic writings and statutory regulations. By recognizing personal data breaches as a type of security incident, organizations can implement measures to prevent and mitigate such incidents, safeguarding individuals' privacy and confidentiality. Therefore, it is important for the framework on personal data breaches under the DPDPA to recognise the nexus between "security incidents" and "personal data breaches".

The upcoming paragraphs analyse the definition of personal data breaches outlined in the Digital Personal Data Protection Act. The research below provides insights into the differences between unauthorized processing of personal data and data breaches. By examining how these incidents are defined and addressed in different regulatory frameworks, a more comprehensive understanding of the complexities involved in addressing such incidents has been provided.

1.3 Definition of Personal Data Breach in DPDPA

PDPB 2019 defined personal data breach as "any unauthorized or accidental disclosure, acquisition, sharing, use, alteration, destruction of or loss of access to, personal data that compromises the confidentiality, integrity or availability of personal data to a data principal".[20] While the DPDPA 2023, defines a personal data breach as," any unauthorized processing of personal data or accidental disclosure, acquisition, sharing, use, alteration, destruction of or loss of access to personal data, that compromises the confidentiality, integrity or availability of personal data".[21]

It is pertinent to note that the definition of 'personal data breach' has evolved over the period of 3 years, i.e., since the withdrawal of PDPB 2019 and the advent of DPDPA 2023. DPDPA 2023 has widened the scope of 'personal data breach' by including 'unauthorized processing of personal data' within the ambit of 'personal data breach.'

Unauthorized processing of personal data, however, can be broadly categorized as the processing of personal data which falls within one of the following three scenarios:

- Processing of personal data which is not authorized by the data fiduciary;
- Processing of personal data not permitted by law; or
- Processing of personal data which is in violation of the purpose for which the data was originally collected.

Both personal data breaches and unauthorized processing can have serious consequences for data subjects and data fiduciaries. Data subjects may suffer harm or loss because of their personal data being compromised, while data fiduciaries may face fines, legal action, or reputational damage.[22]

DPDPA 2023 overlooks the distinction between 'unauthorized processing of personal data' and data breaches. This may lead to a situation where both scenarios are treated similarly in the adjudication process by the Data Protection Board, resulting in duplicate penalties and shared obligations for data fiduciaries. For instance, if the data fiduciary fails to notify a breach, the data fiduciary may face penalties of up to Rs. 200 crores, which is the same penalty imposed for non-fulfillment of additional obligations related to processing children's personal data (also considered unauthorized processing). This lack of differentiation may lead to redundant/dual consequences for data fiduciaries in such cases.

The conflation of 'unauthorized processing' with 'personal data breaches' may also inadvertently lead to a misalignment of internal measures taken by data fiduciaries to identify and mitigate incidents of unauthorized processing.

Preventing unauthorized processing of personal data is the first and foremost step a data fiduciary undertakes to ensure lawful processing of personal data. Consequently, adopting preventive measures to forestall unauthorized processing becomes imperative to ensure the lawfulness of processing. Similarly, adopting mitigating efforts in the event of a 'data breach' becomes essential for the safeguarding of personal data.

The preventive measures to proscribe the unauthorized processing of personal data may include assigning passwords, granting limited access to systems, audit trails, log-on procedures etc.,[23]

Whereas mitigating efforts for data breach may include maintaining offline, encrypted backups of data and regularly testing the backups, maintaining a basic cyber incident response plan, conducting regular vulnerability scanning, implementing firewalls, etc.[24]

As highlighted above, ensuring that personal data processing is carried out in an authorized manner is the primary consideration to ensure compliance with the principles of lawfulness, fairness, and transparency. The below illustration further exemplifies the distinction between unauthorized processing and personal data breaches:

When a social media platform faces a situation where personal data collected and processed by them is leaked on an online hacking platform, it falls under the category of data breach. On the other hand, if the social media platform does not offer adequate information about their processing activities in their privacy notice to users, leading to the absence of informed consent by the users, this may be considered an instance of unauthorized data processing.

While the General Data Protection Regulation (GDPR) defines a data breach 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" (Article 4(12)), the UK Information Commissioner's Office (ICO) defines a data breach "is a security incident that has affected the confidentiality, integrity, or availability of personal data" (ICO, 2021).[25]

Similarly, the GDPR defines unauthorized processing as processing of personal data without the consent or knowledge of the data subject or in violation of the purpose for which the data was originally collected (Article 4(2)), the UK ICO defines it as the processing of personal data in a manner that is not authorized by the data controller or permitted by law (ICO 2021).[26]

Further, the Australian Privacy Act 1988 and the Office of the Australian Information Commissioner (OAIC) also differentiate between the two concepts in some manner. Principle 6 of the Australian Privacy Principles mentioned under the Privacy Act 1988 elucidate the obligation of the organization to process the data for the primary purpose only and states that:

"An APP entity can only use or disclose personal information for a purpose for which it was collected (known as the 'primary purpose'), or for a secondary purpose if an exception applies."

Whereas, a data breach is defined as an unauthorized access or disclosure of personal information, or loss of personal information.

The above-mentioned paragraphs outline the importance of keeping the two concepts, unauthorized processing and data breaches, distinct from each other and detail the challenges arising from the consolidation of these two separate concepts. The next portion of this chapter further catalogs the challenges which may be encountered by the organizations (data fiduciaries) and the supervisory authorities by the conflation of these two topics.

1.4 Conflation of Personal Data Breach and Unauthorised Processing: Implications and Way Forward

Defining personal data breaches in a manner which includes unauthorized processing can create three distinct sets of challenges for organizations which process personal data. These are highlighted below:[29]

Response and Mitigation Strategies

The approaches for responding to and mitigating unauthorized processing and data breaches are entirely distinct.

→ Prevention of unauthorized processing of personal data generally involves compliance with the principles of Preventing unauthorized processing of personal data involves adhering to principles such as Purpose Limitation, Lawfulness, Fairness and Transparency. On the other hand, responding to and mitigating a data breach typically involves reporting to supervisory authorities, notifying data subjects if necessary, and implementing security measures. Hence, it is evident that both the scenarios are divergent and require separate response and mitigation strategies.

Reporting and Notification Requirements

The obligation to report and notify data breaches to both the supervisory authority and the affected individuals differ significantly.

→ Reporting and notification requirements of breach incidents and unauthorized processing incidents are completely diverse. Depending on the jurisdiction, organizations may be required to report data breaches to data protection authorities or notify affected individuals. If unauthorized processing is included in the definition of a data breach, incidents which exemplify as unauthorized processing but do not qualify as data breach will be erroneously reported to data protection authorities as "data breach" incidents. Organizations may need to determine whether reporting or notification is required even if there was no unlawful access or disclosure of personal data.

Enforcement Mechanism

Penalties for data breaches and unauthorized processing are separate and are not commonly applied across different jurisdictions.

→ The enforcement mechanism for both the scenarios remains separate across the globe. The penalties imposed on the data fiduciary in the event of unauthorized processing are traditionally different and distinct than the penalties imposed in the case of a data breach.

Further, it is important to highlight that the DPDPA already imposes penalties for unauthorized processing of personal data. The penalties are outlined in Schedule of the Act and include failing to fulfill additional obligations concerning children under Section 9 and not complying with the provisions of the Act, such as processing data only for lawful purposes with the Data Principal's consent as outlined in the Act.

Therefore, it is worth considering that if the definition of unauthorized processing is included within the definition of a personal data breach, it could result in duplicative penalties for the same offense.

In conclusion, it is clear that data breaches and unauthorized processing are distinct concepts and should be treated as such. While the Digital Personal Data Protection Act incorporates unauthorized processing within the definition of data breaches, it is important to recognise the underlying distinction between these concepts. This will enable effective regulation and compliance with data protection laws, ultimately safeguarding the privacy and security of individuals' data.

In the implementation of the DPDPA it will therefore be important for the Data Protection Board to take into account the nuanced distinction between unauthorised processing and personal data breaches. In the absence of the same, Data Fiduciaries may end up bearing hefty and dual costs for a singular instance of non-compliance.

2

PERSONAL DATA BREACHES – A COMPARATIVE PERSPECTIVE UNDER DATA PROTECTION LAWS

This chapter undertakes a study of various obligations under data protection regulations in APAC and EU, such as complying with prescribed criteria and thresholds, and promptly notifying supervisory authorities and affected individuals. Identifying the commonalities in obligations, it brings to light guidance for personal data breach reporting under the data protection framework in India.

The obligation to report and notify personal data breaches is mentioned under Section 8(6) of the DPDPA. This Section requires that in the event of personal data breach, the Data Fiduciary shall notify the Board and each affected Data Principal, in such form and manner as may be prescribed.[30]

Personal data breaches are a significant issue in today's interconnected world, impacting individuals and organizations alike. It is essential to grasp legal responsibility due to the increasing occurrence and seriousness of these breaches. Compliance with data protection laws in different jurisdictions can be achieved by studying global regulations and best practices. This chapter undertakes a study of various obligations under data protection regulations in APAC and EU, such as complying with prescribed criteria and thresholds, and promptly notifying supervisory authorities and affected individuals. Identifying the commonalities in obligations, it brings to light guidance for personal data breach reporting under the data protection framework in India.

2.1 Data Breach Response: A Comprehensive Examination of Breach Reporting Obligations:

There are no standard criteria or thresholds for breach reporting requirements as these criteria and thresholds vary across jurisdictions. Singapore, South Korea, Brazil, Japan, European Union and Australia prescribe an obligation to report a data breach to the supervisory authority in case it affects more than 500/1000 or more individuals, or the breach is likely to result in a high risk to natural persons[31]. Similarly, the respective laws of these jurisdictions provide

an additional obligation to notify the affected individuals in case the breach is likely to result in harm or damage to the individual whose personal information has been compromised.

Content of a Breach Report or Notification and Timelines

Global regulations prescribe the content of the above-mentioned notifications to make sure that affected data principals adopt adequate precautions to avoid harmful consequences of breach. The notifications generally include the nature of the personal information that has been breached, the number of individuals affected by the breach, the cause and extent of the breach, description of likely consequences, etc.

Furthermore, emphasis is placed on the data fiduciaries' liability to report data breaches in the prescribed time which helps data fiduciaries to come up with a quick response plan to address data breaches. European Union and Singapore prescribe 3 days' time to report a breach incident[32], while on the other hand Brazil, South Korea, Japan, Australia do not specify time for reporting data breach. Instead, the regulations state that an organization should report a breach incident as soon as the entity becomes aware of the breach[33]. This makes it necessary for these organizations to come up with an incident response plan to rectify the incident within a reasonable time in order to avoid leakage of as much personal information as possible. Similarly, as per the regulatory framework of Singapore, Japan, European Union, Brazil, South Korea & Australia, the obligation to inform supervisory authority of the breach incident falls upon the data fiduciary.

Notifiability of a data breach: Taking a risk-based approach

Organizations are required to assess whether a data breach is notifiable as it is likely to result in significant harm[34] to the affected individuals. Given the likelihood of harm arising from a data breach, notification ensures affected individuals are aware and able to take steps to protect themselves (e.g., change password, cancel credit card, monitor account for unusual activities).

To provide certainty to organizations on the data breaches that are notifiable, the Personal Data Protection (Notification of Data Breaches) Regulations 2021 provides the personal data (or classes of personal data) that is deemed to result in significant harm to affected individuals if compromised in a data breach. Where a data breach involves any of the prescribed personal data, the organization will be required to notify the affected individuals and the Commission of the data breach.[35]

Similarly, other APAC jurisdictions set a concrete threshold for reporting obligations and prescribe criteria for the organizations to report breaches to the authorities and notify the affected individuals. Personal Information Protection Commission (PPC) of Japan prescribe guidelines that suggest that business operators (i) make necessary investigations and take any necessary preventive measures, and / or (ii) make public the nature of the breach and steps taken to rectify the problem, if appropriate and necessary.[36]

Further, entities functioning in the Australian jurisdiction must report an eligible data breach. An "eligible data breach" occurs when all the conditions prescribed are satisfied. The Office of the Australian Information Commissioner (OAIC) has issued a Notifiable Data Breaches (NDB) scheme wherein any organization or agency that are covered under the Privacy Act 1988 must notify affected individuals and the OAIC when a data breach is likely to result in serious harm to an individual whose personal information is involved.

There are a number of key criteria to examine when determining if "serious" harm is likely to result from a breach which should be assessed holistically and taken into account: the kinds of information, sensitivity, security measures protecting the information, the nature of the harm (i.e. physical, psychological, emotional, financial or reputational harm) and the kind(s) of person(s) who may obtain the information. The OAIC has also released several guidance notes relating to the regime which include topics such as the security of personal information and whilst these are not legally binding, they are considered industry best practice.[37]

> To properly address data breaches, breach notification is a vital process with staged actions and protocols. The impact on operations and reputation is reduced by using a staged approach, minimizing further harm.

Implementing a Phased Approach for Data Breach Reporting

Globally, guidelines issued by supervisory authorities such as the European Data Protection Board and Brazilian Data Protection Authority, Personal Information Protection Commission of Japan provide for the reporting of breaches in a phased manner in the event the nature of the breach requires so.[38]

The Guidelines on breach reporting issued by the European Data Protection Board (EDPB) state that depending on the nature of a breach, further investigation by the data controller may be necessary to establish all the relevant facts relating to the incident.[39] Article 33(4) of GDPR therefore states that where, and in so far as, it is not possible to provide the information at the same time, the information may be provided in phases without undue further delay. This means that the GDPR recognizes that controllers will not always have all the necessary information concerning a breach within 72 hours of becoming aware of it, as full and comprehensive details of the incident may not always be available during this initial period. As such, it allows for notification in phases.[40]

In Brazil, as per the guidelines issued by the Brazilian data protection authority (ANPD), if the data controller does not have complete information about the incident or is unable to notify all holders within the recommended period, the communication to the ANPD may be carried out in stages: preliminary and complementary. The data controller must justify the impossibility of complete communication. Supplemental communication should be sent promptly, within 30 calendar days of the preliminary communication.[41]

Similarly, the guidelines issued by Personal Information Protection Commission (PPC), Japan prescribe two stages of reporting obligations: a preliminary and a final report. The amended APPI requires a business operator to submit a preliminary report "promptly after the recognition of the occurrence of a potential data breach" and further prescribes the submission of a final report within 30 days from the recognition

of a data breach (60 days is the deadline for data breaches likely to have been committed for an improper purpose, such as a cyberattack).[42]

Manner of reporting and notifying a data breach - Ensuring Consistency and Transparency

In addition to the notification obligations of organizations with respect to a data breach, it is also imperative to specify the manner in which such notifications are to be made. Global authorities prescribe guidance/ guidelines which attempt to eliminate ambiguity and ensure consistency in compliance.

In Australia, entities with obligations to comply with the Privacy Act must comply with the mandatory data breach notification regime. The regime requires that where it is not practicable to notify the affected individuals individually, an organization that has suffered an eligible data breach must make a public statement on its website containing certain information as required under the Privacy Act and take reasonable steps to publicize the contents of the statement.[43] The notification to the OAIC should be made using the online Notifiable Data Breach form.[44]

In Brazil, the Brazilian data protection authority's ('ANPD') Inspection General Coordination published a new form for sending security incident reports by data fiduciaries to the ANPD. The form specifies various methods through which affected individuals will be notified. These methods include individual written communication, public announcement on the controller's website, social media or applications, individual written communication with acknowledgement of receipt. (Electronic message / letter / email, etc.)[45]

Similarly, the Personal Data Protection Commission (PDPC) of Singapore issued an Advisory Guidelines on Key Concepts in the Personal Data Protection Act. The guidelines categorically mention that as there are many different modes of notification that could evolve with technology, organizations may determine the most efficient and effective mode of notification to inform affected individuals. The guidelines further elucidate the manner of providing notification to the affected individuals by way of a recommendation wherein the individuals are informed through personal phone calls by trained personnel to address any immediate questions and allay their concerns.[46]

> While the DPDPA specifies that data fiduciaries are obligated to inform the board and affected data principals in the manner as may be prescribed (Section 8(6)), it is important for the prescribed rules to adopt a clear, concise, and nuanced approach to notification, in line with global regulations. This could involve undertaking a graded approach for reporting breaches to the relevant authorities and notifying individuals whose data has been impacted.

Hence, it is evident that global data protection authorities have implemented statutory obligations in a consistent manner while allowing for necessary adaptations. For example, the EDPB guidelines on reporting a data breach permit organizations to carry out the reporting process in stages to avoid compliance burdens. Similarly, the OAIC recommends the use of an online form to report the breach to supervisory authorities, while the PDPC of Singapore exemplifies making personal phone calls through trained professionals to inform affected individuals about breaches.[47] Global data protection statutes and authorities prioritize compatibility and coherence across sectors operating internationally. However, the DPDPA lacks clarity and uniformity in this aspect. The forthcoming chapter explores the limitations of the DPDPA's regulatory approach and emphasizes the significance of sectoral regulatory authorities. With a rise in breach incidents, sectoral regulatory authorities can ensure compliance within their industries. The chapter provides an overview of breach incidents globally in each sector, highlighting the importance of sector-specific data protection measures. Overall, it emphasizes the need for a sector-specific approach to data protection for an effective and consistent regulatory framework.

3

Data breach requirement under different sectors

This chapter intends to analyze the sectoral regulations and statutes that describe the data breach obligations for different sectors such as insurance, banking & finance and healthcare. These sectors are more vulnerable to security incidents since these sectors involve large scale processing of personal & sensitive personal data. Consequently, the regulation of these sectors requires highly focused supervisory authorities to yield effective remedial actions promptly.

In the Banking Finance Services and Insurance sector (BFSI), India has been at the forefront of attacks targeted at the Asian region, with 7.4% of the targeted attacks in the year 2022 being towards the Indian subcontinent. Whether it was nationalized banks, cryptocurrency exchanges or wallets, NBFCs, or credit card data leaks, India emerged as Asia's newfound hotspot for cyberattacks.[48]

Further, in 2023, Over 1.6 million cyber-attacks were blocked on Indian insurance companies every day in January. On average, insurance sector applications face 430,000 attacks each, which is close to the overall average of 450,000 attacks per app across all industries, according to the report by Indusface, an application security SaaS Company funded by TCGF II (Tata Capital).[49]

Additionally, the healthcare industry in India had faced 1.9 million cyberattacks in the year 2022, as per the data published by cybersecurity think tank CyberPeace Foundation and Autobot Infosec Private Ltd. The attacks came from a total of 41,181 unique IP addresses.[50]

The data above emphasizes the vulnerability and hazards that the insurance, banking and finance, and healthcare sectors face. As a result, regulatory and supervisory entities have built strong frameworks to reduce cyber threats and protect personal data. The following paragraphs outline the guidelines provided by authorities in different sectors.

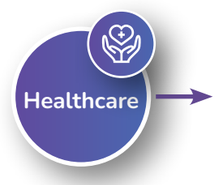
3.1 Sectoral regulations in India: Compliance Obligations and Statutory Guidelines Across Various Sectors

In India, there are separate reporting requirements for companies operating under different sectors. Under the IT Act and the Directions issued by Computer Emergency Response Team (CERT-In), service providers, intermediaries, data centers, government organizations and body corporates are required to report certain kinds of cyber security incidents (including data breaches) to CERT-In. The Directions mandate that such a report must be filed within six hours of noting or being notified of the incident in the prescribed format.[51]

Further, there are also various sector-specific reporting obligations that apply to entities in different sectors:[52]

In India, the insurance sector is governed by Insurance Regulatory & Development Authority of India (IRDAI). IRDAI (Protection of Policyholders' Interests) regulations 2017, requires the insurer to maintain total confidentiality of policyholder information, unless it is legally necessary to disclose the information to statutory authorities. Moreover, the IRDAI (Maintenance of Insurance Records) Regulations, 2015, stipulates that Insurers are required to ensure that: (i) the system in which the policy and claim records are maintained has adequate security features; and (ii) the records pertaining to policies issued and claims made in India (including the records held in electronic form) are held in data centres located and maintained in India.

RBI in its guidelines titled as "Cyber Security Framework in Banks" states that "It has been decided to collect both summary level information as well as details on information security incidents including cyber-incidents." Hence, Banks are required to report the security incidents promptly, within 2-6 hours in the format provided in Annex-3 to the guidelines"



Under the current legal framework for healthcare service providers the supervisory authority for breach reporting in the healthcare industry is Data Protection Officer (DPO) of National Digital Health Mission (NDHM). The NDHM draft Health Data Management Policy 2022 mentions that the data fiduciary will ensure that any instance of non-compliance with the provisions of the Policy, or any instance of unauthorized or accidental disclosure, acquisition, sharing, use, alteration, destruction of or loss of access to personal data that compromises the confidentiality, integrity or availability of personal data to a data principal is promptly notified to relevant entities as may be required by applicable law, including the Information Technology (The Indian Computer Emergency Response Team and Manner of Performing Functions and Duties) Rules, 2013. This highlights the multiplicity of reporting data breach incidents such as any organizations falling under the category of healthcare industry will have to report the breach incident to the Indian Computer Emergency Response Team as well as to the Data Protection Officer of the National Digital Health Mission (NDHM)

Additionally, there are also inconsistencies in definitions of data breach across these sectors. As per the CERT-In Rules, "cyber security breach" means unauthorized acquisition or unauthorized use by a person as well as an entity of data or information that compromises the confidentiality, integrity or availability of information maintained in a computer resource.[53] The recently issued Information and Cyber Security Guidelines 2023, by the Insurance Regulatory Authority of India, define an incident as the occurrence of any exceptional situation that could compromise the Confidentiality, Integrity or Availability of Information assets of Organization. Further, the guidelines lay more emphasis on defining the 'security incidents' by providing a list of events that shall be categorized as security incidents.[54]

Regulations issued by the RBI, however, do not specifically define "cyber security incident" or incident pertaining to information security.[55]

In conclusion, industries in India, such as insurance, banking, and healthcare, have obligations to protect customer data. The rising cyber threats on the organizations operating under these industries highlight the need for strong cybersecurity measures. Organizations must proactively safeguard data, report breaches promptly, and the DPDPA should adopt a harmonized approach to ease compliance burdens.

3.2 Fostering Harmony: Global Approaches to Align Sectoral Regulations with National Data Protection Laws

DPDPA, under Section 38, contains the provisions on consistency of the Act with other laws:

Section 38(1): The provisions of this Act shall be in addition to, and not in derogation of the provisions of any other law for the time being in force

Section 38(2): In the event of any conflict between a provision of this Act and a provision of any other law for the time being in force, the provision of this Act shall prevail to the extent of such conflict.

Given the multitude of regulatory obligations imposed by various regulatory authorities on organizations operating within specific sectors, it is crucial for the law to acknowledge the significance of guidelines prescribed within these sectors. Adopting an approach that minimizes conflicts will alleviate the compliance burden faced by data fiduciaries.

Section 38(2) of the Act may create ambiguity surrounding the application of sectoral guidelines to data fiduciaries that operate in multiple sectors such as IRDAI (Protection of policyholders' interests) regulations 2017, National Digital Communications Policy, 2018 and various other authorities.

Globally the data privacy laws provide for better clarity with respect to obligations specified in other statutes. Principle 7 of the Australian Law Reform Commission's Guiding Principles emphasizes the importance of coherence and consistency in Australian privacy laws. It suggests that any proposals for legal remedies or causes of action related to privacy invasion should align with existing laws and regulatory frameworks, promoting uniformity across jurisdictions. This principle also highlights the significance of avoiding unnecessary overlaps between different legal regimes to maintain coherence and consistency.[56]

The South Korean Personal Information Protection Act (PIPA) also mentions its relationship with other acts. Article 6 of PIPA states that the protection of personal information shall be governed by this Act, except where special provisions exist in other laws.[57] The Act on Promotion of Information and Communications Network Utilization and Information Protection, etc. ("Network Act") previously regulated personal information processing by online service providers but was consolidated into the amended PIPA. Effective from August 5, 2020, online service providers are now governed by the PIPA's dedicated "Special Section" for personal information processing while providing online services.[58]

Similarly, Article 60 of General Data Protection Regulation (GDPR) prescribes Cooperation between the lead supervisory authority and the other supervisory authorities concerned. Article 60(1) further states that the lead supervisory authority shall cooperate with the other supervisory authorities concerned in accordance with this Article in an endeavor to reach consensus. The lead supervisory authority and the supervisory authorities concerned shall exchange all relevant information with each other.[59]

Singapore too, provides for a harmonious approach for interpreting various privacy laws of the country. In addition to the Personal Data Protection Act, the Singapore data protection regime consists of various general or sector / industry-specific guidelines issued by the Personal Data Protection Commission ("Commission"). While these guidelines are advisory in nature and not legally binding, they indicate the manner in which the Commission will interpret the Act. Therefore, it is best practice to carefully observe and follow these guidelines.[60]

It is therefore clear that the global data protection statutes, in addition to being self-contained, also consider the legal frameworks of different sectors, thus ensuring that they are compatible with existing laws.

Through an analysis of the practices adopted by various countries, three distinct approaches have been identified. The first approach, exemplified by South Korean jurisdiction, involves consolidating all provisions related to personal data processing into a single primary data protection law, which also includes separate sections for sector-specific requirements.

The second approach, exemplified by the GDPR, emphasizes cooperation among supervisory authorities to enhance law enforcement and alleviate compliance burdens for data fiduciaries, promoting consistency and collaboration within the data privacy framework.

The third approach, as used by the Singapore jurisdiction, involves issuing sector-specific guidelines, which serve as advisory references for data fiduciaries to navigate compliance with multiple laws, thereby reducing their compliance burden. Further, the global statutes also provide for collaboration and cooperation among different supervisory authorities. This ensures that these authorities work together in a harmonious and coordinated manner, sharing information and expertise as needed to effectively regulate and oversee various aspects of the global economy. This approach helps to promote stability and sustainability in the global system, as well as improve the overall efficiency of global data protection framework.

Post conducting a thorough analysis of the global statutory framework and best practices employed by supervisory authorities, it becomes essential to present recommendations for optimizing the breach notification system. These suggestions draw inspiration from various countries' approaches to minimizing friction between sectoral laws and national data protection regulations.

4

RECOMMENDATIONS

The first section of this report delved into the conceptual nuances of personal data breaches and the regulatory approaches adopted in jurisdictions globally. Based on an analysis of common trends and breach reporting mechanisms which have been found to be practically implementable, some recommendations are made below for both rule-making pertaining to personal data breach reporting as well as for the Data Protection Board to investigate and adjudicate on breaches. The intent of these recommendations is to advocate for a comprehensive, concise, and robust framework for regulation of personal data breaches.

1. Distinguishing between Personal Data Breaches and Unauthorised Processing

Personal data breach is defined under Section 2(u) of DPDPA[61]. It is important to note that the definition of a personal data breach in the DPDPA, which includes unauthorized processing, lacks clarity and creates confusion in the legislation. It is recommended that concepts be treated separately in implementation and adjudicatory proceedings under the law.

In implementing the law and in framing rules surrounding the breach reporting and notification mechanisms, the Central Government should take into consideration the distinction between instances of unauthorised processing and instances of personal data breaches, in line with technical and global regulatory understanding of these concepts.

Further, the Data Protection Board, in adjudicating and investigating upon complaints received pertaining to personal data breaches should also factor in this underlying distinction. In the absence of the same, Data Fiduciaries may end up paying hefty penalties twice for a singular instance of non-compliance.

2. Risk-Based Approach for Breach Reporting

Section 8(6) of the DPDPA mentions that the data fiduciary must inform the board and affected individuals of a personal data breach. The manner of doing the same is expected to be prescribed through rules by the Central Government. In drawing up these procedures, reference may be made to global best practices used by different authorities worldwide as a reference. Many global data protection authorities have issued guidance and guidelines to assist data fiduciaries in complying with their obligations. These guidelines outline the compliance requirements for various data protection laws. Below are some examples of best practices adopted by various global authorities, accompanied by recommendations for the Indian data protection framework:

2.1 Breach Reporting

- Supervisory authorities around the globe have varying reporting requirements for personal data breaches. In Singapore, for example, the Personal Data Protection Commission requires breaches to be reported within three days. Some countries, however, such as Brazil, South Korea, Japan, and Australia, do not establish a precise timeline. To avoid fines and penalties, data fiduciaries must rigorously adhere to the reporting timelines.
- Further, the breach reporting requirements, including the criteria and thresholds, vary across different jurisdictions. Countries like Singapore, South Korea, Brazil, Japan, European Union, and Australia require reporting a data breach to the supervisory authority if it affects a certain number of individuals or if it poses a high risk to them. Additionally, there is an obligation to notify affected individuals if the breach is likely to result in harm or damage to their personal information.

2.2 Content of Breach Report and Breach Notification

- The content of a breach report is similar across various jurisdictions. Typically, it involves providing information on the date the organization discovered the data breach, steps taken by the organization in response to the breach, and the number of individuals affected, among other details.

2.3 Manner of Notifying and Reporting Breach

- Different global authorities have prescribed different methods for reporting and notifying breaches. For example, the Notifiable Data Breaches (NDB) scheme issued by the Office of the Australian Information Commissioner (OAIC) provides a Notifiable Data Breach form that may be a useful reference for the Data Protection Board. According to the OAIC, if it is not practical to notify affected individuals individually, an organization that has experienced an eligible data breach should make a public statement on its website that contains certain information required by the Privacy Act and take reasonable steps to publicize the contents of the statement. Similarly, the Board may consider the form issued by the Brazilian data protection authority (ANPD) for communicating a data breach.

Therefore, it is recommended that any future rules or guidelines related to data breach reporting must be precise and clear, explicitly outlining the aspects of reporting breaches, including timelines and procedures. This will provide clear guidance to data fiduciaries and facilitate compliance with breach reporting obligations.

Additionally, it is suggested that the DPDPA adopts a risk-based approach for reporting data breaches. This means that breaches are reported and notified if they are likely to result in significant risk to the affected individuals or organizations.

By taking a risk-based approach, data fiduciaries can prioritize their resources and focus on the most critical breaches, rather than reporting inconsequential and minor incidents. Moreover, penalties for non-compliance with breach notification requirements should be commensurate with the level of risk to rights of data principals caused by the breach. In simpler terms, the approach would require data fiduciaries to report only significant breaches, which would help them allocate their resources more effectively. The penalties for non-compliance should reflect the severity of the risk posed by the breach.

3. Breach Reporting in a Phased Manner

- To ease the reporting burden on data fiduciaries, supervisory authorities and data protection statutes around the world have provided exemptions for reporting breaches within the prescribed timeline. This exemption allows data fiduciaries to report the breach in stages, permitting them to provide complete information after an initial reporting of the breach if they

don't have all the information at the time of the breach. Examples of this phased breach reporting can be seen in different jurisdictions. For instance, Article 33(4) of GDPR allows providing information in phases without undue further delay if it's not possible to provide the information at the same time. In Brazil, ANPD guidelines allow communication of breaches in stages: preliminary and complementary, if the data fiduciary doesn't have complete information or is unable to notify all holders within the recommended period. Similarly, PPC guidelines in Japan prescribe two stages of reporting obligations: preliminary and final reports.

The DPDPA framework should allow a phased approach for reporting a breach, wherein the data fiduciary can provide information in stages instead of providing complete information at the time of the breach. This approach is suggested to reduce the compliance burden on data fiduciaries, as it may not always be possible to gather all relevant information immediately after the breach has occurred.

By allowing a phased approach, the data fiduciary can provide initial information on the breach and follow up with additional information as it becomes available. This approach has been adopted by other global data protection authorities, such as GDPR, ANPD, and PPC, and has been found to be a useful way to manage breach reporting requirements.

4. Harmonizing Sectoral Regulations

- According to Section 38(1) of the DPDPA, the Act shall be construed as consistent with other laws, but Section 38(2) contradicts this by stating that the Act's provisions will override any conflicting provisions in other laws. This approach creates an interpretational challenge and could create compliance challenges particularly in industries like banking, insurance, and healthcare where there is a multiplicity of regulations on cybersecurity and data protection. CERT-In and sectoral regulators such as RBI, IRDAI, etc. have created guidelines based on the unique needs and requirements of these industries.
- The DPDPA can benefit from examining how other countries and their regulatory bodies have approached creating data protection laws that accommodate the requirements of specific sectors. For instance, the approach, adopted by South Korea, consolidates all provisions related to personal data processing into a comprehensive law, including separate sections for specific sectoral requirements. GDPR's approach focuses on cooperation and coherence among different supervisory authorities to improve law enforcement and reduce the compliance burden on data fiduciaries. Singapore's approach involves issuing industry or sector-specific guidelines to reduce the compliance burden on data fiduciaries, who can refer to the guidelines to ensure compliance with different laws. These guidelines are advisory in nature and provide data fiduciaries with necessary guidance to comply with multiple laws.

- By examining these laws and the regulatory bodies that oversee them, the DPDPA framework can gain valuable insights into how to create rules and regulations under the DPDPA which take into consideration sector-specific nuances that balance the need for data protection with the unique needs and challenges of each sector.
- Further, data protection statutes across the world provide guidance for the adoption of a provision in law that provides consistency with other privacy laws. The need for such provisions is exemplified by the approach taken by countries like Singapore and Australia. Article 6 of the Personal Data Protection Act (PIPA) of Singapore states that the protection of personal information shall be governed by the Act, except where special provisions exist in other laws. The approach in Australia is similar, with Principle 7 of the Guiding Principles issued by the Australian Law Reform Commission (ALRC) recommending that the privacy laws of the country should be coherent and consistent. These examples illustrate the importance of ensuring consistency and coherence in data protection laws, even when other laws may provide special provisions or exemptions.

The DPDPA framework should allow a phased approach for reporting a breach, wherein the data fiduciary can provide information in stages instead of providing complete information at the time of the breach.

To ensure that DPDPA and sectoral regulations are interpreted complementary to each other and to protect sensitive data in these vulnerable sectors, it's recommended to clarify the inherent legislative intent of Section 38 and adopt a more consistent approach.

REFERENCES

[1] Information Technology Act 2000, https://www.meity.gov.in/writereaddata/files/itbill2000.pdf

[2] Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules 2011, https://www.meity.gov.in/writereaddata/files/GSR313E_10511%281%29_0.pdf

[3] The Personal Data Protection Bill 2019, http://164.100.47.4/BillsTexts/LSBillTexts/Asintroduced/373_2019_LS_Eng.pdf

[4] The Personal Data Protection Bill 2019, Clause 41, http://164.100.47.4/BillsTexts/LSBillTexts/Asintroduced/373_2019_LS_Eng.pdf

[5] Times of India, "Centre withdraws Personal Data Protection Bill, 2019: Will present new legislation, says IT minister," https://timesofindia.indiatimes.com/india/centre-withdraws-personal-data-protection-bill/articleshow/93323625.cms

[6] Digital Personal Data Protection Bill 2022, https://www.meity.gov.in/writereaddata/files/The%20Digital%20Personal%20Data%20Potection%20Bill%2C%202022_0.pdf

[7] Digital Personal Data Protection Act 2023, https://www.meity.gov.in/writereaddata/files/Digital%20Personal%20Data%20Protection%20Act%202023.pdf

[8] ibid

[9] Cheng and Liu, "Enterprise data breach: causes, challenges, prevention, and future directions: Enterprise data breach," https://www.researchgate.net/publication/318152978_Enterprise_data_breach_causes_challenges_prevention_and_future_directions_Enterprise_data_breach

[10] Seh, Zarour, Alenezi, Sarkar, Agrawal, Kumar, & Khan, "Healthcare Data Breaches: Insights and Implications, https://www.mdpi.com/2227-9032/8/2/133

[11] GDPR Article 4(12), https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679

[12] Information Commissioner's Office (ICO), Personal data breaches: a guide, https://ico.org.uk/for-organisations/report-a-breach/personal-data-breach/personal-data-breaches-a-guide/

[13] ibid

[14] ibid

[15] Peter Carey, "Data Protection: A Practical Guide to UK Law," https://global.oup.com/academic/product/data-protection-9780198853565?cc=in&lang=en

[16] National Institute of Standards and Technology (NIST), Computer Security Resource Center Glossary, https://csrc.nist.gov/glossary/term/security_incident

[17] National Cyber Security Centre, "What is a cyber incident," https://www.ncsc.gov.uk/information/what-cyber-incident

[18] NIST, "Computer Security Incident Handling Guide," https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-61r2.pdf

[19] European Data Protection Board (EDPB), "Guidelines 9/2022 on personal data breach notification under GDPR," https://edpb.europa.eu/system/files/2023-04/edpb_guidelines_202209_personal_data_breach_notification_v2.0_en.pdf

[20] The Personal Data Protection Bill 2019, Clause 3(29), http://164.100.47.4/BillsTexts/LSBillTexts/Asintroduced/373_2019_LS_Eng.pdf

[21] Digital Personal Data Protection Act 2023, Section 2(u), https://www.meity.gov.in/writereaddata/files/Digital%20Personal%20Data%20Protection%20Act%202023.pdf

[22] Peter Carey, "Data Protection: A Practical Guide to UK Law," https://global.oup.com/academic/product/data-protection-9780198853565?cc=in&lang=en

[23] Donaldson and Lohr, "Health Data in the Information Age: Use, Disclosure, and Privacy," https://www.ncbi.nlm.nih.gov/books/NBK236546/

[24] Cybersecurity and Infrastructure Security Agency (CISA), "Protecting Sensitive and Personal Information from Ransomware-Caused Data Breaches," https://www.cisa.gov/sites/default/files/publications/CISA_Fact_Sheet-Protecting_Sensitive_and_Personal_Information_from_Ransomware-Caused_Data_Breaches-508C.pdf

[25] GDPR Article 4(12), https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679;

ICO, "Personal data breaches: a guide" https://ico.org.uk/for-organisations/report-a-breach/personal-data-breach/personal-data-breaches-a-guide/

[26] ICO, UK GDPR data breach reporting (DPA 2018), https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/personal-data-breaches/#whatisa

[27] Office of the Australian Information Commissioner (OAIC), Chapter 6: APP6 Use or disclosure of personal information, https://www.oaic.gov.au/privacy/australian-privacy-principles/australian-privacy-principles-guidelines/chapter-6-app-6-use-or-disclosure-of-personal-information

[28] OAIC, Part 1: Data breaches and the Australian Privacy Act, https://www.oaic.gov.au/privacy/privacy-guidance-for-organisations-and-government-agencies/preventing-preparing-for-and-responding-to-data-breaches/data-breach-preparation-and-response/part-1-data-breaches-and-the-australian-privacy-act;

Privacy Act 1988, https://www.legislation.gov.au/Details/C2023C00130

[29] GDPR, Articles 33 and 34, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679;

Data Protection Commission, Data Protection Commission announces decision in WhatsApp inquiry, https://www.dataprotection.ie/en/news-media/press-releases/data-protection-commission-announces-decision-whatsapp-inquiry

Data Protection Commission announces decision in Facebook data scraping inquiry, https://www.dataprotection.ie/en/news-media/press-releases/data-protection-commission-announces-decision-in-facebook-data-scraping-inquiry

[30] Digital Personal Data Protection Act 2023, Section 8(6), https://www.meity.gov.in/writereaddata/files/Digital%20Personal%20Data%20Protection%20Act%202023.pdf

[31] Singapore- Personal Data Protection Act 2012, Section 26B(3)(a), https://sso.agc.gov.sg/SL/PDPA2012-S64-2021?DocDate=20210129;

Brazil- Brazilian General Data Protection Law, Article 48, https://iapp.org/media/pdf/resource_center/Brazilian_General_Data_Protection_Law.pdf;

Japan- Act on the Protection of Personal Information, Article 24, https://www.japaneselawtranslation.go.jp/en/laws/view/4241/en#je_ch1at2;

EU- GDPR, Article 34, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679;

Australia- Notifiable Data Breaches Scheme, https://www.oaic.gov.au/privacy/notifiable-data-breaches/about-the-notifiable-data-breaches-scheme

[32] GDPR, Article 33, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679;

Personal Data Protection Act 2012, Section 26D, https://sso.agc.gov.sg/Act/PDPA2012

[33] Brazil- Brazilian General Data Protection Law, https://iapp.org/media/pdf/resource_center/Brazilian_General_Data_Protection_Law.pdf;

South Korea- Personal Information Protection Act, Article 34(1), http://www.pipc.go.kr/cmt/english/news/selectBoardArticle.do?nttId=6699&bbsId=BBSMSTR_000000000128&bbsTyCode=BBST03&bbsAttrbCode=BBSA03&authFlag=Y&pageIndex=1;

Japan- Act on the Protection of Personal Information, Article 26, https://www.japaneselawtranslation.go.jp/en/laws/view/4241/en#je_ch1;

Australia- Privacy Act 1988, Sections 27, 28, and 29, https://www.legislation.gov.au/Details/C2023C00130

[34] Significant harm could include severe physical, psychological, economic and financial harm, and other forms of severe harms that a reasonable person would identify as a possible outcome of a data breach.

[35] Personal Data Protection Commission, "Advisory Guidelines on Key Concepts in the Personal Data Protection Act," https://www.pdpc.gov.sg/-/media/Files/PDPC/PDF-Files/Advisory-Guidelines/AG-on-Key-Concepts/Advisory-Guidelines-on-Key-Concepts-in-the-PDPA-17-May-2022.pdf

[36] IAPP, "Practical notes for Japan's important updates of the APPI guidelines and Q&As," https://iapp.org/news/a/practical-notes-for-japans-important-updates-of-the-appi-guidelines-and-qas/;

DLA Piper, Data Protection Laws of the World – Japan, https://www.dlapiperdataprotection.com/index.html?t=breach-notification&c=JP

[37] DLA Piper, Data Protection Laws of the World – Australia, https://www.dlapiperdataprotection.com/index.html?t=breach-notification&c=AU;

OAIC, About the Notifiable Data Breaches scheme, https://www.oaic.gov.au/privacy/notifiable-data-breaches/about-the-notifiable-data-breaches-scheme

[38] EDPB, "Guidelines 9/2022 on personal data breach notification under GDPR," https://edpb.europa.eu/system/files/2023-04/edpb_guidelines_202209_personal_data_breach_notification_v2.0_en.pdf;

DLA Piper, Brazil, https://www.dlapiperdataprotection.com/index.html?t=breach-notification&c=BR&c2=;

IAPP, "Practical notes for Japan's important updates of the APPI guidelines and Q&As," https://iapp.org/news/a/practical-notes-for-japans-important-updates-of-the-appi-guidelines-and-qas/

[39] EDPB, "Guidelines 9/2022 on personal data breach notification under GDPR," https://edpb.europa.eu/system/files/2023-04/edpb_guidelines_202209_personal_data_breach_notification_v2.0_en.pdf

[40] ibid

[41] DLA Piper, Data Protection Laws of the World – Brazil, https://www.dlapiperdataprotection.com/index.html?t=breach-notification&c=BR;

ANPD, Security incident reporting, https://www.gov.br/anpd/pt-br/canais_atendimento/agente-de-tratamento/comunicado-de-incidente-de-seguranca-cis

[42] IAPP, "Practical notes for Japan's important updates of the APPI guidelines and Q&As," https://iapp.org/news/a/practical-notes-for-japans-important-updates-of-the-appi-guidelines-and-qas/

[43] OAIC, Part 4: Notifiable Data Breach (NDB) Scheme, https://www.oaic.gov.au/privacy/privacy-guidance-for-organisations-and-government-agencies/preventing-preparing-for-and-responding-to-data-breaches/data-breach-preparation-and-response/part-4-notifiable-data-breach-ndb-scheme#identifying-eligible-data-breaches;

DLA Piper, Data Protection Laws of the World – Australia, https://www.dlapiperdataprotection.com/index.html?t=breach-notification&c=AU

[44] OAIC, About the Notifiable Data Breaches scheme, https://www.oaic.gov.au/privacy/notifiable-data-breaches/about-the-notifiable-data-breaches-scheme

[45] ANPD, ANPD's Inspection General Coordination publishes a new form for sending Security Incident Reports, https://www.gov.br/anpd/pt-br/assuntos/noticias/coordenacao-geral-de-fiscalizacao-da-anpd-divulga-novo-formulario-para-envio-de-comunicados-de-incidentes-de-seguranca

[46] PDPC, Advisory Guidelines on Key Concepts in the Personal Data Protection Act, https://www.pdpc.gov.sg/-/media/Files/PDPC/PDF-Files/Advisory-Guidelines/AG-on-Key-Concepts/Advisory-Guidelines-on-Key-Concepts-in-the-PDPA-17-May-2022.pdf

[47] ibid

[48] CloudSek, "Cyber Threats Targeting Global Banking & Finance Customers," https://cloudsek.com/whitepapers-reports/cyber-threats-targeting-global-banking-finance-customers;

India Times, "India's Banking & Financial Services Sector Is Top Target For Cyber Attacks In Asia: Report," https://www.indiatimes.com/worth/news/indian-bfsi-sector-most-cyber-attacks-in-asia-583422.html

[49] Business Standard, "Over 1.6 mn cyber attacks blocked on Indian insurance firms a day in Jan," https://www.business-standard.com/article/finance/over-1-6-mn-cyber-attacks-blocked-on-indian-insurance-firms-a-day-in-jan-123022000404_1.html

[50] CyberPeace Foundation, "Threat Analysis Report based on Captured Cyber Attack on Simulated Healthcare Sector," https://www.cyberpeace.org/wp-content/uploads/2022/12/20221205-Threat-Analysis-report-based-on-captured-Cyber-Attacks-on-simulated-Healthcare-sector_2.pdf;

LiveMint, "Indian healthcare sector suffers 1.9 million cyberattacks in 2022," https://www.livemint.com/technology/tech-news/indian-healthcare-sector-suffers-1-9-million-cyber-attacks-in-2022-11669878864152.html

[51] CERT-In, Directions under sub-section (6) of section 70B of the Information Technology Act, 2000 relating to information security practices, procedure, prevention, response and reporting of cyber incidents for Safe & Trusted Internet, https://www.cert-in.org.in/PDF/CERT-In_Directions_70B_28.04.2022.pdf

[52] Baker Mckenzie, Sector-specific or Non-personal Data Security Breach Notification Requirements, https://resourcehub.bakermckenzie.com/en/resources/data-privacy-security/asia-pacific/india/topics/sector-specific-or-non-personal-data-security-breach-notification-requirements;

Insurance

IRDAI, (Protection of Policyholders' Interests) Regulations 2017, Regulation 19(5), https://irdai.gov.in/document-detail?documentId=385593

IRDAI (Maintenance of Insurance Records) Regulations 2015, Regulations 3(3)(b) & 3(9), https://irdai.gov.in/document-detail?documentId=604674;

Banking and Finance

RBI, Cyber Security Frameworks in Banks, https://www.rbi.org.in/Scripts/NotificationUser.aspx?Id=10435&Mode=0

RBI, Template for reporting Cyber Incidents, https://rbidocs.rbi.org.in/rdocs/content/pdfs/CSFB020616_AN3.pdf;

Healthcare

Ayushman Bharat Digital Mission, Draft Health Data Management Policy, https://abdm.gov.in:8081/uploads/Draft_HDM_Policy_April2022_e38c82eee5.pdf

National Digital Health Mission, Health Data Management Policy, https://abdm.gov.in:8081/uploads/health_data_management_policy_455613409c.pdf

[53] Information Technology (The Indian Computer Emergency Response Team and Manner of Performing Functions and Duties) Rules 2013, Rule 2(i), https://www.meity.gov.in/writereaddata/files/G_S_R%2020%20%28E%292_0.pdf

[54] IRDAI, Information and Cyber Security Guidelines 2023, https://irdai.gov.in/document-detail?documentId=3314780

[55] RBI, Cyber Security Frameworks in Banks, https://www.rbi.org.in/Scripts/NotificationUser.aspx?Id=10435&Mode=0

[56] Australian Law Reform Commission, "Serious Invasions of Privacy in the Digital Era", Principle 7: Privacy laws should be coherent and consistent, https://www.alrc.gov.au/publication/serious-invasions-of-privacy-in-the-digital-era-dp-80/2-guiding-principles/principle-7-privacy-laws-should-be-coherent-and-consistent/

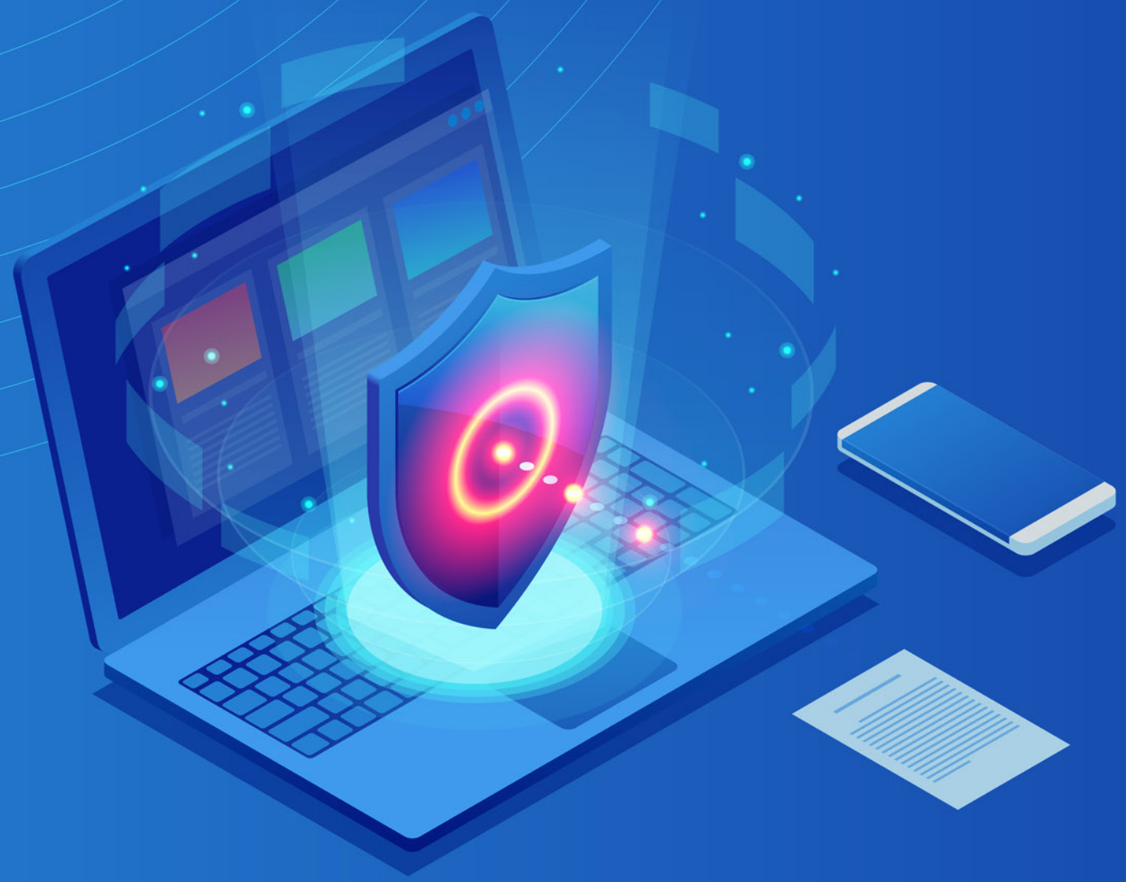
[57] Personal Information Protection Act, Article 6, https://elaw.klri.re.kr/eng_service/lawView.do?hseq=53044&lang=ENG

[58] Personal Information Protection Act https://elaw.klri.re.kr/eng_service/lawView.do?hseq=53044&lang=ENG

[59] GDPR, Article 60, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679

[60] PDPC Guidelines, https://www.pdpc.gov.sg/Guidelines-and-Consultation

[61] Digital Personal Data Protection Act 2023, https://www.meity.gov.in/writereaddata/files/Digital%20Personal%20Data%20Protection%20Act%202023.pdf



Section 2

CONSENT MANAGERS: BEST PRACTICES AND FRAMEWORKS

Executive Summary

This section aims to analyze the approach taken by the Digital Personal Data Protection Act (DPDPA) concerning the role of Consent Managers (CMs). This comprehensive examination will shed light on the challenges associated with this approach. To conduct a thorough analysis, this section will explore the approaches adopted by various sectors in India and examine the practices followed by global authorities, highlighting their best practices. By synthesizing these insights, this section of the report seeks to provide recommendations to enhance the current approach pertaining to the role of CMs in giving, managing, reviewing and withdrawing the consent of data principals through an accessible, transparent and interoperable platform. Through this endeavor, the goal is to contribute towards the improvement of data protection mechanisms and consent management practices.

The first chapter of this section focuses on comprehending the role of CMs as stipulated in the DPDPA. This aims to provide a clear and informative introduction to the topic, emphasizing the importance of effectively managing and reviewing the consent of data principals. It offers valuable insights into the pivotal role played by CMs in efficiently managing the consent of data principals. This chapter essentially aims to shed light on the significance of CMs and their instrumental role in safeguarding the privacy and data protection rights of data principals.

The second chapter explores the involvement of entities resembling CMs in various sectors within India, including banking, finance, and telecom. This analysis focuses on examining the approaches adopted by these frameworks across different sectors, aiming to identify reference points that can enhance the approach taken by the DPDPA. Further, this chapter thoroughly assesses the concerns and challenges associated with these frameworks to comprehensively evaluate their feasibility in effectively managing the consent of data principals.

The third chapter delves into an extensive examination of the risks and challenges intertwined with the current approach employed by the DPDPA. This chapter meticulously elucidates various facets of the existing approach that have the potential to undermine the interests of data principals and compromise data security. By thoroughly analyzing these aspects, it aims to provide a comprehensive understanding of the potential pitfalls and vulnerabilities within the DPDPA's approach, shedding light on the areas that require improvement to better safeguard the rights and security of data principals.

The concluding chapter shifts the focus towards comprehending the global approach to managing the consent of data principals. It aims to explore and analyze the perspective of global authorities in devising frameworks for effectively managing the consent of data principals. By examining the approaches adopted globally, valuable insights are gained into the diverse strategies and practices employed by various jurisdictions. This comparative analysis helps to draw meaningful observations and potential lessons that can inform and enhance the framework for consent management within the context of this study.

1

UNDERSTANDING THE ROLE OF CONSENT MANAGERS

Consent is the ability granted to individuals to determine the nature and extent of personal information that they share with a data fiduciary or processor, as well as its control and processing. It is the foundational pillar of data protection, where explicit affirmative consent is required to establish a systematic and trustworthy framework involving the data principals, organizations and their personal data. Consent Management involves a process of requesting, receiving and storing users' consent parallel to information provided about data acquisition and usage practices, through a consolidated platform hosting multiple data fiduciaries and processors.

The concept of a consent management framework first came to the forefront of Indian technology law and policy through the Personal Data Protection Bill, 2019 and the Data Empowerment and Protection Architecture (DEPA) in 2020, with the objective of ensuring separation of consent flow and data flow. It envisaged a user-centric model for obtaining consent, instead of the onus being on each data fiduciary as the custodian of consent and data. Therefore, the consent manager, expected to be implemented sector-wise, would exempt the existing network of market players and service providers from taking consent again and again, while securing the authentication mechanism from a customer perspective.[1]

The Digital Personal Data Protection Act (DPDPA) too acknowledges the significance of consent management and therefore advances the concept of 'Consent Managers (CM)' to address this need. Section 2(g) of the DPDPA defines the term 'Consent Managers' as a person registered with the Board, who acts as a single point of contact to enable a Data Principal to give, manage, review and withdraw her consent through an accessible, transparent and interoperable platform. The Act takes the concept of CMs a step forward by describing their functions, establishing their scope and stipulating their accountability to the Data Principal. The use of CMs has not been made mandatory, and has instead been proposed as a voluntary, alternative method of seeking consent in addition to other direct ways.

Section 6(9) states that every Consent Manager shall be registered with the Board in such a manner and subject to such technical, operational, financial and other conditions as may be prescribed. However, this leaves great ambiguity in terms of the implementation model that the Act envisages for CMs.

DPDPA's consent management structure has certain operational and functional similarities with the frameworks adopted in India's banking, healthcare and telecom sectors. For example, in the banking sector, the Reserve Bank of India (RBI) has developed a technical infrastructure known as Account Aggregators (AA). AAs are RBI-regulated NBFC which retrieves or collects financial information pertaining to its customer, as specified by the Bank, and presents such information to customer or any other financial user specified by Bank.[2] This unique structure was designed to give consumers and businesses alike simple access to their financial data. Consent, according to the RBI's standards, is critical in the AA environment. Without the customer's explicit authorization, AAs are strictly barred from sharing, accessing, or transferring their financial data.[3]

A consent manager framework has also been adopted for the Health Information Exchange. The National Digital Health Mission Data Management Policy defines a CM as an electronic system that interacts with the data principal and obtains consent from him/her for any intended access to personal data.[4] Further, the Health Information Exchange & Consent Manager (HIE-CM) is defined under the Draft Health Data Management Policy and refers to a digital system which facilitates exchange of health information and management of consent.[5]

Additionally, Telecom Regulatory Authority of India (TRAI) in furtherance of its directions under Telecom Commercial Communication Customer Preference Regulations, 2018 (TCCCPR, 2018), has prescribed the implementation of a Digital Consent Acquisition (DCA) Platform for seeking, maintaining and revoking the customer consent to promotional texts and calls. With the proposed framework, the gathered consent data would be shared on a digital ledger platform for verification by all Access Providers. Only a common short code, being 127XXX, may be used for sending consent-seeking messages, clearly indicating the purpose, scope of consent and name of the PE.[6]

It is worth noting that there are distinct differences between the frameworks discussed earlier and the CM framework adopted by DPDPA. While CMs under DPDPA focus on collecting and managing consent for personal data processing, the AAs collect consent specifically for sharing banking transaction data among participating banks on the network. Moreover, the AA framework is designed to gradually encompass a broader range of financial data, including tax data, pensions data, securities data (such as mutual funds and brokerage), and insurance data, making it accessible to consumers. Under the AA framework, it is evident that consent is intended to be collected for purposes that extend beyond the processing of personal data, and the larger objective is to generally facilitate more efficient exchange of information.[7] While there is significant overlap in these functions, all types of information exchange may not necessarily involve the processing of personal data.

Consent Management involves a process of requesting, receiving and storing users' consent parallel to information provided about data acquisition and usage practices, through a consolidated platform hosting multiple data fiduciaries and processors.

To assess existing practices in India relating to consent management, the specific mechanisms put in place by RBI, TRAI and the Draft Health Data Management Policy have been examined under chapter 2 along with their respective limitations.

2

ANALOGUES FROM EXISTING FRAMEWORKS AND INDUSTRY SECTORS

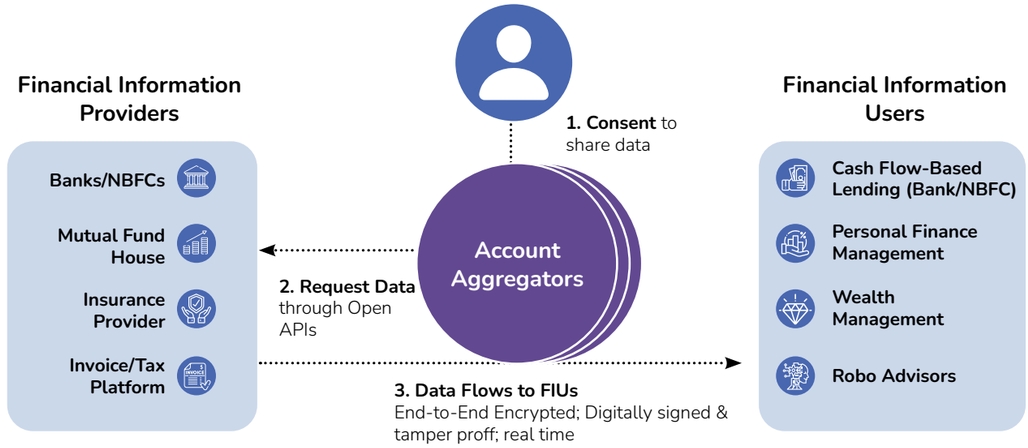
CMs have emerged as a significant aspect of privacy and data protection across diverse sectors in India. Their role in enhancing privacy and data protection has gained prominence, extending from the financial sector to healthcare and beyond. CMs play a vital role in fostering transparency and ensuring a secure environment for data sharing and privacy across different domains. A detailed overview of the roles played by entities resembling Consent Managers (CMs) across various sectors is provided below.

2. 1 Transforming Financial Services: The Emergence of Account Aggregators

The introduction of the AA framework presented a groundbreaking financial data-sharing system with the potential to revolutionize investment and credit practices. The framework aimed to provide consumers with increased access and control over their financial records, while also expanding the customer base for lenders and fintech companies. By leveraging AAs, individuals gain empowerment and autonomy over their personal financial data, which would otherwise be fragmented and inaccessible across various platforms or institutions.[8]

AAs are RBI-regulated entities (with an NBFC-AA license) which enables the customer to securely access and share their financial information (FI) across regulated financial institutions. There are three stakeholders in this process, being FI Providers (bank, banking company, NBFC asset management company, depository, depository participant, insurance company, insurance repository, pension fund, and GST network), FI Users (entity registered with and regulated by any financial sector regulator such as SEBI, RBI, IRDAI, PFRDA, MoF) and the customer. The AA is tasked with obtaining consent from the customer through a standardized consent artefact, which would be verified by the FI Provider.[9]

Account Aggregator empowers the individual with control over their personal financial data, which otherwise remains in silos



Source: Know all about Account Aggregator Network- A financial data-sharing system, PIB[10]

It is worth noting that under the current ecosystem, AAs essentially function as data blind entities. AAs act as interoperable CMs with limited access to consumer data. They are unable to read or resell consumer data. End to end encryption ensures that FI cannot be collected ('aggregated') by AA and used for profiling.[11]

In addition to the AAs that enable data exchange in the finance sector, the regulatory framework in India also introduces the concept of Health Information Exchange and Consent Managers (HIE-CM). These entities perform similar roles as AAs, but specifically in the healthcare industry.

2.2 Uplifting Healthcare Sector through Health Information Exchange & Consent Manager (HIE-CM): Enhancing Data Sharing and Consent Management

HIE-CM had been introduced in the National Digital Health Mission Data Management Policy, aimed at striking a balance between promoting data sharing for improved healthcare outcomes and respecting privacy of individuals. Clause 11 of the policy specifically defines the role of CM and outlined its responsibilities. The policy further elaborated on the methods and procedures for obtaining consent from data principals using CMs.[12]

The rationale behind the introduction of such a policy was that individuals should have control and autonomy over their personal health information by designating specified institutions as CMs. These must be able to fully inform data principals of the objective, extent and duration of data sharing, so as to facilitate specific voluntary consent.

The Draft Health Data Management Policy further defines HIE-CM under the ambit of a digital system.[13] It is essential to emphasize that utilizing HIE-CMs to share health information is entirely optional for the providers of such information. The adoption's voluntary nature ensures that patients retain control over their personal health information and are free to choose the degree of their involvement in the process.[14]

2.3 Driving Innovation in the Telecom Sector: Empowering User Privacy and Consent Management through Digital Consent Acquisition

Through its direction dated 2nd June 2023, TRAI has sought to mandatorily introduce a Digital Consent Acquisition (DCA) Framework for seeking, managing and revoking consent to promotional calls and texts, under the existing TCCCPR, 2018. This aims to combat spam by creating a unified digital ledger for customers to digitally register their consent across all service providers.[15]

The framework prescribed by TRAI will place a strong emphasis on user consent, ensuring that telecom providers have the ability to block any calls or messages that users have not explicitly consented to receive. By making user consent a priority, this framework looks to empower individuals to have greater control over the communications they receive.

This framework's focus on user consent may serve as a cornerstone for creating a more user-centric and privacy-conscious communication environment. By empowering users to have control over their communications, it will promote a cohesive experience for individuals while prioritizing their consent and privacy.

The DCA is to be established by Access Providers and is widely understood as an improvement over the previously existing consent regime, where various Principal Entities obtained and managed consent in a fragmented manner. It would enable verification of customer consent as well as consolidate and identify the process for individuals and telecom companies.[16]

2.4 State Specific Guidelines: Karnataka – e-Sahamati Framework

In December 2021, the Karnataka Government introduced the 'e-Sahamathi' Platform to facilitate data sharing between Data Principals and Third-Party Service Providers (TPSPs). It functions in the form of a portal, where TPSPs may raise requests for individual or bulk customer data, which may then be approved by the Data Principal. E-Sahamathi also propounds the concept of 'open consent', which a data principal may give to all or specific TPSPs even before they raise consent requests. There are three significant benefits to such a framework: (1) it eliminates the need for physical document verification, (2) it restricts data processing to the specific purposes for which consent has been granted by the citizen, and (3) it ensures data authenticity as government entities and universities share datasets with digital signatures.[17]

2.5 Exploring the Synergy Between Electronic Consent Framework and DEPA

The Electronic Consent Framework (ECF) was introduced to create an open, secure, user-centric, and application-agnostic consent management mechanism, the specifications of which can be applied across sectors. It involves four parties, the Data Provider (original holder of data about the User), Data Consumer (accessing and using the data), Consent Collector (maybe Data Consumer, Data Provider or any other service provider) and the User. ECF and DEPA both envision a shift to digital equivalents of the physical paper-based consent acquisition process, in the form of consent artifacts. These electronic documents are traceable, verifiable and specify the parameters and scope of data sharing that a user wishes to consent to.[18]

The roles and responsibilities of the consent collector have been clearly outlined. It is the duty of the consent collector to ensure that the user is provided with clear information regarding the scope and purpose of data sharing. If the user agrees to the specified sharing scope, they may be prompted to digitally sign the consent, resulting in the inclusion of their digital signature within the consent artifact. Alternatively, the consent collector may obtain data sharing authorization through different means, such as having the user click a button or sign a physical form. Moreover, the consent artifact includes provisions for specifying a 'revoker' for revoking consent, as well as options for notifying the Data Consumer and Data Provider.

There has been a tectonic shift across Indian industries to implement and take advantage of the Digital India initiative. Primacy has been given to user-centric experiences and data interoperability, and each of the abovementioned consent management framework seeks to empower data principals with greater control over their personal information and its use. However, it is important to note that these frameworks are not devoid of their respective drawbacks, which have been discussed in the following paragraphs.

There has been a tectonic shift across Indian industries to implement and take advantage of the Digital India initiative. Primacy has been given to user-centric experiences and data interoperability, and each mentioned consent management framework seeks to empower data principals with greater control over their personal information and its use.

2.6 Challenges and Issues with Existing Frameworks

In order to introduce a sector-agnostic consent manager framework as proposed in the DPDPA, the challenges posed by existing frameworks need to be addressed to reduce potential risks to data security. The CM framework does bear certain similarities with AA and HIE-CM, being data blindness, consent flow logs, notifications of changes to consent, and a grievance redressal mechanism, yet it would be prudent to analyze the concerns of each industry-specific framework as against an overarching consent management regime.

The challenges to the AA framework are twofold. Firstly, there is a potential risk to data security as the AA framework permits the sharing of extensive amounts of sensitive personal information with potentially unlimited entities, without specific purposes outlined. This raises concerns about the protection and misuse of such data. Following the emergence of alleged unauthorized sharing of financial information, which led to cases of fraud with customers, the RBI is poised to conduct a review of the business model of AAs.

Secondly, there are operational challenges as well as it is essential to establish a robust consent architecture and maintain comprehensive audit trails. The Financial Information Providers (FIPs) will need to implement interfaces that facilitate the submission of consent artifacts and mutual authentication by AAs, ensuring a secure flow of financial information.[19]

Further, the framework established by the National Digital Health Mission (NDHM) also faces its own set of challenges. One notable challenge is the absence of specific provisions that address corporate governance concerns related to Consent Managers (CMs). This lack of explicit guidelines can lead to ambiguity and potential issues regarding the governance and accountability of CMs.

Additionally, the NDHM policy does not impose restrictions on CMs engaging in other business activities. This creates a significant concern related to data resale and profiling.

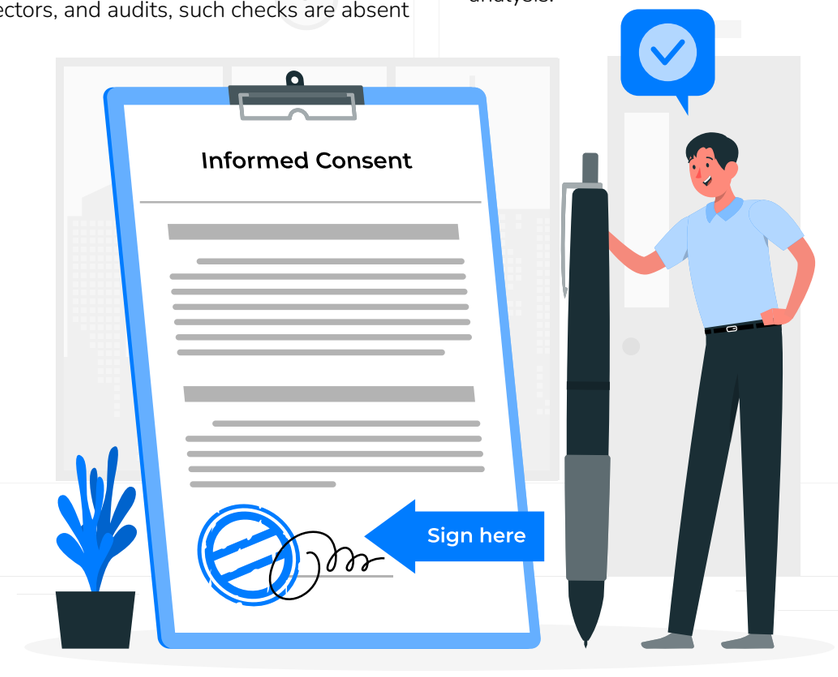
> It is imperative that before operationalising the concept of CM in the DPDPA, the Indian statutory authorities thoroughly examine the CM mechanism in both the banking and healthcare sectors.

While the RBI guidelines for AA mandate certain disclosures regarding the transfer of shares and control, as well as documentation on technical protocols, corporate details such as the board of directors, and audits, such checks are absent for CMs in the health data domain leaves them susceptible to potential malpractices by entities providing consent management services.

The lack of stringent regulations on CMs especially in the health data sector raises concerns about unauthorized use and disclosure of data, breaches of consent, and the potential exploitation of data for commercial gain at the expense of users' privacy and commercial interests. Without proper safeguards and oversight, there is a risk of harm to individuals and communities, both in terms of their privacy rights and potential negative commercial consequences.

Addressing these concerns would be crucial to ensure the responsible and ethical handling of health data by CMs. This would help safeguard the privacy and interests of users and communities, preventing any potential misuse or exploitation of sensitive health information.

Jurisdictions across the world are now prioritizing consent management and have developed their own methodologies to address it. The subsequent chapter delves into these practices and provides a comprehensive analysis.



3

CONSENT MANAGERS UNDER DPDPA: EVALUATING RISKS AND AMBIGUITIES

3.1 Ambiguity Surrounding the Legal Status of Consent Managers

The DPDPA outlines a brief framework for the CMs and defines it as a person registered with the Board, who acts as a single point of contact to enable a Data Principal to give, manage, review and withdraw her consent through an accessible, transparent and interoperable platform. The framework characterizes CMs as a "person," a term further expounded upon in Section 2(s). This definition of "person" encompasses individuals, companies, firms, and other entities, leading to uncertainty regarding the legal status of CMs.

This ambiguity in the definition of CM could lead to confusion in their implementation and may have implications for the way personal data is handled in India.

In other industries, such as banking and healthcare, CMs are clearly defined as entities that permit data transmission between information providers and its recipients. As per the Non-Banking Financial Company - Account Aggregator (Reserve Bank) Directions, 2016, an AA means a non-banking financial company as defined in sub-clause (iii) of clause (f) of section 45-I of the Act, that undertakes the business of an account aggregator, for a fee or otherwise, as defined at clause (iv) of sub-section 1 of section 3 of these directions.[20]

Similarly, the National Digital Health Mission Data Management Policy, under Para 4(e), defines the term CM as an electronic system that interacts with the data principal and obtains consent from him/her for any intended access to personal data.[21]

Hence, it is evident that both the frameworks comprehensively define the legal status of a CM as an entity or an electronic system. These frameworks offer a clear understanding of how CMs function and contribute to data sharing by explaining the CM's role as a mediator in data exchange.

Further, academic literature from around the world emphasizes the importance of establishing the entity status of Consent Managers (CMs). One such paper, titled "Consent Management Architecture for Secure Data Transactions," advocates for the development of a personalized communication interface. The authors argue that this interface would enable individuals to effortlessly view, manage, and exercise control over their consent in a transparent and standardized manner.

The paper, therefore, makes a compelling case for the implementation of a Consent Manager platform in the form of an interface. Such a platform would empower individuals by providing them with the ability to easily select and switch service providers based on their consent preferences. By streamlining the process, this interface would enhance user autonomy and foster greater choice and flexibility in selecting service providers.[22]

The reference to national laws and global academic literature emphasizes the crucial need to clearly define the legal status of consent managers. It is evident that the absence of a clear legal status for CMs creates uncertainty and complexity in their expected functions. This lack of clarity hampers CMs' ability to understand their rights and responsibilities and impedes their operational efficiency in providing services. Addressing this issue by establishing a clear legal framework and recognition for CMs would enable them to fulfill their role as intermediaries in data sharing effectively and ensure smooth functioning in consent-driven data exchange.

Further, it is important to highlight that alongside the ambiguous legal status of CMs, the DPDPA lacks clear instructions on the operations of CMs and procedures for withdrawing consent. The subsequent paragraphs delve into this matter in greater detail.

3.2 Uncertainty Regarding the Functionalities of Consent Managers and Consent Withdrawal Procedures

The lack of clear rules and guidelines surrounding the functionalities, as well as roles and responsibilities of CMs may create significant ambiguity.

Grievance Redressal and Appeals Procedure

The DPDPA in Section 6(8) mentions that the CM shall be an entity that is accountable to the Data Principal and acts on behalf of the Data Principal.[23]

This provision establishes a clear legal relationship between the CM and the data principal, emphasizing the CM's duty to act in the best interests of the data principal. Given the relationship between a CM and a Data Principal, it is the CM's responsibility to prioritize the data principal's best interests and ensure that their personal data is used only for the authorized purposes for which consent was originally granted. Though the DPDPA provides a right of grievance redressal to the data principals which obligates the CMs to address the grievances of the data principal, it is noteworthy that as the importance of CMs grows, it becomes necessary to develop a robust mechanism to resolve concerns and develop an appeals framework. These safeguards are required to appropriately address any potential harm that may result from CMs' data-sharing actions. Therefore, it is imperative that DPDPA efficiently safeguard the rights and interests of data principals by providing measures to address grievances and provide an option for recourse.

The frameworks implemented in banking and healthcare sectors serve as examples of well-defined grievance procedures established within the statutory regulations governing those sectors. For instance, under the Directions regarding Registration and Operations of NBFC - AAs, issued pursuant to section 45-JA of the Reserve Bank of India Act, 1934, a comprehensive procedure is listed for addressing and resolving customer grievances/complaints. It stipulates that an AA must have a Board-approved policy in place to handle and resolve customer grievances/complaints, along with a dedicated system specifically designed to address such matters. Further, it states that the AA shall display the name and contact details of the Grievance Redressal Officer who can be approached by the public for complaints against the company. These provisions ensure that AAs have effective mechanisms to address and resolve any grievances or complaints raised by their customers.[24]

Additionally, the Draft Health Data Management Policy which prescribes the utilization of HIE-CM for obtaining consent of data principals also mentions a mechanism of grievance redressal under Clause 32. The policy states that a complaint can be made by the data principal regarding any contravention of the Policy that has caused or is likely to cause harm to the data principal. The data fiduciary is expected to have a procedure and effective mechanisms to redress the grievances of data principals efficiently and in a speedy manner. Further, the data fiduciary is required to designate a Grievance Officer and publish his name and contact details on its website in order to facilitate effective redressal.[25]

The existence of mechanisms to address grievances in the banking and healthcare sectors demonstrates the significance attributed to the rights of data principal. It, therefore, highlights the need for clarity around the grievance redressal and appeals mechanism for the CM setup in the DPDPA as well.

Governance and Oversight Mechanism

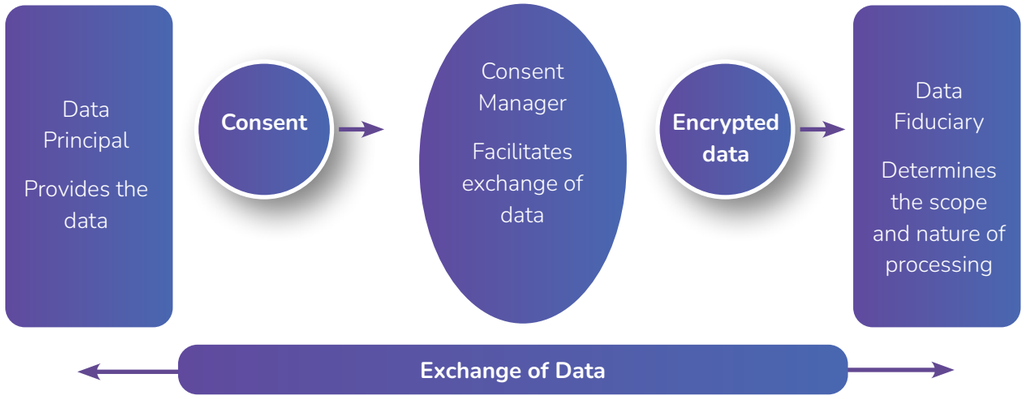
It is the obligation of every CM to get registered with the Data Protection Board in accordance with Section 6(9) of the DPDPA. However, to guarantee the autonomy and integrity of the institutional structure, it is imperative to clarify the Data Protection Board's role in overseeing

It is evident that the absence of a clear legal status for CMs creates uncertainty and complexity in their expected functions. This lack of clarity hampers CMs' ability to understand their rights and responsibilities and impedes their operational efficiency in providing services.

and controlling CM institutions in detail. By adopting such elements, the data protection framework can create a strong regulatory structure that enables effective governance of CMs while also fostering openness and accountability within the ecosystem.

The Data Protection Board can draw inspiration from the rule-making process utilized by the Reserve Bank of India (RBI) to regulate AAs (AAs) when developing governance mechanisms for CMs. The RBI guidelines provide valuable insights into such aspects as AA registration procedures, AA responsibilities and functions, data security standards, pricing regulations, auditing requirements, risk management practices, and corporate governance considerations. The Data Protection Board could draw inspiration from such frameworks in order to create a solid governance framework for CMs that assures adherence to best practices and encourages effective data management and protection.[26]

An effective governance mechanism plays a crucial role in overseeing the operations of CMs and ensuring their accountability to data principals. Alongside safeguarding the credibility of CMs, it is essential to clearly define the responsibilities they must fulfill to facilitate efficient consent management. The following paragraphs present a case for establishing a definitive role for CMs in relation to their obligations in consent management.



In addition to the challenges listed above, a significant tenet of the CM framework as described by the DPDPA is the centralization of consent management. A centralized setup would pose concerns across various channels including security, privacy and data protection.

3.3 Concerns Arising from Centralized Consent Management

Centralized consent management, where a singular entity or software manages the consent of multiple users, has the potential to raise a few concerns related to privacy and security.

The sheer concentration of data in a single location increases the risk of data breaches, making it an attractive target for cybercriminals. Additionally, a centralized system can provide an opportunity for bad actors to have access to large amounts of personal data, potentially leading to privacy violations.

Privacy authorities around the world are increasingly enacting or considering legislation to prevent the collection and consolidation of private data in a centralized system. For example, in 2011, the Office of the Privacy Commissioner of Canada, supported by the Ontario Privacy Commissioner, provided guidance titled "At Your Fingertips – Biometrics and the Challenges to Privacy." The guidance emphasized in great detail the importance of storing data locally rather than in centralized databases, as centralization increases the risk of data loss or inappropriate cross-linking of data across systems.[27]

Academic literature worldwide consistently emphasizes the drawbacks of storing data in centralized databases. This viewpoint is reinforced in a research paper titled "Secure decentralized electronic health records sharing system based on blockchains," where the authors assert that employing a decentralized file system offers enhanced security without compromising performance.

The paper's authors argue that a decentralized file system presents superior security features while maintaining a comparable level of performance to centralized systems. This perspective aligns with the global academic discourse that favors decentralized architectures for data storage.

The absence of a single point of failure in a decentralized system eliminates the vulnerability present in centralized systems, where a single failure could result in the compromise of all stored data. Furthermore, decentralized systems alleviate communication bottlenecks that can impede efficient data transfer in centralized setups.[28]

The concerns associated with centralized consent management highlight the need for a more privacy-conscious and secure approach.

After shedding light on the risks and concerns inherent in the current framework recommended by DPDPA, it becomes crucial to examine the approach employed by international authorities in effectively managing user consent.

4

GLOBAL APPROACH: EXAMINING REGULATIONS AND PREVALENT PRACTICES

4.1 Industry associations and supervisory authorities

Acknowledging the significance of consent management, industry associations and regulatory authorities across the globe have established diverse frameworks and best practices to alleviate the compliance burden placed on organizations.

By prescribing these frameworks and best practices, these bodies aim to provide organizations with practical guidance and standardized approaches for consent management. These resources are designed to streamline the compliance process, reduce ambiguity, and ensure that organizations can meet the requirements set forth by applicable data privacy regulations.

Organizations can leverage these frameworks to implement comprehensive consent management strategies tailored to their specific industry and regulatory requirements. By adhering to these prescribed frameworks, organizations can demonstrate their commitment to responsible data handling, build trust with their customers, and mitigate potential risks associated with non-compliance.

These frameworks and best practices are detailed below:

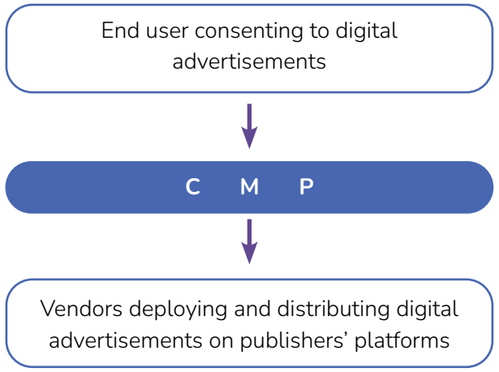
(a) Interactive Advertising Bureau (IAB)

IAB is the European-level association for the digital marketing and advertising ecosystem. It has prescribed a Transparency & Consent Framework (TCF), recently updated in 2023, which is an accountability tool that relies on standardization to facilitate compliance with certain provisions of the ePrivacy Directive and the GDPR.[29]

The framework may be used as a valuable point of reference for understanding the technical and operational aspects involved in the functioning of consent managers. Though the TCF's applicability is limited to the context of digital advertising and marketing, some elements of it may be replicable in cross-industry use cases as well.

(i) Legal Status of Consent Managers

The IAB TCF Policies define Transparency and Consent Management Platform (Consent Management Platform or CMP) as the company or organization which is entrusted with ensuring transparency for end users along with the centralization of consents given and objections raised by them. The CMP acts as an intermediary between a publisher (i.e., the entity responsible for operating a digital property for instance a blog or website), an end user (i.e., the individuals toward whom advertisements are targeted), and vendors (i.e., the company responsible for delivery of the digital advertisements).



Under the TCF, a consent management platform performs the following functions:

- Providing transparency to end users;
- Assisting Vendors and Publishers in establishing Legal Bases for processing;
- Acquiring user consent as needed and managing user objections, and communicating Legal Basis, consent or and/or objection status to the ecosystem.

A CMP may be the party that surfaces, usually on behalf of the publisher, the User Interface to a user, though that may also be another party.[30]

The definition of CMP under the framework unambiguously clarifies the legal standing of the CMP as a separate company or organization, eliminating any uncertainty around the platform being merely a software operated by vendors or publishers.

(ii) Obligations and Accountability of CMs

The framework provides specific guidelines for the operation of Consent Management Platforms (CMPs). These obligations include reminding users of their right to withdraw consent or object to processing for any Vendor or Purpose and following the requirements set by the relevant Authorities. CMPs are also required to resolve conflicts in Signals or merge Signals before transmitting them, in accordance with the Policies and Specifications.[31]

IAB Europe is responsible for periodically reviewing and verifying a CMP's compliance with the Policies and/or Specifications, following established procedures that are periodically updated. In cases where CMPs commit willful and/or severe violations of the Policies, they may face suspension from participating in the Framework.[32]

The periodic review and verification process conducted by IAB Europe ensures compliance and holds CMPs accountable for their actions

This provision emphasizes the importance of ensuring CMPs adhere to the established standards and guidelines to maintain the integrity and effectiveness of the consent management ecosystem. The periodic review and verification process conducted by IAB Europe ensures compliance and holds CMPs accountable for their actions. By enforcing consequences for non-compliance, the Framework aims to foster a trustworthy and responsible environment for consent management.[33]

(iii) Functional Role of CMPs

Under the framework, the CMP's role has been established as an intermediary between Publishers, end users, and Vendors. This

classification establishes that the CMP's responsibilities lie in facilitating exchange of data, rather than determining the means and scope of data processing.[34]

(b) UK Information Commissioner Office (ICO)

While the ICO, as the supervisory authority for data protection in the United Kingdom, does not prescribe guidelines for consent management platforms, it suggests the use of preference-management tools like privacy dashboards to allow people to easily access and update their consent settings to manage consent. It is quite evident that the UK follows a model of consent management wherein the data user (i.e., the data fiduciary) establishes mechanisms for consent management in-house and incorporates a consent management tool along with the other services it provides to the data principal.[35]

The contours of operation of consent management platforms or tools should be spelt out clearly to achieve the three-fold objective of (I)users' empowerment, (II) accountability and transparency in functioning of consent managers, (III) and ease of integration with digital service providers.

While the framework implemented by the IAB and the recommendations of ICO on incorporation of privacy dashboards offer some insight, it is equally important to examine proposals for technical interventions like consent managers in other jurisdictions. The succeeding section examines this facet of consent management.

4.2 Regulatory Approaches to Consent Management- A Global Perspective

With the increasing significance of consent, statutory authorities have taken a proactive stance in addressing challenges related to seeking informed, affirmative, and action-based consent. To address the challenges associated with obtaining and managing consent in a compliant manner, regulatory authorities are taking steps to integrate consent management principles into their laws.

The following paragraphs demonstrate the changes made in various legislation because of the increased emphasis on consent management:

Germany

In Germany, data protection and the associated consent related obligations find their foundation in the right to informal self-determination granted in the Basic Law. In this context, on 20 May 2021, the Bundestag (German Parliament) adopted a draft law entitled the "Telecommunications and Telemedia Data Protection Act" (TTDSG), which aimed to amend the Telecommunications Act (TKG) and the Telemedia Act (TMG), thereby adapting both laws within the meaning of the ePrivacy Directive of the EU to the GDPR.[36]

Section 26 of the TTDSG offers the choice of utilizing approved services known as "Personal Information Management Services" (PIMS) for consent management. PIMS allows users to either grant or reject consent for specific data processing, with the information centrally stored. Websites can then access the stored information in PIMS, aiming to provide users with enhanced control and security over their consent choices.[37]

Additionally, the German Federal Ministry for Economic Affairs and Energy, in a press release further explained the process of consent management with respect to obtaining consent for placing cookies on the user's terminal equipment:

"With regard to cookies, the TTDSG is also intended to achieve user-friendly and competitive consent management, which should include recognized services, browsers and TeleMedia providers."[38]

France

In France, consent management primarily focuses on the use of cookies and the optimization of the opt-out consent mechanism. The French data protection authority, CNIL, issued a directive in October 2020 concerning cookies and other tracking technologies, which required all website operators to implement it by the end of March 2021. This directive covers various important aspects, including GDPR-compliant consent, the discontinuation of opt-out mechanisms where explicit consent is required, compliance with transparency requirements, an easily accessible option for revoking opt-ins, and the ability to verify all opt-ins.

The cookie and tracking directive in France is highly comprehensive and provides detailed guidance ranging from the technical aspects to the visual design of consent management on websites. Its aim is to ensure that consent practices related to cookies and trackers align with the requirements of the GDPR while also promoting transparency and user control over their personal data.[39]

Brazil

Consent management holds significant importance in Brazil, particularly in the realm of open finance. It entails obtaining explicit permission from consumers to share their financial data with Third-Party Providers, also referred to as TPPs. Consumers are empowered with the facility to grant, manage, modify, revoke, or close active consents for data sharing with third-party providers. Consent management plays a crucial role within Brazil's open finance initiative, which seeks to foster competition and innovation in the financial sector by enabling consumers to share their financial data with other institutions.

To enable this process, Brazil's open finance framework may require the participating financial institutions to offer clear and user-friendly tools for consent management. These tools may include a dashboard or interface displaying active consents, shared data, and purposes.

Through the dashboard, users may easily modify or revoke consents and access a history of past consents. This will ensure users maintain complete control over their financial data, making informed decisions about access and purpose.[40]

An examination of the laws and regulations in the above stated jurisdictions makes it clear that a precise replication of the Indian model of consent managers, as proposed under the DPDPA, is not currently being implemented globally. However, for limited use cases, such as consent related to cookies in the EU in general or consent related to financial data-sharing, there are some frameworks which have been adopted in other jurisdictions.

4.3 Prevalent industry practices for consent management

In today's regulatory landscape, laws and regulations are giving greater significance to informed consent as a crucial legal foundation for processing personal data. As a result, organizations are increasingly realizing the importance of efficiently managing the consent they acquire in accordance with these relevant statutes. This entails implementing robust consent management practices and systems to ensure compliance with data protection regulations and establish transparent and trustworthy relationships with data subjects.

As an industry practice, many businesses have adopted the use of Consent Management Platforms (CMPs) or platforms with consent management capabilities to effectively manage and monitor the personal data of their customers. Irrespective of the specific data privacy regulations they must adhere to, organizations require

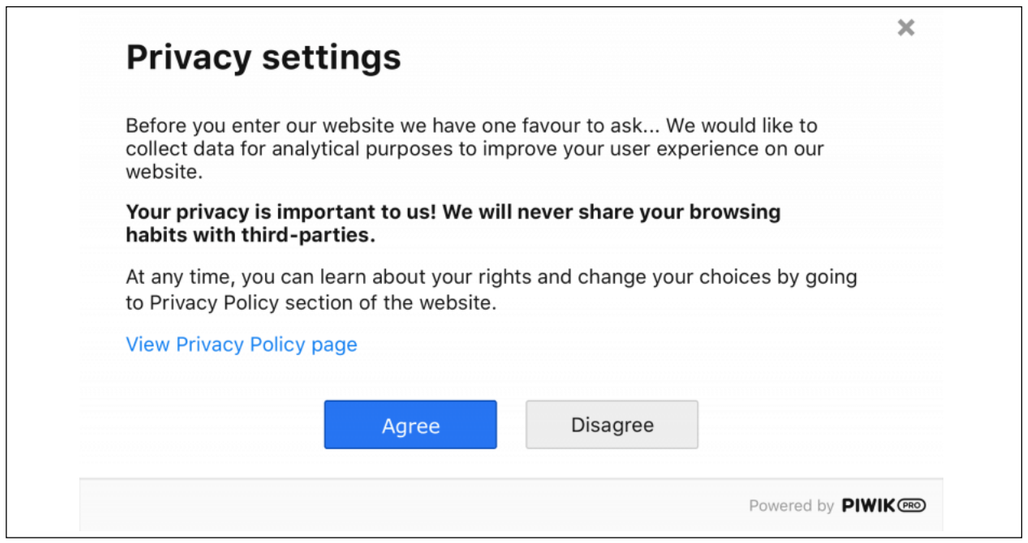
a clear understanding of which users have provided consent for different types of data processing. Moreover, it is crucial for them to maintain robust evidence of consent. Additionally, organizations seek streamlined processes to handle these tasks, not only for their own convenience but also to ensure a user-friendly experience for their customers.[41]

A CMP is a software solution that helps an organization to legally collect, document and manage consents in line with data protection laws and regulations like the EU's GDPR, California's CCPA, or Brazil's LGPD.[42]

CMPs play a crucial role in assisting organizations with compliance and avoiding potential fines by ensuring adherence to relevant legal provisions. These platforms promote transparency by providing users with comprehensive information about how their personal data is processed. Additionally, CMPs facilitate the association of a user's identity with their consent, enabling them to easily withdraw their consent when desired.

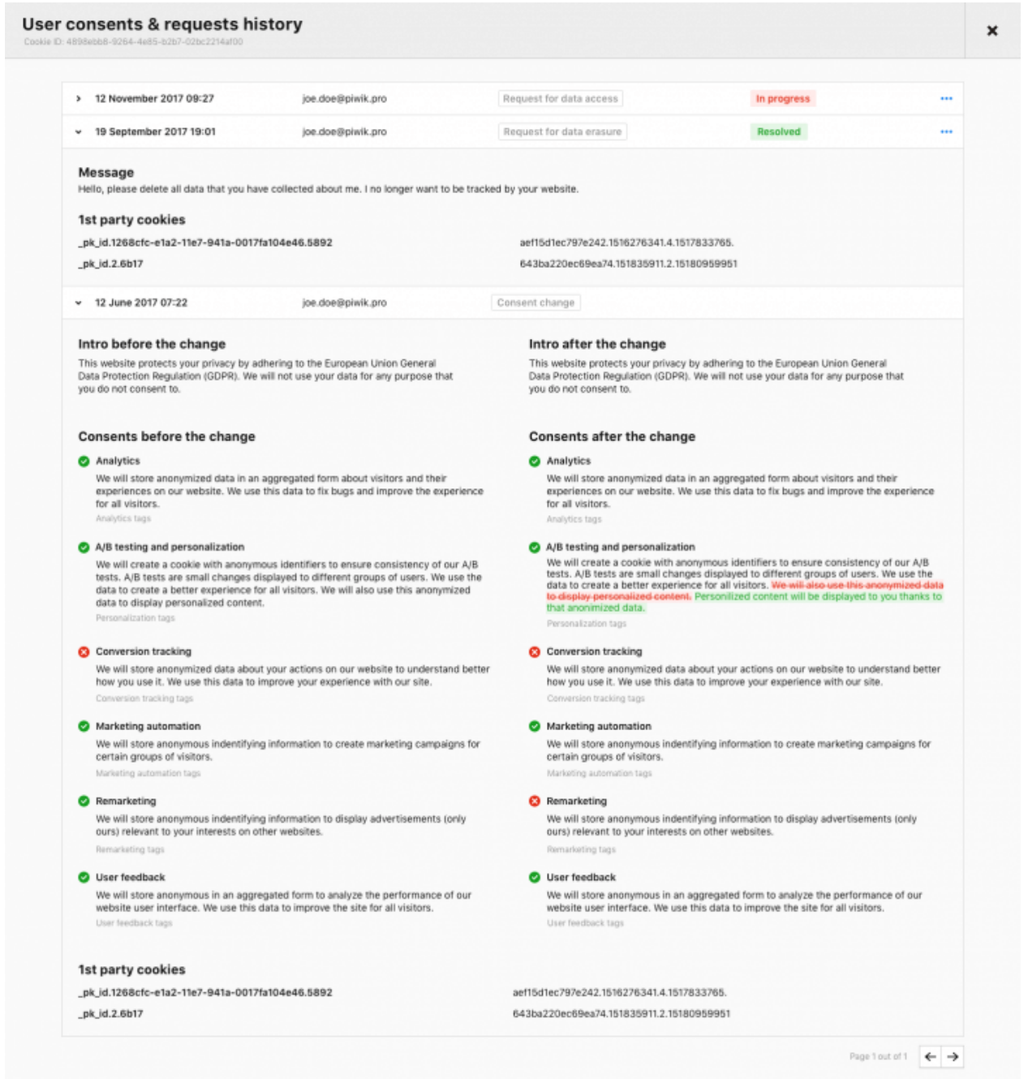
By implementing CMPs, organizations can effectively navigate the complexities of data privacy regulations and avoid penalties for non-compliance. These platforms provide the necessary tools and mechanisms to ensure that businesses meet the requirements set forth by laws such as the GDPR or other applicable data protection regulations.[43]

Collection of consent is the core functionality of the CMP. The consent is collected in a detailed manner wherein the users are first informed that their personal data is being processed. Next, detailed information about the scope of data processing is included in the Privacy Policy or a pop-up notice (or both). At the same time, users decide if they agree to the specific purposes of processing. The principle of free consent is followed consistently while the collection of consent.



Source: Single Consent Form, Piwik PRO Consent Manager[44]

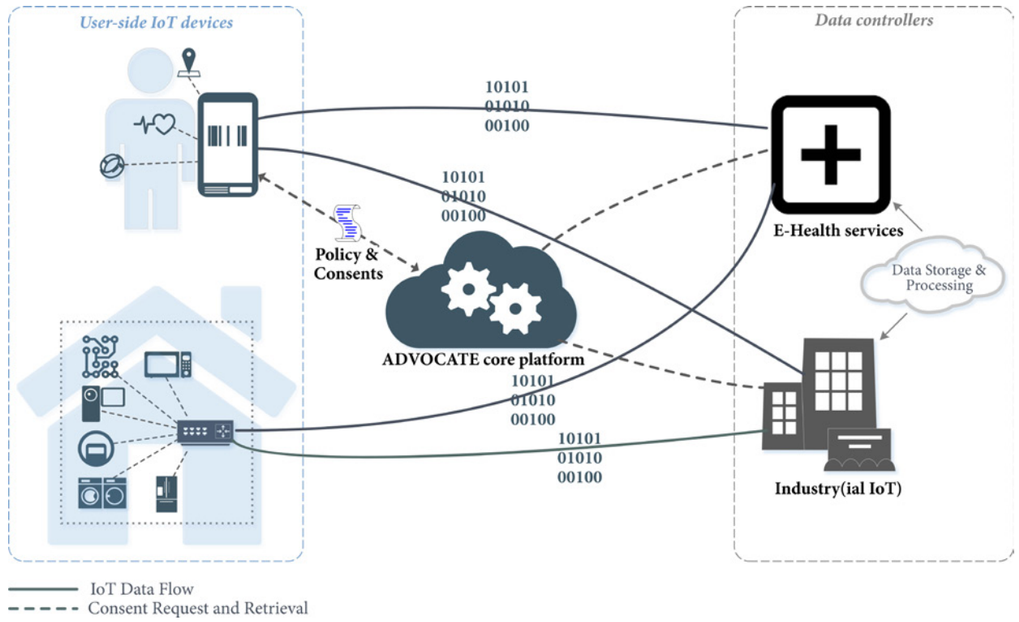
Additionally, a record of collected data is maintained to ensure compliance with various data privacy laws.



Source: Consent Manager Admin Panel, Piwik PRO Consent Manager[45]

Several researchers have advocated for the implementation of a robust Consent Management Platform (CMP) to effectively handle the consent of data principals. In one study, the focus was on leveraging a blockchain-based platform specifically designed for managing consent in the context of Internet of Things (IoT) devices.[46] The idea behind proposing a CMP for consent management is to provide data principals with more control over their consents and to create policies that correspond to data principals' consents.

An illustration of the framework proposed in the paper is given below:



Source: A Blockchain-Based Platform for Consent Management of Personal Data Processing in the IoT Ecosystem[47]

It is evident that the CMPs have been adopted as a best industry practice to manage the consent of the data principals and to facilitate the interoperability of the data. These platforms provide essential functionalities for obtaining and recording consent, enabling organizations to establish transparent and accountable data processing practices.

However, it is worth noting that consent management solutions which are popularly used by organizations are in the nature of B2B solutions. Therefore, organizations providing these solutions are ultimately accountable to data fiduciaries by whom they are onboarded.

5

RECOMMENDATIONS

The thorough evaluation of frameworks adopted in specific industries, such as the IAB framework which is utilized in the context of digital advertising or the Account Aggregator framework which is currently implemented in the banking and finance sector in India, establishes that a reference point for and industry and use-case agnostic framework for consent managers does not yet exist.

The proposal under the Digital Personal Data Protection Act 2023 to institute consent managers which (I) seem to function across industries and different types of digital products and services, and (II) are accountable to the data principals may therefore prove to be difficult to implement.

In this background, we propose the following set of recommendations:

1. Avoiding technical prescriptions in the legislation

The DPDPA introduces consent managers as a means to effectively manage the consent of data principals. However, it is important to acknowledge that various sectors have developed their own frameworks to address consent-related issues. These include the Account Aggregator framework by RBI for banking and finance, Health Information Exchange under ABDM for health data, Digital Consent Acquisition proposed by TRAI for telecom, and the Karnataka e-sahamati framework.

The various sectoral frameworks in place encompass their specific guidelines for organizations operating within those sectors. Introducing a consent manager framework within the DPDPA may potentially create a conflict with the existing initiatives already in effect. Furthermore, sectoral regulators or industry associations are better positioned to assess the unique intricacies of user consent within their respective contexts. They can then develop appropriate guidance or obligations for consent managers operating within their specific sectors.

Therefore, we recommend that subsequent rules which outline the operational framework for Consent Managers under the DPDPA should ensure that CMs as a technical intervention should not become a mandate.

2. Clarity on scope and functioning through delegated legislation

Alternatively, if the legislative intent is to create an overarching mechanism for operation of consent managers across industry sectors, we recommend that delegated legislation should shed clarity on the legal status of consent managers.

Entities akin to consent managers, including account aggregators and health information exchange managers, have well-defined legal statuses. For instance, account aggregators are classified as Non-Banking Financial Companies, while the National Digital Health Mission Data Management Policy, specifically in Para 4(e), defines Consent Managers as electronic

systems. Hence, to explicitly delineate the legal standing of consent managers, it is imperative to establish a precise and unambiguous definition that recognizes them as distinct legal entities and not merely categorize them as “persons”.

3. Recognition of existing industry practices around consent management

In the context of the DPDPA, consent managers are envisioned to be responsible to data principals. However, adopting an ecosystem where data principals choose a specific entity’s consent management solution could necessitate businesses to restructure their technical architectures to accommodate multiple consent management solutions. On the contrary, current industry practices suggest that organizations integrate consent management tools and solutions at the backend to streamline their internal processes for legal compliance.

After examining global statutes and practices, it is apparent that numerous jurisdictions have endorsed the adoption of consent management platforms to facilitate user consent management. For instance, in Germany, the “Telecommunications and Telemedia Data Protection Act” (TTDSG) provides the option to utilize approved services called “Personal Information Management Services” (PIMS) for consent management. Likewise, Brazil’s open finance framework may require the participating financial institutions to offer clear and user-friendly tools for consent management. Furthermore, as an industry-wide practice, many businesses have embraced the use of Consent Management Platforms (CMPs), or platforms equipped with consent management capabilities to efficiently handle and oversee the personal data of their customers.

Therefore, it is recommended that the existing practices and operational models for consent managers, such as utilizing consent management platforms, be acknowledged and legally recognized under the DPDPA framework. This would entail holding consent managers accountable to data fiduciaries through contractual obligations, allowing them to align with industry norms while fulfilling their responsibilities.

4. Operational guardrails for consent managers

In furtherance of the above recommendation, it is recommended that if consent managers are to be legally recognized under the DPDPA framework, the subsidiary rules and regulations under the law may prescribe operational guardrails for the functioning of such entities. The nature of such guardrails may be inspired from efforts undertaken globally.

For instance, the Transparency & Consent Framework (TCF) by the Interactive Advertising Bureau (IAB) may serve as a good reference point. It provides guidelines for consent management platforms (CMPs) in the digital advertising and marketing sector. Similarly, The UK’s Information Commissioner’s Office (ICO) and France’s CNIL provide guidelines for consent management platforms (CMPs). These guidelines cover technical and visual aspects of cookie consent management on websites, aiming to ensure compliance with GDPR requirements and empower users to have control over their personal data.

These requirements may encompass technical specifications aimed at promoting interoperability among consent managers. By prescribing these technical standards, the DPDPA can ensure that consent managers can effectively communicate and exchange consent-related information, facilitating seamless and efficient consent management processes. This approach promotes consistency, compatibility, and collaboration among consent managers, enhancing the overall effectiveness and reliability of the consent management framework established by the DPDPA.

REFERENCES

[1] Niti Aayog, Draft Data Empowerment and Protection Architecture, https://www.niti.gov.in/sites/default/files/2023-03/Data-Empowerment-and-Protection-Architecture-A-Secure-Consent-Based.pdf;

The Personal Data Protection Bill 2019, http://164.100.47.4/BillsTexts/LSBillTexts/Asintroduced/373_2019_LS_Eng.pdf

[2] PIB, Know all about Account Aggregator Network- A Financial data-sharing system, https://pib.gov.in/PressReleaseIframePage.aspx?PRID=1753713;

RBI, Directions regarding Registration and Operations of NBFC - Account Aggregators under section 45-IA of the Reserve Bank of India Act 1934, https://www.rbi.org.in/Scripts/bs_viewcontent.aspx?Id=3142

[3] ibid

[4] National Digital Health Mission: Health Data Management Policy, https://abdm.gov.in:8081/uploads/health_data_management_policy_455613409c.pdf

[5] Draft Health Data Management Policy, https://abdm.gov.in:8081/uploads/Draft_HDM_Policy_April2022_e38c82eee5.pdf

[6] Telecom Regulatory Authority of India (TRAI), Direction regarding implementation of Digital Consent Acquisition (DCA) under TCCCPR 2018, https://www.trai.gov.in/sites/default/files/PR_No.50of2023.pdf;

TRAI, Direction under section 13, read with sub-clauses (i) and (v) or clause (b) or sub-section (1) or section 11, or the Telecom Regulatory Authority or India Act, 1997 (24 of 1997) regarding implementation of Digital Consent Acquisition under Telecom Commercial Communications Customer Preference Regulations, 2018 (6 of 2018), https://www.trai.gov.in/sites/default/files/Direction_02062023.pdf

[7] PIB, Know all about Account Aggregator Network- A Financial data-sharing system, https://pib.gov.in/PressReleaseIframePage.aspx?PRID=1753713

[8] PIB, Know all about Account Aggregator Network- A Financial data-sharing system, https://pib.gov.in/PressReleaseIframePage.aspx?PRID=1753713;

Niti Aayog, Draft Data Empowerment and Protection Architecture, https://www.niti.gov.in/sites/default/files/2023-03/Data-Empowerment-and-Protection-Architecture-A-Secure-Consent-Based.pdf

[9] RBI, Master Direction- Non-Banking Financial Company - Account Aggregator (Reserve Bank) Directions 2016,
https://www.rbi.org.in/Scripts/BS_ViewMasDirections.aspx?id=10598

[10] PIB, Know all about Account Aggregator Network- A Financial data-sharing system,
https://pib.gov.in/PressReleaseIframePage.aspx?PRID=1753713

[11] ibid;

RBI, Directions regarding Registration and Operations of NBFC - Account Aggregators under section 45-IA of the Reserve Bank of India Act 1934,
https://www.rbi.org.in/Scripts/bs_viewcontent.aspx?Id=3142

[12] National Digital Health Mission: Health Data Management Policy,
https://abdm.gov.in:8081/uploads/health_data_management_policy_455613409c.pdf

[13] Draft Health Data Management Policy,
https://abdm.gov.in:8081/uploads/Draft_HDM_Policy_April2022_e38c82eee5.pdf

[14] ibid

[15] TRAI, Direction regarding implementation of Digital Consent Acquisition (DCA) under TCCCPR 2018,
https://www.trai.gov.in/sites/default/files/PR_No.50of2023.pdf;

TRAI, Direction under section 13, read with sub-clauses (i) and (v) or clause (b) or sub-section (1) or section 11, or the Telecom Regulatory Authority or India Act, 1997 (24 of 1997) regarding implementation of Digital Consent Acquisition under Telecom Commercial Communications Customer Preference Regulations 2018,
https://www.trai.gov.in/sites/default/files/Direction_02062023.pdf

[16] The Hindu Business Line, "Pesky calls: Telcos to roll out platform to take consent of users in 2 months,"
https://www.thehindubusinessline.com/news/pesky-calls-telcos-to-roll-out-platform-to-take-consent-of-users-in-2-months/article66931113.ece

[17] Karnataka e-Sahamathi Framework,
https://esahamathi.karnataka.gov.in/

[18] Ministry of Electronics and Information Technology (MeitY), Electronic Consent Framework,
https://dla.gov.in/sites/default/files/pdf/MeitY-Consent-Tech-Framework%20v1.1.pdf

[19] Times of India, "Evolution and challenges of account aggregators in India,"
https://timesofindia.indiatimes.com/blogs/kembai-speaks/evolution-and-challenges-of-account-aggregators-in-india/

[20] RBI, Non-Banking Financial Company - Account Aggregator (Reserve Bank) Directions 2016,
https://www.rbi.org.in/Scripts/bs_viewcontent.aspx?Id=3142

[21] National Digital Health Mission: Health Data Management Policy,
https://abdm.gov.in:8081/uploads/health_data_management_policy_455613409c.pdf

[22] Hyysalo, Hirvonsalo, et. al., "Consent Management Architecture for Secure Data Transactions,"
https://www.scitepress.org/papers/2016/59413/59413.pdf

[23] Digital Personal Data Protection Act 2023, Section 6(8), https://www.meity.gov.in/writereaddata/files/Digital%20Personal%20Data%20Protection%20Act%202023.pdf

[24] RBI, Master Direction- Non-Banking Financial Company - Account Aggregator (Reserve Bank) Directions 2016,
https://www.rbi.org.in/Scripts/NotificationUser.aspx?Id=10598&Mode=0

[25] Draft Health Data Management Policy,
https://abdm.gov.in:8081/uploads/Draft_HDM_Policy_April2022_e38c82eee5.pdf

[26] RBI, Directions regarding Registration and Operations of NBFC - Account Aggregators under section 45-IA of the Reserve Bank of India Act 1934,
https://www.rbi.org.in/Scripts/bs_viewcontent.aspx?Id=3142

[27] Office of the Privacy Commissioner of Canada, "Data at your Fingertips Biometrics and the Challenges to Privacy"
https://www.priv.gc.ca/en/privacy-topics/health-genetic-and-other-body-information/gd_bio_201102/

[28] Shuaib, Abdella et. al., "Secure decentralized electronic health records sharing system based on blockchains,"
https://www.sciencedirect.com/science/article/pii/S1319157821001051

[29] Interactive Advertising Bureau (IAB), The Transparency & Consent Framework (TCF) v2.2,
https://iabeurope.eu/transparency-consent-framework/

[30] IAB, Transparency & Consent Framework (TCF) Policies,
https://iabeurope.eu/iab-europe-transparency-consent-framework-policies/

[31] Managing Purposes and Legal Bases, IAB TCF Policies,
https://iabeurope.eu/iab-europe-transparency-consent-framework-policies/

[32] Accountability, IAB TCF Policies,
https://iabeurope.eu/iab-europe-transparency-consent-framework-policies/

[33] Policies for Vendors, Accountability, IAB TCF Policies,
https://iabeurope.eu/iab-europe-transparency-consent-framework-policies/

[34] IAB TCF Policies,
https://iabeurope.eu/iab-europe-transparency-consent-framework-policies/

[35] Information Commissioner's Office, What methods can we use to provide privacy information?,
https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/individual-rights/the-right-to-be-informed/what-methods-can-we-use-to-provide-privacy-information/#how3;

Niti Aayog, Draft Data Empowerment and Protection Architecture,
https://www.niti.gov.in/sites/default/files/2023-03/Data-Empowerment-and-Protection-Architecture-A-Secure-Consent-Based.pdf

[36] Consent Management in Europe – an overview of the situation in Germany, France, Italy and the UK,
https://www.commandersact.com/en/consent-management-europe/

New German Telecommunications-Telemedia Data Protection Act,
https://www.gesetze-im-internet.de/ttdsg/TTDSG.pdf

[37] Deloitte, New German Telecommunications-Telemedia Data Protection Act, https://www2.deloitte.com/dl/en/pages/legal/articles/telekommunikation-telemedien-datenschutz-gesetz.html

[38] Law to protect privacy in the digital world passed, https://www.bmwk.de/Redaktion/DE/Pressemitteilungen/2021/05/20210528-gesetz-zum-schutz-der-privatsphaere-in-der-digitalen-welt-beschlossen.html

[39] CNIL, Cookies and other trackers: the CNIL publishes amending guidelines and its recommendation, https://www.cnil.fr/fr/cookies-et-autres-traceurs/regles/cookies/lignes-directrices-modificatives-et-recommandation

[40] Open Finance Brazil, https://www.bcb.gov.br/en/financialstability/open_finance;

Open Finance Brazil FAQ, https://www.bcb.gov.br/en/about/faq

[41] Osano, Consent Management Without the Complexity, https://www.osano.com/solutions/consent-management-platform

[42] ibid

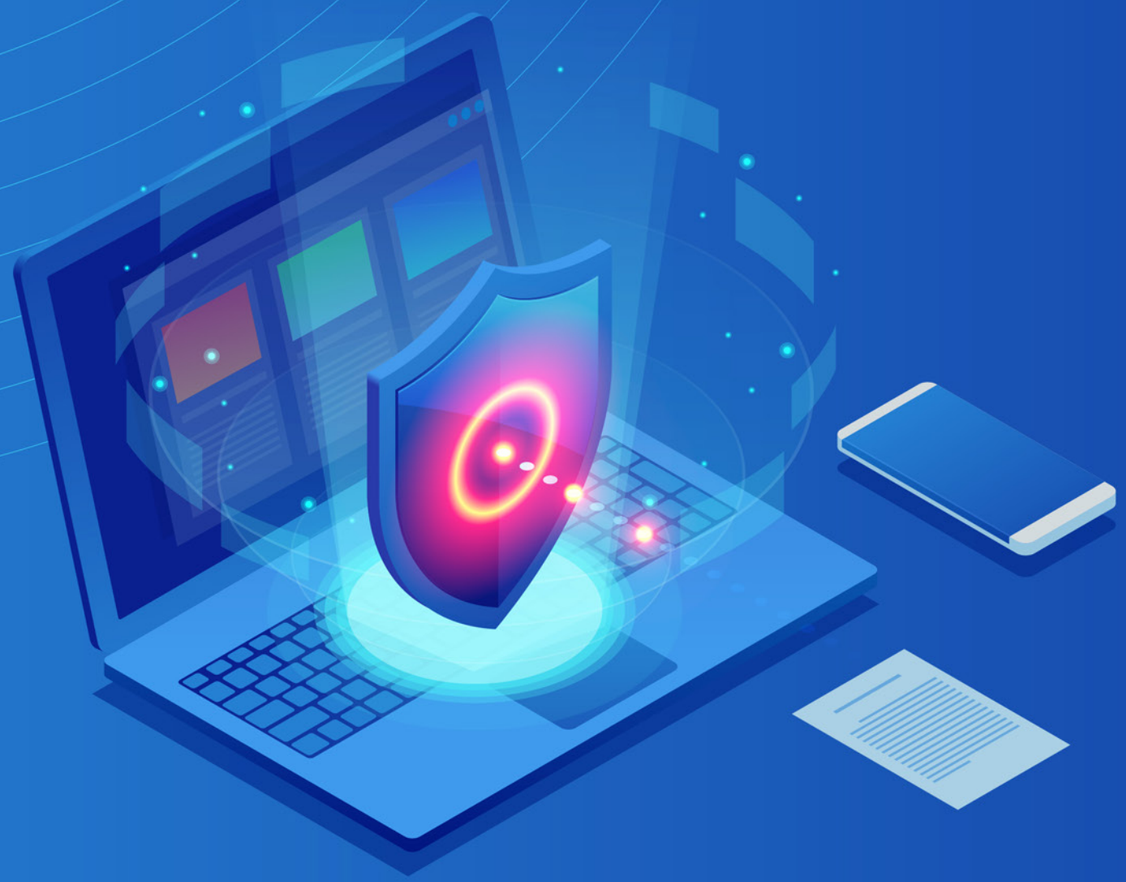
[43] Osano, Consent Management Without the Complexity, https://www.osano.com/solutions/consent-management-platform

[44] ClearCode, Single Consent Form- Piwik PRO Consent Manager, https://clearcode.cc/blog/consent-management-platform/#the-iab%E2%80%99s-gdpr-transparency-and-consent-framework

[45] ClearCode, Consent Manager Admin Panel- Piwik PRO Consent Manager, https://clearcode.cc/blog/consent-management-platform/#the-iab%E2%80%99s-gdpr-transparency-and-consent-framework

[46] Rantos, Drosatos et. al., “A Blockchain-Based Platform for Consent Management of Personal Data Processing in the IoT Ecosystem,” https://www.hindawi.com/journals/scn/2019/1431578/

[47] ibid



Section 3

TOOLS AND MODALITIES FOR CROSS-BORDER DATA FLOWS: A PRIMER FOR POLICYMAKERS

Executive Summary

This section of the report seeks to analyze and explore the provisions of the Digital Personal Data Protection Act 2023 (DPDPA) regarding the facilitation of cross-border data transfers. It also addresses possible implementation challenges and concerns that may arise from this approach. Additionally, it examines the regulatory practices related to cross-border data transfers worldwide. By referring to global practices from various jurisdictions, it evaluates the existing framework proposed under the Act for cross-border data transfers. The purpose of this section is to propose regulatory recommendations that can effectively and efficiently implement the legal requirements necessary to facilitate cross-border data transfers.

The first chapter provides a comprehensive overview of the significance of international data transfers and their role in promoting global trade and services. It highlights the importance of facilitating cross-border data transfers in today's interconnected world. It further delves into the approach taken by the DPDPA regarding cross-border data transfers.

It argues that there are ambiguities in the DPDPA pertaining to aspects such as the requirements for lawful data transfers, the safeguards for protecting personal data during transfers, or the conditions for cross-border data sharing.

The second chapter focuses on a critical analysis of the possible concerns surrounding the negative listing approach implemented by the DPDPA regarding cross-border data transfers. It scrutinizes the effectiveness of this approach in ensuring the secure transfer of personal data across borders. Key concerns addressed include the lack of clarity in the regulatory process for cross-border data flows, absence of guidelines for notifying restricted countries for cross-border data transfer and disregarding established tools and mechanisms for data transfers.

Furthermore, the chapter presents a comprehensive overview of the mechanisms adopted globally for facilitating cross-border data transfers. By considering international practices and approaches, this section of the report aims to provide a broader perspective on the subject matter, allowing for a more informed assessment of the limitations and concerns associated with the negative listing approach.

The concluding chapter conducts an in-depth analysis of data transfer frameworks specific to different jurisdictions. By studying the practices of diverse jurisdictions, this analysis aims to capture a comprehensive understanding of the global landscape regarding data transfers.

The findings from this section contribute to the overall understanding of the regulatory landscape and facilitate the development of informed recommendations for regulatory changes or improvements in the field of data transfers.

1

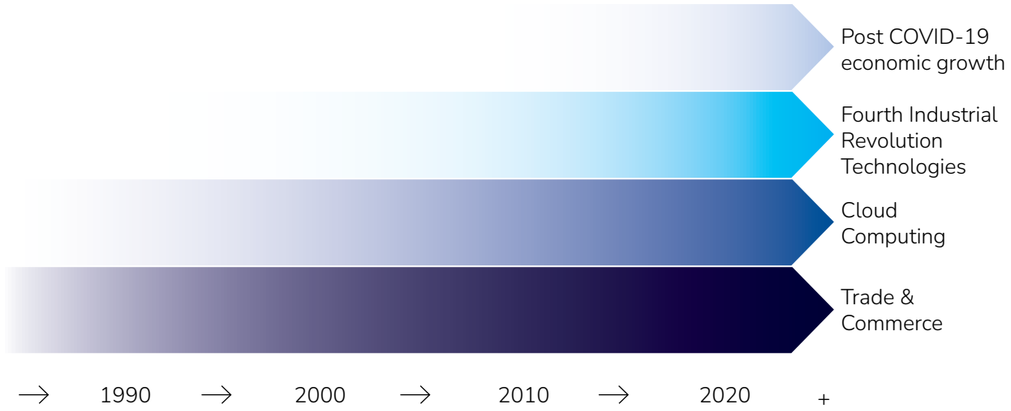
UNDERSTANDING THE SIGNIFICANCE OF INTERNATIONAL DATA TRANSFERS

In the digital era, the ability to access, utilize, and transfer data across borders plays a crucial role in driving economic growth. In every industry, be it manufacturing, services, agriculture, or retail, data is a fundamental resource, and its seamless global circulation is vital. Whether through direct means or by leveraging expansive data infrastructure like cloud computing, the interconnectedness of the world has facilitated international economic engagement, enabling individuals, startups, and small businesses to partake in global market opportunities.[1]

Cross-border data transfers play a vital role in facilitating global trade and services. These transfers enable businesses of all sizes to meet their basic needs, from internal communication to streamlining supply chains across different locations. Small and medium-sized enterprises can expand their reach and compete based on product quality rather than geographical limitations, connecting with potential customers worldwide.

The free flow of data is also essential for traditional industries like manufacturing, healthcare, education, and finance, as they often need to transfer information related to their tangible goods and services. Regardless of whether a company conducts direct online sales, data transfers across borders are frequently required to support their operations.[2]

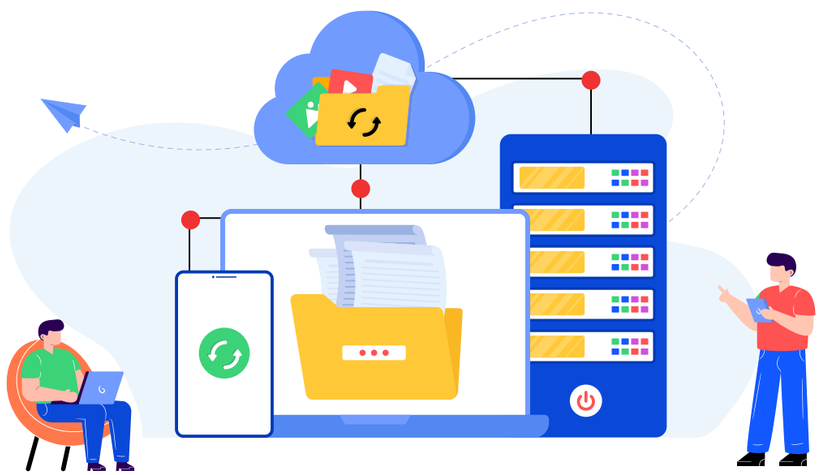
The increasing importance of cross-border data flows over time



Source: World Economic Forum, A Roadmap for Cross-Border Data Flows: Future-Proofing Readiness and Cooperation in the New Data Economy[3]

Under the Digital Personal Data Protection Act 2023 (DPDPA), Section 16 recognizes the significance of cross-border data transfers and grants the Central Government the authority to notify specific countries or territories outside India to which a Data Fiduciary cannot transfer personal data.[4]

The Act seeks to set up a framework to facilitate cross-border data transfers. It is, however, important to highlight that the Act lacks clarity and the specificities of notifying restricted jurisdictions and the process for the same will only be outlined in the future through delegated legislation. The Act fails to provide clear guidelines regarding the countries which are not eligible for data transfer. Additionally, it's not clear whether any supplementary mechanisms will have to be adhered to ensure secure transfers of personal data to non-restricted countries. Addressing these aspects is crucial to streamline the data transfer process and facilitate compliance for data fiduciaries. The succeeding chapters elaborate on these ambiguities in-depth.



2

DPDPA'S NEGATIVE-LISTING APPROACH: ANALYZING POTENTIAL IMPACT

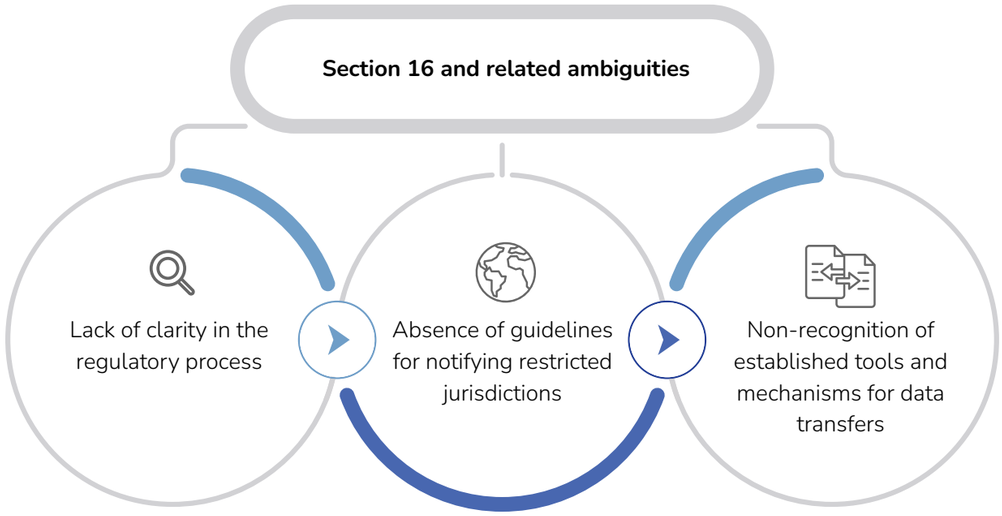
Considering the escalating pace of global data flows and the potential risks associated with national security, data breaches, and privacy concerns, it is crucial for a country's economic growth to prioritize the establishment of a robust legal framework that governs cross-border data transfer. Such a framework serves as a crucial foundation that enables the smooth execution of various research and development endeavors. Additionally, it plays a pivotal role in safeguarding intellectual property, upholding the dignity of human rights, and guaranteeing the essential security of personal data. By providing a structured and reliable system, a nation's data protection framework can foster innovation while ensuring that ethical considerations are upheld, enabling progress in a responsible and secure manner. Its implementation promotes a harmonious balance between the advancement of knowledge and technology and the protection of fundamental human values.5

The idea of a list of restricted jurisdictions for transfers of personal data in the DPDPA is novel. However, the notion of a negative list of jurisdictions has been implemented as a policy intervention in the context of trade restrictions outlined in Chapter 2 of the Foreign Trade Policy issued by the Directorate General of Foreign Trade (DGFT). The policy prohibits the

When contrasted against earlier iterations of data protection laws in the country, the DPDPA, through Section 16, takes a liberal approach towards facilitating cross-border data transfers. The provision outlines that data transfers outside the territory of India will be generally permitted, barring transfers to countries which are notified as restricted.

However, the lack of specific provisions or guiding principles in the Act regarding cross-border data flows may create a sense of regulatory uncertainty for entities required to comply with these obligations. This uncertainty may eventually hinder the envisioned ease-of-doing business, as organizations would face challenges in navigating the requirements for cross-border data transfers. Without clear guidelines or a framework in place, businesses may struggle to establish efficient and compliant processes for international data transfers, which could have unintended negative consequences.

The subsequent paragraphs outline the concerns linked to the present framework of cross-border data transfers as embraced by the DPDPA.



2.1 Lack of clarity in the regulatory process

Most jurisdictions worldwide establish independent bodies or boards dedicated to data protection. For instance, in Saudi Arabia, Data Fiduciaries may only store and process Personal Data outside Kingdom of Saudi Arabia after obtaining written approval from the relevant "Regulatory Authority" and the Regulatory Authority must coordinate with the National Data Management Office (NDMO). The term "Regulatory Authority" refers to an independent governmental or public entity with regulatory responsibilities in a specific sector, as defined by a legal instrument. In cases where Data Fiduciaries are not subject to specific Regulatory Authorities, the NDMO assumes the roles and functions of these authorities. Therefore, Data Fiduciaries must coordinate with the NDMO and obtain their approval before sharing Personal Data with entities located outside of Saudi Arabia.[8]

Similarly, in Malaysia, under the Personal Data Protection Act 2010 (PDPA), a data user may not transfer personal data to jurisdictions outside of Malaysia unless that jurisdiction has been specified by the Minister. The Personal Data Protection Commissioner (Commissioner) appointed under the PDPA is further considering issuing a guideline on the mechanism and implementation of cross border data transfer and has sought feedback on the important matters to be considered in the proposed guideline.[9]

Further, in Algeria, the transfer of personal data by a data fiduciary to a foreign State is only permitted if authorized by the national authority in accordance with the Law on protection of natural persons in personal data processing. Furthermore, such a transfer can only occur if the receiving State guarantees an adequate level of protection for the privacy and fundamental rights and freedoms of individuals in relation to the processing of said data.[10]

The DPDPA does not provide much clarity on the composition of the Data Protection Board. The Central Government exercises control over the composition and structure of the Data Protection Board, raising concerns about the independence of the appointed board members, who are entrusted with investigating issues of non-compliance with the Act. The DPDPA provides limited insight into the functioning and operational independence of the Data Protection Board. To ensure independence, the Act could take inspiration from institutions like the RBI and SEBI in establishing the Data Protection Board.[11]

Additionally, it is essential to emphasize the lack of well-defined guidelines for notifying restricted countries in the context of cross-border data transfers. This ambiguity introduces significant uncertainty in the notification process and gives rise to numerous concerns. The following paragraphs provide a comprehensive exploration of these concerns.

2.2 Absence of guidelines for notifying the restricted jurisdictions

Section 16 of the DPDPA addresses the transfer of personal data outside India. It grants authority to the Central Government to notify specific countries or territories to which a Data Fiduciary cannot transfer personal data.[12]

It is relevant to point out that this provision is a limited one and bestows complete discretion on the Central Government to notify restricted jurisdictions for data transfers.

The provisions of the DPDPA do not prescribe guiding principles or outline a framework based on which the determination of ineligible countries shall be made under Section 16. This may arguably cross the threshold of excessive delegated legislation. In India, it is firmly established that fundamental and primary legislative functions should be carried out by the legislature itself and cannot be delegated to the executive.

Additionally, the negative list approach to cross-border data transfers with minimal guidance around its execution raises a number of concerns. Specifically, there is no clarity surrounding whether any conditions or supplementary mechanisms will be prescribed for transferring personal data to non-restricted jurisdictions.

In the context of Indian law, there have been notable instances where the courts have taken a clear stance against excessive delegation, considering it unconstitutional. For instance, in the case of Gwalior Rayon Mills Mfg. (WVG) Co. Ltd. v. Assistant Commissioner of Sales Tax, the Supreme Court expressed its opinion that one of the well-established principles in Constitutional Law is that the authority granted to the legislature to enact laws cannot be delegated to any other body or authority. This signifies that the legislature must retain the responsibility of fulfilling its primary legislative function, rather than delegating it to external entities.[13]

Similarly, in the case of Ramesh Birch v. U.O.I, the Supreme Court emphasized that the primary legislative function should generally be performed directly by the legislature itself, without reliance on third parties or intermediaries. This further reinforces the idea that the power and duty to legislate should not be shifted to other entities but should be exercised by the legislative body itself.[14]

Additionally, the negative list approach to cross-border data transfers with minimal guidance around its execution raises a number of concerns. Specifically, there is no clarity surrounding whether any conditions or supplementary mechanisms will be prescribed for transferring personal data to non-restricted jurisdictions. The absence of explicit clarity around execution of section 16 of the Act may introduce uncertainty during the drafting of contractual agreements between data fiduciaries and processors. This absence of clear guidelines in the DPDPA creates uncertainty for foreign investors considering investments in India. The existence of well-defined standards, like the European Standard Contractual Clauses (SCC), provides confidence and clarity when entering contracts. One of the main advantages of the European SCC is that these contain clauses regulating the transfer and processing of personal data which are deemed to be in compliance with the European General Data Protection Regulation (GDPR). The Act could also benefit from adopting insights from international frameworks such as the Organization for Economic Co-operation and Development (OECD) and the US-Mexico-Canada Trade Agreement (USMCA) to enhance its regulatory approach.[15]

Further, DPDPA can also refer to the European Commission's recently approved adequacy decision for the EU-U.S. Data Privacy Framework. This decision provides a comprehensive level of detail by explicitly addressing the obligations arising from the EU-U.S. Data Privacy Framework. Additionally, it outlines the limitations and safeguards that

It is crucial to recognize that the process of determining the suitability of a country for data transfer is both lengthy and arduous.

come into play when personal data transferred to the United States is accessed by U.S. public authorities, specifically for purposes of criminal law enforcement and national security.[16]

It is also important to note that the transfer of personal data could face a sudden halt for business entities in the absence of clearly defined criteria for restricting transfers to a jurisdiction and without a transition period for compliance. While a negative list approach to data transfers is novel, one may assume that a process similar to adequacy assessment may be undertaken to notify a jurisdiction as being restricted for data transfers. Based on this assumption, a perusal of adequacy assessment approaches globally provides an insight into the extent of evaluation involved in this process. For example, when evaluating the adequacy status of a third country, the United Kingdom follows a four-phase approach: (1) Gatekeeping, (2) Assessment, (3) Recommendation, and (4) Procedural.

During the Gatekeeping phase, the UK considers whether to initiate an adequacy assessment for a particular country, taking into account policy factors that align with UK interests. In the Assessment phase, information regarding the level of data protection in the target country is collected and analyzed, focusing on its data protection laws and practices. The Recommendation phase involves providing a recommendation to the Secretary of State.

Lastly, the Procedural phase entails the creation of pertinent regulations and their submission to Parliament.[17]

Similarly, the decision-making process of the European Commission involves considering various criteria, such as commercial relations, data flow volume, privacy protection quality, political relationship, promotion of common values, and shared objectives at an international level. This approach can lead to arbitrary or subjective decisions, creating obstacles to the free movement of data.[18]

Therefore, a possible drawback of this approach is that it would likely involve in-depth evaluation and deliberation processes to determine the jurisdictions to which transfer of personal data must be restricted.

Further, it is important to highlight that the negative listing approach in the Act does not provide guidance on the process of adding or removing countries from the list if they fail to uphold the aspects related to India's national security, nor does it address how privacy and security concerns would be addressed under this strategy.

A negative list approach is undoubtedly a step forward in terms of ensuring liberal data transfers to promote innovation in the digital economy. The DPDPA itself is a principle-based legislation which forms the baseline for data protection regulation in the country. However, it is parallelly important for the rules and regulations framed thereunder to ensure that transfers of personal data to non-restricted jurisdictions are safe, secure, and consider existing mechanisms for data transfers that are deployed across industry sectors.

2.3 Non-recognition of established tools and mechanisms for data transfers

Across the globe, different jurisdictions employ diverse approaches to facilitate the safe and efficient transfer of data across geographical borders. However, in its limited recognition of negative listing as the only viable mechanism for

While undertaking the evaluation of countries for the negative list may not be a hindrance in and of itself, the lack of clarity around the process surrounding the making of this decision, as well as around the factors taken into consideration for restricting transfers to a jurisdiction may create business and policy uncertainty.

enabling transfer of personal data beyond the Indian territory, the provisions of the Act hamper the ability of organizations to undertake secure transfers of personal data to non-restricted countries.

Furthermore, there may be legitimate reasons to transfer personal data outside India to a jurisdiction on the negative list. A growing number of companies are increasingly establishing their Global Capability Centers (GCCs) in India.[19] It is feasible that such global organisations may, for a number of administrative reasons, have to transfer, for instance, employee's personal data outside India to a jurisdiction which may be on the negative list. To exonerate Data Fiduciaries from unforeseen liabilities, it is important to also take

into consideration these types of scenarios and supplement the negative listing approach with a recognition of established tools and mechanisms for international data transfers.

As detailed in the succeeding paragraphs, there are valid reasons for jurisdictions to recognize several valid legal routes for data transfers. The technical architecture within which data is being shared may differ, along with the purposes of data sharing, or the intended recipient of the data. All these factors necessitate the existence of a multitude of mechanisms enabling data transfers, to ensure that organizations are best placed to opt for the means which are least onerous while ensuring compliance with the principles of the law.

Contractual Clauses

The use of contractual clauses was first prescribed by the General Data Protection Regulation (GDPR). According to GDPR, contractual clauses ensuring appropriate data protection safeguards can be used as a ground for data transfers from the EU to third countries. This includes model contract clauses – so-called standard contractual clauses (SCCs) – that have been "pre-approved" by the European Commission.

Further, numerous organizations and third countries are in the process of developing or have already issued their own model contractual clauses. These clauses are based on aligned principles that are also reflected in the SCCs of the European Union.[20]

Apart from the European Union, several other countries use contractual clauses as a viable method to transfer data. Brazil uses contractual clauses as an adequate guarantee of compliance with the principles and rights provided to the data principals by Brazilian General Personal Data Protection Act (LGPD).[21]

Similarly, the ASEAN member states have implemented Model Contractual Clauses (ASEAN MCCs) as standardized data protection clauses to facilitate the cross-border transfer

It is crucial for a comprehensive and effective data protection framework to incorporate a bouquet of legally recognized measures for facilitating secure and compliant cross-border data transfers.

of personal data. These ASEAN MCCs can be incorporated into contractual agreements between data exporters and importers as a basis for allowing such transfers. The ASEAN MCCs serve as a baseline set of contractual clauses applicable in all ASEAN Member States, aiming to provide flexibility while adhering to the principles of the ASEAN Framework on Personal Data Protection. Businesses have the option to customize the MCCs to meet their specific needs, as long as the amendments align with the principles of the ASEAN Framework on Personal Data Protection.[22]

The implementation of contractual clauses as a data transfer mechanism offers several key advantages. Firstly, SCCs are standardized and pre-approved by relevant regulatory authorities, making them readily available and easy to adopt. Unlike other compliance mechanisms that necessitate prior authorization from a national data protection authority or incur higher implementation costs, SCCs provide a cost-effective and streamlined approach.

There exist some practical challenges that arise in the implementation of SCCs. The requirement to negotiate and execute separate agreements with each data exporter and importer, especially for new categories of data or purposes not covered by existing agreements, may be burdensome, particularly for small and medium-sized enterprises. Additionally, some jurisdictions require the prior approval of Data Protection Authorities for the use of standard contractual clauses, creating a bottleneck to their adoption.[24]

While contractual clauses may be accompanied with some compliance costs and obligations which can impact small businesses and start-ups,[25] however, the advantages of employing contractual clauses as an effective data transfer method largely outweigh the disadvantages associated with their use. The widespread adoption of these clauses across different jurisdictions underscores their status as a favored mechanism for data transfers. While some critics argue that contractual clauses may present limited drawbacks, such as potential delays in negotiations or the heightened compliance costs and increased obligations, these issues are relatively minor compared to the protections and facilitation they offer for cross-border data transfers.[26]

In conclusion, it is imperative to point out that as businesses continue to navigate the complexities of data protection, these clauses remain an indispensable tool for safeguarding privacy, promoting international collaboration, and ensuring the secure exchange of information across borders.

Binding Corporate Rules

Globally, Binding Corporate Rules (BCRs) are seen as a comprehensive framework of enforceable regulations designed to govern the processing of personal data. In the European Union, these rules guarantee the implementation of adequate safeguards to protect the rights of data subjects when transferring personal data between entities within a corporate group to countries outside the European Economic Area (EEA) that lack the necessary level of legal protection[27]. BCRs require approval from the appropriate national data protection authority to ensure compliance with the applicable data

SCCs offer flexibility as parties have the option to supplement them with additional clauses or integrate them into broader commercial contracts, if these provisions do not contradict the clauses directly or indirectly, and do not compromise the rights of data subjects. This flexibility allows organizations to tailor the clauses to their specific needs and incorporate them seamlessly into their existing contractual frameworks.[23]

protection regulations.[28] BCRs are particularly suited to multinational companies that want to regulate intra-group transfers on a worldwide basis to ensure compliance with requirements on the transfer of personal data outside the EEA.

In Singapore as well, the PDPC recognizes the requirement for adoption of BCRs in scenarios where the recipient of personal data is an entity which is related to the organization which is transferring the personal data.[29]

BCRs serve as an effective data transfer mechanism due to several advantages they offer. One key benefit is the considerable flexibility they provide to corporate groups, as updates to BCRs typically do not require explicit approval from data protection authorities. This flexibility reduces administrative burden and allows organizations to adapt their data protection practices more efficiently.

While BCRs may not be the most appropriate data transfer mechanism for smaller companies or for recipient companies which are outside the corporate group, they provide a unique utility for individual members of a corporate group.[30] By establishing a comprehensive set of rules, BCRs streamline the data transfer process within the group and provide a more cohesive approach to data protection.[31]

Certifications

Article 46(2)(f) of GDPR prescribes approved certification mechanisms as a new tool to transfer personal data to third countries in the absence of an adequacy agreement. The European Data Protection Board had adopted guidelines on certification as a tool for transfers. The main purpose of these guidelines is to provide clarification on the practical use of this transfer tool.

The Guidelines provide clarity on the use of certification as a means of demonstrating appropriate safeguards for cross-border data transfers outside the European Economic Area (EEA). Data exporters can rely on certification to verify that controllers or processors outside the EEA offer sufficient protection against specific transfer risks. To ensure the validity of the certification, the data exporter must confirm its status, coverage of the intended transfer, and whether it includes transit of data. It is also important to assess whether onward transfers are involved and whether adequate documentation exists for those transfers. Additionally, the data exporter must ensure the existence of a legally binding document, such as a contract or certification agreement, between the certification body and the data importer. This document should outline the importer's commitment to apply the certification criteria to all personal data transferred under the certification. The use of certification should be appropriately addressed in the agreements between controllers and processors or in data sharing agreements, depending on the roles of the parties involved.[32]

The above stated tools for cross-border data transfers are prevalent across jurisdictions globally. However, the DPDPA takes a limited approach to facilitating the safe and secure transfer of personal data outside the Indian territory. Additionally, the law also disregards the risk-based approach implemented by statutes like GDPR for data transfers. This approach entails evaluating the level of risk associated with transferring data to a third country. Data fiduciaries assess the risks involved before transferring data, even if the receiving country provides adequate safeguards for data security. This approach enhances accountability for data fiduciaries throughout the data transfer process.[33]

The existing mechanisms for cross-border data transfer offer data fiduciaries a structured framework to facilitate their data sharing activities. These mechanisms serve as valuable guidelines and references for data fiduciaries, enabling them to navigate the complexities of transferring data across borders. Different jurisdictions around the world have implemented a range of these mechanisms to govern data transfers. The third chapter provides a detailed exploration of the specific practices adopted by these jurisdictions.

3

JURISDICTION-SPECIFIC EXAMINATION OF DATA TRANSFER FRAMEWORKS

In today's interconnected world, the secure transfer of data across borders is crucial for global transactions. Recognizing this importance, countries worldwide have established dedicated mechanisms to facilitate and optimize cross-border data transfers. These mechanisms aim to simplify the transfer process, boost efficiency, and address uncertainties that may arise during such exchanges. The examples that follow exemplify the diverse approaches adopted by different countries, further underscoring the significance of these mechanisms in promoting seamless cross-border data flows.

Singapore

The Personal Data Protection Act of 2012, amended by the Personal Data Protection (Amendment) Act 2020, includes restrictions on offshore data transfers. These restrictions mandate that organizations must ensure the receiving organization outside of Singapore provides "comparable protection" in accordance with the standards outlined in the Act.[34]

Israel

Cross-border data transfers are restricted, allowing them only under specific circumstances. These include transfers to European Union (EU) Member States, transfers from an Israeli company to its foreign subsidiaries, transfers with the explicit consent of the individual, or transfers facilitated by a written agreement that obligates the data importer to adhere to Israeli data protection laws to a significant extent.[35]

Egypt

Egypt prioritizes the principle of adequacy to facilitate the transfer of data across borders. The Egyptian Personal Data Protection Law No.151 of 2020 sets regulations on the transfer of personal data to foreign countries. According to Article 14 of the law, the transfer of collected or processed personal data to a foreign country is prohibited unless that country ensures a level of personal data protection equal to or higher than what is specified in the law. In addition, a relevant license or permit from the Centre is required for such transfers. However, there are exceptions to this rule, primarily based on the consent of the data subject.

Furthermore, the law allows a data fiduciary or processor to grant access to personal data to another controller or processor outside Egypt under certain conditions. These conditions include having a conformity of work nature or purpose between the controllers or processors involved and a legitimate interest in the personal data by either the controllers, processors, or the data subject. It is also required that the level of legal and technical protection of the personal

data provided by the data fiduciary or processor abroad is not lower than the level of protection offered in Egypt.[36]

Indonesia

Indonesia allows cross-border data transfers under certain conditions. The data fiduciary must ensure that the receiving country provides an equal or higher level of personal data protection than what is mandated by the Personal Data Protection (PDP) Law, known as the "Adequacy of Protection" requirement. The PDP law is closely aligned with the European Union's General Data Protection Regulation (GDPR).[37] If the receiving country does not meet this adequacy standard, the data fiduciary must establish appropriate safeguards to ensure the protection of personal data. If neither adequacy nor appropriate safeguards are present, the data subject's prior consent is required for the transfer.

Currently, the absence of a PDP Agency and implementing regulations to the PDP Law means that the standards set by the General Data Protection Regulations still largely apply in practice. This means that data exporters or transferors have certain obligations, such as ensuring the effectiveness of supervision by relevant governmental institutions and providing access to electronic systems and data when required for supervision and law enforcement purposes. The data exporter or transferor also needs to coordinate with the Directorate General for Informatics Application (DITJEN APTIKA) within the Ministry of Communication and Informatics (MOCI) and submit certain reports to them prior to the transfer.[38]

Saudi Arabia

Under the Personal Data Protection Law (PDPL) in Saudi Arabia, personal data can be disclosed to an entity outside the territory for a limited set of purposes; to perform a contractual obligation relating to the Kingdom, to serve the interests of the Kingdom, for performance of an obligation involving the Data Subject, or to fulfill purposes set out in the Regulation.[39]

However, these transfers must still meet certain conditions. They should not compromise national security or the vital interests of Saudi Arabia, and adequate guarantees must be in place to maintain the confidentiality of the transferred personal data, meeting the standards set by the PDPL and the Executive Regulations. Furthermore, the transfer should involve only the minimum amount of personal data necessary, and approval from the competent authority, as defined in the Executive Regulations, is required.[40] Personal data may be transferred outside the jurisdiction, without meeting these conditions, in scenarios of extreme necessity to preserve the life of a Data Subject or to prevent, examine, and treat diseases.[41]

In certain cases, the competent authority may grant exemptions to the Data Controller, allowing them to bypass these conditions. The exemption can be granted if the transfer does not jeopardize national security or the vital interests of Saudi Arabia, if the competent authority, alone or jointly with other parties, determines that the personal data will receive an acceptable level of protection outside of Saudi Arabia, and if the personal data in question is not classified as sensitive data.[42]

Australia

In Australia, the Privacy Act stipulates that the transfer of personal information to organizations outside the country is permitted only if the entity has taken appropriate measures to ensure that the overseas recipient adheres to the Australian Privacy Principles (APP) concerning that personal information. This approach, known as the "Accountability Approach," establishes a framework that holds APP entities responsible for ensuring that overseas recipients handle individuals' personal information in compliance with the APPs. Consequently, the APP entity is held accountable if the overseas recipient mishandles the information.[43]

There is an exception for this general rule in scenarios where the APP entity reasonably believes that:

- The recipient of the information is subject to a law, or binding scheme, that has the effect of protecting the information in a way that, overall, is at least substantially similar to the way in which the APPs protect the information
- There are mechanisms that the individual can access to take action to enforce that protection of the law or binding scheme

Further, transfers of personal data to third countries are only permissible if there is a legal basis for the processing/transfer and one of the following applies:

- approved adequate/whitelisted jurisdictions
- to holders of specific certifications or followers of specific code of conduct programs each approved by the relevant data protection and security authority
- approved standard contractual clauses
- binding corporate rules
- derogations, such as consent, contract performance, necessity to establish, exercise or defend legal claims.[44]

Dubai

According to Article 26 of DPL No. 5 of 2020 ("DPL"), the transfer of personal data outside the DIFC is permitted if it is to a country or jurisdiction with adequate data protection measures or if it complies with the provisions specified in Article 27 of the DPL. Article 27 outlines the conditions for such transfers, which include the use of appropriate safeguards adopted by third countries, transfers conducted through SCCs, BCRs, certifications, and other approved methods.[45]

To summarise the various approaches discussed above, Israel restricts cross-border data transfers but allows them under specific circumstances, including transfers to EU Member States, transfers within an Israeli company's subsidiaries, transfers with consent, or transfers facilitated by written agreements complying

Countries worldwide have implemented various mechanisms and regulations to facilitate cross-border data transfers. Examples from Israel, Egypt, Indonesia, Dubai, Australia, and Saudi Arabia demonstrate different approaches to governing such transfers, and exemplify the diversity in policy approaches for the Indian data protection framework.

with Israeli data protection laws. Egypt emphasizes the principle of adequacy, permitting data transfers to foreign countries that offer an equal or higher level of data protection. Indonesia's data transfer approach is closely aligned with the GDPR.[46]

Saudi Arabia generally prohibits data transfers unless specific conditions are met, such as protecting life or vital interests, disease prevention, or obligations involving the country. However, transfers must comply with strict conditions to maintain national security, confidentiality, and minimum necessary data, subject to approval by the competent authority. Dubai sets forth conditions for data transfer,

requiring that such transfers may proceed only if the importing country offers adequate safeguards or if certain transfer mechanisms, such as BCRs, SCCs, certifications, and others, are utilized. Australia employs the "Accountability Approach" to ensure overseas recipients adhere to Australian Privacy Principles.

The DPDPA can get insights into the various elements to consider and specific provisions that can be incorporated to streamline cross-border data transfers by referring to the approaches employed by these countries. Different aspects work for different countries, and the DPDPA framework can refer to the same to gain insight about the benefits and limitations of these approaches for data transfers. For example, the DPDPA can examine Australia's accountability principle, Egypt's emphasis on adequacy and consent, Indonesia's requirements for adequate protection and Saudi Arabia's conditions for data transfers outside the country.

By considering and incorporating the best practices and mechanisms observed in other jurisdictions, the DPDPA can establish a comprehensive framework that promotes efficient and secure cross-border data transfers. This would provide clarity to businesses operating in India and create a conducive environment for global trade and services, enabling seamless data flows while ensuring the protection of individuals' privacy and data rights.

The data protection regulatory framework in India can explore additional aspects to enhance the facilitation of cross-border data transfers. This may include providing clearer guidelines on the obligations of businesses engaged in such transfers, and exploring various mechanisms for data transfers, such as standard contractual clauses, binding corporate rules, certifications, and more.

4

RECOMMENDATIONS

The preceding chapters shed light on the framework for cross-border data transfers under the Digital Personal Data Protection Act 2023. It is clear that in a hyper-digitized world with a focus on rapid, efficient transactions, communication, and information exchange, transfers of data (including personal data) across national borders are inevitable.

Though the legislative approach of the Act simplifies the process of data transfers when contrasted against earlier iterations. There are nonetheless practical challenges that can emerge as a result of this framework.

In light of the same, we propose a few recommendations below.

1. Enhanced Regulatory Clarity and Certainty

In the context of negative listing, it is imperative to create a sense of business and regulatory certainty. By doing so, data fiduciaries can have a better understanding of the requirements and expectations when engaging in such transfers, which in turn allows for more efficient planning and decision-making.

For example, the European Commission's recently approved adequacy decision regarding the EU-U.S. Data Privacy Framework provides a comprehensive overview of all specific aspects. Within this decision, the Commission thoroughly evaluates the obligations arising from the EU-U.S. Data Privacy Framework, along with the restrictions and protections in place when personal data is transferred to the United States and accessed by U.S. public authorities for national security and criminal law enforcement reasons.[47]

Further, examination of different data transfer mechanisms implemented by various jurisdictions like Israel, Singapore, Australia, and others reveals that these countries have taken proactive steps to establish comprehensive frameworks for data transfers beyond their jurisdictions. These mechanisms provide detailed guidelines and requirements for such transfers. Referring to the manner of detailing in these mechanisms can be highly beneficial in developing a specific set of criteria to enhance the negative listing approach.

We therefore recommend defining a definite set of criteria and outlining the process for determination of countries to which transfer of personal data from India is restricted. In defining the criteria, privacy and security considerations must hold paramount importance, along with safeguarding business and economic interests.

Additionally, it is important that once countries are notified as restricted for transfers of personal data, there may be a mechanism for periodic

and systematic review of their status, however, such review must not come at the expense of legal continuity of systems and processes for data transfers. To ensure business continuity, we also recommend an adequate transition period to be prescribed in consultation with the industry when new territories or jurisdictions are categorized as being 'restricted' for transfers of personal data.

2. A Risk Based Approach for Data Transfers

Data fiduciaries have a crucial responsibility to carefully evaluate the risks associated with data transfers. Before engaging in any transfer of data, it is essential for them to conduct a comprehensive assessment to identify potential risks and vulnerabilities. This assessment should consider factors such as the nature of the data being transferred, the destination country's data protection laws and practices, and any potential threats to data security or privacy.[48]

A risk-based approach broadens the scope of permitted transfers, allowing certain data transfers to proceed, even where the text of the laws of the importing country do not satisfy exporting country's requirements, so long as certain conditions are met. This approach is adopted by the European Data Protection Board (EDPB).[49]

In furtherance of our above stated recommendation which places emphasis on privacy and security as the foremost consideration for transfers of personal data, we recommend that India's data protection framework must adopt a risk-based approach for data transfers by considering various measures such as retaining a classification of personal data, specifically in the context of sensitive personal data. Such classification will then enable the creation of a graded approach towards implementing international data transfers. For instance, with the creation of categories of personal data, it may be possible to craft a spectrum of eligibility for notified jurisdictions. In effect, this would mean that while some jurisdictions may be deemed entirely safe and trusted to transfer Indian residents' personal data to, other jurisdictions may not be deemed safe enough to transfer sensitive personal data to.

> In outlining the process through which determination of restricted countries is made, it will become important to balance two competing interests; first, ensuring agility in the process so as to enable jurisdictions to be notified when warranted in the interests of national security, and two, ensuring operational stability for businesses which engage in cross-border data transfers.

REFERENCES

[1] The Brookings Institution, "Regulating for a digital economy: Understanding the importance of cross-border data flows in Asia," https://www.brookings.edu/research/regulating-for-a-digital-economy-understanding-the-importance-of-cross-border-data-flows-in-asia/

[2] U.S. Chamber of Commerce, "Business Without Borders: The Importance of Cross-Border Data Transfers to Global Prosperity," https://www.huntonak.com/images/content/3/0/v3/3086/Business-without-Borders.pdf

[3] World Economic Forum, "A Roadmap for Cross-Border Data Flows: Future-Proofing Readiness and Cooperation in the New Data Economy," https://www3.weforum.org/docs/WEF_A_Roadmap_for_Cross_Border_Data_Flows_2020.pdf

[4] Digital Personal Data Protection Act 2023 Section 16, https://www.meity.gov.in/writereaddata/files/Digital%20Personal%20Data%20Protection%20Act%202023.pdf

[5] Global Data Alliance, "Cross-Border Data Policy Index," https://globaldataalliance.org/resource/cross-border-data-policy-index/

[6] Directorate General of Foreign Trade, Foreign Trade Policy 2023, General Provisions Regarding Imports and Exports, https://content.dgft.gov.in/Website/dgftprod/4f665d2f-20cc-4887-ae6a-5ec912bc0d44/FTP2023_Chapter02.pdf

[7] Financial Action Task Force, High-Risk Jurisdictions subject to a Call for Action - June 2023, https://www.fatf-gafi.org/en/publications/High-risk-and-other-monitored-jurisdictions/Call-for-action-June-2023.html

[8] IAPP, "How to prepare for Saudi Arabia's Personal Data Protection Law," https://iapp.org/news/a/how-to-prepare-for-saudi-arabias-personal-data-protection-law/;

DLA Piper, Data Protection Laws of the World – Saudi Arabia, https://www.dlapiperdataprotection.com/index.html?t=authority&c=SA

[9] Personal Data Protection Act 2010 Section 129, https://www.kkd.gov.my/pdf/Personal%20Data%20Protection%20Act%202010.pdf;

DLA Piper, Data Protection Laws of the World – Malaysia, https://www.dlapiperdataprotection.com/index.html?t=transfer&c=MY

[10] DLA Piper, Data Protection Laws of the World – Algeria, https://www.dlapiperdataprotection.com/index.html?t=law&c=DZ

[11] Hindustan Times, "Looking at the cross-border data flow regime in the DPDP Bill 2022," https://www.hindustantimes.com/ht-insight/economy/looking-at-the-cross-border-data-flow-regime-in-the-dpdp-bill-2022-101680090578675.html

[12] Digital Personal Data Protection Act 2023 Section 16, https://www.meity.gov.in/writereaddata/files/Digital%20Personal%20Data%20Protection%20Act%202023.pdf

[13] Gwalior Rayon Mills Mfg. (WVG) Co. Ltd. v. Assistant Commissioner of Sales Tax, https://main.sci.gov.in/jonew/judis/6374.pdf

[14] Ramesh Birch v. U.O.I, https://main.sci.gov.in/jonew/judis/7960.pdf

[15] Office of the United States Trade Representative, Agreement between the United States of America, the United Mexican States, and Canada, https://ustr.gov/trade-agreements/free-trade-agreements/united-states-mexico-canada-agreement/agreement-between;

OECD, Recommendation of the Council concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data, https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0188

[16] European Commission, EU-US Data Privacy Framework, https://ec.europa.eu/commission/presscorner/detail/en/qanda_23_3752

[17] U.K. DCMS and DSIT, International data transfers: building trust, delivering growth and firing up innovation, https://www.gov.uk/government/publications/uk-approach-to-international-data-transfers/international-data-transfers-building-trust-delivering-growth-and-firing-up-innovation

[18] European Commission, Communication from the Commission to the European Parliament and the Council, Exchanging and Protecting Personal Data in a Globalised World, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM%3A2017%3A7%3AFIN

[19] Nasscom – Zinnov India GCC Trends Half Yearly Analysis, https://nasscom.in/knowledge-center/publications/nasscom-zinnov-india-gcc-trends-half-yearly-analysis

[20] European Commission, Standard contractual clauses for data transfers between EU and non-EU countries, https://commission.europa.eu/law/law-topic/data-protection/international-dimension-data-protection/standard-contractual-clauses-scc_en

[21] General Personal Data Protection Act (LGPD), Article 35, https://iapp.org/resources/article/brazilian-data-protection-law-lgpd-english-translation/;

DLA Piper, Data Protection Laws of the World – Brazil, https://www.dlapiperdataprotection.com/index.html?t=transfer&c=BR&c2=

[22] European Commission, Joint Guide to ASEAN Model Contractual Clauses and EU Standard Contractual Clauses, https://commission.europa.eu/system/files/2023-05/%28Final%29%20Joint_Guide_to_ASEAN_MCC_and_EU_SCC.pdf

[23] European Commission, New Standard Contractual Clauses, https://commission.europa.eu/law/law-topic/data-protection/international-dimension-data-protection/new-standard-contractual-clauses-questions-and-answers-overview_en

[24] U.S. Chamber of Commerce, "Business Without Borders: The Importance of Cross-Border Data Transfers to Global Prosperity," https://www.huntonak.com/images/content/3/0/v3/3086/Business-without-Borders.pdf

[25] Information Technology and Innovation Foundation, "The Role and Value of Standard Contractual Clauses in EU-U.S. Digital Trade," https://itif.org/publications/2020/12/17/role-and-value-standard-contractual-clauses-eu-us-digital-trade/

[26] U.S. Chamber of Commerce, "Business Without Borders: The Importance of Cross-Border Data Transfers to Global Prosperity," https://www.huntonak.com/images/content/3/0/v3/3086/Business-without-Borders.pdf

[27] European Commission, Binding Corporate Rules, https://commission.europa.eu/law/law-topic/data-protection/international-dimension-data-protection/binding-corporate-rules-bcr_en

[28] General Data Protection Regulation, Article 47, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&from=EN

[29] Personal Data Protection Commission (PDPC), Advisory Guidelines on Key Concepts in the PDPA, https://www.pdpc.gov.sg/-/media/Files/PDPC/PDF-Files/Advisory-Guidelines/the-transfer-limitation-obligation---ch-19-(270717).pdf

[30] IAPP, "BCRs: 'Best case route' or 'better call reinforcements'?," https://iapp.org/news/a/bcrs-best-case-route-or-better-call-reinforcements/

[31] PWC, Binding Corporate Rules, The General Data Protection Regulation, https://www.pwc.com/m1/en/publications/documents/pwc-binding-corporate-rules-gdpr.pdf

[32] European Data Protection Board, Guidelines 07/2022 on certification as a tool for transfers, https://edpb.europa.eu/system/files/2023-02/edpb_guidelines_07-2022_on_certification_as_a_tool_for_transfers_v2_en_0.pdf;

EDPB adopts guidelines on certification as a tool for transfers, https://edpb.europa.eu/news/news/2022/edpb-adopts-guidelines-certification-tool-transfers-and-art-65-dispute-resolution_en

[33] European Data Protection Law Review, A Risk-Based Approach to International Data Transfers, https://edpl.lexxion.eu/data/article/17963/pdf/edpl_2021_04-010.pdf

[34] Personal Data Protection Act 2012, Section 26, https://sso.agc.gov.sg/Act/PDPA2012?ProvIds=P14-#pr13-;

PDPC, Advisory Guidelines on Key Concepts in the PDPA, https://www.pdpc.gov.sg/-/media/Files/PDPC/PDF-Files/Advisory-Guidelines/the-transfer-limitation-obligation---ch-19-(270717).pdf

[35] Privacy Protection (Transfer of Data to Databases Abroad) Regulations, https://www.gov.il/BlobFolder/legalinfo/legislation/en/PrivacyProtectionTransferofDataabroadRegulationsun.pdf;

DLA Piper, Data Protection Laws of the World – Israel, https://www.dlapiperdataprotection.com/index.html?t=transfer&c=IL

[36] DLA Piper, Data Protection Laws of the World – Egypt, https://www.dlapiperdataprotection.com/index.html?t=transfer&c=EG

[37] DLA Piper, Data Protection Laws of the World – Indonesia, https://www.dlapiperdataprotection.com/index.html?t=law&c=ID

[38] ibid

[39] Saudi Authority for Data Protection and Artificial Intelligence,), Personal Data Protection Law, Article 29(1), https://sdaia.gov.sa/en/SDAIA/about/Documents/Personal%20Data%20English%20V2-23April2023-%20Reviewed-.pdf

[40] Saudi Authority for Data Protection and Artificial Intelligence,), Personal Data Protection Law, Article 29(2), https://sdaia.gov.sa/en/SDAIA/about/Documents/Personal%20Data%20English%20V2-23April2023-%20Reviewed-.pdf

[41] Saudi Authority for Data Protection and Artificial Intelligence,), Personal Data Protection Law, Article 29(3), https://sdaia.gov.sa/en/SDAIA/about/Documents/Personal%20Data%20English%20V2-23April2023-%20Reviewed-.pdf

[42] DLA Piper, Data Protection Laws of the World – Saudi Arabia, https://www.dlapiperdataprotection.com/index.html?t=transfer&c=SA&c2=

[43] Office of the Australian Information Commissioner, Overseas data flows, https://www.oaic.gov.au/engage-with-us/submissions/privacy-act-review-issues-paper-submission/part-8-overseas-data-flows;

Baker Mckenzie, International Data Transfer, https://resourcehub.bakermckenzie.com/en/resources/data-privacy-security/asia-pacific/australia/topics/international-data-transfer#:~:text=Yes.,overseas%20disclosures%20rather%20than%20transfers.

[44] ibid

[45] Dubai International Financial Centre, Data Export & Sharing Handbook, https://www.difc.ae/application/files/6316/6126/5296/DIFC-DP-GL-04_Rev.01_DIFC_DATA_EXPORT_AND_SHARING_HANDBOOK.pdf;

DLA Piper, Data Protection Laws of the World – Dubai, https://www.dlapiperdataprotection.com/index.html?t=transfer&c=AE2

[46] DLA Piper, Data Protection Laws of the World – Indonesia, https://www.dlapiperdataprotection.com/index.html?t=law&c=ID

[47] European Commission, EU-US Data Privacy Framework, https://ec.europa.eu/commission/presscorner/detail/en/qanda_23_3752

[48] European Data Protection Law Review, A Risk-Based Approach to International Data Transfers, https://edpl.lexxion.eu/data/article/17963/pdf/edpl_2021_04-010.pdf

[49] IAPP, "EDPB's data transfer recommendations adopt a risk-based approach with teeth," https://iapp.org/news/a/edpbs-data-transfer-recommendations-adopt-a-risk-based-approach-with-teeth/

CONCLUSION

The first part of this report (Part 1) delved into three key regulatory dimensions of the data protection framework in India; personal data breaches, consent managers, and cross-border data transfers. The research and analysis brought forth emphasizes that the Digital Personal Data Protection Act 2023 may have set a baseline structure for regulating these aspects of data protection, however, delegated legislation through rules and notifications will establish the practical implementation standards.

On personal data breaches, an examination of data protection laws and breach reporting requirements across jurisdictions reveals that adopting a risk-based approach to personal data breach reporting and notification is crucial to ensuring a governance mechanism which assures both effective compliance and meaningful information sharing with regulators and data principals. Across jurisdictions, through laws, guidance, and academic study, there is broader consensus that a risk-based approach in the context of personal data breaches could entail numerous interventions; defining personal data breaches clearly, identifying a threshold beyond which breaches are reportable/notifiable, adopting a phased approach to reporting data breaches, and outlining the information to be shared with data principals or the concerned supervisory authority in a manner which aligns with the overarching regulatory intent.

An evaluation of prevalent industry practices in consent management and existing frameworks for consent managers across segments in India sheds light on several key ambiguities that delegated legislation will need to address to operationalise the consent manager framework established by the DPDPA 2023. Ensuring interoperability, accountability, and transparent functioning of consent managers will be key to the functioning of consent managers in tandem with existing platforms used by data fiduciaries to manage the consent lifecycle internally.

Finally, the last section of this report on cross-border data transfers acknowledges the liberal approach to international data flows adopted under the DPDPA 2023. In a thriving digital economy that serves as a hub for provision of digital services, ensuring secure and efficient transfers of data is key to achieving economic growth. However, there remains some key elements of the cross-border data transfer framework which will have to be clarified through rules and notifications for a practicable implementation of the Act. This includes defining criteria and processes for notification of territories which are to be included in the list of restricted jurisdictions, as well as ensuring a viable transition period after changes are made to such notified jurisdictions.

A nasscom Initiative

Data Security Council of India (DSCI) is a premier industry body on data protection in India, setup by nasscom, committed to making the cyberspace safe, secure and trusted by establishing best practices, standards and initiatives in cybersecurity and privacy. DSCI brings together governments and their agencies, industry sectors including ITBPM, BFSI, telecom, industry associations, data protection authorities and think-tanks for policy advocacy, thought leadership, capacity building and outreach initiatives. For more info, please visit www.dsci.in

DATA SECURITY COUNCIL OF INDIA

Nasscom Campus, Fourth Floor, Plot. No. 7-10, Sector 126, Noida, UP - 201303

+91-120-4990253 | research@dsci.in | www.dsci.in

DSCI_Connect dsci.connect dsci.connect data-security-council-of-india dscivideo