REPORT ON DIGITAL PERSONAL DATA PROTECTION RULES 2025

# DPDP RULES

KAUTILYA SOCIETY - INDIA

MAR 2025

TABLE OF CONTENTS

KAUTILYA SOCIETY

KAUTILYA SOCIETY

# REPORT ON THE COMMENTS SENT ON THE DIGITAL DATA PROTECTION RULES, 2025

A COLLABORATIVE EFFORT OF THE KAUTILYA SOCIETY INDIA.

## CHILDREN'S DATA

### INTRODUCTION

It is not deniable that children are more exposed users in the digital ecosystem, who time and again face increased risk associated with data exploitation, profiling, and display of harmful content. To address these growing concerns, lawmakers globally have tried to incorporate better frameworks for children's privacy. India's Digital Personal Data Protection Act (DPDPA) of 2023 and the Digital Personal Data Protection Rules of 2025 are crucial for developing data protection rules for the country's benefit. It is pivotal that the children's personal data is considered for responsible and ethical processing while also emphasizing their safety and rights.

### GLOBAL PERSPECTIVES

#### 1. European Union

In today's digital economy, children's personal data has become a critical cause of concern. With children's increased usage of online services, their data is collected, processed and often exploited without adequate protections, raising serious privacy issues. The European Union's overarching General Data Protection Regulation1 (the "GDPR") recognises that children's personal data should be afforded special protections because they may be less aware of the risks and consequences of data sharing. The GDPR has influenced privacy laws beyond the European Union, and is often considered as a gold standard for data protection, transparency, and accountability. The primary principle behind the GDPR is that it views personal data as the property of the individual, not data controllers or processors. It applies to all EU citizens, wherever they may be situated and regardless of the organisation's location.

Under Article 8 of the GDPR2, the age of consent for the processing of personal data is set at 16 years. However, individual member states have the discretion to lower this threshold to a minimum of 13 years. For children below the established age of consent in respective countries, the GDPR mandates that organisations obtain verifiable consent from a parent or legal guardian before processing the child's personal data. Data controllers are required to make "reasonable" efforts under Article 8(2)[3] to verify that such consent is genuinely provided by individuals

[1] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) [2016] OJ L 119/1.
[2] Reg 2016/679 art 8.
[3] Reg 2016/679 art 8(2).

holding parental responsibility (although no specific procedure is prescribed for the same, resulting in vague interpretations from different regulators).

## 2. USA

In the United States, the primary regulation of children's data is governed by the Children's Online Privacy Protection Act (COPPA), which was enacted in 1998 and is enforced by the Federal Trade Commission (FTC)[4]. COPPA specifically targets websites, applications, and online services aimed at children under the age of 13 or those that knowingly gather information from this demographic. The law mandates that businesses provide succinct privacy policies, secure verifiable parental consent prior to collecting personal data, and grant parents the ability to review or erase their child's information. Failure to comply with these requirements can result in substantial penalties; for example, in 2019, YouTube faced a $170 million fine for breaching COPPA regulations.

In addition to COPPA, several federal laws oversee children's data within specific areas. The Family Educational Rights and Privacy Act (FERPA) restricts educational institutions from revealing students' academic records without obtaining parental approval. This has implications for platforms such as Google Classroom. Similarly, the Health Insurance Portability and Accountability Act (HIPAA) safeguards children's medical information managed by healthcare providers; however, it does not encompass most health records maintained by schools[5].

## 3. Australia

In the evolving landscape of digital regulation, Australia and India have recently introduced significant legislative measures aimed at enhancing online safety and data protection. Australia's Online Safety Amendment (Social Media Minimum Age) Act 2024,[6] while not in effect yet, establishes a minimum age requirement for social media usage. While the bill does

[4] Federal Trade Commission, 'Children's Online Privacy Protection Rule (COPPA)' (Federal Trade Commission, 16 CFR Part 312) https://www.ftc.gov/legal-library/browse/rules/childrens-online-privacy-protection-rule-coppa accessed 13 February 2025

[5] Reena Bajowala and Ashley Taylor, 'A Roundup of State Laws Related to Children's Privacy' (Loeb & Loeb LLP, 1 August 2023) https://www.loeb.com/en/insights/publications/2023/08/a-roundup-of-state-laws-related-to-childrens-privacy accessed 13 February 2025

[6] Online Safety Amendment (Social Media Minimum Age) Act 2024.

not dictate the how such compliance is to be done, some form of minimum age assurance procedure is to be expected.[7]

The SMMA Act amends the Online Safety Act 2021 to set a minimum age of 16 for social media account holders, within the meaning of the age restricted user within the meaning of section 5 of the Act.[8] While such an implementation is to be deferred at least 12 months after Royal Assent[9] and also incorporates a review of the same after 2 years,[10] it is to be noted that currently, such minimum age in Australia is 13 years. [11] Social media platforms are mandated to implement reasonable measures[12] to prevent individuals under this age from creating accounts. Non-compliance can result in substantial civil penalties, reaching up to AUD 49.5 million.[13] The Act provides exemptions for services primarily focused on messaging, online gaming, health, or education, as well as those deemed 'low risk' by the eSafety Commissioner. The Bill also provides a 'categorical rule-making' power to exclude certain services from the definition.

The Minister's Second Reading Speech expressed the government expectation of the broader definition to cover major social media platforms like TikTok, Facebook, Snapchat, Reddit, Instagram, and X, addressing parental concerns.[14]

### 4. Singapore and Japan

In the realm of data protection for children's personal information, both Singapore and Japan have established frameworks to safeguard young individuals' privacy, albeit with differing approaches and levels of specificity.

[7] Tech Policy Press, 'Online Safety Amendment (Social Media Minimum Age) Bill 2024' (*Tech Policy Press*) <http://techpolicy.press/tracker/online-safety-amendment-social-media-minimum-age-bill-2024/> accessed 11 February 2025.
[8] Online Safety Amendment (Social Media Minimum Age) Bill 2024, Point 2.
[9] Online Safety Amendment (Social Media Minimum Age) Bill 2024, s 63E of Part 4A.
[10] Online Safety Amendment (Social Media Minimum Age) Bill 2024, Point 16.
[11] House Of Representatives in The Parliament Of The Commonwealth Of Australia, *Explanatory memorandum* <https://parlinfo.aph.gov.au/parlInfo/download/legislation/ems/r7284_ems_b9c134ac-a19a-47b2-9879-b03dda6e3c1a/upload_pdf/JC014726.pdf;fileType=application%2Fpdf#search=%22legislation/ems/r7284_ems_b9c134ac-a19a-47b2-9879-b03dda6e3c1a%22> accessed 11 February 2025.
[12] Online Safety Amendment (Social Media Minimum Age) Bill 2024, Point 2.
[13] Online Safety Amendment (Social Media Minimum Age) Bill 2024, Division 2.
[14] Kwok Tang and others, 'Online Safety: Australia's Social Media Minimum Age Bill' (Herbert Smith Freehills, 3 December 2024) <https://www.herbertsmithfreehills.com/insights/2024-12/online-safety-australias-socia-media-minimum-age-bill> accessed 11 February 2025.

While the PDPA, the key legislation related to data protection in Singapore does not provide for any special protection with respect to Children, the advisory Guidelines by the PDPC contain certain provisions. It considers Children's data to be sensitive personal data and a higher standard of protection under the PDPA is accorded.[15] The Advisory Guidelines On The PDPA For Children's Personal Data In The Digital Environment also state that Any organisation that handles children's personal data should appropriately implement, "Basic and Enhanced Practices" as listed in the PDPC's Guide to Data Protection Practices for ICT Systems, to address potential risks and harms to children in the digital environment. While it states 'minors' as those under 21,[16] it carves out the exception that those at least 13 may give their consent, if the policy on the collection, use and disclosure as well as all the intricacies that come along with the consent are readily/sufficiently understandable by them. For any person below age 13, the consent of the individual that can legally give consent on behalf of the minor is required.

Japan's Approach to the Data Protection of Children is covered under their umbrella Act on the Protection of Personal Information ("APPI").[17] Similar to Singapore while the act in itself soes not accord any comprehensive protection on this front, The APPI Guidelines (General Rules) issued by PPC ("Guidelines") require Businesses to obtain consent from a minor's legal representatives, such as a person with parental authority over the minor, for the Business to process the minor's personal information, if the minor does not have the capacity to assess the consequences of giving consent to the Business.[18]

The requisite age of consent is not defined in the act, it is only indicated in the periodical Q&A by the PPC that the specific age at which someone is considered a child can vary depending on the type of personal information involved and the nature of the business, but generally speaking, individuals aged 12 to 15 and under are considered children. Lastly, it is also to be noted that in last year's interim summary (July 2024), the need for specific provisions for Children's Data Protection and more robust clarifications on items such as obtaining consent from the legal representatives, in situations in which consent of the data subjects is requires,

[15] Rule 6 of https://www.pdpc.gov.sg/-/media/files/pdpc/pdf-files/advisory-guidelines/advisory-guidelines-on-the-pdpa-for-children's-personal-data-in-the-digital-environment_mar24.pdf; PDPC's decision in Singapore Taekwondo Federation [2018] SGPDPC 17 at [21]-[27].
[16] r 8.1 https://www.pdpc.gov.sg/-/media/files/pdpc/pdf-files/advisory-guidelines/ag-on-selected-topics/advisory-guidelines-on-the-pdpa-for-selected-topics-(revised-may-2024).pdf
[17] APPI
[18] Guidelines, Section 2-16.

measures for safe management and age criterion etc which was observed and it is yet to be seen whether such provisions make it to the expected upcoming amendments.[19]

## POSITIVE OUTCOMES

There are several positive implications in the Act regarding children's safety. By limiting excessive data gathering, outlawing targeted advertising without parental approval, and guaranteeing tighter cybersecurity protections, the Digital Personal Data Protection (DPDP) Rules 2025 has taken positive steps to improve children's online privacy in India. An educational app, for example, can only gather the information required for learning and must remove it when it is no longer required. However, there are certain shortcomings.

## COMMENTS

The Draft Rules establish essential protections for children's data; however, they encounter operational ambiguities, compliance challenges, and deficiencies in addressing practical complexities.

The following are some of the observations made with certain recommendations:

| Specific Head | Summary | Recommendation |
|---|---|---|
| **Verifiable Parental Consent and Age Factor** | Authentication of parental consent is unclear and resource-intensive; no clear verification method or distinction between platform types. | Define "appropriate technical measures"; limit scope to child-focused platforms; align age threshold with GDPR. |
| **Reliable Details for Verification** | No accuracy checks for "reliable details"; no obligation for regular re-verification. | Specify acceptable proofs (e.g., government IDs); require annual updates or fraud-based re-verification. |
| **Government-Issued Tokens (e.g., DigiLocker)** | Assumption of security is unrealistic; no safeguards for government databases; lack of alternatives in low-digital-access areas. | Mandate encryption, audits, and offline alternatives (e.g., physical ID verification). |

[19] https://www.amt-law.com/en/insights/others/publication_0029311_en_001/

| | | |
|---|---|---|
| **Data Minimization and Third-Party Sharing** | Vague criteria may allow excessive data collection and third-party sharing; no restrictions on advertising to children. | Implement data minimization; ban third-party commercial data sharing and targeted ads for minors. |
| **Persons with Disability's Consent** | No standardized method to verify guardianship, leading to inconsistent enforcement. | Establish a centralized database of legal guardians and an appeal mechanism. |
| **Rule 11 (Exemptions for Child Data Processing)** | "Extent necessary" is vague and can be misused by educational institutions for excessive monitoring. | Provide clear guidelines on necessary interest, especially for educational institutions. |
| **Email Communications** | No clear process for email data security, consent validation, or mandatory breach notifications. | Require explicit opt-in consent, secondary authentication, and mandatory notifications for breaches. |

## DATA PRINCIPALS

### INTRODUCTION

Personal data has emerged as a critical asset in the digital age, influencing economic activities, governance mechanisms, and individual privacy rights. The proliferation of data-driven technologies has necessitated robust legal frameworks to regulate data processing and protect individuals' personal information. In this context, India's Digital Personal Data Protection (DPDP) Act, 2023[20], represents a significant step toward safeguarding digital privacy while balancing the interests of businesses and the state.

Central to this framework is the Data Principal, a legal entity that denotes the individual to whom the personal data pertains. The Data Principal is the primary stakeholder in the data protection ecosystem, possessing fundamental rights over their data access, control, and processing (Government of India, 2023).

[20] Digital Personal Data Protection Act 2023.

The DPDP Act defines the Data Principal as any individual whose personal data is collected and processed, granting them specific rights to regulate its usage. The legislation establishes a consent-driven model of data governance, wherein informed consent forms the bedrock of lawful data processing. Unlike previous regulatory frameworks, which provided limited individual control, the DPDP Act ensures that Data Principals have enforceable rights, including the right to access, correct, erase, and restrict the processing of their personal data.[21] Furthermore, recognizing the evolving nature of digital transactions, the Act also allows Data Principals to nominate a legal representative to exercise their rights in cases of incapacity or death, thereby ensuring the continuity of data protection mechanisms.

By mandating stringent obligations on Data Fiduciaries—organizations that collect and process data—the DPDP Act ensures that individuals are not subjected to arbitrary surveillance, unlawful data monetization, or privacy violations.[22] This approach aligns with global best practices, including the General Data Protection Regulation (GDPR) of the European Union, which similarly prioritizes individual control over personal data. The rights conferred upon the Data Principal, therefore, serve a dual purpose: they empower individuals to protect their digital identity and impose necessary checks on data-processing entities, fostering a culture of responsible data management.

Given the increasing instances of data breaches, unauthorized surveillance, and algorithmic bias, the recognition and protection of Data Principals in legal frameworks have become paramount. By institutionalising the Data Principal's role, the DPDP Act and Rules redefine the power dynamics in digital interactions, ensuring that individuals are not merely passive subjects in the data economy but active participants with legally enforceable rights.[23] This shift is instrumental in strengthening India's data governance landscape, fostering public trust in digital services, and reinforcing the constitutional right to privacy as recognized in Justice K.S. Puttaswamy v. Union of India (2017).[24]

[21] Ministry of Electronics and Information Technology, *Title of the Report* (Government of India, 2023).
[22] Srikrishna Committee, *A Free and Fair Digital Economy: Protecting Privacy, Empowering Indians* (Government of India 2018).
[23] A Ramanathan, *Data Protection in India: Legal Framework and Challenges* (Oxford University Press 2024).
[24] *Justice K S Puttaswamy v Union of India* (2017) 10 SCC 1.

## GLOBAL PERSPECTIVES

Different jurisdictions across the globe have adopted unique legislative frameworks to safeguard individuals' rights. This includes the **General Data Protection Regulation (GDPR)** in the European Union, the **Australian Privacy Principles (APPs)** under Australia's Privacy Act 1988, and India's **Draft Digital Personal Data Protection (DPDP) Act 2023 and Rules 2025.** All of these provide varying degrees of protection for data subjects, also called data principals.

### Definition of Data Principals

The data principals' concept is unique to privacy laws, defining the rights and protections afforded to such individuals. The GDPR refers to data principals as "data subjects," defined as identifiable natural persons whose personal data is processed.[25] It applies to all individuals within the EU and extends extraterritorially to entities processing the data of EU residents.

Under the Australian Privacy Act, data principals are called "individuals," defined as natural persons whose personal data is collected and processed by Australian organizations with an annual turnover exceeding AUD 3 million.[26] Meanwhile, the Draft Digital Personal Data Protection Rules 2025 defines a "data principal" as an individual to whom personal data relates. The legislation primarily applies to data processed within India but includes extraterritorial applicability if it concerns Indian residents.

The DPDP 2025 framework appears to be less comprehensive and vague than the GDPR and APPs regarding granting rights to the data principals or individuals or data subjects, despite all three legislations granting fundamental privacy rights to such individuals.

### Right to Access and Correction

The GDPR grants data subjects the right to access their personal data and request corrections.[27] Organizations must provide a copy of the processed data and correct inaccuracies within a specified timeframe. Similarly, under the APPs, individuals can request access and correction of their personal data.[28], and organizations must take reasonable steps to correct inaccuracies.

[25] General Data Protection Regulations, art. 4.
[26] Australian Privacy Act, 1988.
[27] General Data Protection Regulations, art. 15 & 16.
[28] Australian Privacy Principles, art 12 & 13.

In contrast, DPDP 2025 provides similar rights but lacks explicit provisions mandating the data fiduciary to provide access within a strict timeframe. The absence of a clear timeline for data access and correction could lead to delays in addressing inaccuracies. To address this, DPDP 2025 should specify a maximum timeframe (e.g., 30 days, as in GDPR) for fulfilling access and correction requests.

**Right to Erasure**

GDPR gives individuals the "right to be forgotten," allowing them to request data erasure under specific conditions.[29] The APPs do not explicitly mention this right but require organizations to destroy or de-identify data when it is no longer required.[30] DPDP 2025 permits data principals to request deletion, but the grounds for rejection by data fiduciaries are not well-defined.

The limitation in DPDP 2025 lies in the vague criteria for rejecting erasure requests, which could allow data fiduciaries to retain unnecessary data. To improve this, DPDP 2025 should establish clear conditions under which a data principal's request for erasure can be denied, similar to GDPR.

**Right to Data Portability**

GDPR grants individuals the right to request their personal data in a structured, machine-readable format and transfer it to another service provider (Art. 20). The APPs do not explicitly provide this right. DPDP 2025 also lacks any provision for data portability.

India’s DPDP, 2025 explicitly lacks the provision of data portability restricting consumer choice and competition. Such a provision must be added to the list of rules to allows the data principals seamlessly transfer their data between service providers, enhancing user control over personal data.

**Right to Withdraw Consent**

GDPR allows individuals to withdraw consent at any time, and organisations must cease data processing unless there is a legal basis to continue.[31] The APP has no provision for consent withdrawal but lays the burden of responsible use of personal data on the organisation itself.

[29] General Data Protection Rules, art. 17.
[30] Australian Privacy Principles, s. 11.2.
[31] General Data Protection Rules, art. 7(3).

DPDP 2025 allows data principals to withdraw consent, but it remains unclear whether previously collected data must be deleted.[32] This ambiguity creates an uncertainty regarding the management of previously collected data post-withdrawal. The law should clearly mention that data fiduciaries must cease processing and delete data as soon as consent is withdrawn, ensuring better privacy control.

**Right to Grievance Redressal**

Under GDPR, data subjects can lodge complaints with supervisory authorities, which can impose significant penalties.[33] The APPs allow complaints to be filed with the Office of the Australian Information Commissioner (OAIC). DPDP 2025 requires data principals to first approach the data fiduciary and/or consent manager in respect of any act or omission by them[34], and if unresolved, escalate to the Data Protection Board of India.

The DPDP's rule underscores the problem of lack of clarity regarding the Data Protection Board's independence and enforcement powers. To strengthen accountability, DPDP 2025 should clearly define the Board's powers and ensure its autonomy to prevent conflicts of interest.

**Right to Nominate**

GDPR and APPs do not provide an explicit right for individuals to nominate representatives posthumously. DPDP 2025, however, allows data principals to nominate another person to exercise their rights in case of incapacity or death. This provision is a unique strength of DPDP 2025 compared to GDPR and APPs.

## POSITIVE OUTCOMES

The Digital Personal Data Protection (DPDP) Rules of 2025 expand India's data protection system by implementing complete data management and user privacy standards. The new DPDP Act of 2023 serves as the foundation for these regulatory measures to expand by championing transparency alongside user control[35] and accountability standards.[36] All Data Fiduciaries must provide readable notices about processing practices and users need 48 hours

[32] Draft Digital Personal Data Protection Rules 2025, rule 3(c)(i).
[33] General Data Protection Rules, art 77-79.
[34] Draft Digital Personal Data Protection Rules 2025, s. 13.
[35] Digital Personal Data Protection Rules 2025, r 13.
[36] Digital Personal Data Protection Rules 2025, r 3.

[37]for data retention request decisions and breach incidents must be notified within 72 hours.[38] Through these rights users achieve both personal data access and editing privileges which allows them to maintain accurate information about their digital footprint.

The rules contain specific provisions that safeguard vulnerable populations by establishing parental authorizations for child data[39] processing along with measures to accommodate disabled persons. The requirement exists for data notices to maintain a straightforward language format that is easy to understand. Data can only leave the country with government authorization whereas organizations must keep information for three years since user contact. Significant Data Fiduciaries are required by law to perform annual audits as a measure to stop algorithmic bias.

Under the new regulations, organizations must implement both complaint resolution systems and encryption with access controls.[40] The holistic system proposes the maintenance of organizational requirements alongside individual rights to build trust throughout India's digital domains without decreasing innovation.[41]

## COMMENTS

| Specific Head | Summary | Recommendation |
|---|---|---|
| **Consent and Privacy Notices** | Rule 3 mandates standalone, clear privacy notices, increasing compliance burdens; lacks implementation details, creating uncertainty in consent mechanisms, offline data collection, and legacy data handling. | Standardize privacy notice templates and guidelines to ensure clarity and uniformity, including offline data collection. |
| **Security Safeguards** | Rule 6 requires encryption and security measures but lacks clear definitions, creating compliance uncertainties; rigid baseline security framework limits flexibility. | Define key terms like "encryption, obfuscation, masking"; allow industry-specific risk-based compliance approaches. |

[37] Digital Personal Data Protection Rules 2025, r 8.
[38] Digital Personal Data Protection Rules 2025, r 7.
[39] Digital Personal Data Protection Rules 2025, r 10.
[40] Digital Personal Data Protection Rules 2025, r 6.
[41] Rajmohan K, "First Read on the Digital Personal Data Protection Rules 2025: Here's What You Need to Know" (*Internet Freedom Foundation*, January 9, 2025) <https://internetfreedom.in/first-read-on-the-dpdp-rules-2025/>

| | | |
|---|---|---|
| **Personal Data Breach Notification** | Rule 7 mandates reporting all breaches without distinguishing severity, risking overreporting; lacks clarity on reporting mechanisms; rigid timelines may be impractical; penalties do not consider company size or harm caused. | Define risk-based reporting thresholds; align breach reporting with CERT-In guidelines; introduce tiered reporting timelines and proportional penalties. |
| **Data Retention and Erasure** | Rule 8 requires erasure for inactive users with a 48-hour notice but lacks timelines for processing erasure or correction requests, leading to enforcement ambiguity. | Define clear deadlines for responding to erasure and correction requests to ensure accountability and prevent delays. |
| **Rights of Data Principals** | Rule 13 requires disclosure of user rights and grievance redressal timelines but allows companies to set response durations, potentially causing delays; lacks safeguards against excessive or frivolous requests. | Mandate fixed response timelines for data rights requests while allowing some variation for practical flexibility. |
| **Other Relevant Concerns** | DPDP Rules allow exemptions for certain data fiduciaries without clear thresholds or criteria; lacks protections for sensitive personal data, weakening safeguards for highly sensitive information. | Define clear exemption criteria and reintroduce protections for sensitive personal data in line with global best practices. |

## DATA DELETION, MINIMIZATION AND RETENTION IN INDIA: REGULATORY EVOLUTION AND GLOBAL COMPARISONS

### INDIA'S DATA DELETION POLICY: BEFORE AND AFTER THE DPDP ACT

Before the enactment of the Digital Personal Data Protection (DPDP) Act, 2023[42], India's data deletion policies were primarily governed by the Information Technology (IT) Act, 2000[43], along with its subsequent amendments and associated rules viz.,. The IT Act contained

[42]Digital Personal Data Protection (DPDP) Act, 2023.
[43] Information Technology (IT) Act, 2000.

provisions regarding data retention but lacked explicit mandates for data deletion. Section 7[44] of the IT Act addressed the retention of electronic records, stipulating that when any law requires documents, records, or information to be retained for a specific period, such requirements are satisfied if the records are maintained in electronic form.

It further required that such records remain accessible for future reference, be preserved in their original format (or an equivalent representation), and include details that facilitate identification of the origin, destination, date, and time of dispatch or receipt. Similarly, Section 67C of the IT Act, 2000 required intermediaries to preserve and retain specific information for a duration and in a manner prescribed by the Central Government.

The Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules, 2011[45] under the IT Act further regulates data storage, protection, and deletion, requiring organisations to adopt security measures and delete personal data when no longer required.

The DPDP Act, 2023, introduced more explicit provisions concerning data deletion, aiming to strengthen individual data protection rights. Section 9[46] of the Act mandates that personal data should not be retained beyond the period necessary to achieve the purpose for which it was collected, unless retention is required for legal or business purposes. This provision ensures that data fiduciaries (organisations handling personal data) cannot store user data indefinitely without a valid justification.

***The Act grants individuals, referred to as Data Principals, the Right to Erasure, which allows them to request the deletion of their personal data when it is no longer necessary for its***

[44]Information Technology Act 2000, s 7.
Retention of electronic records.—(1) Where any law provides that documents, records or information shall be retained for any specific period, then, that requirement shall be deemed to have been satisfied if such documents, records or information are retained in the electronic form, if— (a) the information contained therein remains accessible so as to be usable for a subsequent reference; (b) the electronic record is retained in the format in which it was originally generated, sent or received or in a format which can be demonstrated to represent accurately the information originally generated, sent or received; (c) the details which will facilitate the identification of the origin, destination, date and time of despatch or receipt of such electronic record are available in the electronic record: Provided that this clause does not apply to any information which is automatically generated solely for the purpose of enabling an electronic record to be despatched or received. (2) Nothing in this section shall apply to any law that expressly provides for the retention of documents, records or information in the form of electronic records.

[45] Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules, 2011

[46] Digital Personal Data Protection Act 2023, s 9

***original purpose. Once a request is made, data fiduciaries are obligated to delete the requested data, enhancing individuals' control over their personal information***.[47]

Prior to the DPDP Act, India's data deletion policies were implicit, focusing primarily on retention rather than deletion, with sector-specific laws imposing certain restrictions. The DPDP Act, however, establishes clear guidelines on data retention limits and provides individuals with a legally enforceable right to request data deletion. This marks a significant shift toward a more comprehensive data protection framework, bringing India closer to global standards of privacy and security.[48]

Prior to the enactment of the Digital Personal Data Protection (DPDP) Act, India's data deletion policies were primarily governed by sector-specific regulations.[49] For instance, the Reserve Bank of India (RBI) mandated that payment system operators store all payment data within the country to safeguard sensitive financial information[50]. Similarly, the Securities and Exchange Board of India (SEBI) required financial institutions to store certain critical data sets within India.[51] These regulations aimed to ensure that sensitive data remained within national borders, thereby enhancing data security and privacy.

## DATA STORAGE IN INDIA: REGULATORY FRAMEWORK AND INDUSTRY TRENDS

The Digital Personal Data Protection Act, 2023, establishes a framework for processing digital personal data in India. Notably, the Act does not mandate that personal data be stored exclusively within India[52]. Instead, it allows for the storage and processing of personal data outside the country, provided that such processing adheres to the Act's provisions and respects the rights of Indian citizens. This approach offers flexibility to data fiduciaries while ensuring

[47] Ministry of Electronics & IT, 'Salient Features of the Digital Personal Data Protection Bill, 2023' (Press Information Bureau, 9 August 2023) https://pib.gov.in/PressReleaseIframePage.aspx?PRID=1947264 accessed 16 February 2025.
[48] AZB & Partners, 'Digital Personal Data Protection Act, 2023 – Key Highlights' (AZB & Partners, 11 August 2023) https://www.azbpartners.com/bank/digital-personal-data-protection-act-2023-key-highlights/ accessed 16 February 2025.
[49] Anirudh Burman, 'Understanding India's New Data Protection Law' (Carnegie Endowment for International Peace, 3 October 2023) https://carnegieendowment.org/research/2023/10/understanding-indias-new-data-protection-law accessed 16 February 2025.
[50] Reserve Bank of India, 'Storage of Payment System Data' (26 June 2019) https://www.rbi.org.in/commonman/english/scripts/FAQs.aspx?Id=2995 accessed 16 February 2025.
[51] Wong Jin Nee & Teo, 'A concise guide to patent law in Malaysia' (Lexology, 18 March 2019) https://www.lexology.com/library/detail.aspx?g=a20cdde5-c59c-4c4d-a462-f27a1a0a8f0e accessed 16 February 2025.
[52] Bloomberg, 'India seeks to relax data storage rules in boost for business' (The Economic Times, 18 July 2023) https://economictimes.indiatimes.com/tech/technology/india-seeks-to-relax-data-storage-rules-in-boost-for-business/articleshow/101853100.cms accessed 16 February 2025.

that the protection of personal data remains paramount[53]. The Act empowers the government to restrict the transfer of personal data to certain countries through specific notifications. This means that while data can generally be stored and processed abroad, the government retains the authority to designate specific nations where data transfer may be prohibited, ensuring national security and the privacy of citizens are upheld. The Digital Personal Data Protection Act, 2023, provides a balanced approach by permitting cross-border data storage and processing, subject to compliance with its provisions and potential government-imposed restrictions on specific countries.

In India, data storage practices vary across industries and are influenced by both regulatory requirements and business needs. The country has a rapidly growing data center industry, with major hubs in cities like Mumbai, Chennai, and Bangalore. As of 2024, India's data center capacity stood at 950 MW, with projections to reach 1,800 MW by 2026.[54] This growth is driven by increasing digitization and data localization trends within the country. Despite generating 20% of the global data, India currently holds only a 3% share of global data center capacity, highlighting significant potential for expansion. [55]

## INDIA'S DATA LOCALIZATION LANDSCAPE: BALANCING DOMESTIC INFRASTRUCTURE AND GLOBAL STORAGE

Indian firms are advancing tech indigenisation across hardware and software, driven by policy shifts and localisation demands. CloudPhotonix, founded by telecom industry veterans, is supplying transceivers to networks moving away from Chinese components, leveraging India's push for self-reliance in photonics. Meanwhile, DigiBoxx offers local cloud storage, anticipating stricter data localisation mandates under laws like the Digital Personal Data Protection Act, 2023. Despite higher costs, firms prioritise compliance, security, and reputation. With the global optical transceiver market set to grow and local storage gaining

[53] Jean Hurley, 'Interview: Gaurav Bhalla on data storage and data localization laws in India' (Global Relay Intelligence & Practice, 19 June 2024) https://www.grip.globalrelay.com/interview-gaurav-bhalla-on-data-storage-and-data-localization-laws-in-india/ accessed 16 February 2025.

[54] Koul S, "India Set to Cross 1800 MW in Data Centre Capacity by 2026: CBRE Report" *www.business-standard.com* (May 15, 2024) https://www.business-standard.com/technology/tech-news/india-set-to-cross-1800-mw-in-data-centre-capacity-by-2026-cbre-report-124051501256_1.html

[55] PricewaterhouseCoopers (PwC) India and The Associated Chambers of Commerce and Industry of India (ASSOCHAM), 'The Strategic Role of Data Centres in Empowering India's Digital Revolution' (PwC India, 2024) https://www.pwc.in/assets/pdfs/the-strategic-role-of-data-centres-in-empowering-indias-digital-revolution.pdf accessed 16 February 2025.

traction, industry leaders see these shifts as commercially driven and crucial for India's digital ecosystem.[56]

India's approach to data localization has evolved over the past decade, driven by objectives such as enhancing national security, fostering economic growth, preventing foreign surveillance, and strengthening data protection enforcement. The government's stance has shifted from strict data localization mandates to a more flexible framework that permits cross-border data flows under specific conditions.[57]

In practice, India's data storage landscape is a blend of localized and international infrastructures. Several sectors, notably telecommunications and finance, have implemented stringent data localization requirements[58]. For instance, the Reserve Bank of India mandates that all payment data be stored domestically, leading to compliance actions against global payment firms that failed to adhere to these norms.[59]

## STANDARD CONTRACTUAL CLAUSES AND INTERNATIONAL DATA TRANSFERS

Standard Contractual Clauses (SCCs) are pre-approved contractual terms established by the European Commission to facilitate the transfer of data outside the European Economic Area (EEA). For a compliant transfer, both parties must sign an agreement that includes these clauses in their original, unaltered form. According to the European Commission, SCCs can be incorporated into any contractual arrangement between the parties involved.[60]

SCCs serve as a ready-to-use and easily implemented tool. This ease of use is particularly valuable for SMEs and other companies that may lack the resources to negotiate individual contracts with every commercial partner. Moreover, SCCs stand apart from other compliance methods that either require prior authorization from a national data protection authority—such

[56] Companies look to localise data storage' (The Hindu, 16 February 2025) https://www.thehindu.com/sci-tech/technology/companies-look-to-localise-data-storage-telecom-tech/article69085479.ece accessed 16 February 2025.
[57] Anirudh Burman and Upasana Sharma, 'How Would Data Localization Benefit India?' (Carnegie Endowment for International Peace, 14 April 2021) https://carnegieendowment.org/research/2021/04/how-would-data-localization-benefit-india?lang=en accessed 16 February 2025.
[58] Karthika Rajmohan, 'Data Localization: India's Tryst with Data Sovereignty' (Tech Policy Press, 23 January 2025) https://www.techpolicy.press/data-localization-indias-tryst-with-data-sovereignty/ accessed 16 February 2025.
[59] Reserve Bank of India, 'Storage of Payment System Data' (RBI, 26 June 2019) https://www.rbi.org.in/commonman/english/scripts/FAQs.aspx?Id=2995 accessed 16 February 2025.
[60] iubenda, 'Standard Contractual Clauses (SCCs), a complete guide' (iubenda, no date) https://www.iubenda.com/en/help/107560-standard-contractual-clauses accessed 16 February 2025.

as ad hoc contracts for data transfers—or tend to be more expensive to implement, like certification schemes.[61]

**SCCs in the European Union**

In 2010, the European Commission approved a set of model contract clauses to meet the requirements of the EU Data Protection Directive, which was later replaced by the GDPR in May 2018. For many years, Google Cloud customers subject to European data protection laws have used these 2010 Standard Contractual Clauses—also known as Model Contract Clauses—to legitimize the transfer of their customers' personal data overseas while using our services.

On 4 June 2021, the European Commission introduced new Standard Contractual Clauses to further safeguard personal data. These updated clauses replaced the 2010 version and provide a framework for lawful data transfers under specific conditions. By imposing various contractual obligations, these SCCs enable the secure flow of personal data governed by the GDPR to recipients outside the European Economic Area.[62]

**Alternatives to SSCs**

- **Binding Corporate Rules (BCRs)** - These are internal data protection policies adopted by multinational companies to facilitate the international transfer of data within the same corporate group. Although BCRs are used exclusively for internal data flows, Article 47 of the GDPR recognizes them as a legitimate means to ensure compliance with data protection standards.
- **Derogations** - On the other hand, derogations provide exceptions under Article 49 of the GDPR that allow personal data to be transferred without additional safeguards in certain situations. However, these exceptions are applicable only to specific transfers and come with strict requirements. For instance, a derogation can be used if the user has given explicit consent after being fully informed of all potential risks if the transfer is necessary to fulfil a contract, or if it is essential for reasons of significant public interest.

**Schrems Judgement II**

[61]European Commission, 'The New Standard Contractual Clauses – Questions and Answers' (European Commission, 25 May 2022) https://commission.europa.eu/document/download/b9d3d16b-9003-45e7-acef-409562b4bf8b_en?filename=questions_answers_on_sccs_en.pdf accessed 16 February 2025.
[62]Sprinto, 'What are EU Standard Contractual Clauses? A Complete Guide' (Sprinto, 4 months ago) https://sprinto.com/blog/standard-contractual-clauses/ accessed 16 February 2025.

In its landmark ruling in Data Protection Commissioner v Facebook Ireland Ltd and Maximillian Schrems ("Schrems II"), the Court of Justice of the European Union (CJEU) dramatically reshaped the framework for cross-border personal data exchanges. The Court invalidated the EU-US Privacy Shield—a limited adequacy decision that had enabled free commercial data flows between Europe and the United States under Article 45 of the GDPR. However, the CJEU upheld the use of Standard Contractual Clauses (SCCs) as an alternative route for international data transfers, while imposing significant new conditions on their application.

The decision analysed the adequacy of international data transfers. The ruling invalidated the EU-US Privacy Shield, highlighting that transfers to jurisdictions with inadequate privacy safeguards do not meet EU standards. However, the Court maintained that Standard Contractual Clauses ("SCCs") remain a valid mechanism for data transfers, provided that companies rigorously assess the legal environment of the recipient country.

The Court emphasized that SCCs are not a one-size-fits-all solution. Instead, organizations must conduct a case-by-case analysis to ensure that the level of data protection in the destination country is essentially equivalent to that guaranteed in the EU. This means evaluating local laws, including any potential governmental access to personal data, and determining whether these factors might undermine the protections offered by the SCCs.

Furthermore, Schrems II placed the onus on companies to implement supplementary measures when necessary. If the legal framework of the recipient country does not offer adequate protection, data exporters and importers are responsible for adding safeguards—whether through additional contractual terms, technical measures, or organizational policies—to bridge the gap in data protection.

Companies must ensure that their data transfer mechanisms do not compromise the rights of individuals under EU law, thereby upholding the stringent privacy standards set by the EU even beyond its borders.[63]

[63] Laura Bradford, Mateo Aboy and Kathleen Liddell, 'Standard contractual clauses for cross-border transfers of health data after Schrems II' (2021) 8(1) *Journal of Law and the Biosciences* lsab007 https://doi.org/10.1093/jlb/lsab007 accessed 16 February 2025.

**Recommendations and Comments as per the SCC Practice**

| Standard Contractual Clause Practice | Summary | Recommendation |
|---|---|---|
| **SCCs in the European Union** | The European Commission introduced new Standard Contractual Clauses (SCCs) on June 4, 2021, replacing the 2010 version. SCCs enable GDPR-compliant international data transfers by imposing contractual obligations on data importers outside the EEA. | Organizations transferring data outside the EU must assess recipient countries' legal environments and implement supplementary measures when necessary. |
| **Alternatives to SCCs** | Binding Corporate Rules (BCRs) allow intra-group data transfers within multinational corporations, while Article 49 derogations provide limited exceptions for data transfers without additional safeguards. | BCRs should be encouraged for multinational firms, while derogations should be used only in exceptional cases due to their strict requirements. |
| **Schrems II Judgment** | The CJEU invalidated the EU-US Privacy Shield but upheld SCCs for international transfers, requiring companies to assess the legal landscape of recipient countries and implement additional safeguards if necessary. | Companies must conduct case-by-case analyses of destination country laws, implement technical or contractual safeguards, and ensure data protection equivalence. |
| **India's Cross-Border Data Transfer Policy** | Section 16 of India's DPDP Act permits data transfers except to "blacklisted" countries, but lacks detailed procedural guidelines or criteria for determining these lists, creating regulatory ambiguity. | Clear criteria and guidelines should be established for blacklisting or whitelisting countries, with independent oversight to ensure transparency and prevent misuse. |

## DATA DELETION AND RETENTION POLICIES IN FOREIGN JURISDICTIONS

### Provisions Present in Europe for Data Deletion

a) Under the General Data Protection regulation, the right to data deletion or erasure is primarily covered under Article 17, also known as the "Right to be Forgotten".[64]

b) **Grounds for Erasure under GDRP**– Individuals can request data deletion if:

- The data is no longer necessary for its original purpose.
- Consent is withdrawn, and there is no other legal basis for processing.
- The individual objects to processing, and there are no overriding legitimate grounds.
- The data was processed unlawfully.
- The data must be erased to comply with a legal obligation.The data was collected in relation to offering information society services to children.

c) **Exceptions** – The right to erasure does **not** apply when processing is necessary for:

- Exercising the right to freedom of expression and information.
- Compliance with a legal obligation.
- Public interest in health, scientific, or historical research.
- Establishing, exercising, or defending legal claims.

d) **Obligation to Inform Third Parties** – If the data has been shared with third parties, the controller must take reasonable steps to inform them of the deletion request.

### Provisions for Retention of Data

Under the GDPR there isn't a retention period for deleting data in general. Instead, the regulation requires that personal data be kept only for as long as is necessary to fulfil the purposes for which it was collected (Article 5(1)(e)). However, if request deletion of personal data ( "right to erasure" under Article/Recital 17), the data controller must act without undue delay and in any event respond within one month of receiving your request. That one-month period can be extended by up to two additional months if the request is complex or if there are a large number of requests, but the controller must inform you about any such extension within the initial one-month period. (this is mentioned under recital 12 (3)).

[64] . Regulation (EU) 2016/679 (General Data Protection Regulation), art 17 https://gdpr-info.eu/art-17-gdpr/ accessed 16 February 2025

**The Provisions for Data deletion Present in USA**

The United States does not have a federal law at the national level that is directly comparable to the European Union's General Data Protection Regulation (GDPR); instead, individual states have enacted their own data privacy laws, with the most prominent being California's Consumer Privacy Act (CCPA) which is often considered the closest equivalent to GDPR in the US. In **CCPA- Section 1798.105**[65]**,** which talks about Right to request Deletion ,States Consumers have the right to request that a business delete their personal data. Businesses must comply unless an exemption applies. Businesses must also instruct **service providers** and **contractors** to delete the data. Further detail of what are the conditions where the request for Data deletion can be denied is present of 4th and 5th page of CCPA updated till 12/24[66] there are other acts like the Health insurance Portability and accountability Act- specifically on medical data, Children's online Privacy Protection Act- Data on Children. **Note - NO RETENTION PERIOD FOR PERSONAL DATA IS MENTIONED.**

**The provisions Under DPDPA, 2023**

Article 12 of DPDPA states: 12. (1) A Data Principal shall have the right to correction, completion, updating and erasure of her personal data for the processing of which she has previously given consent, including consent as referred to in clause (a) of section 7, in accordance with any requirement or procedure under any law for the time being in force.

(3) A Data Principal shall make a request in such manner as may be prescribed to the Data Fiduciary for erasure of her personal data, and upon receipt of such a request, the Data Fiduciary shall erase her personal data unless retention of the same is necessary for the specified purpose or for compliance with any law for the time being in force.[67]

---

[65] California Consumer Privacy Act 2018, s 1798.105 https://leginfo.legislature.ca.gov/faces/codes_displaySection.xhtml?sectionNum=1798.105.&lawCode=CIV accessed 16 February 2025.

[66] California Consumer Privacy Act 2018 https://cppa.ca.gov/regulations/pdf/ccpa_statute.pdf accessed 16 February 2025.

[67] Digital Personal Data Protection Act 2023 https://www.meity.gov.in/writereaddata/files/Digital Personal Data Protection Act 2023.pdf accessed 16 February 2025.

***Under the Third Schedule of DPDPA, rules.***[68]

| S. NO. | CLASS OF DATA FIDUCIARIES | PURPOSES | TIME PERIOD |
|---|---|---|---|
| 1. | **Data Fiduciary who is an e-commerce entity having not less than two crores registered users in India** | For all purposes, except for the following:<br>(a) Enabling the Data Principal to access her user account; and<br>(b) Enabling the Data Principal to access any virtual token that is issued by or on behalf of the Data Fiduciary, is stored on the digital facility or platform of such Data Fiduciary, and may be used to get money, goods or services | Three years from the date on which the Data Principal last approached the Data Fiduciary for the performance of the specified purpose or exercise of her rights, or the commencement of the Digital Personal Data Protection Rules, 2025, whichever is latest |
| 2. | **Data Fiduciary who is an online gaming intermediary having not less than fifty lakhs registered users in India** | For all purposes, except for the following:<br>(a) Enabling the Data Principal to access her user account; and<br>(b) Enabling the Data Principal to access any virtual token that is issued by or on behalf of the Data Fiduciary, is stored on the digital | Three years from the date on which the Data Principal last approached the Data Fiduciary for the performance of the specified purpose or exercise of her rights, or the commencement of the Digital Personal Data Protection Rules, 2025, whichever is latest |

[68] Third Schedule, Digital Personal Data Protection Rules https://www.meity.gov.in/writereaddata/files/259889.pdf accessed 16 February 2025.

| | | | |
|---|---|---|---|
| | | facility or platform of such Data Fiduciary, and may be used to get money, goods or services | |
| 3. | **Data Fiduciary who is a social media intermediary having not less than two crore registered users in India** | For all purposes, except for the following:<br>(a) Enabling the Data Principal to access her user account; and<br>(b) Enabling the Data Principal to access any virtual token that is ssued by or on behalf of the Data Fiduciary, is stored on the digital facility or platform of such Data Fiduciary, and may be used to get money, goods or services | Three years from the date on which the Data Principal last approached the Data Fiduciary for the performance of the specified purpose or exercise of her rights, or the commencement of the Digital Personal Data Protection Rules, 2025, whichever is latest. |

KAUTILYA SOCIETY

## SUGGESTIONS FOR DPDPA RULES

| Specific Head | Summary | Recommendation |
|---|---|---|
| **Broadened Scope of Coverage** | The current provisions of Schedule 3 in the DPDPA Rules set a three-year retention period for large data fiduciaries but exclude smaller entities. | Expand the definition of data fiduciaries to include smaller platforms handling personal data. |
| **Digital Boom and Micro-Economies** | Many small-scale e-commerce and service platforms handle significant personal data despite not meeting the user threshold. | Ensure that all data fiduciaries, regardless of size, comply with data retention and deletion rules. |
| **Uniform Consumer Protection** | Exempting smaller fiduciaries creates a regulatory loophole, increasing privacy risks for consumers. | Amend Schedule 3 to extend data deletion and right-to-be-forgotten obligations to all data fiduciaries. |
| **Fairness and Accountability** | Holding only large fiduciaries accountable creates an unfair standard in data protection. | Introduce tiered obligations ensuring proportional regulation without compromising consumer rights. |

## SIGNIFICANT DATA FIDUCIARY AND THEIR OBLIGATIONS

### INTRODUCTION

The classification of data-handling entities is crucial to ensuring that organizations processing large volumes of sensitive personal data are subject to heightened accountability and transparency requirements.

In India, the Supreme Court's ruling in *K.S. Puttaswamy v Union of India*[69] recognized privacy as a fundamental right, laying the groundwork for a structured data protection framework suited to the country's evolving digital landscape. The Digital Personal Data Protection Act, 2023 (DPDPA) builds upon this foundation by defining a Data Fiduciary as any entity that, alone or

[69] [2017] 10 SCC 1.

jointly, determines the purpose and means of processing personal data.[70] This concept closely aligns with the GDPR's "data controller",[71] ensuring a structured approach to data governance.

To address the varying degrees of risk associated with data processing, the Act introduces the concept of a Significant Data Fiduciary (SDF) under Sections 2(z) and 10,[72] designating entities that handle large volumes of personal data or process particularly sensitive information that may pose risks to individual rights, national security, electoral democracy, or public order. This classification enables the Central Government to impose tailored regulatory obligations, akin to the GDPR's safeguards for high-risk processing under Article 35, even though jurisdictions like Europe and Singapore do not explicitly categorize data fiduciaries in this manner. However, the Draft DPDP Rules, 2025, which were expected to provide clarity through detailed guidelines and measurable thresholds, leave key aspects undefined, creating potential inconsistencies in enforcement.

## OBLIGATIONS OF SIGNIFICANT DATA FIDUCIARY UNDER THE DPDP ACT, 2023

### 1. Appointment of a Data Protection Officer (DPO)

Significant Data Fiduciaries are required to appoint a Data Protection Officer (DPO), who acts as the central point of contact for regulatory authorities and data principals. The DPO is responsible for monitoring compliance, conducting audits, and ensuring that data practices align with the legal framework.[73]

### 2. Conducting Data Protection Impact Assessments (DPIA)

SDFs must regularly carry out Data Protection Impact Assessments (DPIAs) to assess the potential risks to individual privacy and help ensure that appropriate safeguards are in place.[74]

### 3. Periodic Data Audits

Regular audits of data processing activities are mandatory to verify compliance with the DPDPA. These audits ensure that data is being processed for its intended purpose, access to it is limited to authorized personnel, and any third-party processors adhere to the same privacy standards.[75]

### 4. Enhanced Transparency Measures

[70] Digital Personal Data Protection Act 2023, s 2(i)
[71] Regulation (EU) 2016/679, art 4(7).
[72] Digital Personal Data Protection Act 2023.
[73] Digital Personal Data Protection Act 2023, s 10(2)(a).
[74] Digital Personal Data Protection Act 2023, s 10(2)(c)(i).
[75] Digital Personal Data Protection Act 2023, s 10(2)(c)(ii).

Significant Data Fiduciaries are expected to adopt heightened transparency measures. This includes providing detailed privacy notices to data principals, outlining how their data is being used, who it is shared with, and for what purposes. SDFs must also ensure that data principals can easily access and manage their consent preferences.[76]

**5. Reporting of Data Breaches**

In the event of a data breach, Significant Data Fiduciaries must notify the Data Protection Board of India and impacted data principals within a prescribed time frame. Failure to do so could result in hefty penalties and reputational damage.[77]

## INTERNATIONAL PRACTICES

### General Data Protection Regulation (GDPR)

GDPR does not have an exact equivalent, although it envisages similar ideas of concern with respect to 'significance' – involving, in particular, situations when there are (or might be):

(i) legal or other major effects on individuals stemming from decisions that are solely based on automated processing and/or individual profiling;

(ii) clear requirements with respect to conducting a prior impact assessment in terms of protecting data; and

(iii) high numbers of individuals in each of multiple European countries who are likely to be substantially affected by processing operations[78].

The GDPR also provides for the imposition of obligations like **Data Protection Impact Assessments and Data Protection Officers (DPOs)** for organizations handling sensitive data.[79]

### California Consumer Privacy Act (CCPA)

Similarly in the ***California Consumer Privacy Act***, there is no recognition of '**SDF**s' but businesses whose processing of consumers' personal information presents a significant risk to

[76] Digital Personal Data Protection Act 2023, s 10(2)(b).
[77] DLA Piper, 'Breach Notification in India' (DLA Piper Data Protection Laws of the World, 2024) https://www.dlapiperdataprotection.com/?t=breach-notification&c=IN accessed 12 February 2025.
[78] S&R Associates, 'How Much and How Bad? Significant Others in India's New Data Regime' (S&R Law, 2024) https://www.snrlaw.in/how-much-and-how-bad-significant-others-in-indias-new-data-regime/ accessed 11 February 2025.
[79] Regulation (EU) 2016/679, art 35.

consumers' privacy or security will conduct a risk assessment similar to DPIA.[80] Similarly, though there is no recognition of SDFs, the CCPA directs the California privacy protection agency to make rules requiring businesses to do annual independent cybersecurity audits if the processing presents significant risk to consumers' privacy or security.[81] This is similar to DPDPA mandating SDFs to conduct a data audit by an independent auditor. However, there is no necessity to appoint a Data Protection Officer under CCPA, unlike the DPDPA.

**Singaporean Personal Data Protection Act (SPDPA)**

Also, in the ***Singaporean Personal Data Protection Act***, the responsibility of DPIA-like assessment lies for every organisation to process personal data based on deemed consent and not only SDFs.[82] Similarly, **every** organisation must designate an individual to ensure that the organisation complies with the PDPA similar to DPOs. However, PDPA does not mandate any data audit by an independent auditor.

## THE ADDITIONAL OBLIGATIONS UNDER THE DRAFT DPDP RULES, 2025

### (i) Data Protection Impact Assessment

DPIA is a systematic process that helps organizations identify, assess, and mitigate risks associated with processing personal data, particularly when it may significantly impact individuals' rights and freedoms. It ensures compliance with data protection regulations, upholds privacy rights, and fosters trust through accountability and proactive risk management.[83] Based on the analysis, appropriate measures should be selected and implemented to address identified risks.[84]

[80] California Consumer Privacy Act of 2018 [1798.100 - 1798.199.100](14)

[81] California Consumer Privacy Act of 2018 [1798.100 - 1798.199.100] (14)

[82] Personal Data Protection Act 2012 (Singapore), s 26C.

[83] Information Commissioner's Office, 'Data Protection Impact Assessments' (ICO, 2024) https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/accountability-and-governance/guide-to-accountability-and-governance/data-protection-impact-assessments/ accessed 12 February 2025.

[84] F Bieker and others, 'A Process for Data Protection Impact Assessment Under the European General Data Protection Regulation' (2016) 21 Lecture Notes in Computer Science 21–37 https://doi.org/10.1007/978-3-319-44760-5_2 accessed 9 February 2025.

## EVOLUTION OF DPIA IN INDIA DATA PRIVACY LAWS

The evolution of impact assessments in India reflects a shift from regulatory oversight-driven mechanisms to proactive, data controller-led compliance frameworks. The first expert committee on privacy, the A.P. Shah Committee Report (2012) proposed the Privacy Impact Assessments (**PIA**) as a discretionary tool under the proposed Privacy Commissioner, allowing regulators to assess privacy risks in policies and projects. ***This approach placed the responsibility on regulatory bodies rather than on data controllers.*** However, with the rise of global data protection standards, particularly the GDPR in 2016, the focus shifted towards Data Protection Impact Assessments, a mandatory and preventive mechanism requiring ***data controllers*** to assess risks before processing high-risk personal data.

This transition was later reflected in India's Personal Data Protection Bill, 2019, and subsequently in the Digital Personal Data Protection Act, 2023, which codified DPIAs as a compliance obligation for significant data fiduciaries. Unlike privacy impact assessments, which functioned as an enforcement mechanism for regulators, data protection impact assessments represent a self-regulatory, ex-ante risk assessment tool that places accountability directly on data fiduciaries. This shift marks a critical moment in India's privacy framework, embedding risk-based compliance within corporate data governance. It also provided for the alignment of Indian laws with the broader global movement towards data protection laws that place direct compliance obligations on data controllers, rather than relying solely on regulatory oversight.

Thus, while the A.P. Shah Committee did not introduce DPIA as recognized under GDPR, it marked the first step in conceptualizing privacy risk assessments in India, albeit as a Commissioner-driven mechanism rather than a direct compliance obligation on data controllers. This evolution illustrates how privacy regulation in India transitioned from a state-centric oversight model to a more decentralized, controller-driven compliance framework, aligning with international best practices.

KAUTILYA SOCIETY

## THE DRAFT DPDP RULES

The Act mandates periodic Data Protection Impact Assessments, which involve outlining the rights of Data Principals, specifying the purpose of processing their personal data, assessing and managing risks to their rights, and addressing any additional requirements that may be prescribed.

### Rule 12(1) & (2): DPIA Requirement

Under **Rule 12** of the DPDP Rules 2025, a Significant Data Fiduciary has additional obligations regarding DPIAs. Specifically, **Rule 12(1)** mandates that a *Significant Data Fiduciary must undertake a **DPIA and an audit** once every **twelve months** from the date of its designation to ensure compliance with the provisions of the **Digital Personal Data Protection Act, 2023**, and the rules framed thereunder.*

Furthermore, **Rule 12(2)** requires the Significant Data Fiduciary to ensure that *the individual or entity conducting the **DPIA and audit** submits a report containing **significant observations** to the **Data Protection Board**.*

***Key Issues***

**I. Lack of Clarity in Scope and Methodology**

Section 12 mandates periodic DPIAs but fails to define their scope or methodology. Unlike the GDPR, which outlines clear criteria such as necessity, proportionality, and risks to data subjects, the DPDP Rules do not specify the required mechanisms or types of assessments. This lack of guidance risks inconsistent implementation across data fiduciaries.

**Global Best Practices:**

- **GDPR (Article 35(7)):** Requires DPIAs for high-risk processing and mandates specific assessment criteria, including risk mitigation measures.
- **UK ICO DPIA Guidance:** Provides a structured approach for conducting DPIAs, emphasizing risk evaluation and documentation.

**Recommendation:**

1. **Establish Clear Triggers and Risk Levels**

Define thresholds for mandatory DPIAs such as large-scale or sensitive data processing, and AI systems, per GDPR Article 35, which mandates assessments for high-risk activities. Categorize risks i.e., low/medium/high based on harm potential, aligning with ISO 31000 risk management principles.[85]

2. **Develop Standardized Assessment Tools**

   Publish official templates for risk evaluation and mitigation, inspired by the UK ICO's DPIA guidelines,[86] to ensure consistency. Include data flow mapping and proportionality checks (e.g., data minimization), reflecting GDPR's purpose limitation principle.[87]

3. **Adopt Proactive Risk Management Measures**

   Use checklists for high-risk scenarios (e.g., cross-border transfers)[88] and mandate stakeholder consultations per GDPR Article 35(9).[89]

4. **Strengthen Institutional Capacity**

   Provide sector-specific handbooks (e.g., healthcare, fintech) with case studies, akin to the EU's GDPR implementation guides.[90] Additionally, DPOs should be trained through workshops modelled after UK ICO's certification programs for compliance readiness.[91]

5. **Implement a Graduated Compliance Timeline**

   Phase enforcement over 12–18 months, prioritizing high-risk sectors, as seen in GDPR's transitional approach.[92] Additionally, pilot the implementation frameworks on a voluntary basis, drawing insights from Singapore's PDPA strategy to refine the approach before full-scale deployment.[93]

---

[85] International Organization for Standardization, ISO 31000:2018 Risk Management – Guidelines (ISO, 2018).
[86] Information Commissioner's Office (UK), 'How to Do a Data Protection Impact Assessment' (Guidance, 2021) https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/accountability-and-governance/guide-to-accountability-and-governance/data-protection-impact-assessments/ accessed 15 February 2025.
[87] Regulation (EU) 2016/679, art 5(1)(c).
[88] Supra Note 18.
[89] Regulation (EU) 2016/679, art 35.
[90] Article 29 Data Protection Working Party, 'Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679' (WP 248 rev.01, 2017) https://ec.europa.eu/newsroom/article29/items/611236 accessed 16 February 2025.
[91] International Organization for Standardization, ISO/IEC 27001:2022 Information Security Management Systems – Requirements (ISO, 2022).
[92] Regulation (EU) 2016/679, art 35.
[93] Personal Data Protection Act 2012 (Singapore).

### II. Absence of Public Accountability

The provision limits reporting to internal compliance mechanisms, without requiring public disclosure or independent oversight. This reduces regulatory transparency, weakens public trust, and may prevent effective enforcement.

**Global Best Practices**

- **GDPR (Article 35(4)):** Mandates supervisory authorities to publish a list of processing activities requiring a DPIA, ensuring clarity and consistency.
- **French CNIL DPIA Guidelines:** Provide sector-specific DPIA lists to help organizations assess compliance risks proactively.

***Case law:***

- Facebook-Cambridge Analytica Scandal (2018). Lack of transparency in data-sharing practices led to global scrutiny and fines, underscoring the need for public accountability.

***Recommendations:***

1. Summary disclosures to data principals mandating simplified summaries of audit findings for affected users.
2. Publish anonymized reports to enhance transparency by sharing redacted findings publicly, as under the EU's Digital Services Act.

**(ii) Algorithmic Due Diligence**

The DPDPA, 2023 marked India's first comprehensive data protection law. While primarily focused on consent and data localization, Section 12 introduced the concept of "Significant Data Fiduciaries", entities subject to heightened obligations, including algorithmic due diligence, a requirement notably absent in earlier frameworks such as the A.P. Shah Committee's 2011 recommendations, which prioritized broad privacy principles without addressing systemic risks posed by automated systems. The Act empowered the government to mandate SDFs to *"verify that algorithmic software does not pose risks to data principals"*,

though specifics were deferred to subsequent rules.[94] This reflected a shift from abstract principles to actionable governance, albeit with ambiguities.

India's framework draws heavily from the EU's GDPR, particularly in mandating DPIAs and algorithmic transparency. However, it diverges by prioritizing state interests over individual recourse, as seen in exemptions for national security and public welfare..[95] In contrast, the EU AI Act (2024), which bans high-risk AI practices such as social scoring, offers a more proactive model for algorithmic governance, highlighting the differences between India's reactive, penalty-driven approach and the EU's preventive strategies.[96]

**DPDP Rules**

***Rule* 12(3): Algorithmic Due Diligence**

***Key issues***

1. **Vague Standards**
   The provision lacks a clear definition of "due diligence" or measurable criteria (e.g., bias testing, accuracy thresholds) to evaluate algorithmic risks, leaving compliance open to interpretation and inconsistent enforcement.
2. **No Redressal Mechanism**
   Users harmed by biased or erroneous algorithmic decisions have no formal process to challenge outcomes, creating an accountability gap compared to frameworks like the GDPR, which guarantees a right to contest automated decisions.

***Global best practices:***

- **GDPR (Article 22):** Grants individuals the right to contest automated decisions affecting their rights, ensuring procedural fairness.[97]

[94] Digital Personal Data Protection Act, 2023.
[95] Ikigai Law, 'From Principles to Practice: A Deep Dive into India's Draft DPDP Rules' (Ikigai Law, 5 January 2025) https://www.ikigailaw.com/article/614/from-principles-to-practice-a-deep-dive-into-indias-draft-dpdp-rules accessed 16 February 2025.
[96] Ibid.
[97] Regulation (EU) 2016/679 (GDPR), art 22.

- **EU AI Act (2024):** Bans high-risk practices (e.g., social scoring) and mandates transparency, risk assessments, and human oversight for AI systems.[98]

***Case law:***

- **SyRI Case (Netherlands, 2020**):[99] A court struck down an algorithmic welfare fraud system for violating privacy rights, emphasizing the need for fairness and transparency.

***Recommendations:***

1. Define Technical Standards
2. Mandate bias testing (e.g., disparate impact analysis), transparency logs (documenting data inputs/outputs), and explainability protocols for algorithms to ensure accountability. These measures align with the EU AI Act's Article 13, which requires technical documentation and risk mitigation for high-risk AI systems.[100]
3. Introduce the Right to Contest
4. Adopt GDPR Article 22(3), granting users the right to challenge automated decisions through appeals and human review. This ensures procedural fairness and addresses the current lack of recourse under the DPDP Rules.
5. Establish Redressal Framework
   Create an independent authority to investigate complaints, modelled after the EU AI Act's oversight mechanisms. The authority should have powers to audit algorithms, impose penalties, and mandate corrective actions.

**(iii) Data Localisation**

**DPDP Rules**

*Rule 12(4)* it has been mentioned that the Union government on the basis of the recommendations of a committee constituted by it can also determine the types of personal data that SDFs must localize within India's borders. This grants the government significant power, with a broad scope of authority. The draft rules proposal to place restrictions on how Data Fiduciaries can share the data of Indian citizens with foreign governments is a positive step but

[98]Proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on Artificial Intelligence (Artificial Intelligence Act) and amending certain Union legislative acts COM(2021) 206 final, arts 5, 13.
[99] Stichting Rijksuniversiteit v Staat der Nederlanden [2020] ECLI:NL:RBDHA:2020:1878 (SyRI Case).
[100] Supra Note 30.

foreign companies operating in India could find themselves in a difficult position and this rule can potentially lead to data localisation. However, the government's approach to **data localisation will be guided by sectoral requirements**, ensuring restrictions are imposed only where necessary, electronics and IT.

**Section 12(4): Data Localization Requirements**

*Key Issues in Section 12(4)*

1. **Ambiguous Scope**

   The provision grants the Central Government unchecked authority to mandate data localization for undefined categories (e.g., "national security" or "public order") without transparent criteria, risking arbitrary enforcement and compliance uncertainty 910. For example, Rule 12(4) empowers the government to specify data that must remain in India, but lacks guidelines for classifying such data, leaving businesses guessing about compliance boundaries.[101]

2. **Impact on Global Operations**

   The lack of clear safeguards for cross-border data flows disrupts international business operations. Unlike the GDPR's structured mechanisms, Section 12(4) imposes restrictions without clarifying how data fiduciaries can lawfully transfer data, leading to fragmented compliance across sectors (e.g., RBI's stringent localization for financial data).[102] This risks conflict with global partners and undermines India's position as a digital economy hub.

*Global Best Practices*

1. **GDPR (Articles 44–49):** Allows cross-border transfers under **adequacy decisions** (e.g., Japan, UK) or safeguards like **Standard Contractual Clauses (SCCs)** and **Binding Corporate Rules (BCRs)**. These mechanisms ensure data protection equivalence while enabling global operations.[103]

[101] Anu Tiwari and others, 'FIG Paper (No. 40 – Data Law Series 6) Draft Digital Personal Data Protection Rules, 2025 – Key Implications for Financial Services Sector' (India Corporate Law, 14 January 2025) https://corporate.cyrilamarchandblogs.com/2025/01/fig-paper-no-40-data-law-series-6-draft-digital-personal-data-protection-rules-2025-key-implications-for-financial-services-sector/ accessed 16 February 2025.
[102] Uddhav Gupta, 'Cross-Border Data Transfers in DPDP Act' (The Legal Journal on Technology, 2025) https://www.thelegaljournalontechnology.com/post/cross-border-data-transfers-in-dpdp-act accessed 16 February 2025.
[103] Ibid.

2. **China's PIPL (2021):** Localizes "important data" (e.g., critical infrastructure, population health) but explicitly defines categories and requires risk assessments, balancing sovereignty with transparency.[104]

**Case Law: Schrems II (2020):** The EU Court invalidated the EU-US Privacy Shield, emphasizing the need for enforceable safeguards against foreign surveillance. This underscores the importance of **auditable mechanisms** for cross-border transfers.[105]

***Recommendations***

1. Publish Localization Criteria

   Categories like "national security data" or "health data" should be defined subject to restrictions, mirroring China's PIPL. For example, limit localization to data tied to critical infrastructure or electoral integrity, with public consultation to ensure transparency.

2. Adopt GDPR-Style Mechanisms

   Mandate SCCs or BCRs for transfers to non-adequate countries, per GDPR Article 46.

3. Strengthen Accountability

   Establish an independent committee to review localization mandates, preventing arbitrary use of Section 12(4).

4. Harmonize Sectoral Law

   The provisions should clarify interactions between DPDP Rules and sector-specific regulations (e.g., RBI's data storage mandates) to avoid compliance overlaps.

## CONCLUSION/ ANALYSIS

The draft DPDP Rules, 2025, do not introduce any substantial additions to the existing definition of a Data Fiduciary. Notably, Section 12, which outlines the additional obligations of an SDF, does not clarify the criteria for such classification. Instead, Section 2 of the DPDP Rules states that all definitions shall align with those provided in the DPDPA, 2023.

However, the Act itself lacks clarity on key terms used in Section 10, such as "potential impact on Indian sovereignty" and "risk to electoral democracy", which remain vaguely worded.

[104] Ibid.
[105] Data Protection Commissioner v Facebook Ireland Ltd and Maximillian Schrems (Case C-311/18) [2020] ECLI:EU:C:2020:559.

These undefined terms create ambiguity regarding the criteria for classifying an entity as an SDF and the corresponding compliance obligations. The draft rules had an opportunity to provide interpretative guidance on these terms but failed to do so.

The imposition of heightened compliance requirements without adequately defining the fundamental criteria governing SDF classification exacerbates uncertainty in the law's application. The absence of clear regulatory thresholds and sector-specific considerations may lead to inconsistent enforcement and compliance burdens that disproportionately impact certain industries. A more structured approach, incorporating detailed definitional guidance and consultative rulemaking, would be essential to ensuring legal clarity, regulatory certainty, and effective implementation of India's data protection framework.

---

## GOVERNMENT POWERS AND EXEMPTIONS GRANTED UNDER THE DPDP ACT

The Act (DPDP Act 2023) has sparked fiery debates about Government overreach and whether or not the privacy measures that are to be implemented through the act adhere to a global standard. Several key aspects of the DPDP Act are included within these comments, with a special emphasis on Section 7(b) of Rule 5, Rule 15 and Rule 22 of the Act as well as similarities to regulations in New Zealand, Japan and the European Union (EU). It also draws attention to the difficulties faced by SMEs and the function of the Data Protection Board (DPB).

### KEY PROVISIONS OF THE DPDPA

1. ***Section 7(b) of Rule 5: Government Processing of Personal Data***

Section 7 of the DPDPA lays down what is considered as 'certain legitimate uses' as per the Act. It provides scenarios where a Data Fiduciary (DF) may process the personal data of a Data Principal, which is, firstly, for a **specified purpose** for which voluntary consent has been provided to the DF. Secondly, it lays down other scenarios, which include: -

**Section 7(b):** For the State and its instrumentalities to provide or issue to the Data Principal such subsidy, benefit, service, certificate, licence or permit as may be prescribed, either when DP has previously consented to the processing of her personal data by the state for any subsidy, benefit…and when such personal data already exist in state records.

This processing of personal data is subject to standards issued by the Central Government. This is where the DPDP Rules come into picture. Rule 5 incorporates this exemption provided to the government, and the Second Schedule lays down the relevant standards for such processing.

### A. Concerns

Firstly, **Rule 5** proposes that state agencies can process personal data without fresh consent, as long as they inform users. However, the broad purposes lack clear limits, raising concerns about misuse. Furthermore, an unclear definition of **"instrumentalities**" raises fear of state surveillance. Additionally, the standards laid down under the Second Schedule are very wide in ambit and lack clarity regarding the extent to which such data can be processed, effectively giving all-encompassing powers to the State.

### B. Comparative Analysis with New Zealand, Japan and the EU

***New Zealand:*** **The Privacy Act 2020** mandates that all agents who use any data renotify the user that their data is being used again. If the data is used for a purpose that is significantly different, new consent is required. This restricts data reuse and guarantees transparency. For instance, without new consent or a legislative exception, the Ministry of Social Development (MSD) cannot utilize the same information for a housing subsidy when someone applies for a student allowance.

***Japan:*** **The Act on the Protection of Personal Information (APPI)** prohibits, unless a specified exemption exists, government agencies from using personal data for purposes other than those for which it was originally intended without obtaining new consent. Administrative organs are required by Article 8 of the APPI to refrain from significantly changing the original purpose of usage. In doing so, individual rights are safeguarded.

***EU:*** Article 23 of the **General Data Protection Regulation (GDPR)** mandates that the government processing exemptions must be "necessary and proportionate" and adhere to the core principles of fundamental privacy rights. To ensure that there remains a balance between State interests and individual privacy, the GDPR requires that any restriction on data subject rights be accompanied by explicit protections. Further, the concept of Judicial Review which is contained within the GDPR is lacking in the DPDP, thus allowing a greater capacity for misuse.

### 2. *Rule 15: Exemptions for Research, Archival, and Statistical Purposes*

Rule 15 states that the provisions of the DPDPA shall not apply to the processing of personal data necessary for research, archiving or statistical purposes, if it is carried on in accordance with the standards specified in **Second Schedule.** As per Section 17(2) of the DPDPA, the provisions of the Act shall further not apply to the processing of personal data for these purposes, as long as the data is not used to take any decision specific to a Data Principal. However, several of the standards prescribed under the rules in the Second Schedule are similar to the general obligations that would already apply to data processing within the ambit of the DPDPA. For instance, the Rules require DFs to ensure purpose limitation, make reasonable efforts to ensure accuracy, adopt reasonable security safeguards, and be accountable for the observance of such standards – all of which are pre-existing obligations for the DFs as per the DPDPA.

#### A. Concerns

There is ambiguity within the Act itself, which leaves space for a potentially broad interpretation of the permissible bounds of data processing. This ambiguity leads to a high risk of individuals or organisations exploiting this exemption as a loophole to justify data collection that would be beyond the legitimate-use case scenarios that the drafters had in mind for this specific rule. The lack of specificity raises massive concerns about potential misuse that could include sharing of personal data, unethical commercial exploitation and surveillance under the guise of research.

#### B. Comparative Analysis

***New Zealand:*** The **Public Records Act 2005** complements the Privacy Act 2020 by providing a framework for the creation, maintenance, and disposal of public records. Archives New Zealand, led by the Chief Archivist, oversees the management of public records and has the authority to issue instructions to public offices regarding the maintenance and control of records, especially digital information that is 25 years old or older. Under the Privacy Act, limits on retention (IPP 9) state that personal information should not be kept longer than necessary for the purposes for which it was collected. However, if the data holds archival value, it may be retained for historical or research purposes, provided it is stored securely. When conducting research, government agencies must balance the need for data with individuals' privacy rights. This involves processes such as anonymization, obtaining informed consent, and ensuring ethical considerations in research methodology.

***Japan*:** Under Article 61 of the APPI, the government is permitted to use personal data for research, archiving, or statistical purposes, provided that such use aligns with legal provisions and safeguards individual privacy rights. The law recognizes the utility of personal data in research and statistics while emphasizing its protection. To enable these functions, the APPI allows for the creation and use of "Anonymously Processed Information," which refers to data that has been modified to remove personal identifiers, ensuring individuals cannot be identified. This anonymized data can be used beyond the original scope of collection, including for research and statistical analysis, without requiring individual consent.

The APPI imposes strict guidelines to ensure the anonymization process is thorough and prevents re-identification. When anonymized data is provided to third parties, the law mandates that the categories of information and the means of sharing must be publicly disclosed. These measures ensure that research and statistical uses of data are balanced with privacy protections.

***EU*:** While Article 89 of the GDPR does allow exemptions for certain causes such as research and preservation, it also has stringent measures to maintain balance of research and privacy through protections such as data reduction and anonymisation**.**

### 3. Rule 22*: Call for Information by the Government*

As per this rule, the Central Government may, for purposes specified in the Seventh Schedule, require any DF or intermediary to furnish such information as may be called for, specify the time period within which the same shall be furnished and, where disclosure in this regard is likely to affect the security of the State, require the DF or intermediary to not disclose the same, except with the previous written permission of the authorised person. The source of this power to call for information is Section 36 of the DPDPA.

Notably, neither the DPDPA nor the Rules specify safeguards (such as review and oversight mechanisms that exist under other laws like the Telecommunications Act, 2023 and the IT Act) for the issuance of these information requests. That said, any processing of information by the Central Government will need to satisfy the constitutional safeguards prescribed by the Supreme Court in the landmark decision on the right to privacy, in Justice K. S. Puttaswamy and Anr. v Union of India and Ors.

#### A. Concerns

There is a concerning lack of oversight mechanisms within the DPDP. It raises significant fears of potential misuse of power under the specified exemptions. Without proper checks and

balances, these provisions could be exploited fair beyond their intended purpose. Additionally, the broad scope of the Seventh Schedule increases the risk of excessive government intrusion into citizens' personal data, which would lead to potential infringement of privacy rights. Clear and well-defined guidelines, independent oversight and accountability provisions are absolutely essential to maintain a wall between wrongdoers on the one hand, and individuals' privacy and data protection rights on the other.

### B. Comparative Analysis

***New Zealand*:** The government possesses legal authority to compel both private and public entities to disclose personal data in the interest of national security. While the Privacy Act primarily governs the handling of personal information by agencies, it includes exceptions for disclosures necessary to maintain the law, including for the prevention, detection, investigation, prosecution, and punishment of offenses.

This provides a legal basis for information sharing in national security contexts. This authority is primarily outlined in the Intelligence and Security Act 2017, which governs the operations of the Government Communications Security Bureau (GCSB) and the New Zealand Security Intelligence Service (NZSIS). To balance national security interests with individual privacy rights, several safeguards are implemented. In particular, a dual-authorization process is required for warrant approvals to , which must be authorized by both the Attorney-General and a Commissioner of Intelligence Warrants.

***Japan***: Japan's APPI contains provisions that allow certain personal information to be withheld from disclosure when national security is at stake. Article 78(1)(iv) states that information may be withheld if its disclosure is likely to cause harm to national security, damage relationships with other countries or international organizations, or cause disadvantages in negotiations with other nations. This decision is at the discretion of the head of an administrative organ under Article 82. Additionally, Article 74(2)(i) exempts certain personal information files from the public personal information file register if they pertain to national security matters.

However, while the APPI grants exemptions for national security-related disclosures, it does not explicitly grant the government the authority to compel individuals or organizations to disclose personal data for such purposes. Any such authority, if it exists, would likely be found in other legislation or regulations specifically addressing national security.

***EU*:** Article 86 of the GDPR grants public authorities, as well as private bodies operating in the public interest, the right to disclose personal data when required by national laws governing public access to official documents.

### CONCLUSION

The DPDP Act, 2023, marks a weighty step in the right direction in India's data governance landscape. However, certain concerns with respect to overreach, surveillance risks, and lack of oversight arise when exemptions for government processing under Section 7(b), Rule 15, and Rule 22 are necessary to address, especially when contrasted with global standards such as GDPR, Japan's APPI and New Zealand's Privacy Act.

Section 7(b) allows government data processing without fresh consent. This raises fears of unchecked surveillance. In contrast, New Zealand and Japan mandate renotification and restrict data reuse. GDPR ensures necessity, proportionality, and judicial review, which the DPDP lacks.

Rule 15 exempts data processing for research and archiving but lacks clear boundaries, risking misuse for unauthorised data collection

Strengthening oversight, clarifying exemptions, and incorporating judicial safeguards are essential to align India's data governance with global best practices.

---

## PROCESSING OF DATA OUTSIDE INDIA

### INTRODUCTION

The Digital Personal Data Protection (DPDP) Rules, 2025, mark a significant step in India's data governance framework, emphasizing data sovereignty, national security, and individual privacy. Rule 14 of the DPDP Rules empowers the Central Government to regulate, restrict, or prohibit cross-border data transfers based on national interests. This ensures greater control over personal data, preventing potential misuse while aligning with global data protection trends.

This part of our comments project analyses Rule 14's provisions, comparing India's approach with international standards like the EU-GDPR, Japan's APPI, and the US model. It also evaluates data localization benefits, best practices in data processing, and key regulatory compliance strategies. By integrating global best practices, these regulations aim to strike a

balance between economic growth, digital security, and individual rights in India's evolving digital landscape.

## RULE 14 OF THE DPDP RULES, 2025

The Indian government has taken a decisive step toward data sovereignty and by introducing draft regulations under the Digital Personal Data Protection (DPDP) Act. These regulations empower the central government to regulate, restrict, or prohibit the transfer of personal data to foreign entities, organizations, or individuals.[106] Rule 14 clearly mandates that any transfer of personal data to foreign nations, entities, or individuals will be governed by general or specific directives from the Central Government. This allows for adaptability by enabling the government to impose tailored restrictions suiting national interests.[107]

Rule 14 grants the Central Government the authority to regulate data transfers by:

- Imposing restrictions on the movement of personal data.
- Completely prohibiting transfers to specific countries, entities, or individuals.[108]
- Issuing directives or notifications without predefining a list of restricted regions.

This framework ensures the government maintains the flexibility to address evolving threats and concerns in real time. While Rule 14 does not specify when restrictions will take effect, Section 17(2) of the DPDP Act provides clarity on this matter. It empowers the government to regulate cross-border data transfers based on:[109]

- National security concerns.
- Threats to the sovereignty or integrity of the state.
- Risks to individual privacy.

This ensures that government interventions can be strategic, security-driven, or focused on privacy, making it a comprehensive safeguard.

[106] Bhupender, "Unveiling Rule 14: The Game-Changer in National Security and Digital Privacy" (Inventiva, 13 January 2025) <https://www.inventiva.co.in/trends/unveiling-rule-14-the-game-changer-in-national-security-and-digital-privacy/> accessed 13 February 2025.
[107] Bhupender, "Unveiling Rule 14: The Game-Changer in National Security and Digital Privacy" (Inventiva, 13 January 2025) <https://www.inventiva.co.in/trends/unveiling-rule-14-the-game-changer-in-national-security-and-digital-privacy/> accessed 13 February 2025.
[108] Payeel, "Facebook said it may stop operating in Europe in 2020 if the EU suspends all data transfers to the US" (Inventiva, 25 September 2020) <https://www.inventiva.co.in/stories/facebook-may-stop-in-europe/> accessed 13 February 2025.
[109] Digital Personal Data Protection Act, 2023, s 17(2).

## POSITIVE ASPECTS

The new draft rules apply to both Indian and International organizations operating in India. Under the DPDP Act, these entities, recognized as Data Fiduciaries, must comply with government directives on data transfers. This requires adherence to the following:

Cross-border data transfers must align with:

- The government's specific orders or restrictions.
- Processing methods and algorithms that safeguard user privacy and security.
- For businesses, this establishes a regulatory framework that ensures compliance while enabling secure and lawful data transfers.

### 1. Strengthening national security

Data sovereignty has become a critical national security concern in the digital era. By regulating data transfers, the government can:

**Prevent Data Misuse:** Limiting transfers to certain countries or entities safeguarding sensitive personal information from exploitation.

**Protect Strategic Information:** Restricting data flow ensuring vital national intelligence remains within the country's borders.

**Ensure Privacy:** It will protect privacy since the government examines algorithms and processing techniques to lower privacy threats.

This legal structure follows the global trend, as China and the EU impose strict data localization and protection regulations.

### 2. Flexibility

A key feature of Rule 14 is its flexibility. Unlike global regulations that specify a fixed list of restricted countries, the DPDP rules empower the government to:[110]

- Adapt dynamically to shifting geopolitical and technological landscapes.
- Address emerging issues as they arise.
- Respond swiftly to potential data breaches or misuse by foreign entities.

[110] Digital Personal Data Protection Rules, 2025, rule 14.

This adaptability makes the DPDP Act a forward-thinking and responsive regulatory framework.

## LEGAL ANALYSIS

The Digital Personal Data Protection Act (DPDPA) was designed to safeguard the personal data of Indian residents while acknowledging the global nature of data exchange. Chapter IV, Section 16 of the Act grants the Indian government the authority to impose restrictions on cross-border data transfers by Data Fiduciaries. The provision states:

*"The Central Government may, by notification, restrict the transfer of personal data by a Data Fiduciary for processing to such country or territory outside India as may be so notified."*[111]

This establishes a **"blacklist"** approach, permitting data transfers to all countries except those explicitly restricted by the government. This approach differs from earlier drafts of the legislation, which considered a **"whitelist"** model that would have allowed transfers only to pre-approved nations. The shift reflects the government's effort to balance data protection with India's integration into global data networks.[112]

Additionally, Section 17 specifies exemptions, where Chapter II which outlines Data Fiduciary obligations, does not apply. These include cases related to legal proceedings, judicial and regulatory functions, and the enforcement of contractual rights. The Act also grants the government broad discretion to impose additional safeguards or restrictions on **Significant Data Fiduciaries**—entities handling large volumes of sensitive data or operating in high-risk sectors.[113]

DPDP Rules have thus continued from this end and has permitted the transfer of personal data to any country or territory outside the territory of India by data fiduciary in two scenarios

(a) transfer of data within the territory of India is allowed and

(b) transfer of data outside the territory of India in connection with any activity related to offering of goods or services to Data Principals within the territory of India is also allowed.[114]

[111] Digital Personal Data Protection Rules, 2025, rule 14.
[112] Concur, "Cross-Border Data Transfers under the Digital Personal Data Protection Act, 2023: A Comparative Analysis with GDPR" (Linkedin, 24 August 2024) <https://www.linkedin.com/pulse/cross-border-data-transfers-under-digital-personal-protection-8gquf/> accessed 13 February 2025.
[113] Concur, "Cross-Border Data Transfers under the Digital Personal Data Protection Act, 2023: A Comparative Analysis with GDPR" (Linkedin, 24 August 2024) <https://www.linkedin.com/pulse/cross-border-data-transfers-under-digital-personal-protection-8gquf/> accessed 13 February 2025.
[114] Digital Personal Data Protection Rules, 2025, rule 14.

These transfers are however subject to restriction of such requirements as specified by the central government.

The rules do not specify which activities offering what goods and services comes within the ambit of the provision. The rules like the Act have provided discretion to the government with regards to the requirements for the processing of personal data. Such an approach is less structural and rely heavily on government notification.

The rules are also reflective of the pragmatic approach taken to integrate the economic realities with the notion of privacy and data regulations. The rules have adopted a general and wider acceptability to data transfer subject to the specified orders made by the central government to restrict the availability of such personal data to foreign state or entity or agency of such state. This approach re-ensures the privacy notion of the data principles and is in consonance with the backlist approach of the government.

## COMPARATIVE ANALYSIS WITH OTHER JURISDICTIONS

### 1) EU-GDPR

To treat any personal data, you must have a legal basis (such as consent) under the GDPR and the Indian law. Consent and legitimate interests are two of the six legal bases under the GDPR that allow you to process personal data. The "legitimate interests" defense is frequently the first line of defense for companies adhering to the GDPR because of the freedom it provides.[115] Processing for direct marketing, stopping fraud, or protecting the network and information security of IT systems are a few examples of activities that would be considered legitimate interests, albeit the GDPR does not offer a comprehensive list.[116]

Additionally, the DPDPA permits the use of personal data for specific "legitimate uses."[117] However, this is not the same as the GDPR's broader "legitimate interests" defense. Among the nine permissible uses listed in the DPDPA, the following are pertinent to businesses:

[115] Luke Irwin, What Is Legitimate Interest Under the GDPR?, available at https://www.itgovernance.eu/blog/en/the-gdpr-legitimate-interest-what-is-it-and-when-does-it-apply

[116] European Commission, What does 'grounds of legitimate interest' mean?, available at https://commission.europa.eu/law/law-topic/data-protection/reform/rules-business-and-organisations/legal-grounds-processing-data/grounds-processing/what-does-grounds-legitimate-interest-mean_en#:~:text=Your%20company%2Forganisation%20has%20a,security%20of%20your%20IT%20systems

[117] Section 7, Digital Personal Data Protection Act, 2023

(i) voluntary provision of data, in which the user freely contributes data to the designated purpose. For example, when a consumer gives you their personal information so you can create a receipt for the purchase;

(ii) in accordance with any Indian laws or judgments; and

(iii) for work-related reasons.Unlike the GDPR's legitimate interests premise, this provision's scope does not permit a broad variety of data processing activities.

All things considered, Indian law has a significantly smaller range of permissible applications and is far more consent-centric. Therefore, while assessing DPDPA compliance, firms need to take this into consideration. Updating user experiences and privacy policies, which mostly depend on justifiable interests. The exemptions granted by Indian law must also be carefully considered. One example of a processing activity that is exempt[118] from the standard notice and consent framework is data gathering for fraud prevention, which could be justified as being required to prevent a crime.

**2) JAPAN**

The *Act on the Protection of Personal Information (APPI)* applies to private business operators (data controllers) that maintain personal information databases for business purposes in Japan.[119] A personal information database is defined as a searchable collection of personal information.[120]

While the APPI does not explicitly define "data processors," it establishes rules for third parties handling personal information on behalf of operators. Akin to the GDPR, the APPI has extraterritorial applicability, covering cases where businesses outside Japan process personal data of Japanese residents in connection with goods or services.[121]

Data Transfer Restrictions

The APPI imposes restrictions on data transfers to:

1. Third parties processing data on behalf of a controller (data processors).
2. Recipients in countries without adequate privacy protection, as determined by the Personal Information Protection Commission (PPC).

[118] Section 17(1)(c), Digital Personal Data Protection Act, 2023
[119] Article 2(5), APPI.
[120] (Article 2(4), APPI).
[121] (Article 75, APPI).

Cross-Border Transfers

Personal data may be transferred outside Japan only if the recipient:

1. Is in a jurisdiction deemed adequate by Japan, such as the EEA or the UK.
2. Has implemented equivalent protective measures, which may include a contractual agreement ensuring compliance with APPI and intra-group policies or privacy frameworks like the Asia-Pacific Economic Cooperation Cross Border Privacy Rules System (APEC).[122]

Exceptions to Transfer Restrictions

Transfers to jurisdictions without APPI-level protection are allowed if:

1. The data subject consents
2. Other Japanese laws permit the transfer.
3. The transfer is necessary to protect a person's life, body, or property when obtaining consent is difficult, promote public health or child welfare when consent is difficult to obtain and assist government authorities in legal matters where obtaining consent interferes with operations.[123]

**3) USA**

The United States lacks a comprehensive federal data protection law equivalent to the GDPR or India's DPDP Act. Instead, it relies on a patchwork of sector-specific regulations, such as HIPAA[124] for healthcare data and GLBA[125] for financial data, alongside state-level laws like the California Consumer Privacy Act (CCPA).[126] This fragmented approach often results in inconsistencies in data protection requirements across different jurisdictions.[127]

The two frameworks differ significantly in their approach to consent. India's DPDP Rules mandate explicit, informed consent for all data processing activities, with strict requirements for consent management and withdrawal.[128] The US approach, on the other hand, does for implied consent and opt-out procedures, providing more flexibility but possibly compromising

[122] Article 24, APPI; Article 11-2, Enforcement Rules & Guidelines on Data Transfers).
[123] Article 28, APPI.
[124] Health Insurance Portability and Accountability Act 1996.
[125] The Gramm-Leach-Bliley Act 1999.
[126] California Consumer Privacy Act 2018.
[127] Cyril Amarchand Mangaldas, 'Comparing Global Privacy Regimes under GDPR, DPDPA, and US Data Protection Laws' (Cyril Amarchand Mangaldas Blog, 18 January 2024) https://corporate.cyrilamarchandblogs.com/2024/01/comparing-global-privacy-regimes-under-gdpr-dpdpa-and-us-data-protection-laws/ accessed 15 February 2025
[128] DPDP Rules 2025, Rule 3.

individual privacy protections.[129] A notable distinction is India's introduction of consent managers as registered entities, a feature absent in the US system.

A sharp disparity is also seen in cross-border data transfers. Particularly after the EU-US Privacy Shield was declared illegal in 2020, which caused uncertainty in transatlantic data transfers, the US lacks a cohesive policy in this area.[130] Standard contractual clauses (SCC) and other procedures are frequently used by organizations; however, they might not offer the same degree of protection as India's DPDP Rules. India has more stringent regulations on data localization, requiring that specific types of data stay inside its boundaries. In contrast, the US allows for more unrestricted cross-border data transfers by giving data protection regulations precedence over geographical limitations. [131] This difference highlights the US's market-driven strategy and India's emphasis on data sovereignty.

These distinctions are further highlighted by data breach response regulations. While US standards differ by state and industry and frequently permit more flexible reporting periods, India's DPDP Rules enforce a rigorous 72-hour notification period for violations.[132] Furthermore, although US requirements typically have a wider scope, the Indian framework focuses more emphasis on particular technology standards and security measures.

Both frameworks recognize the need for extra protections when it comes to children's data, but India's DPDP Rules place stricter criteria for parental consent and verification than the US Children's Online Privacy Protection Act (COPPA).[133] The Indian framework gives parents greater precise control over their children's data processing activities and requires the periodic renewal of parental consent.

Lastly, there are notable differences in enforcement structures. While the US depends on a number of regulatory agencies, such as the Federal Trade Commission, state attorneys general, and several industry-specific authorities, India has set up a centralized Data Protection Board

[129] Khyati Singh, 'Data Protection Frameworks of India and the US: Data Sovereignty vs Market Flexibility' (Manohar Parrikar Institute for Defence Studies and Analyses, 30 January 2025) https://www.idsa.in/publisher/issuebrief/data-protection-frameworks-of-india-and-the-us-data-sovereignty-vs-market-flexibility/ accessed 15 February 2025.
[130] Case C-311/18, Data Protection Commissioner v Facebook Ireland Limited and Maximillian Schrems ECLI:EU:C:2020:559.
[131] 'Preventing Access to U.S. Sensitive Personal Data and Government-Related Data by Countries of Concern' (Federal Register, 8 January 2025) https://www.federalregister.gov/documents/2025/01/08/2024-31486/preventing-access-to-us-sensitive-personal-data-and-government-related-data-by-countries-of-concern accessed 15 February 2025.
[132] DPDP Rules 2025, Rule 7.
[133] Children's Online Privacy Protection Act 2001.

with extensive supervisory authority. Different levels of accountability for organizations and uneven enforcement may result from this decentralized strategy.

## BENEFITS OF DATA LOCALIZATION

Globalisation riding the wave of digitalisation leads to geopolitical adjustments. These innovative methods were made possible by the unrestricted flow of data between countries and the absence of borders in business relations. However, since the phrase "data localisation" was coined, nations have begun to re-evaluate their approaches to data governance. Data security and localisation are important challenges as a result of India's growing investments in information and communication technology (ICT), according to studies.[134]Standards for data localisation could offer several benefits. They might help monitor and stop companies all around the world from gathering personal data through digital footprints. By ensuring that a nation's data is quickly accessible when needed, they also reduce the conflict of jurisdiction brought on by cross-border data sharing. This prevents delays in the administration of justice in cases involving data breaches and ensures that citizens' data remains within the country's borders. Localisation would also help combat foreign power surveillance and espionage.[135]
A balanced data localisation law may protect Indian consumers' privacy while also serving the country's economic and national objectives.

It is uncertain whether these local approaches will be effective in assisting Indians in achieving their declared goals. Through partnerships with scalable cloud service providers, data centres are accessible from anywhere in India or the world. Any company or organisation can access data centre services for a fee, regardless of location. However, consumers continue to be mindful of the privacy implications of companies' data collecting and storage practices.

The Reserve Bank of India (RBI) issued a directive in 2018 mandating that businesses handling the financial data of Indian consumers retain and process that data within Indian borders. Data localisation is beneficial since it restricts data processing and storage inside a country's

[134] **ETCIO.com**, 'Data Localisation in India: Significance and Economic Impact' (*ET CIO*, 13 August 2021) https://cio.economictimes.indiatimes.com/news/strategy-and-management/data-localisation-in-india-significance-and-economic-impact/85292096 accessed 13 February 2025..
[135] Tech STL, 'How Would Data Localization Benefit India?' (STL Tech, 8 February 2023) https://stl.tech/blog/how-would-data-localization-benefit-india/ accessed 13 February 2025.

boundaries. Several nations have enacted data localisation regulations because cross-border data transfers give rise to security concerns.

As a result, Indian businesses need to gather confidential customer information for processing and archiving in local data centres.India's data localisation standards, which mark a significant change in how businesses manage and retain data, are explained by the Companies Act, RBI Directives, and IRDAI regulations, among other laws. These rules aim to strengthen data security, promote the development of local data infrastructure, and give more control over sensitive data.

Lastly, although India's data localisation laws present challenges for businesses, they also foster innovation and collaboration within the local data ecosystem. By embracing these standards with strategic thinking and a commitment to data protection, businesses can manage the problems of compliance and foster sustainable growth in the digital age.

One especially interesting document is a report authored by the *Committee of Experts, which is chaired by Justice B. N. Srikrishna*. The report provides comprehensive explanations for why personal data ought to be localised. The same committee then developed a 2018 legislative draft known as the Personal Data Protection Bill based on its findings. The Indian government submitted the 2019 bill to the Indian legislature based on this draft. Hence, data localisation can be a driving force in India as a nation which is emerging in technological and several other aspects.[136]

## BEST PRACTICES IN DATA PROCESSING

It is anticipated that companies will generate 2.5 quintillion bytes of information every day in the contemporary digital era. Businesses may boost output, automate processes, and enhance customer satisfaction by ensuring that the unstructured data is converted into meaningful information through proper data processing as this also helps in increasing the efficiency.[137]

[136] Amlegals, 'Data Localization in India: Implications for Businesses and Data Security' (Law Firm in Ahmedabad, 29 May 2024) https://amlegals.com/data-localization-in-india-implications-for-businesses-and-data-security/# accessed 13 February 2025.
[137] Xerago, 'Data Processing' (Xerago Xtelligence) https://www.xerago.com/xtelligence/data-processing accessed 13 February 2025.

Data processing plays a vital role in various aspects of business and technology:

1. Businesses provide actionable insights that improve making choices by using processed data that could be readily accessible.
2. On the other hand , streamlined workflows and automated processes help to reduce errors and optimise processes.[138]
3. Businesses utilise data to evaluate market behaviour and forecast trends; consumer behaviour analysis allows personalisation, increasing engagement and satisfaction. This not only ensures the profit is generated but also minimizes the loses.[139]

## EFFECTIVE PRACTICES IN INDUSTRIES IN DATA PROCESSING

### 1) Healthcare

The healthcare sector relies heavily on data processing for predictive and real-time monitoring:

• The Mayo Clinic tracks vital signs and enhances treatments using real-time data analytics from wearable devices to reduce hospital readmissions. [140]

• Mount Sinai Hospital forecasts patient deterioration using AI-driven analytics to enhance critical care outcomes. Using such ai-driven technologies in gathering and collecting data ensures that there is a boost in the health sector.[141]

### 2) Retail

Retail businesses utilise data processing to increase operational effectiveness and satisfaction among customers:

• Walmart examines 2.5 petabytes of data per hour to optimise inventory management and supply chain logistics.

• Amazon enhances engagement and revenue by leveraging behavioural data to offer personalised, real-time recommendations.[142]

### 3) Finance

Financial institutions utilise data analytics to identify fraud and guarantee secure transactions:

[138] Information Commissioner's Office, 'A Guide to Data Security' (ICO) https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/security/a-guide-to-data-security/ accessed 13 February 2025.
[139] GeeksforGeeks, 'Best Practices for Data Management' (GeeksforGeeks) https://www.geeksforgeeks.org/best-practices-for-data-management/ accessed 13 February 2025..
[140] Xerago (n 32).
[141] ICO (n 33).
[142] GeeksforGeeks (n 34).

• JPMorgan Chase uses predictive analytics to examine 100 million transactions daily in order to identify and prevent fraud which otherwise could be very hard to track.[143]

• PayPal uses Talend's real-time fraud detection algorithms to safeguard transactions globally. During the recent years, we have seen a growing trend regarding the use of this technology.

**4) Manufacturing**

Manufacturers utilise data processing to boost production efficiency and lower operational risks:

• By using IoT-powered data to optimise manufacturing productivity, General Electric (GE) has decreased equipment downtime by 30%.[144]

• Tesla analyses real-time manufacturing data to boost production rates and lower errors and due to this was able to secure great profits during the recent years.[145]

To ensure efficient data processing, businesses should implement the following best practices:

i. Workflow automation: Improving efficiency and lowering human error.
ii. Data Quality Assurance: Maintaining correctness through routine data validation and cleaning procedures.
iii. Data Security Measures: To protect sensitive data, encryption, authentication, and compliance procedures are put into place.
iv. Scalability via Cloud Computing: Making use of cloud-based technologies to meet growing data needs.
v. Conducting routine audits and compliance checks to make sure that legal and industry standards are being followed.[146]

**KEY DATA MANAGEMENT STRATEGIES**

Businesses should use structured data management techniques to expedite data governance and utilisation:

i. Establishing SMART goals entails establishing precise, quantifiable, and attainable objectives.
ii. Implementing data governance involves allocating responsibilities for administration, compliance, and data security.[147]

[143] ICO (n 33).
[144] Xerago (n 32).
[145] ICO (n 33).
[146] GeeksforGeeks (n 34).
[147] ICO (n 33).

iii. Preserving Data Accuracy: Verifying and purifying datasets to get rid of irregularities.
iv. Improving Privacy and Compliance: Limiting access and upholding laws like HIPAA and GDPR.
v. Enhancing Data Integration: Use mapping techniques and standardise formats to ensure seamless data flow.[148]
vi. Maintaining metadata and documentation: improving accessibility and traceability of data.[149]
vii. Data Lifecycle Management Implementation: Establishing policies for deletion and retention to optimise storage.
viii. Establish a single source of truth using Master Data Management (MDM) to guarantee
ix. data consistency.[150]
x. Using business intelligence tools to make informed decisions by drawing conclusions.[151]

## LEGAL AND COMPLIANCE CONSIDERATIONS

Regulatory compliance plays a critical role in data security and ethical data processing:

i. UK GDPR Security Principle: Organisations must use suitable organisational and technical safeguards to secure personal data.[152]
ii. Data Integrity & Confidentiality: Technologies like encryption and pseudonymization aid in safeguarding personal data.
iii. Constant Security Monitoring: Regular testing and assessments lower the risks that accompany data.[153]

## KEY OBSERVATIONS AND RECOMMENDATIONS

| Specific Focus | Summary | Recommendation |
|---|---|---|
| **Lack of Specificity in Data Transfer Requirements** | Rule 14 does not define which activities, goods, or services are subject to cross-border data transfer | Clearly define the scope of restricted data transfers and adopt a sector-specific approach, with stricter regulations for sensitive sectors like finance and healthcare. Introduce |

[148] Xerago (n 32).
[149] GeeksforGreeks (n 34).
[150] Xerago (n 32).
[151] GeeksforGeeks (n 34).
[152] ICO (n 33).
[153] Xerago (n 32).

| | | |
|---|---|---|
| | restrictions, leading to regulatory ambiguity. | consultation processes with industry stakeholders before imposing new restrictions. |
| **Balancing National Security and Global Business Operations** | The discretionary nature of restrictions creates uncertainty for businesses, impacting international data flows and industries like IT, e-commerce, and finance. | Establish objective criteria for imposing restrictions, ensuring transparency. Implement a risk-based framework where data fiduciaries can apply for "safe transfer" approvals based on security compliance. |
| **Learning from International Frameworks** | Countries like the EU (GDPR), Japan (APPI), and the U.S. (CCPA) have structured cross-border data transfer mechanisms ensuring compliance while maintaining flexibility. | Develop an "adequacy assessment framework" similar to GDPR, allowing seamless transfers with countries having strong data protection laws. Define standardized security requirements (encryption, anonymization) for cross-border transfers. |
| **Impact on Startups, SMEs, and the Digital Economy** | Overly restrictive cross-border rules could raise costs and compliance burdens for startups and SMEs relying on global cloud services, reducing competitiveness. | Implement a tiered compliance model with simplified requirements for startups and SMEs. Provide regulatory sandboxes and compliance assistance programs. |
| **Clarifying Data Localization and Interoperability with Other Laws** | Rule 14 interacts with existing localization policies under RBI, IRDAI, and sectoral laws, creating compliance confusion. | Clearly define how DPDP cross-border rules align with existing data localization mandates to ensure regulatory consistency. |

**COMPANIES MANAGING CONSENT**

**Who are the companies managing consent? Are they defined in the Acts/ Rules?**

**DEFINITION ACCORDING TO THE DPDP ACT 2023 AND THE DPDP DRAFT RULES 2025:**

- **Rule 4, Draft DPDP Rules along with the First Schedule**, outline the registration process and obligations of a Consent Manager, as defined in Section 2(g) of the DPDP Act.
- To determine whether companies managing consent qualify as Consent Managers, specific criteria must be met as per ***Part A of the First Schedule, which requires the applicant to be a company incorporated in India***.
- Therefore, ***companies incorporated under the Companies Act, 2013, can manage consent in accordance with the Draft DPDP Rules, 2025.***

Global Practice

- **General Data Protection Regulation (GDPR)** in the European Union **does not explicitly define the term "Consent Manager**."[154] Instead, it assigns the responsibility of obtaining and managing consent to the data controller and data processors.
- **California Consumer Privacy Act (CCPA)** in the United States also do not provide a specific definition of a Consent Manager but establish consent requirements that companies, service providers or businesses must comply with.[155]
- **Brazil's General Data Protection Law (LGPD)** also do not define Consent Managers explicitly but emphasize consent governance under the broader obligations of data controllers and processors.[156]
- GDPR and CCPA provide obligations where businesses develop their own consent mechanisms. This approach represents a significant departure from the decentralized consent management seen in jurisdictions like the EU and the US, where it operates

[154]Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) [2016] OJ L119/1.

[155] California Consumer Privacy Act of 2018, California Civil Code § 1798.100–1798.199.100 (2018) https://oag.ca.gov/privacy/ccpa accessed 12 February 2025.

[156] Lei No 13.709, de 14 de Agosto de 2018 (Brazilian General Data Protection Law) https://iapp.org/media/pdf/resource_center/Brazilian_General_Data_Protection_Law.pdf accessed 12 February 2025.

without direct regulatory oversight, emphasizing mostly on compliance with "Consent".

**WHAT ARE THE TYPES OF COMPANIES MANAGING CONSENT?**

The Draft Rules **(Schedule 1, Part A, Item 1)** specify only that the entity must be a company incorporated in India. The following are the types of companies, as defined under the Companies Act, 2013, may be eligible to manage consent:

- Private Limited Company (Pvt Ltd) – Restricts share transfer, requires a minimum of 2 and a maximum of 200 members.
- Public Limited Company (Ltd) – Can issue shares to the public and requires at least 7 members with no maximum limit.
- One Person Company (OPC) – A single-member company with limited liability.
- Limited Liability Partnership (LLP) – A hybrid structure offering limited liability to partners.
- Section 8 Company – A not-for-profit company established for charitable purposes.

**FRAMEWORK AND REGISTRATION REQUIREMENTS**

***Registration under DPDP Act, 2023 & DPDP Rules, 2025***

(i) Incorporation with Companies Act, 2013.

To incorporate a company in India[157], the following steps are required:

- Registration with the Ministry of Corporate Affairs (MCA) through the SPICe+ (Simplified Proforma for Incorporating Company Electronically) portal.
- Promoters must obtain a Digital Signature Certificate (DSC) for online document authentication and a Director Identification Number (DIN) to be legally recognized as company directors.
- The Board must undertake drafting of Memorandum of Association (MoA) and Articles of Association (AoA) to define the company's objectives and governance structure.
- After successful registration, the Registrar of Companies (RoC) issues a Certificate of Incorporation, formally recognizing the company as a legal entity.

[157] Section 7 of the Companies Act, 2013.

- A valid Indian address must be provided as the official registered office, which serves as the company's primary point of contact for legal and compliance matters.
- Companies must obtain a Permanent Account Number (PAN) for taxation purposes and a Tax Deduction and Collection Account Number (TAN) for deducting taxes at the source.
- Compliance with Foreign Direct Investment (FDI) Policy, if applicable.

In addition to standard incorporation procedures, companies managing consent must comply with the DPDP framework:

(ii) Compliance with the DPDP Act and DPDP Rules, 2025:

- Incorporated Company must mandatorily register with DPBI as a Consent Manager and must meet the requirements detailed in the First Schedule. **(Rule 4 r/w Schedule 1)**

***Comment:*** *The DPDPA's requirement for Consent Managers to be Indian-registered companies limits their ability to enforce consent revocations or data rights against foreign entities, as cross-border compliance relies on voluntary adherence without mutual legal agreements or standardized interoperability frameworks.*

***Recommendation/ Best Practice:*** *Adopt adequacy decisions and Standard Contractual Clauses (SCCs) to enforce cross-border compliance, ensuring foreign entities honor Indian consent withdrawals. (GDPR)*

- Companies functioning as Consent Managers must have a net worth of at least ₹2 crore to ensure financial stability. **(Schedule 1, Part A, Item 4)**
- Memorandum and Articles of Association must reflect data protection commitments, with amendments subject to approval from the DPBI. **(Schedule 1, Part A, Item 7)**

***Comment:*** *Delays in approvals for MoA/ AoA by DPBI could create operational burdens. There should be specific timeline for approvals as well as registrations with DPBI.*

- The company must demonstrate adequate technical infrastructure, financial stability, and operational competence to handle consent securely and effectively. **(Schedule 1, Part A, Item 2)**
- The volume of business likely to be available to and the capital structure and earning prospects of the applicant are adequate. **(Schedule 1, Part A, Item 5)**

***Comment:*** *The requirement for companies to demonstrate "adequate" infrastructure, financial stability, and operational competence lacks clear benchmarks, creating ambiguity in eligibility assessment. Similarly, subjective terms like "volume of business" and "earning prospects" (Schedule 1, Part A, Items 2 and 5) risk inconsistent evaluations. Defining measurable standards would enhance transparency and fairness.*

(iii) Operational Framework: **(Schedule 1, Draft DPDP Rules, 2025)**

- **Registration Requirements:**
  - Must be an Indian-incorporated company with a minimum net worth of ₹2 crore.
  - Must demonstrate sound financial, technical, and operational capacity.
- **Platform Functionality:**
  - Required to develop and maintain accessible interoperable platform either by website/app enabling Data Principals to give, manage, review, and withdraw consent.
  - The platform must be independently certified for compliance with data protection standards.

***Comment:*** *The Act mandates interoperability, technical standards for the platform as well as cross-sector data formats remain undefined, risking inconsistent implementation.*

***Recommendation:*** *Integrate standardized technical protocols for consent interoperability, enabling seamless cross-platform consent synchronization akin to the Transparency and Consent Framework's universal consent signals by IAB Europe, thus, providing compliance with GDPR.*[158]

  - The platform must remain "data blind" i.e., no access the actual content of personal data to the Consent Manager itself.
  - The platform must be accessible in all 22 languages.

***Comment****: While the DPDP framework mandates multilingual accessibility to ensure inclusivity, it lacks explicit guidelines on user interface (UI) design. Without standardized UI*

[158] Interactive Advertising Bureau, 'IAB Tech Lab – CMP API v2' https://github.com/InteractiveAdvertisingBureau/GDPR-Transparency-and-Consent Framework/blob/master/TCFv2/IAB%20Tech%20Lab%20-%20CMP%20API%20v2.md accessed 14 February 2025.

*directives, the effectiveness of consent mechanisms may be undermined, as users could struggle to navigate or understand their options, eroding trust in the consent process.*

***Recommendation:*** *DPDP Rules should ensure that consent interfaces are simple and user friendly. For Instance, the CPRA mandate to include* ***"Do Not Sell or Share My Personal Information"*** *link provides easy understandability. Such key options should be easy to find, clearly labeled, and simplified for users of all strata to effectively use the platform.*

- **Record Maintenance:** Must securely maintain detailed records of all consent transactions, including consents given, withdrawn, and associated notices, typically for at least seven years.
- **Conflict of Interest Prevention:** Mandatory disclosure of any financial or managerial ties with Data Fiduciaries to ensure independent operation.
- **Prohibition on Subcontracting:** Consent Managers cannot subcontract or transfer their responsibilities without prior approval from the Data Protection Board.
- **Security Measures**: Implementing reasonable security measures to prevent personal data breaches is essential to protect the platform and the data it handles.

***Comment:*** *The security measures required of the Consent Manager are vaguely defined as "reasonable" without specific guidelines, unlike the detailed obligations imposed on Data Fiduciaries and Processors.*

- **Audit Mechanisms:** Maintaining effective audit mechanisms ensures continuous monitoring and compliance with technical and organizational controls, registration conditions, and regulatory obligations.

***Global Practice:***

- **GDPR** does not have "Consent managers" but rather it adopts a business-led compliance model, allowing organizations to develop and manage their own consent mechanisms, thus, placing the responsibilities and obligations of a consent manager on the businesses themselves. **Therefore, there are no registration or operational framework as such.**
- Similarly, **CCPA as amended by the California Privacy Rights Act, 2020 (CPRA),** the consent management falls under the **internal obligations of businesse**s to comply under the Act. Therefore, while there are no registration or operational framework, CPRA does provide for registration requirement for businesses to fall under the

compliance framework of the CPRA. It applies to organizations that conduct business in California and satisfy at least one of the following conditions[159]:

i. They have a gross annual revenue of $25 million or more.
ii. They buy, receive, or sell the personal information of at least 50,000 California residents, households, or devices.
iii. They obtain 50% or more of their annual revenue from selling California residents' personal information.
iv. The CCPA does not apply to nonprofit organizations, government agencies, or certain kinds of financial institutions — for example, a California resident cannot avoid paying off a debt by asking the debt collecting agency to delete their personal information.

**ROLE AND RESPONSIBILITIES**

| Specific Head | Summary | Recommendation |
|---|---|---|
| **Facilitating Consent** | Users should have granular control over consent, specifying purposes (e.g., clinical trials vs. marketing) and withdrawing consent in real time. Best practices from GDPR require explicit, unbundled consent requests and the ability to withdraw without affecting prior processing. | Implement purpose-by-purpose consent with distinct, non-bundled requests. Introduce real-time technical protocols for withdrawal, ensuring immediate cessation of processing upon opt-out. Maintain auditable logs to track consent actions for compliance. |
| **Security and Compliance Monitoring** | Consent managers play a key role in preventing data breaches and ensuring compliance. | Provide detailed guidelines on the responsibilities of consent managers in breach notification processes, ensuring smooth integration into organizational workflows. |
| **Relationship with Data** | Consent Managers must act as fiduciaries, prioritizing Data Principals' interests, operating | Require Consent Managers to offer grievance redressal, maintain machine-readable consent records, |

[159] California Privacy Rights Act of 2020, California Civil Code § 1798.100 (2020).

| | | |
|---|---|---|
| **Fiduciaries and Data Principals** | independently of Data Fiduciaries to prevent conflicts of interest, and providing user-friendly consent management tools. | and ensure transparency by publishing details of promoters, directors, and major shareholders. Ensure they serve as encrypted conduits for data transfers with strict fiduciary duties. |

## DATA PROTECTION BOARD

### INTRODUCTION

The legal basis for data privacy and protection in India is outlined in the Digital Personal Data Protection (DPDP) Rules, 2025, which were implemented by the Indian government. The creation of the Data Protection Board (DPB), which is charged with upholding compliance, resolving disputes, and protecting individuals' right to privacy, is a crucial part of these regulations. In order to ensure that companies and organizations follow the guidelines set forth in the DPDP Act, the DPB is meant to act as the principal enforcement body for data protection issues.

Evaluating the DPB's compliance with international best practices is crucial given the global data protection landscape. As models for data protection governance, nations like the United States (California) and Australia have set up regulatory agencies like the California Privacy Protection Agency (CPPA) and the Office of the Australian Information Commissioner (OAIC), respectively. These organizations actively participate in drafting laws, carrying out audits, and raising consumer awareness in addition to enforcing compliance.

KAUTILYA SOCIETY

Concerns about the DPB's independence, autonomy, and enforcement powers are brought up by the DPDP Rules, 2025. A greater examination of the board's appointment practices, decision-making structure, and operational transparency is necessary. Its efficacy is limited in comparison to its international counterparts by the lack of proactive enforcement tools and legislative advisory powers. In addition, the DPB's funding model and structural independence are still unclear, which calls for revisions to guarantee that it operates as a strong regulatory body.

This paper highlights weaknesses in the DPB's operations and structure by comparing it to other international data protection authorities. Additionally, it makes suggestions to improve its efficacy and guarantee that India's data protection framework complies with international

norms. In order to guarantee accountability, transparency, and consumer-centric enforcement, the document also assesses important clauses under the DPDP Rules, 2025, pointing out areas that require improvement.

This analysis seeks to offer helpful insights toward bolstering the DPB's regulatory framework by referencing well-known models like the OAIC and CPPA. The objective is to create a transparent, impartial, and well-resourced data protection institution that can successfully defend individual rights in India's changing digital environment.

## GLOBAL OUTLOOK

### *Australia*[160]*:*

The Office of the Australian Information Commissioner (OAIC) is an independent national regulator responsible for privacy and freedom of information, operating under the Attorney-General's Department. It enforces the **Privacy Act 1988, Freedom of Information Act 1982, and Australian Information Commissioner Act 2010**, overseeing compliance, investigating complaints, conducting Commissioner-initiated investigations, reviewing FOI decisions, and issuing enforcement actions such as compensation awards, civil penalties, and Federal Court proceedings. The OAIC provides **guidance on privacy principles**, conducts **monitoring activities**, and assesses the security and accuracy of information, particularly regarding tax file numbers and data-matching programs. It also examines **proposed laws and policies for privacy risks**, undertakes research, and reports findings to the Minister and Parliament. The Commissioner has **advisory functions**, offering recommendations to government entities on legislative and administrative privacy concerns. Reporting mechanisms ensure transparency, requiring investigations, assessments, and compliance audits to be documented and submitted to Parliament. Enforcement tools include **Privacy Impact Assessments (PIAs)**, **enforceable undertakings**, and **external dispute resolution schemes** to ensure compliance with privacy laws. The Commissioner also has investigative powers to conciliate complaints, compel documents, hold compulsory conferences, and transfer cases to other dispute resolution bodies.

| Specific Head | Summary | Recommendation |
|---|---|---|
| **Appointment Process for Data** | The OAIC follows a merit-based appointment system | Implement a similar merit-based appointment system for the Data |

[160] https://www.legislation.gov.au/C2004A03712/2014-03-12/text

| | | |
|---|---|---|
| **Protection Board Members** | with strict eligibility criteria for its commissioners, ensuring expertise and leadership. | Protection Board members in India, with eligibility criteria including leadership skills, legal expertise, and experience in privacy and FOI issues. |
| **Authority to Recommend Legal Changes** | The OAIC has the power to propose legal reforms and assess the impact of legislation on privacy, while the Data Protection Board lacks such powers. | Empower the Data Protection Board to suggest legal changes and assess the privacy implications of future legislation, rather than limiting it to an adjudicatory role. |
| **Checks on Government Powers** | The DPDP Rules and Act grant extensive powers to the Central Government, including appointment procedures and data requests, without independent oversight. | Establish a mechanism ensuring that future legislation aligns with privacy laws, reducing excessive government control over data protection matters. |

***US (California Consumer Privacy Act):***

**The California Consumer Privacy Act of 2018** gives consumers certain rights over the personal information businesses collect about them and requires businesses to inform consumers about how they collect, use, and retain their personal information. This landmark legislation was the first comprehensive consumer privacy law passed in the United States.

As of January 1, 2023, California residents have the **following rights**:

- L – Right to LIMIT the use and disclosure of sensitive personal information collected about them.
- O – Right to OPT-OUT of the sale of their personal information and the right to opt-out of the sharing of their personal information for cross-context behavioral advertising.
- C – Right to CORRECT inaccurate personal information that businesses have about them.
- K – Right to KNOW what personal information businesses have collected about them and how they use and share it.

- E – Right to EQUAL treatment. Businesses cannot discriminate against consumers for exercising their CCPA rights.
- D – Right to DELETE personal information businesses have collected from them (subject to some exceptions).

Businesses that are subject to the CCPA must honor these rights and provide methods by which consumers can exercise these rights. They must also comply with the law's purpose limitation and data minimization rules. This means businesses must limit the collection, use, and retention of your personal information to only those purposes that: (1) a consumer would reasonably expect, (2) are compatible with the consumer's expectations and disclosed to the consumer, or (3) purposes that the consumer agreed to, as long as the consent given wasn't obtained through dark patterns. For all of these purposes, the business' collection, use, and retention of the consumer's information must be reasonably necessary and proportionate to serve those purposes.

Businesses also have additional responsibilities, including making certain disclosures to consumers about their privacy practices, such as posting a privacy policy.

**Implementation:**

**The California Privacy Protection Agency** was created to protect Californians' consumer privacy. Established in 2020 by Proposition 24, the Agency is governed by a five-member board. The Agency implements and enforces the CCPA, and has several responsibilities, including:

- Promoting public awareness of consumers' rights and businesses' responsibilities under the CCPA.
- Adopting regulations in furtherance of the CCPA. The Agency may issue regulations to achieve the CCPA's goals, including rules that implement consumers' rights and the responsibilities of business(es) with the goal of strengthening consumer privacy.
- Enforcing the CCPA. The Agency is tasked with enforcing the CCPA through administrative enforcement actions. It can investigate possible violations, audit businesses to ensure compliance with the CCPA, and bring enforcement actions.
- Cooperating with other agencies with jurisdiction over privacy laws and with data processing authorities in California, other states, territories, and countries to ensure consistent application of privacy protections.
- Providing technical assistance and advice to the Legislature with respect to privacy-related legislation.

**Control Environment**[161]

Under the direction of the Executive Director and the Chief Deputy Executive Director, the executive team maintains high ethical standards and attentive oversight of the Agency. The Agency is governed by a five-member board, which provides oversight of the executive team. The Board delegates all aspects of the operations of the Agency to the Executive Director, except for regulations and resolution of enforcement. CPPA maintains a managerial hierarchy to ensure that policies and procedures are developed and effectively communicated throughout the Agency. CPPA's organizational structure provides for the delegation of decision-making authority to the most qualified staff at various management levels. This structure groups employees by division and function to ensure the appropriate segregation of duties and sufficient levels of review of staff work. This structure also allows for the effective execution of duties and ensures accountability within the chain of command.

The CPPA prioritizes extensive job outreach to diverse, qualified candidates and comprehensive staff development to establish and maintain a competent workforce. The Department of General Services (DGS), Office of Human Resources supports the Agency in this work through contracted services. CPPA works with DGS and the CPPA Public Affairs team to advertise job postings and conduct extensive outreach to prospective candidates through popular job-search platforms and social media. For positions requiring specific qualifications, such as a law degree, CPPA staff shares job postings with diverse legal associations and their listservs. CPPA seeks to ensure that the pool of candidates is representative of the state's diversity.

The CPPA also prioritizes staff development to help maintain an efficient workforce. The Agency provides training opportunities for employees. Management provides timely feedback to employees during the probationary period to ensure skills are aligned with the Agency's objectives. Management and senior staff provide ongoing coaching and mentorship to facilitate professional growth. Executive staff receive annual reviews to help motivate and hone their skills to support the Agency's mission.

**CPPA has three levels of accountability**.

First, board members serve at the pleasure of their appointing authority and can be removed at any time. Second, board members conduct an annual evaluation of the Executive Director (ED), who is responsible for the Agency's operations. Board members provide information to

[161] https://cppa.ca.gov/pdf/state_leadership_accountability_report.pdf.

the board chair on the ED's performance, and the board chair shares the findings with the ED in a closed-session meeting. The ED is an at-will employee who serves at the pleasure of the board. Third, CPPA employees are civil service employees, and their conditions of employment are governed by civil service laws and regulations and by collective bargaining agreements. Management provides feedback and assessment during probationary reports and annual reviews to ensure that employees are meeting the requirements of their roles as indicated in their duty statements. If an employee is not meeting the expectations of their position, managers provide guidance and resources.

**Primary Duties of the CPPA**

1. **Education**
    - Promotes public awareness of data privacy rights and responsibilities.
    - Provides guidance to businesses and the California Legislature.
    - Appoints Chief Privacy Auditors for compliance audits.
    - May award grants for educational initiatives.
2. **Rulemaking**
    - Adopts and updates existing CCPA regulations.
    - Issues new rules on automated decision-making, consumer opt-outs, data correction, cybersecurity audits, and geolocation use.
    - Develops mechanisms for universal opt-out consent.
3. **Enforcement & Violations**
    - Investigates violations, conducts hearings, and imposes fines ($2,500 per unintentional violation, $7,500 per intentional violation).
    - Coordinates enforcement with the California Attorney General.
4. **Funding**
    - Annual budget of $10 million.
    - 97% of fines reinvested in CPPA operations; 3% for educational grants.
5. **Voluntary Certification**
    - Certifies businesses that voluntarily comply with CPRA, potentially setting a global privacy standard.

KAUTILYA SOCIETY

**COMMENTS**

| RULE | PROVISION | GAP | SUGGESTION | JURISPRUDENCE |
|---|---|---|---|---|
| 16 | Appointment of Chairperson and other Members | The executives will be appointing the chairperson and the members, and it is the Government that has the sole discretion to decide that who shall be on Board. | There is a need for an independent member which can be preferably a judicial member to ensure due compliance and enforcement of the provisions. | Justice Srikrishna Committee, in its report, recommended that in order to ensure independence, the Selection Committee shall also include the CJI or her nominee.<br><br>Reference can be taken from the Competition Act, 2002 that provides single selection committee for the appointment of the chairperson and the members of the commission comprising of the CJ or his nominee, two members from executives and two independent experts of the respective domains. |
| 18 | Procedure for meetings of Board and | The case of emergent situation is not | Firstly, there should be a fixed time frame under | There should be transparency is decision making and; |

KAUTILYA SOCIETY

| | | | | |
|---|---|---|---|---|
| | authentication of its orders, directions and instruments. | made clear and it gives a lot of discretion to the Chairperson to act on his own. | which the decision of the chairperson can be put forward before the members for | In case of conflicts, the resolution process should abide by the principle of nemo judex in causa sua (no one can be |
| | | Secondly, it does not provide for any mechanism in case of conflicts between the members. | ratification rather than providing for ratification at "next meeting".<br><br>There should be a mechanism where the conflicts are resolved when the members are divided on a certain issue. | judge in their own cause). |
| 19 | Functioning of Board as digital office. | No clear framework is provided on its working and no clarity as how the digital technologies will be inculcated. | A clear guidelines and framework in this regard can be provided. | |
| | | | | |
| 20 | Terms and conditions of appointment and service of | The autonomy given to the Board in matter of appointment | Clarify the extent to which the Board has autonomy with | There is need for transparent appointment and service provisions |

| | | | | |
|---|---|---|---|---|
| | officers and employees of Board | of employees for efficient discharge of its functions is ambiguous vis-à-vis the Central Government's overarching control. | regards to appointment while at the same time maintaining Government's oversight. | for public employees. |

## SECURITY SAFEGUARDS

### INTRODUCTION

The new Rule 6 under the 2025 Sensitive Personal Data or Information (SPDI) Rules[162] significantly adds to the security obligations of the Data Fiduciaries. This rule has replaced the old Rule 8 of the 2011 SPDI Rules[163], which was much more prescriptive and detailed regarding data protection. The amendments were made to ensure that security practices are strengthened further to avoid any data breaches and to continue the compliance with international best practices, such as IS/ISO/IEC 27001, which is the world's best-known standard for information security management systems (ISMS)[164].

### KEY PROVISIONS OF RULE 6: THE 2025 SPDI RULES

Data Fiduciaries must use the appropriate data security measures such as encryption, obfuscation, masking, or virtual tokenization to protect personal data. The access control mechanism must be in place, which ensures that only authorized personnel deal with sensitive data. Logs and monitoring of access to personal data are important in detecting and preventing unauthorized access. For one, the continuity and data back-up of businesses must be provided with the requisite strength for confidence, integrity, and availability. Data Fiduciaries will have to store audit logs and personal data access logs for a period of not less than a year in the

[162] Rule 6, Draft Digital Data Protection Rules 2025.
[163] Rule 8, Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011.
[164] International Organization for Standardization, 'ISO/IEC 27001:2022 Information Security, Cybersecurity and Privacy Protection — Information Security Management Systems — Requirements' (ISO, October 2022) https://www.iso.org/standard/27001.

interest of facilitating compliance and investigations after the occurrence of breaches. In addition, contracts entered between Data Fiduciaries and Data Processors must provide security safeguards provisions in their respective obligations. Organizations must also meet technical and organizational standards to ensure the effective observance of security practices.

**COMPARISON WITH 2011 SPDI RULES (RULE 8)**

The 2011 SPDI Rules mainly referred to general security requirements for body corporates dealing with sensitive data. Rule 8 included a documented information security program which consisted of managerial, technical, operational, and physical security controls. Compliance with globally recognized security standards such as IS/ISO/IEC 27001 were required along with annual independent audits to prove security compliance. SPDI 2025 Rules, especially Rule 6, is in a different league of scope and detail. Unlike the 2011 rules, the 2025 rules impose explicit technical safeguards such as encryption, access controls, logging, and backups. They also introduce explicit requirements for monitoring and log retention for at least one year. Further, the 2025 rules not only introduce contractual obligations but force Data Processors into compliance with security measures. This shift to an enforcement-oriented approach is intended to reduce the risks and enhance data protection practice.

**RELEVANCE UNDER THE DIGITAL PERSONAL DATA PROTECTION ACT (DPDPA) 2023**

The Digital Personal Data Protection Act of 2023[165] only further mandates the need to keep security practices stringent. A Data Fiduciary is held liable under law to ensure reasonable security measures for breach[166], failing which attracts huge amounts of penalty up to INR 250 Crores[167]. Security practices must be in tune with global standards to reduce risks and build greater trust in data handling. This law lays emphasis on the need to apply security measures as a fundamental responsibility to safeguard private data in this digital age and not just to comply with a regulatory requirement.

**YAHOO DATA BREACH**

A good case in point concerning poor security is the Yahoo breaches. Yahoo experienced two significant hacks in 2013 and 2014, where three billion and 500 million user accounts were leaked. The company came under heavy criticism for delaying publicly disclosing the hacks that occurred in 2014 by two years, until September 2016. Regulatory action ensued, when the

[165] Digital Personal Data Protection Act (DPDPA) 2023.
[166] Section 8, Digital Personal Data Protection Act (DPDPA) 2023.
[167] Schedule 1, Digital Personal Data Protection Act (DPDPA) 2023.

SEC fined Yahoo $35 million for failing to disclose the hack promptly. The company also had to settle the $117.5 million class-action lawsuit after the breach occurred[168]. This serves as a reason for the enforcement of proactive security measures, effective and timely notification of breaches, and compliance with the regulations stipulated in Rule 6 of the 2025 SPDI Rules.

Thus, with Rule 6 in the 2025 SPDI Rules, this is the next big step India has taken regarding data protection laws. This rule prescribes some specific security measures, mandatory monitoring, and contract obligations, and it is strong enough to secure personal data of individuals.

Such increased requirements result in more stringent compliance costs in the hands of small organizations but are important in ensuring data safety and avoiding data breaches. It was demonstrated by incidents like the Yahoo data breach that failure to institute strong security controls can lead to severe financial and reputational repercussions.

**COMMENTS**

| Specific Head | Summary | Recommendation |
|---|---|---|
| **Definition and Scope of Security Measures** | Rule 6(1)(a) requires encryption, masking, and virtual tokens but lacks adaptability to evolving security protocols. | Introduce a periodic review clause for encryption updates and clearly define "appropriate security measures" using GDPR's Article 32 as a reference. |
| **Incident Detection and Response Time** | Rule 6(1)(g) mandates logging and monitoring but lacks strict detection and notification timelines. | Require organizations to detect breaches within a set period and notify the Data Protection Board within 72 hours, following GDPR standards. |
| **Accountability and Third-Party Data Processors** | Rule 6(1)(f) mentions contractual obligations but lacks enforcement mechanisms for monitoring third-party processors. | Expand Rule 6(1)(f) to require regular audits of third-party data processors to ensure compliance. |

[168] Hacked, Hacker, Hire: Lessons from the Yahoo Data Breaches (So Far)' (The National Law Review, 20 April 2017) https://natlawreview.com/article/hacked-hacker-hire-lessons-yahoo-data-breaches-so-far.

| | | |
|---|---|---|
| **Periodic Risk Assessments** | No mandated risk assessments exist, whereas countries like Japan and Canada require periodic evaluations. | Introduce mandatory annual Data Protection Impact Assessments (DPIAs) for security evaluations. |
| **Enhancing User Rights and Awareness** | Security measures are incomplete without user awareness and control over personal data. | Require data trustees to provide regular security updates and guidance on personal data protection, similar to the CCPA. |
| **Lack of Specificity in Notice Content (Rule 3)** | Rule 3 lacks a uniform standard for privacy notices, making them complex and difficult to understand. | Introduce a standardized notice template, use plain language, and include a visual summary following GDPR's layered privacy policy model. |
| **Absence of a Strict Notification Timeline (Rule 7)** | Rule 7 does not specify a deadline for reporting breaches, leading to delays. | Implement a 72-hour breach notification timeline for authorities and immediate notification for sensitive data breaches. |
| **Lack of Mandatory Breach Risk Assessment (Rule 7)** | No requirement for fiduciaries to assess and document breach risks before notification. | Mandate breach risk assessments to determine "significant harm" and document mitigation measures. |
| **Ambiguity in Notification Methods (Rule 7)** | No standardized method for notifying affected data principals, risking ineffective communication. | Require multi-channel notifications (SMS, email, website) and establish dedicated breach assistance helplines. |

# CREDITS

# TEAM RMLNLU

Yash Bhatnagar
**Convener**
Fifth Year

Maanya Kocher
**Jt. Convener**
Fourth Year

Debjyoti Samaddar
**Fifth Year Member**

Shubhangi Verma
**Fifth Year Member**

Yash Tiwari
**Fifth Year Member**

Aditi Joshi
**Fourth Year Member**

Aditi Singh
**Fourth Year Member**

Avesta Vashishtha
**Fourth Year Member**

Kanak Goel
**Fourth Year Member**

Rituraj Kumar
**Fourth Year Member**

Vaibudha Brighu
**Fourth Year Member**

Ashish Chauhan
**Third Year Member**

Anshika Sah
**Third Year Member**

Divyansh Gangwar
**Third Year Member**

Dhairya Kumar
**Third Year Member**

Khushi Pandey
**Third Year Member**

Tarun Ranjan
**Third Year Member**

Isha Aggarwal
**Third Year Member**

Upanshu Shetty
**Third Year Member**

Arnav Kaushik
**Second Year Member**

Daksh Arora
**Second Year Member**

Liesha Mishra
**Second Year Member**

Navya Pandey
**Second Year Member**

Varuni Jha
**Second Year Member**

Saumya Tripathi
**Second Year Member**

# TEAM RGNUL

Aarish Alam
**Second Year Member**

Nidash Parashar
**Third Year Member**

Insha
**Second Year Member**

# TEAM NLUO

Sparsha S
**Fourth Year Member**

# TEAM NUSRL

Sumit Kumar Singh
**Second Year Member**

Gaurav Mandal
**Second Year Member**

Astik
**First Year Member**

Aishwarya Singh
**First Year Member**

# TEAM NALSAR

Saundarya D. Nair
**First Year Member**

Bhavesh Ostwal
**Second Year Member**

# TEAM SLS PUNE

Krish Vikram
**Third Year Member**

Kriti Sood
**Third Year Member**

Shashwat Shivam
**Second Year Member**

The Kautilya Society at Dr. RMLNLU extends a heartfelt thanks to the student members who volunteered for the project and also would like to thank the faculty co-ordinators and Conveners of these societies for being a part of this initiative.

# CONVENERS

**Rajiv Gandhi National Law University - K-Soc**

**Sarakshi Kapila**

---

**National Law University, Odisha- K-Soc**

**Mandar Prakhar** **Siddharth Melepurath**

---

**National University of Study and Research in Law- Ranchi - K-Soc**

**Sumit Kumar Singh** **Gaurav Mandal**

---

**NALSAR University of Law- Hyderabad- K-Soc**

**Goyam Pitalia**

---

**Symbiosis Law School, Pune - K-Soc**

**Krish Vikram** **Kriti Sood**

---