Panjab University Law Magazine (MAGLAW)
ISBN: 2582-3507, Volume Iv Issue I, pp 38-49

THE NEW FRONTIER OF DATA PROTECTION: UNDERSTANDING INDIA'S DPDP RULES AND GLOBAL COMPLIANCE

Vishwajeet Kumar Chaudhary[*]
Divyansha Verma[**]

ABSTRACT

The new Draft Digital Personal Data Protection Rules, 2025 mark a transformative step in India's data privacy landscape, implementing the Digital Personal Data Protection Act, 2023. This paper examines the core provisions of these rules, including consent management, data breach reporting, cross-border data transfers, and personal information safeguards, highlighting their significance in the digital economy. Through a comparative analysis of international frameworks such as the GDPR and CCPA, this paper highlights both similarities and differences that influence India's strategy for global data protection compliance. It further explores the challenges in implementing these rules, including issues related to regulatory enforcement, and stakeholder preparedness. The paper concludes by proposing potential solutions to ensure effective compliance and operational efficiency, positioning the DPDP Rules as a critical step in aligning India's data privacy regulations with international standards.

KEYWORDS: *Digital Personal Data Protection Rules, Data Privacy, Digital Personal Data Protection Act, 2023, Global Compliance, GDPR*

INTRODUCTION

Privacy is recognized as a fundamental value and many laws frame this as an individual's right to control personal information. Global laws mandate that personal data be processed lawfully, fairly, and transparently, imposing accountability on data collectors while universally embracing fairness and data minimization. Privacy, autonomy, transparency, accountability, and fairness together form the foundational pillars of data protection worldwide. India's Digital Personal Data Protection Act, 2023 (DPDP Act)[1] is explicitly built on

[*] RMLNLU, Kanpur
[**] RMLNLU, Kanpur

1 THE DIGITAL PERSONAL DATA PROTECTION ACT 2023, No. 22, Acts of Parliament, 2023 (India).

these time-tested norms, setting the stage for a focused analysis of how the DPDP Rules will give them concrete effect.

While the Act established the foundations for personal data governance, its full implementation was delayed until January 2025, when the government released the draft Digital Personal Data Protection Rules for public consultation.[2] These draft rules provide detailed guidance on essential operational aspects such as data breach reporting protocols, consent management, children's data protection, cross-border transfers, and the functioning of the Data Protection Board of India (DPB). As stakeholders engage in the 45-day consultation period, which concludes on February 18, 2025, it becomes imperative to understand the potential implications of these rules for effective implementation.

This paper looks at the key provisions of the draft DPDP Rules, emphasizing those that will have the greatest impact on stakeholders' obligations and rights within India's developing data protection framework. The goal is to provide a clearer understanding of how these rules may change data protection practices and highlight areas of particular concern for businesses, individuals, and regulatory bodies.

SALIENT FEATURES OF THE RULES

1. Effect and Enforcement

Rule 1 of the DPDP Rules outlines a phased timeline for implementation. While Rules 16-20, concerning the Data Protection Board (DPB) and Appellate Tribunals, take effect immediately, Rules 3, 15, 21, and 22 related to data fiduciaries and consent managers will be enforced later. This step by the MeitY would ideally provide businesses and organizations with time to align their operations, even if clarity on specific timelines will be crucial for effective preparation.

2. Notice for Consent

According to Rule 3, data fiduciaries must give data principals distinct, understandable disclosures outlining the processing of their personal data. These notifications ought to include information on the data being processed, why it is being processed, and any services or advantages that may arise from it. They must also provide a direct link to the fiduciary's website or app, detail how consent can be withdrawn as easily as it was given, and outline how to exercise data rights or file complaints with the Data Protection Board (DPB). The notice should be transparent, distinct, and user-friendly to ensure informed consent.

---

2 Draft Digital Personal Data Protection Rules 2025 (India).

3. Consent Manager

Rule 4 and the First Schedule lay down the framework for Consent Managers under the DPDP Act, 2023. Section 2(g) of the Act[3] defines a consent manager as a person registered with the Board who facilitates data principals in giving, managing, reviewing, and withdrawing their consent through a platform that is accessible, transparent, and interoperable.

Furthermore, to qualify for registration, a consent manager must be a company incorporated in India, meet prescribed capital adequacy, minimum net worth, and earning capacity requirements, and obtain independent certification demonstrating conformity with data protection standards issued by the DPB. They must maintain thorough consent records for a minimum of seven years, guarantee data security, and grant data principal access to their consent records. They have to disclose shareholdings over 2%, stay clear of conflicts of interest with data fiduciaries, and get the Data Protection Board's (DPB) clearance before making any changes to control.

Consent managers must operate independently, facilitate the onboarding of data fiduciaries to their platforms, and enable secure data sharing. However, the DPDP Rules, 2025, do not detail specific procedures for onboarding. This framework is similar to the RBI's consent management guidelines for account aggregators,[4] emphasizing interoperability, transparency, and accountability in handling data consents.

4. Processing of Personal Data by Government Organizations

Rule 4 grants the Government wide authority to request information from data fiduciaries or intermediaries for reasons such as national security, legal compliance, or assessing their classification as Significant Data Fiduciaries (SDF). It can also impose restrictions on disclosures that could affect India's sovereignty or security. Government entities are permitted to process personal data to deliver public benefits, provided the processing is lawful, accurate, and secure. Furthermore, sharing personal data with foreign entities may need to comply with localization requirements to safeguard against foreign surveillance.

5. Intimation of data breach

---

3 THE DIGITAL PERSONAL DATA PROTECTION ACT 2023, § 2(g), No. 22, Acts of Parliament, 2023 (India).

4 Master Direction - Non-Banking Financial Company - Account Aggregator (Reserve Bank) Directions, 2016, available at https://www.agloc.org/pdf/NBFCAcct Aggregator%20Directions-02-09-16.PDF, accessed on 20 January 2025.

Rule 7 of the Draft Digital Personal Data Protection (DPDP) Rules 2025 establishes the process and timeline for reporting personal data breaches under the DPDP Act 2023. It mandates data fiduciaries to inform both the Data Protection Board (DPB) and the affected data principals promptly. Notifications to data principals should be sent via their user accounts or preferred communication methods and must provide information about the nature, scope, timing, and location of the breach. They should also outline the potential impact, the safety measures taken, and provide contact details for further assistance. At the same time, a preliminary report containing similar details must be submitted to the DPB.

Within 72 hours, or a longer period if approved by the DPB through a written request, data fiduciaries must submit a detailed report to the DPB. This report should include key details such as the breach findings, steps taken to mitigate risks, results of any investigations, remedial actions implemented, and records of notifications sent to affected individuals. Besides notifying the DPB, data fiduciaries may also be required to report the breach to other authorities, including CERT-In within six hours of detection, and, where applicable, to sector-specific regulators such as SEBI, IRDAI, or RBI.

The DPDP framework requires that all breaches be reported, in contrast to the GDPR, which only mandates notifications for breaches that pose significant risks to data subjects. The option to request extensions for submitting detailed reports provides flexibility, but establishing clear criteria for these extensions would improve transparency. Furthermore, requiring the same reporting measures for all breaches, regardless of their severity, could benefit from reconsideration to balance compliance demands with practical implementation.

6. Retention Period of Data and Erasure

Rule 7 of the Draft Digital Personal Data Protection Rules mandates that certain data fiduciaries, such as social media platforms, e-commerce companies with more than 20 million Indian users, and online gaming intermediaries with over 5 million users, must delete personal data if it no longer serves the original purpose. This situation arises when the individual whose data is being processed does not interact with the data fiduciary for the intended purpose or does not exercise their rights concerning their data.

In these instances, data fiduciaries are permitted to keep the data for a maximum of three years from the last interaction with the user or from when the regulations were put into effect, whichever is later. Before deleting the data, the DF must notify the data principal at least 48 hours in advance and offer an

opportunity for re-engagement. For DFs below these thresholds, data retention policies are more flexible, but the purposes and timelines must still be clearly outlined at the consent stage.

7. Processing of children's personal data

Rule 10 of the Draft Digital Personal Data Protection (DPDP) Rules 2025 outlines the obligations of data fiduciaries when processing the personal data of children and individuals with disabilities. Before processing such data, data fiduciaries must obtain consent from parents or guardians. In order to ensure that the identity of parents or guardians is legitimate and verifiable, data fiduciaries must set up reliable mechanisms to verify them. These systems can include either voluntarily provided identity details accessed through services like Digital Locker, government-authorized virtual tokens, or parent data already available with the Data Fiduciary.

Some categories of Data Fiduciaries, including healthcare providers, educational institutions, and critical service providers, are exempt from limits on tracking or behavioral monitoring of minors and are not required to acquire parental agreement. This exception is restricted to certain uses, such as safety, education, or healthcare, in order to protect the child's wellbeing. To avoid harm and adhere to the DPDP Rules, businesses must use a risk-based approach to age verification and monitoring.

For children, Data Fiduciaries must implement technical and organizational measures to ensure verifiable parental consent, including age and identity verification using approved methods. For persons with disabilities, Data Fiduciaries must verify the lawful guardian's authority as appointed by a court or competent authority under applicable guardianship laws.

8. Obligations of significant data fiduciaries

Rule 12 imposes special requirements on Significant Data Fiduciaries. They must undertake yearly audits and Data Protection Impact Assessments (DPIAs), with the results reported to the Data Protection Board. They must also verify that any algorithmic methods used to handle personal data respect the rights of the data principals. Furthermore, Rule 12(4) places limits on certain cross-border data transfers, potentially necessitating data localization requirements. Ambiguities in detecting SDFs and ensuring algorithmic compliance may cause practical challenges.

9. Cross-border transfer of personal data

Rule 14 of the Draft Digital Personal Data Protection (DPDP) Rules 2025 introduces additional checks on the transfer of personal data abroad, supplementing the provisions of the DPDP Act 2023. While the Act permits the free transfer of personal data to any country except those restricted by government notification, Rule 14 specifies that data fiduciaries must comply with prescribed requirements before transferring data to foreign governments, entities, or agencies. For Significant Data Fiduciaries (SDFs), the Government, based on a committee's recommendations, may designate specific personal data sets and traffic data that cannot be transferred outside India, potentially mandating data localization.

The Government may require data fiduciaries to disclose personal data to foreign states or entities through specific orders to ensure that such data remains protected under the DPDP Act. This measure is intended to safeguard against foreign surveillance and align with India's strategic interests. Rule 14 also allows the Government to refuse data requests from foreign entities if they threaten national security, public order, individual privacy, or diplomatic interests. These rules highlight the emphasis on oversight and protection in cross-border data transfers, particularly in sensitive cases. Businesses operating across borders must assess how these localization and compliance requirements may affect their operations and legal obligations.

10. Rights of Data Principal

Under Rule 13 of the Draft Digital Personal Data Protection Rules, data fiduciaries must provide transparent mechanisms on their websites or apps for data principals to exercise their rights, such as accessing or erasing personal data. They must outline the identifiers needed for identity verification, like usernames or file/customer IDs, and detail their grievance redressal processes, including clear response timelines. The data principals may designate representatives to manage their personal information. Consent Managers and data fiduciaries must make these procedures easy, accessible, and well stated to let data principals exercise their rights.

11. Reasonable security safeguards

Data fiduciaries are required to implement robust security measures, such as encryption, obfuscation, virtual token mapping, and strict access controls. These measures must be reinforced through clear contractual agreements with data processors, outlining roles and responsibilities for data protection. Additionally, they are to monitor and limit access to personal data, keep detailed activity logs, identify and address unauthorized access, and take corrective actions to safeguard personal data while ensuring operational continuity.

12. Data Protection Board (DPB)

The DPDP Rules mandate the setting up of a Board with experience in data governance, law, technology, and regulation. The Chairperson and Members shall be appointed by search committees, assuring independence. The terms of the Board, including salary, are established, along with safeguards against conflicts of interest. The Board will now have the option of conducting deliberations online, reducing the necessity for physical attendance.

13. Government's Power to call for information

Under the DPDP Rules 2025, the government has broad authority to call for information from data fiduciaries or intermediaries for purposes such as national security, legal compliance, or SDF assessment, as outlined in Schedule 7. Authorities must specify timelines, and disclosure may be restricted if it affects India's sovereignty, integrity, or security.

14. Exemptions Provisions

Rule 15 of the DPDP Rules 2025 specifies exemptions for processing personal data for research, archiving, and statistical purposes, provided that high requirements are followed. Data fiduciaries must put in place technological and organizational protections to ensure lawful processing, data minimization, accuracy, limited retention until the purpose is met, and strong security controls to prevent breaches. The exemptions prohibit using personal data for individual-specific decisions and emphasize responsible data governance. Additionally, specific fiduciaries, such as healthcare and educational institutions, are exempt from certain provisions related to children's data, provided processing is limited to essential activities ensuring the child's well-being and safety. These measures collectively uphold accountability and lawful use while balancing the need for exemptions in specified contexts.

Comparing the DPDP Rules with GDPR and CCPA

The Draft DPDP Rules 2025 draw heavily from established global frameworks like GDPR[5] and CCPA,[6] reflecting a growing emphasis on individual privacy rights and organizational accountability. While GDPR remains the gold standard for protecting EU residents' data, an obligation that many Indian firms struggle to meet,[7] U.S. businesses are simultaneously preparing for potential federal privacy

---

5 The General Data Protection Regulation, [2016] OJ L 119/1.

6 The California Consumer Privacy Act, 2018 Cal. Legis. Serv. Ch. 55 (A.B. 375) (WEST).

7 Devika Singh, *Most Indian organisations struggling with GDPR compliance: EY Survey*, BUSINESS TODAY (Aug 14, 2018), https://www.businesstoday.in/latest/ corporate/story/most-indian-organisations-struggling-with-gdpr-compliance-ey-survey-109342-2018-08-14.

legislation that could streamline state laws such as CCPA. In the meantime, CCPA has already emerged as a de facto global benchmark. California is home to many of the world's largest technology companies, such as Google, Facebook, and others, which have structured their privacy programs around CCPA requirements. Because these multinational platforms also operate in India's digital market, compliance with CCPA effectively informs their global data handling practices.

The DPDP Rules mirror principles such as consent, transparency, and data subject rights while also addressing India's unique priorities, including child safety, consumer centric provisions, erasure obligations and cross border governance. A concise comparison of the DPDP Rules with the GDPR and the CCPA is as follows:

CONSENT AND TRANSPARENCY

- **GDPR (Articles 7 & 12):** Requires organizations to obtain clear, informed, and unambiguous consent. Consent must be freely given, specific, informed, and revocable. Transparency is emphasized through detailed privacy notices.
- **CCPA (Section 1798.100(b) & Section 1798.120):** Consumers have the right to opt out of the sale of personal data and must be informed about how their data is being collected and used.
- **DPDP Rules 2025 (Rule 4):** Mandates explicit consent for processing and provides individuals with the right to withdraw consent at any time, aligning closely with GDPR.

DATA SUBJECT RIGHTS

- **GDPR (Articles 15-22):** Grants individuals rights such as access, rectification, erasure (right to be forgotten), data portability, restriction of processing, and the right to object.
- **CCPA (Sections 1798.105-1798.125):** Provides rights to know, delete, and opt out of data sales. It also grants non-discrimination rights for exercising privacy rights.
- **DPDP Rules 2025 (Rule 6):** Ensures rights similar to GDPR and CCPA, including access, correction, erasure, and grievance redressal mechanisms.

PENALTIES FOR NON-COMPLIANCE

- **GDPR (Article 83):** Imposes fines up to €20 million or 4% of global turnover, whichever is higher, based on the severity of violations.

- **CCPA (Section 1798.155):** Penalties range from $2,500 for unintentional violations to $7,500 for intentional violations per affected individual.
- **DPDP Rules 2025 (Rule 20):** Specifies fines for non-compliance, aligning with global practices to ensure accountability.

SCOPE AND APPLICABILITY

- **GDPR (Article 3):** Applies extraterritorially, covering organizations processing data of individuals in the EU, regardless of where the organization is based.
- **CCPA (Section 1798.140):** Applies to businesses meeting specific thresholds and processing data of California residents.
- **DPDP Rules 2025 (Section 3):** Applies to data fiduciaries processing personal data within India, with provisions for cross-border applicability.

CROSS-BORDER DATA TRANSFERS

- **GDPR (Chapter V, Articles 44-50):** Allows transfers only to countries with adequate protection levels or under binding agreements like Standard Contractual Clauses (SCCs).
- **CCPA (Section 1798.185):** Primarily focuses on transparency rather than cross-border transfer mechanisms.
- **DPDP Rules 2025 (Rule 17):** Permits cross-border data transfers subject to government-notified conditions and lists of allowed countries, emphasizing sovereignty in data governance.

AUTOMATED DECISION-MAKING AND PROFILING

- **GDPR (Article 22):** Provides individuals with rights to object to decisions based solely on automated processing, including profiling.
- **CCPA:** Does not directly regulate automated decision-making but emphasizes transparency about data usage.
- **DPDP Rules 2025 (Rule 10):** Expected to regulate automated decision-making to ensure fair processing and accountability.

CHILD PRIVACY PROTECTIONS

- **GDPR (Article 8):** Requires parental consent for processing data of children under 16 (member states can lower it to 13).
- **CCPA (Section 1798.120(c))**: Provides additional protections for children under 16, requiring opt-in consent for selling their data.

- **DPDP Rules 2025 (Rule 13):** Exempts certain child-related data processing activities (e.g., by educational institutions) while emphasizing consent and safeguards for other cases.

DATA BREACH NOTIFICATIONS

- **GDPR (Article 33):** Requires notifying the supervisory authority within 72 hours of discovering a breach.
- **CCPA (Civil Code Section 1798.150):** Provides consumers with the right to sue for breaches of unencrypted personal data.
- **DPDP Rules 2025 (Rule 18):** Mandates reporting data breaches to the Data Protection Board within a specified timeframe, ensuring accountability.

CLARIFICATIONS & CONCERNS

Unclear Criteria for Significant Data Fiduciaries

The Draft DPDP Rules 2025 leave certain aspects open to interpretation, necessitating further clarification from the Ministry of Electronics and Information Technology (MeitY). For instance, Rule 12 does not currently define which entities will be designated as Significant Data Fiduciaries, leaving the specifics of their additional obligations to future notifications. Furthermore, the mandated requirements for annual audits and Data Protection Impact Assessments (DPIAs) may impose considerable compliance burdens, particularly for organizations with limited resources.

Ambiguity in Algorithmic Verification

The mechanism for SDFs to verify algorithmic software remains ambiguous under the existing framework. This lack of clarity raises concerns about how such provisions will be operationalized and implemented in practice, highlighting the need for detailed guidance to ensure effective compliance and fairness in enforcement.

Issues with Parental Verification

Another critical concern is the mechanism for parental verification. The rules require platforms to obtain parental consent before processing a child's data, which involves verifying parental identities through trusted identification systems or virtual tokens. However, in the absence of robust fraud-resistant systems, this provision poses risks of misuse and potential privacy violations. A similar issue is

evident in Australia's recently enacted Online Safety Amendment Bill 2024,[8] which bans children under 16 from accessing major social media platforms and enforces strict age verification protocols. While such measures aim to protect minors, they also introduce challenges for platforms in securely processing verification data and managing sensitive personal information, potentially amplifying privacy and cybersecurity concerns.

Burden of Breach Reporting Timelines

The stipulated timelines for reporting personal data breaches have garnered attention. Although notifying data subjects via in-app alerts is a praiseworthy initiative, requiring companies to swiftly furnish comprehensive breach details such as its nature, extent, location, and timing to the Board may impose undue strain. This could result in disclosures that are either premature or insufficiently analyzed. Balancing timely reporting with thorough assessment is essential to ensure accuracy without overburdening organizations.

Concerns Over Expansive Government Powers

Lastly, similar to the regulatory framework in the telecom sector, the government under the new DPDP Rules wields broad powers and enjoys certain exemptions. It is imperative for stakeholders to engage in thoughtful deliberation to balance the need for oversight with the risk of fostering an excessively intrusive surveillance state. Overreach in surveillance could risk diluting the fundamental objectives of the Act and its rules, ultimately compromising their intended effectiveness.

CONCLUSION

The draft Digital Personal Data Protection Rules 2025 are an important step in implementing the Digital Personal Data Protection Act, 2023, and shaping India's data protection policies. With the Ministry of Electronics and Information Technology (MeitY) starting its consultation process, organizations have a chance to contribute to the framework and align with the evolving regulations. Stakeholders should seize this chance to refine their internal processes, focusing on key provisions such as parental consent verification, breach reporting, and the handling of cross-border data transfers. Proactive engagement with these rules will be vital to maintaining compliance and safeguarding privacy standards.

---

8 The Online Safety Amendment (Social Media Minimum Age) Act 2024.

The Rules provide insights into how the Digital Personal Data Protection Act will be implemented, but areas like Data Protection Impact Assessments (DPIAs), audits, and compliance timelines require further clarity. Reports suggest that the government may give the industry up to two years for full implementation, while key steps, such as setting up the Data Protection Board (DPB), could be prioritized. This timeline gives businesses time to prepare but also highlights the need for prompt action.

For organizations, embedding privacy by design throughout the product lifecycle is essential. By doing so, they not only ensure regulatory compliance but also build user trust and foster a culture of privacy. Adopting these principles will not only mitigate risks but also drive long-term business value, establishing India's commitment to data security and aligning it with global standards like GDPR and CCPA.