The Dialogue®
INFORM ENGAGE IDEATE

Primer

# Navigating the Draft Digital Personal Data Protection Rules 2025

## Potential Implications for Online Gaming Sector

**January, 2025**

Primer

# Navigating the Draft Digital Personal Data Protection Rules 2025

## Potential Implications for Online Gaming Sector

**Author:** Kriti Singh, Chief of Staff & Programme Manager, Online Gaming Policy

**Inputs:** Kamesh Shekar, Senior Programme Manager, Data Governance & Privacy Policy

**The Dialogue** is a public policy think tank with a vision to drive a progressive narrative in India's policy discourse. Founded in 2017, we believe in facilitating well-researched policy debates at various levels to help develop a more informed citizenry, on areas around technology and development issues. The Dialogue has been ranked as the world's Top 10 think tanks to watch out for, by the Think Tank and Civil Societies Programme (TTCSP), University of Pennsylvania in their 2020 and 2021 rankings.

**For more information**
Visit thedialogue.co

**Suggested Citation**
*Primer: Navigating the Draft Digital Personal Data Protection Rules 2025 – Potential Implications for Online Gaming Sector* (January, 2025). The Dialogue.

**Catalogue No**
TD/OG/PR/0125/01

**Publication Date**
January 28, 2025

# Contents

# Abbreviations

| S.No | Abbreviation | Full Form |
|---|---|---|
| 1. | DPDP | Digital Personal Data Protection (Act) |
| 2. | SDF | Significant Data Fiduciary |
| 3. | DPIA | Data Protection Impact Assessment |
| 4. | KYC | Know Your Customer |
| 5. | MeitY | Ministry of Electronics and Information Technology |
| 6. | DPB | Data Protection Board |
| 7. | COPPA | Children's Online Privacy Protection Act |
| 8. | GDPR | General Data Protection Regulation |
| 9. | RBI | Reserve Bank of India |
| 10. | CERT-IN | Computer Emergency Response Team – India |
| 11. | IT Rules | Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 |
| 12. | SRBs | Self-Regulatory Bodies |

# 1. Introduction

Online gaming platforms rely heavily on user data for personalisation, multiplayer functionality, matchmaking, and in-game purchases. Under the Draft Digital Personal Data Protection Rules (Rules),[1] these platforms face significant compliance requirements. Platforms processing large-scale sensitive and children's data may qualify as Significant Data Fiduciaries (SDFs), further heightening their regulatory responsibilities.

Though not fully implemented, the IT Rules impose due diligence obligations under Rule 4(1) on online gaming intermediaries. These rules adopt principle-based approaches, assigning self-regulatory bodies (SRBs) responsibilities for verification, redressal, and adjudication. By mandating age-gating at 18 years for 'permissible online real-money games,' the IT Rules aim to enhance user safety and accountability. However, the DPDP Rules introduce stricter and distinct data-handling requirements, creating overlapping compliance burdens for *all* gaming companies. These include obtaining parental or guardian consent, even for free-to-play games.

India's demographic landscape presents additional challenges. With 254 million individuals aged 15 to 24 forming a large segment of the online gaming user base, the DPDP Act's designation of 18 years as the 'age of majority' complicates compliance and may impact growth. This approach disregards the digital maturity and evolving online behaviours of a digitally native generation transitioning into adulthood. In contrast, other Indian legal frameworks and global norms adopt varied age thresholds for consent, offering a more nuanced perspective on age and responsibility.

This primer examines key aspects of the draft Rules and their potential impact on online gaming platforms, including real money games, e-sports, casual games, and video games. Here is a preliminary analysis.

[1] THE GAZETTE OF INDIA : EXTRAORDINARY. (2025). In *THE GAZETTE OF INDIA* (p. 2) [Press-release]. https://www.meity.gov.in/writereaddata/files/259889.pdf#page=28.00

# 2. Key Provisions

## 1. Significant Data Fiduciary (SDF) Classification

Gaming platforms that process large volumes of personal data, including sensitive or children's data, are likely to be classified as SDFs. As SDFs, these platforms must assess their data collection and usage practices to comply with the following obligations:

- The Act authorises[2] the government to notify entities as SDFs based on factors such as:
  - The volume and sensitivity of the data processed
  - Risks to the rights of the Data Principal
  - Potential impacts on India's sovereignty, electoral democracy, and public order

- Platforms may need to store specific data, such as gameplay logs or communications, within India. This requirement could impact cross-border data flows, particularly for platforms relying on global servers. These platforms must prepare for data localisation mandates,[3] which may affect user experience and operational efficiency.

- SDFs must conduct annual Data Protection Impact Assessments (DPIAs) to evaluate risks to data principals. Platforms may need to incorporate DPIAs into their data-handling workflows to maintain compliance and minimise risks.

- Additionally, platforms must ensure that algorithms used for matchmaking, content moderation, and personalisation are transparent, verifiable, and unbiased. Gaming companies must evaluate and validate these algorithms to meet regulatory standards.

## 2. Cross-border Data Transfers

Gaming companies must ensure compliance with cross-border data transfer requirements, which may mandate the local storage and processing of specific data types.

- Rule 14 restricts cross-border data transfers in cases where foreign states or their agencies request access, enforcing compliance with specific procedural safeguards. Additionally, the Rules empower the government to localise certain data, including "traffic data" (currently undefined), for SDFs and potentially all Data Fiduciaries, to prevent unauthorised access by foreign states.

[2] "The Central Government may notify any Data Fiduciary or class of Data Fiduciaries as Significant Data Fiduciary, on the basis of an assessment of such relevant factors as it may determine, including— Processing of personal data of children. Additional obligations of Significant Data Fiduciary. (a) the volume and sensitivity of personal data processed; (b) risk to the rights of Data Principal; (c) potential impact on the sovereignty and integrity of India; (d) risk to electoral democracy; (e) security of the State; and (f) public order." However, the Rules did not expand on the process of designation.
[3] Presently, there is no rule specifying this data localisation mandate, however, the Rules retain the space to do so.

- For instance, if the government classifies gameplay logs or communication data as critical personal data, companies may be required to store and process such data exclusively in India.

- Gaming platforms that process large volumes of user data, particularly in real-money gaming or e-sports, will need to navigate these cross-border transfer restrictions carefully and plan accordingly to remain compliant.

## 3. Consent Requirements

The DPDP Act requires all personal data processing to be accompanied by explicit, informed, and unambiguous consent. For users under 18 years of age, platforms must obtain verifiable parental consent. This departs from global standards like the GDPR (16 years) and COPPA (13 years):

- Platforms must ensure that all data collection is accompanied by valid consent. The Act defines valid "consent" as free, specific, informed, unconditional, and unambiguous, given through a clear affirmative action." Platforms must rely on reliable details, such as government-approved identity tokens or documents, to verify consent.

- Every consent request must include a clear notice detailing the data being processed, the purpose of processing, and ways users can exercise their rights, such as withdrawing consent or filing complaints with the DPB).

- These consent requirements may limit teenage engagement, significantly impacting user acquisition and retention.

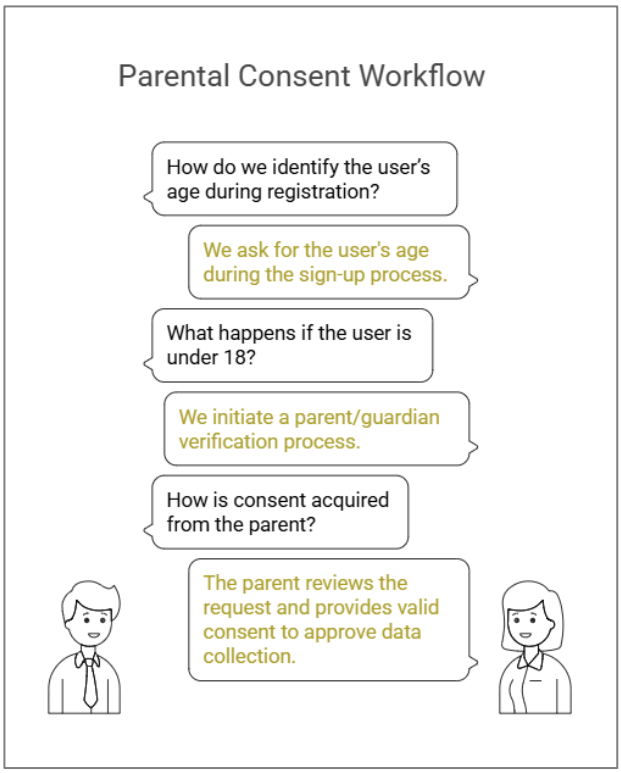


*Figure 1: Parental Consent Workflow*

- The prohibition on behavioural tracking and targeted advertising for children in free-to-play games requires further clarity on the scope, particularly on whether indirect promotional methods— those that could appeal to child audiences—fall under this restriction.

- When users voluntarily provide data during gameplay without an explicit request, platforms must assess whether this constitutes "valid consent" under the Act. Valid consent requires affirmative action and a clear indication of how the data will be used, even if the data is provided voluntarily.

- Platforms are also obligated to notify users regarding legacy data processing. If users fail to respond, the Rules do not provide clear guidance on whether data processing can continue. A

cautious approach would involve halting such processing until explicit consent is obtained or seeking clarification from the DPB on permissible measures.

- While Rule 11, r/w the Fourth Schedule, outlines exemptions for certain classes of institutions or purposes, online gaming companies do not currently fall within these categories. Furthermore, even if partial exemptions are granted in the future, Section 9(2) of the Act would still apply. This section prohibits any data processing that is "detrimental" to the "well-being" of the child. When terminology like "detrimental" or "well-being" is undefined.

## 4. Data Breach Reporting

Gaming companies must implement robust breach detection systems and clear protocols for notifying the DPB and affected users, including the required details of the breach and the mitigation measures taken:

- Companies must report breaches to the DPB without delay, and submit a detailed report within 72 hours, including providing updated information about the breach and steps taken to remediate it.

- Affected users must also be notified promptly, though the Rules do not specify a timeline for user notification.

- Additionally, companies must address overlapping requirements with relevant sectoral guidelines to ensure full compliance. For instance, Rule 2 of CERT-IN Directive 2022 mandates that the data fiduciaries must report a breach within 6 hours of detecting the incident. Moving forward, streamlining breach notification timelines will be essential to bring uniformity across regulations.

## 5. Data Minimisation and Retention

Platforms must implement data retention protocols to comply with the DPDP Rules' data minimisation and erasure requirements. These protocols must ensure that unnecessary data is erased and users are informed about the deletion process.

- Platforms should collect only the essential data required for service delivery.

- While it remains unclear, online gaming intermediaries may be required to delete inactive and redundant user data after three years, unless legal obligations under the Third Schedule dictate otherwise.

# 3. Gaps and Challenges for Online Gaming Companies

### 1. Ambiguity in Child Data Processing and High Age Threshold

- The requirement for parental/guardian consent for users under 18 years old presents operational challenges. This age limit departs from the global standards (13-16 years) and may result in lower engagement from teenage users.
- Additionally, many Indian households, particularly in rural areas, lack digital literacy, making it difficult to secure parental consent and limiting access for younger users.

### 2. Cross-border Data Flows

- Platforms that rely on international servers for live multiplayer gaming may face higher latency if certain types of personal data cannot cross borders freely.
- Uncertainty surrounding potential restrictions on cross-border data flows, particularly for SDFs, complicates expansion plans and disrupts seamless data transmission.

### 3. Overlap with RBI Data Localisation Guidelines

- Gaming platforms involved in real-money transactions must already comply with RBI's data localisation requirements for payment data.
- The DPDP Rules introduce additional localisation requirements for SDFs, which could include non-financial data, e.g.such in-game chat logs This adds operational complexity and increases cost.
- These mandates could disrupt live multiplayer games by requiring local storage and processing of player data, potentially causing latency issues, increased operational costs, and diminishing the seamless global gameplay experience these games rely on.

### 4. Algorithmic Verification Under SDF Obligations

Platforms classified as SDFs must ensure that the algorithms used for player matchmaking, content moderation, or personalisation are unbiased, accountable, and verifiable. This requirement could result in additional compliance and operational costs.

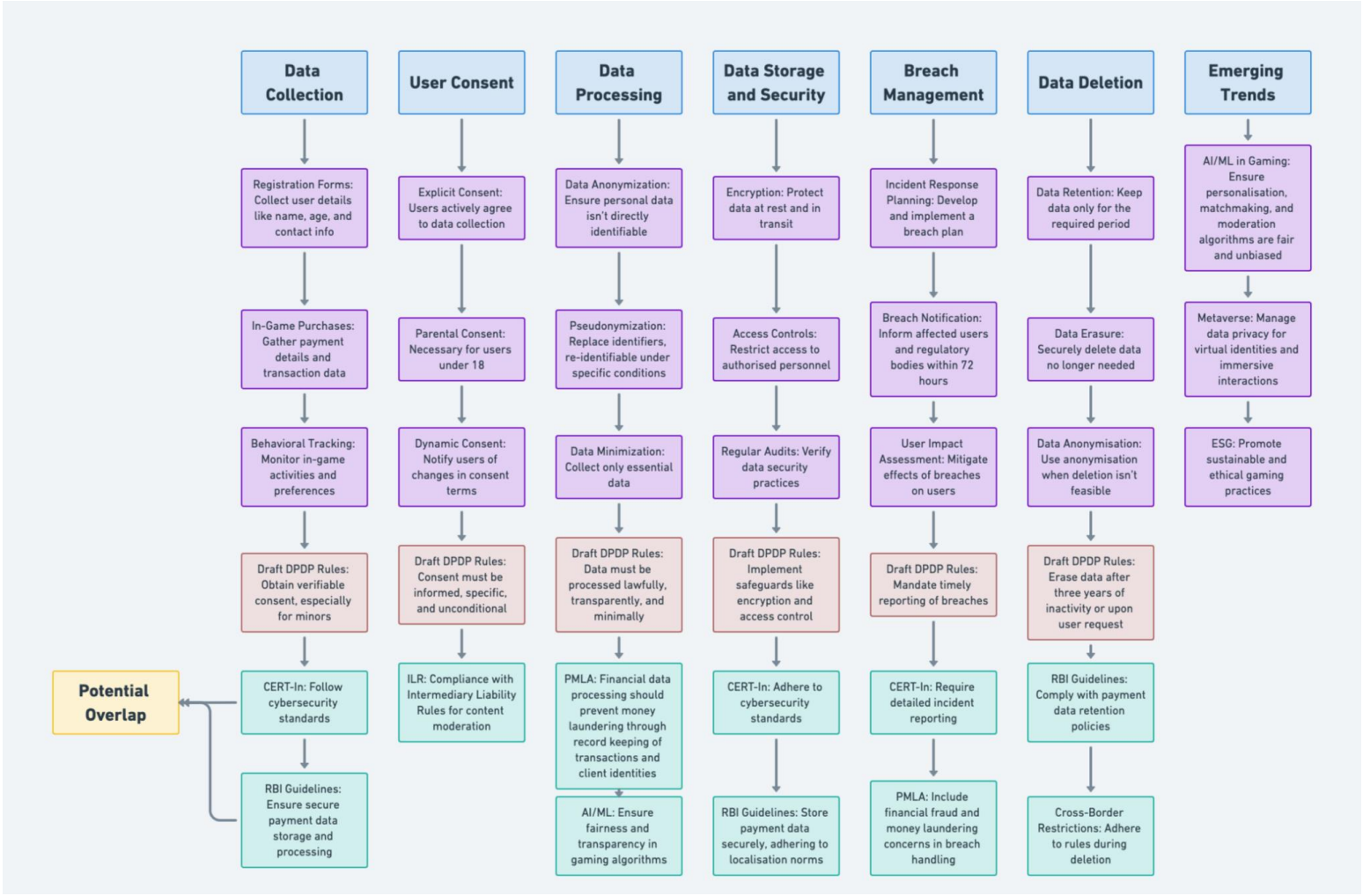


*Figure 2: Data Compliance Lifecycle for Online Gaming Companies*

# 4. Broad Policy Recommendations

## 1. Revisit Age Threshold for Consent

Section 9(5) of the DPDP Act should be revisited to allow for more flexible age limits, especially if data fiduciaries implement robust measures to verify the processing of children's data. The following recommendations could help achieve this :

- **Clear Guidelines**: Establish clear guidelines for verifiable measures, such as age verification systems and parental authentication, to ensure platforms can easily and effectively confirm the identity and age of users.

- **Industry Consultation**: The government should consult with industry stakeholders, including gaming companies, to develop scalable solutions for obtaining verifiable consent and addressing operational challenges.

- **International Alignment**: Align the age threshold for consent with international norms (13-16 years) to balance child protection with wider user engagement, especially among teenagers.

- **Definitional Clarity:** Terms like "detrimental" or "well-being" need to be clearly defined to help companies ascertain whether data processing falls within permissible limits. Clear definitions will also assist in identifying specific categories of game formats, such as those offering edutainment or games like chess. Such categories could potentially be granted exemptions under Rule 11, r/w Fourth Schedule.

## 2. Engagement with Stakeholders for Regulatory Clarity

Form consultation committees that include MeitY, gaming platforms, and industry associations to address the operational challenges posed by the DPDP Rules. Regulatory clarity is essential to ensure the balanced enforcement of the DPDP Rules, particularly in their interaction with existing IT Rules, RBI mandates, and global data protection standards. These consultations will help identify ambiguities and offer practical compliance solutions.

*The draft Digital Personal Data Protection (DPDP) Rules are currently open for public comments. If you have any feedback or input, we encourage you to share them with us. Please feel free to reach out at* ***info@thedialogue.co.***

thedialogue.co

LinkedIn | The Dialogue

X | The Dialogue

Whatsapp | The Dialogue

Instagram | The Dialogue