

# ANTICIPATED IMPACT

OF THE DIGITAL PERSONAL DATA  
PROTECTION ACT, 2023 ON THE  
ONLINE GAMING SECTOR

September 2024

# INDEX

## CHAPTER 1

3

### BACKGROUND

- (i) Online Gaming Sector in India
- (ii) Legislative Journey of the Data Protection Law

## CHAPTER 2

6

### SCOPE OF REPORT

- (i) Unique Requirements of India's Gaming Ecosystem
- (ii) Limitations the Report

## CHAPTER 3

8

### DATA FIDUCIARY OBLIGATIONS IN GAMING

- (i) Free-to-Play Games
- (ii) Real-Money Games
- (iii) Web3/ Emerging Technology Gaming
- (iv) Significant Data Fiduciaries in Online Gaming

### SUMMARY AND RECOMMENDATIONS

(i) Summary of Issues

(ii) Recommendations to the Central Government on Rules under the DPDP Act

- Clarifications and Exemptions Regarding Parental Consent for Online Gaming
- Clarifications on Personal Data Processing
- Timelines for Personal Data
- Processing Restrictions

# Chapter I: Background

---

## (i) Online Gaming Sector in India

The online gaming industry in India has witnessed rapid growth in recent years and has reached an estimated market size close of INR 16,428 crore in 2023, contributing to the direct employment of more than 1 lakh Indians, thanks to an estimated 425 million Indian gamers playing online across platforms.<sup>1</sup> The sector's meteoric rise has been catalyzed by the well documented growth in smartphone adoption, increased affordability of internet services and greater tele-density within the country. In terms of absolute numbers, India now ranks only behind China in terms of the number of gamers. However, in contrast to many other countries, the growth of Indian online gaming has been a 'mobile first' phenomenon, with smartphones being the device of choice for 94 percent Indian gamers.<sup>2</sup>

The low cost of these devices compared to consoles or personal computers has enabled the domestic gaming industry to reach Indian consumers across an array of socio-economic strata and geographies.

*Despite the impressive growth figures stated above, India's domestic online gaming industry forms only a small fraction (about 1.6 percent) of the overall global gaming ecosystem, which is estimated to be a USD 184 billion market.<sup>3</sup>*

There remains tremendous scope for the domestic gaming industry to scale and cater to the large Indian market for online games. To achieve this potential, India's sunrise gaming sector will require not only policy support, but also a conducive regulatory environment which promotes innovation. A robust yet balanced privacy regime, which addresses the risks and operational challenges within the Indian gaming sector, will go a long way towards achieving this untapped potential.

---

1. New frontiers: Navigating the evolving landscape for online gaming in India, Ernst & Young LLP, December 2023, available at [https://assets.ey.com/content/dam/ey-sites/ey.com/en\\_in/news/2023/12/ey-new-frontier-online-gaming-report.pdf](https://assets.ey.com/content/dam/ey-sites/ey.com/en_in/news/2023/12/ey-new-frontier-online-gaming-report.pdf)

2. Gameconomy Primer On India's Gaming Opportunity, Kalaari Capital, January 2023, available at <https://www.kalaari.com/wp-content/uploads/2023/01/Gameconomy-by-Kalaari-Jan-2023.pdf>

3. Dr. Alexander Schudey et al., Game Changer: Accelerating the Media Industry's Most Dynamic Sector, Boston Consulting Group, June 2023, available at <https://www.bcg.com/publications/2023/drivers-of-global-gaming-industry-growth>

## (ii) Legislative Journey of the Data Protection Law

On 12 August 2023, the Parliament of India passed into law the Digital Personal Data Protection Act, 2023<sup>4</sup> (**DPDP Act**) after a marathon period of public consultations, draft iterations and revisions. The mandate for this framework was envisioned by the Hon'ble Supreme Court in its landmark verdict in *KS Puttaswamy v. Union of India* (2017)<sup>5</sup>, where the court ruled in favour of the existence of an implicit 'right to privacy' as a fundamental right, in relation to the 'right to life' under Article 21 of the Constitution of India, 1950.

The right to privacy as understood by the Supreme Court is applicable to all forms of personal information of all persons. The DPDP Act has itself been enacted with a scope applicable to the automated, and partially automated, processing of personal data in digital space.<sup>6</sup>

The wide scope of the law has made future compliance a particular area of focus for the multitude of products, services and entities that comprise Digital India. Final enforcement of the DPDP Act is still awaited and rules regarding its implementation are expected to be published later in 2024.<sup>7</sup>

The first legislative iteration of the law was introduced in November 2019 as the Personal Data Protection Bill.<sup>8</sup> After an enduring consultation process and two further drafts, the final DPDP Act was eventually passed in August 2023. However, this event does not mark the completion of the privacy law's journey.

The DPDP Act empowers the Central Government to notify rules on a range of matters including the manner of obtaining consent, standards for processing data and the classes of data fiduciaries.<sup>9</sup>

In fact, the notification of substantive rules is essential for giving meaningful effect to the provisions of the DPDP Act, as the statute does not provide sufficient guidance to regulated entities by itself. Further, the enforcement of the DPDP Act may take place in phases, with some provisions coming into effect earlier than others. Scope for this manner of enforcement has been provided within the law itself.<sup>10</sup>

---

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

5. (2017) 10 SCC 1

6. Section 2(b), DPDP Act

7. Draft personal data protection rules likely in a month: Ashwini Vaishnav, Business Standard Report, 19 August 2024, available at [https://www.business-standard.com/politics/dpdp-act-rules-to-be-out-for-public-consultation-within-a-month-vaishnav-124081900935\\_1.html](https://www.business-standard.com/politics/dpdp-act-rules-to-be-out-for-public-consultation-within-a-month-vaishnav-124081900935_1.html)

8. Personal Data Protection Bill, 2019, available at [http://164.100.47.4/BillsTexts/LSBillTexts/Asintroduced/373\\_2019\\_LS\\_Eng.pdf](http://164.100.47.4/BillsTexts/LSBillTexts/Asintroduced/373_2019_LS_Eng.pdf).

9. Section 40(2), DPDP Act

10. Section 1(2), DPDP Act



Until the enforcement of the DPDP Act is initiated by Central Government, the existing light-touch privacy framework currently operative in India will continue to remain in force. This older framework was devised under Section 43A of the Information Technology Act, 2000 (**IT Act**),<sup>11</sup> which specified the liability of body corporates possessing, dealing with, or handling any 'sensitive personal data or information' stored in a computer resource. In addition to the IT Act, the Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules, 2011 (**RSPDI Rules**) were notified to guide the information security and data handling processes undertaken by body corporates, which would include online gaming entities.

It is expected that transitioning from this light-touch IT Act framework to the DPDP Act will require significant adjustments on the part of online gaming companies.

---

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

# Chapter II: Scope of Report

---

The DPDP Act introduces multiple new compliances on entities processing personal data in India to provide services to users. While the impact of these compliances will be felt across sectors, this report has been prepared with special focus on gaming companies offering services to users within the country as detailed below.

## (i) Unique Requirements of India's Gaming Ecosystem

The DPDP Act introduces several implementation challenges across digital sectors, where entities are engaged in the processing of digital personal data. However, the nature of the challenges faced by one class of entities may differ as compared to another. For instance, a priority for e-commerce platforms in reference to DPDP Act compliance would be the expected impact on processes for handling and drawing insights from large volumes transaction data collected from individual users to enable revenue growth.<sup>12</sup> However, this aspect of data handling may not be of equal relevance to operators of online games.

Additionally, the online gaming sector within India remains a nascent industry requiring institutional and policy support from regulators to achieve its growth potential and contribute to the Government of India's goal of a USD 1 trillion digital economy.

This industry also forms a core component of the Animation, Visual Effects, Gaming and Comic (**AVGC**) sector identified by a Central Government taskforce and observes participation from many domestic MSMEs.<sup>13</sup>

The small gaming companies and MSMEs present in this bustling operating environment are heavily constrained in terms of resource allocation capacities towards regulatory compliance. Hence, it will be crucial for such smaller entities to understand and anticipate the operational challenges that stem from the enactment of the DPDP Act to remain competitive with their peers across the industry. This report intends to capture some of the focal areas where these constraints may present unique challenges to gaming.

---

12. DPDP Act: Impact on E-Commerce and Services Sector, PwC India, available at <https://www.pwc.in/blogs/digital-data-protection-act.html>

13. Realising the Potential of the AVGC-XR Sector Potential in India, AVGC Promotion Task Force (2022) available at <https://mib.gov.in/sites/default/files/AVGC-XR%20Promotion%20Taskforce%20Report%20-%202022.pdf>.

## (ii) Limitations the Report

It should also be noted that the following analysis is not intended to serve as a comprehensive assessment of regulatory concerns and risks for online games arising out of the DPDP Act. Such an assessment would only be possible once the law is under implementation, and relevant rules are notified. The primary objective of this report is to identify some of the key issues and distinct impacts for the domestic online gaming industry based on our current understanding of this new data protection regime. As elaborated subsequently, these issues largely stem from the obligations imposed on data fiduciaries towards the users whose personal data they collect or process (i.e. Data Principals).

The DPDP Act imposes several such legal duties and compliances on Data Fiduciaries to minimize the consequent data processing risks. Violation of the act's legal requirements may result in severe penalties for the errant Data Fiduciary, which may extend to a maximum of INR 250 crore (approximately USD 30 million) in some circumstances.<sup>14</sup> Gaming companies falling under the definition of a 'Data Fiduciary' would be subject to the gamut of legal requirements and liabilities under the DPDP Act.

Lastly, it should be noted that the DPDP Act identifies and defines another class of entities (i.e. Data Processors) which process data on behalf of a Data Fiduciary.<sup>15</sup> However, specific obligations defined for Data Processors under the law are fairly limited. The minimal implications of these provisions on the gaming sector are therefore not included within the scope of this report.

---

14. The Schedule & Section 33(1), DPDP Act

15. Section 2(k), DPDP Act



# Chapter III: Data Fiduciary Obligations & Gaming

---

The DPDP Act has been developed with the specific purpose of prescribing and enforcing privacy obligations in relation to personal data that is handled or processed in digital form. The primary targets of this law, Data Fiduciaries, have been defined as:

*“any person who alone or in conjunction with other persons determines the purpose and means of processing of personal data;”<sup>16</sup>*

In this respect, digitally published online games typically collect and process a range of personal information from their users (such as the email address, date of birth, age, social media identification, and gender etc.), which may be used by game publishers or operators for a number of crucial game-centric purposes including, among others:<sup>17</sup>

- in-game event participation
- matchmaking
- software improvements
- preventing of fraud or cheating
- monitoring in-game harmful behavior
- player tracking
- development of new features

It is probable that entities operating or publishing various formats of digital/online games in India may be classified as ‘Data Fiduciaries’ (referred to subsequently as **Gaming Data Fiduciaries**) under the DPDP Act, as they may determine both the means and the purpose of processing user personal data. The DPDP Act does not territorially restrict the ‘Data Fiduciary’ status to processing within the country. It is also applicable to the processing of digital personal data abroad, if such processing is in relation to the offering of goods and services to Data Principals inside India.<sup>18</sup>

---

16. Section 2(i), DPDP Act

17. Illustrative list is based on a survey of the Privacy Policies of popular online games by the authors.

18. Section 3(b), DPDP Act

The wide definition for Data Fiduciaries under the DPDP Act encompasses a large variety of entities which collect and process personal data. However, the diversity of purposes of data processing and business models within the gaming sector entails that obligations under the DPDP Act are likely to have disparate impacts on different kinds of Gaming Data Fiduciaries, as illustrated below. Data protection issues may differ across free-to-play, real money and Web3 based online games. This may, in turn, warrant distinguished compliance approaches for these gaming sub-sectors.

---

## (i) Free-to-Play Games

The term ‘free-to-play games’ (**F2P**) generally refers to online games that give players access to a significant portion, though not necessarily all, of their content without demanding direct payment from the user. However, it should be noted that no specific legal definition of F2P games exists under Indian laws. F2P games are designed to be downloaded and played for free and can offer additional features, services, or virtual goods that can be purchased by players through ‘microtransactions’ as a form of monetization.<sup>19</sup>

These in-game purchases can be made for cosmetic items, upgrades, features that enhance the gaming experience, or those which provide a competitive edge to the purchasing player.<sup>20</sup> Advertising may be an additional revenue stream for these kinds of games.

F2P games, which collect user personal information in relation to the services they offer, may be categorized as Gaming Data Fiduciaries in relation to that personal data.

For instance, this information may be collected at the time of registration within the game or during the creation of a user profile for game-centric purposes, as noted above. Data from users may also be collected during gameplay, which can be used to serve targeted advertising to users based on their behaviors, preferences, in-game choices, and location.

---

19. A popular battle-royale game ‘PUBG Mobile’ was reported to earn USD 3.5 billion in revenue through microtransactions in 2020. Details available at <https://in.ign.com/playerunknowns-battlegrounds-mobile/150641/news/pubg-mobile-has-earned-35-billion-via-microtransactions>

20. Popular free-to-play games include such titles as [Battlegrounds Mobile India](#), [Roblox](#), [Clash of Clans](#), [Angry Birds](#), and [8 Ball Pool](#).

Gaming Data Fiduciaries (largely gaming companies operating games and providing access directly to users) will be expected to comply with all obligations generally applicable for non-government Data Fiduciaries.<sup>21</sup> For instance, this would include notice and consent requirements, implementing technical and organizational measures, and providing Data Principals with the right to erasure, under Chapter II of the DPDP Act. However, the following aspects are of particular concern for F2P games.

## Processing of Children's Data:

An important facet of F2P games is that they can largely cater to multiple different age-groups. By implication, F2P games operating within India presently process the personal data of adults, as well as children (below the age of 18 years). The presently applicable RSPDI rules under the IT Act do not mandate any specific obligations in relation to the data of children. However, such distinct obligations are in fact outlined under the DPDP Act. F2P Gaming Data Fiduciaries must obtain verifiable consent of the parent of such child or the lawful guardian,<sup>22</sup> prior to the processing the personal data of a child. The DPDP Act also requires that Gaming Data Fiduciaries:

- Do not undertake any processing of personal data likely to cause any detrimental effect to the well-being of a child,
- Do not undertake tracking or behavioral monitoring of children, and
- Do not target advertising directed at children.<sup>23</sup>

These prescriptions are likely to pose a disproportionate challenge to common industry practices among F2P games, and may even impact how they monetize their user base via advertising. These challenges are elaborated subsequently.

---

21. Various provisions of the DPDP Act provide exemptions for specific use cases and agencies relating to the Government.

22. Section 9(1), DPDP Act

23. Section 9(2) and 9(3), DPDP Act

## Implementing Age-Based Processing Distinctions:

In typical circumstances, F2P Gaming Data Fiduciaries may not be precisely aware of the specific age, or age bracket, of their users. While most F2P online games rely heavily upon content-based age-rating systems for the distribution of their games, these cannot be legally enforced against users within India.<sup>24</sup>

Rather, users are advised to exercise their personal discretion/parental control features<sup>25</sup> while accessing age-appropriate games as per content classification information. It should also be noted that even in relation to age-rating, a statutorily enforced system of rating and content classification is yet to be adopted within India, although precedents do exist for digital content rating in other fields such as video streaming.<sup>26</sup> While a reliable and validated domestic age-rating system may help F2P Gaming Data Fiduciaries distinguish gaming content warranting parental consent compliance under DPDP Act (i.e. content rated appropriate for children), this would not eliminate consent-related complications for F2P games with a user base extending across multiple age groups. Given the limited size and capability of most games operating in the F2P space (which may include independent developers, publishers and other MSMEs) onerous know-your-customer processes would not be a feasible solution to assessing parental consent requirements.

Once the need for obtaining parental consent has been identified, scope is provided within the DPDP Act to prescribe specific processes for obtaining verified parental consent for processing a child's data. As a significant demographic for F2P games comprises minors, this would become a crucial compliance challenge for F2P Gaming Data Fiduciaries.

However, at this stage, the likely mechanism for obtaining parental consent is not clear, with multiple open questions regarding the approach of regulators. In any case, future consent mechanisms, which may involve identity verification and inclusion of non-players, are likely to add additional costs for F2P games.

---

24. The two most prominent systems of age-rating and content classification globally are the Entertainment Software Rating Board (ESRB) and Pan European Game Information (PEGI), for the North America and European regions respectively. However, these systems of classification also inform standards for global online game distribution systems, including popular smartphone application marketplaces. Both rating systems not only distinguish adult appropriate gaming content but also distinguish age-appropriate content for children of different age groups.

25. See information available at <https://pegi.info/page/game-advice> and <https://www.esrb.org/faqs/#are-all-games-required-to-have-a-rating>

26. II(A)(b), Appendix, Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, available at <https://mib.gov.in/sites/default/files/IT%28Intermediary%20Guidelines%20and%20Digital%20Media%20Ethics%20Code%29%20Rules%2C%202021%20English.pdf>

## Scope of Detrimental Processing:

A second identified challenge is the requirement to prevent the detrimental effects on the well-being of a child from the processing of personal data. This is a significant departure from previous iterations of the draft law, where a definition for ‘harm’ was provided, enabling Data Fiduciaries to identify specific harmful outcomes to target and mitigate.<sup>27</sup> F2P Gaming Data Fiduciaries may find it difficult to anticipate the variety of data processing related outcomes which may constitute an ‘intangible detriment’ to a minor Data Principal. In the absence of any further guidance on the scope of this obligation, the compliance burden of this requirement may demand future clarifications from regulators.

## Restrictions on Tracking:

A final substantive concern stemming from these DPDP Act responsibilities is the broadly worded obligation to not undertake tracking or behavioral monitoring of children. The text of the DPDP Act does not clarify what constitutes ‘tracking’ in the context of F2P, or any other formats of online games. This is a crucial aspect for the gaming sector which maintains user profiles or accounts, actively tracking their progress through a game for a range of purposes. Such tracking may be necessary in the case of minors for operating basic in-game features such as matchmaking, or for tackling cheating. Section 9(3) of the DPDP Act provides no qualifying language limiting the prohibition on tracking or behavioral monitoring of children, and hence no leeway in the interpretation of this provision.

This obligation has the potential to directly impact the fundamental business model of F2P games, if players under the age of 18 are barred from having in-game track-able profiles. F2P games also largely rely on in-game purchases and advertising for revenue generation. The DPDP Act’s stringent restrictions could impact the any targeted advertising of children at a granular level enabled by F2P games, which may, in turn, affect their revenues streams. The restriction on behavioral tracking also carries the potential to interfere with various technical tools<sup>28</sup> (including artificial intelligence driven tools) that may be deployed to monitor risks to children within gaming environments and detect toxic behavior, cyber-bullying or predatory activity.

---

27. ‘Harm’, in relation to a Data Principal, meant any bodily harm, distortion or theft of identity, harassment, or prevention of lawful gain or causation of significant loss; under Clause 2(10), Draft Digital Data Protection Bill, 2022 available at [https://www.meity.gov.in/writereaddata/files/The%20Digital%20Personal%20Data%20Protection%20Bill%2C%202022\\_0.pdf](https://www.meity.gov.in/writereaddata/files/The%20Digital%20Personal%20Data%20Protection%20Bill%2C%202022_0.pdf)

28. Child Safety and Protection in the Online Gaming Ecosystem, A. Faraz, J. Mounsef, A. Raza and S. Willis, in IEEE Access, vol. 10, pp. 115895-115913, 2022, doi: 10.1109/ACCESS.2022.3218415.

## (ii) Real-Money Games

Unlike other categories of online games, online real-money games (**RMGs**) have been given a legislative definition in India under the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021:<sup>29</sup>

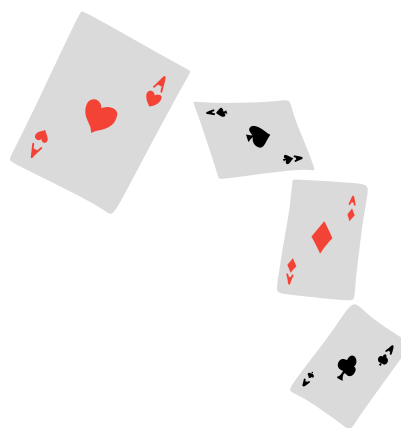
*“an online game where a user makes a deposit in cash or kind with the expectation of earning winnings on that deposit.*

*Explanation.— In this clause, “winnings” means any prize, in cash or kind, which is distributed or intended to be distributed to a user of an online game based on the performance of the user and in accordance with the rules of such online game;”*

RMGs allow players to deposit real-money to participate in skill-based games against other real players to win a prize based on their performances. The RMG platform charges a percentage of the money deposited as a platform fee for the facilitation services they provide to players, which compromises the primary source of revenue. Common formats in the RMG category in India include daily fantasy sports, rummy, poker, pool and chess.<sup>30</sup>

As a consequence of their design, these platforms often require more sensitive personal and financial data from their users for ensuring financial integrity and preventing fraud, which may involve adherence to know-your-customer protocols (**KYC**).<sup>31</sup>

Unlike previous iterations of the law, the DPDP Act does not differentiate between types of personal data based on their sensitivity. Hence, RMG Data Fiduciaries would be required to follow similar notice and consent mechanisms as ones that are



followed by other categories of Data Fiduciaries under the DPDP Act, despite the additional data-types which may be involved.

Another aspect regarding the enhanced kinds of personal data collected by RMGs is that the data protection compliance burden, in some respects, may not be as significant as for F2P games, since RMGs only cater to adults. Under the amended Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, RMGs are restricted from enabling minors to access and play on their real-money platforms.

29. Rule 2(1)(qd), Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, as amended in April 2023, available at <https://www.meity.gov.in/writereaddata/files/Information%20Technology%20%28Intermediary%20Guidelines%20and%20Digital%20Media%20Ethics%20Code%29%20Rules%2C%202021%20%28updated%2006.04.2023%29-.pdf>.

30. Popular platforms offering such formats of games include [First Games](#), [MPL](#), [Spartan Poker](#), [Dream11](#) and [Gameskraft](#), among others.

31. Rule 4(1)(b) of the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021.

This can be ensured through technical solutions such as age-gating mechanisms implemented at the time of user onboarding.<sup>32</sup> By barring minors' access to their platforms, RMGs may be able to dispense with a number of child-related data protection obligations which would otherwise affect other gaming formats. However, important applicable compliance issues under the DPDP Act have been elaborated below:

## User Notice and Consent:

The DPDP Act mandates that all Data Fiduciaries must provide notices to consumers about the collection and use of their data. Due to the more frequent and elaborate data collection points necessary for RMGs, which include KYC and financial personal data of their users (during touchpoints such as registration, user verification, and deposit account creation), RMGs will need to devise more granular notice mechanisms in keeping with the requirements of the law, although the DPDP Act does enable some flexibility to Data Fiduciaries on the form of the notice that may be provided. The DPDP Act obliges Gaming Data Fiduciaries, including RMGs, to provide detailed notices to consumers about how their data will be used, stored, and shared.<sup>33</sup>

Hence, at the stage of onboarding new users, RMG Data Fiduciaries would need to be informed, not only about the game mechanics, but also about how their collected KYC and personal data is processed, stored, and protected.

These notices should cover everything from how the data may be used to identify fraudulent activity in-game, to how it may be shared with third-party vendors for payment processing. Under the DPDP Act, failure to adequately inform users regarding their personal data can result in significant penalties for Data Fiduciaries.<sup>34</sup> On the aspect of processing personal data, consent may need to be sought for each category of personal data, alongside providing the option to refuse consent for specific data categories.<sup>35</sup>

Introducing substantial notice and consent processes could overwhelm players, leading to potential 'consent fatigue' (which refers to the exhaustion of users in having to approve data procession requests). This also has ramifications for the growth potential of RMGs. Overly complex or lengthy notices could deter a player from completing the registration process, leading to the risk of higher user funnel drop-off rates.

---

32. Online gaming intermediaries offering real-money games under the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 are obligated to ensure their players are of adequate age to be competent to enter a contract.

33. Notice given to data principals as per Section 5 of the DPDP Act must inform them of what personal data is collected and for what purposes, how right to withdraw consent and grievance redressal may be exercised, and how complaints to the Data Protection Board under the act may be made.

34. Penalty for general breach of obligations under the DPDP Act may extend to INR 50 crore. The Schedule, DPDP Act

35. Digital Personal Data Protection Act: Know The Impact on Online Gaming Intermediaries, Dharmender Jhamb, Arindam Das, Grant Thornton, December 2023, available at <https://www.grantthornton.in/insights/blogs/digital-personal-data-protection-act-know-the-impact-on-online-gaming-intermediaries/>

Each additional step creates an opportunity for the user to abandon the registration process, affecting user funnel metrics negatively.<sup>36</sup> While simplifying the language of consent forms, or employing just-in-time notices where information is provided can help mitigate some of these effects, RMG Gaming Data Fiduciaries will need to modify and evolve existing notice and consent procedures to comply with the law, and do so in a manner that does not alienate their user base. The implementation of effective consent management frameworks under the DPDP Act will also need to play a vital role in mitigating some of these effects associated with user fatigue.<sup>37</sup>

## Sectoral Data Regulation:

While the personal data obligations for RMGs under the DPDP Act appear somewhat attenuated in contrast to F2P games, the application of sector-specific data processing obligations for RMGs is not precluded by the DPDP Act. Sector specific requirements will continue to be applicable and complement the requirements under the DPDP Act. For instance,<sup>38</sup> the Reserve Bank of India has issued specific requirements for storage of payment systems data (a kind of financial data) only within India, which may also include requirements applicable to digital personal data.<sup>39</sup> In the specific context of RMGs, special attention must be given to Rule 4(12) Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 which requires online gaming intermediaries offering RMGs to verify user identity before accepting any deposits, and also states:

*“Provided that the procedure required to be followed by an entity regulated by the Reserve Bank of India for identification and verification of a customer at the commencement of an account-based relationship shall apply, mutatis mutandis, in identification and verification of the users of such online gaming intermediary.”*

While specific clarity on the nature of ‘KYC’ obligations for the handling of this personal and financial data by RMG online gaming intermediaries is awaited, it is apparent that some form of sectoral data collection and handling obligations will continue to be applicable to RMGs, even as the DPDP Act gradually comes into force.

---

36. A conceptual understanding of drop-off rates is available at <https://userpilot.com/blog/drop-off-rate/>

37. Section 6 of the DPDP Act allows for the registration of Consent Managers (single point of contact for data principals to manage consent) with the Data Protection Board. The details of the accountability and obligations of Consent Managers under this act, once registered, are yet to be prescribed.

38. Section 38 of the DPDP Act states that the provisions of the DPDP Act shall be in addition to, and not in derogation of, other laws in force.

39. Storage of Payment System Data, Reserve Bank of India Notification, dated 6 April 2018, available at <https://www.rbi.org.in/Scripts/NotificationUser.aspx?Id=11244&Mode=0>



### (iii) Web3 / Emerging Technology Gaming

Web3 gaming, often linked with the 'Metaverse',<sup>40</sup> represents a new frontier in immersive digital interaction and online gaming. Incorporating blockchain technology, which uses irrefutable decentralized ledgers for storing any kind of information digitally for public access, Web3 gaming offers a decentralized yet interoperable experience that gives players greater control over their digital assets. While these nascent gaming technologies promises to revolutionize the landscape, they also present unique challenges in terms of user data protection and privacy, particularly in the context of India's DPDP Act.

#### Privacy on the Blockchain:

One crucial aspect of Web3 is the nature of interactions between the blockchain and privacy obligations under the DPDP Act. The DPDP Act mandates that data Fiduciaries inform users about the nature of data being collected, but it is unclear, in many ways, how these laws would apply to decentralized networks. Some Web3 gamers play to earn in native cryptocurrency, which can be used on virtual assets or converted into real fiat money. Users can also buy skins in-game as non-fungible tokens, which if tradeable, may become investment options for players in-game.<sup>42</sup>

Still, Web3 gaming may include many of the same underlying internet technologies as older games, such as communication via internet protocols, or profile logins with social media accounts. Web3 game operators may still collect personal information from users as standard practice, and may hence become Web3 Gaming Data Fiduciaries. Hence, some privacy vulnerabilities and compliance concerns for Web3 games may not be a radical departure from those associated with F2P or RMGs.<sup>41</sup> This would include the requirement for providing specific notice prior to receiving informed consent from the Data Principal.

The blockchain remains the underlying technology for implementing these features and Web3 Gaming Data Fiduciaries will need to be mindful of privacy obligations in relation to any personal data that it processed using the blockchain.

Evidently, there are certain grey areas in terms of compliance by Web3 Gaming Data Fiduciaries deploying blockchain-based technologies.

40. The Metaverse specifically refers to the bundle of next generation technologies such as virtual and augmented reality, expected by some parts of the digital sector to evolve into the third version of the world wide web (i.e. Web3.0)

41. Page 18 of Web3: A Tech and Policy Brief For India, National Law School of India University, December 2022, available at <https://www.nls.ac.in/wp-content/uploads/2022/12/FINAL-NLS-WEB-PRIMER.pdf>

42. Page 10 of Web3 and Digital Entertainment: A Tech and Policy Brief for India, March 2023, available at <https://www.nls.ac.in/wp-content/uploads/2023/03/NLS-Web3-and-Digital-Entertainment-Policy-Brief.pdf>

For instance, in blockchain ledgers which are made public, it may not be possible to trace a user who carried out a transaction on the chain, even if the corresponding public key is made available.<sup>43</sup> This enables anonymity for the involved user. The applicability of the DPDP Act to such information is ambiguous as an individual may not be identifiable by, or in relation to, such data.<sup>44</sup> Alternatively, if information which qualifies as digital personal data is indeed encoded onto a publicly accessible blockchain, this may create challenges for enabling the rights of Data Principals to correction, updating or erasure of their personal data,<sup>45</sup> due to the immutability of information stored on the blockchain.

## Pseudonymous Identities:

Web3 gaming platforms often allow for pseudonymous, or even anonymized, interactions through the creation of digital avatars to interact with the world within the Metaverse. While such avatars may be constructed using vast amounts of biometric data and other personal data for a high level of realism and fidelity,<sup>46</sup> game developers are equally free to venture in the opposite direction to enable pseudonymous avatars which, though individually unique, may not bare any resemblance to the users they represent.

This represents another present grey area in the applicability of the DPDP Act, as such data may, or may not, qualify as personal data under the law. Such complications are further compounded when paired with psychophysical data, such as emotional expressions, behavior, breathing and body movements, which

may in some circumstances identify an individual<sup>47</sup> in the context of a Web3 game. Such kinds of information, when exhibited in a virtual reality environment can generate some 2 million unique data elements.<sup>48</sup>

Depending on the legal interpretation of data in these kinds of circumstances, Web3 gaming in the Metaverse may be considered as a format involving the processing of even more personal data than traditional game<sup>49</sup> formats. Alternatively, such practices may merely be treated as the processing of non-personal data.

---

43. Transactions on a public ledger are typically linked to user-held private keys which is necessary alongside the public key. More information on this aspect of blockchains is available at <https://consensys.io/blog/how-is-blockchain-verifiable-by-the-public-and-yet-anonymous>

44. This is the standard criteria for categorization of any information as personal data, as specified under Section 2(t), DPDP Act.

45. Section 12, DPDP Act

46. Page 247 of Baily Martin, Privacy In A Programmed Platform: How The General Data Protection Regulation Applies To The Metaverse, Harvard Journal of Law & Technology Volume 36, Number 1 Fall 2022, available at <https://jolt.law.harvard.edu/assets/articlePDFs/v36/Martin-Privacy-in-a-Programmed-Platform.pdf>

47. Personal data protection in the Metaverse: operational challenges and regulatory uncertainties, ICTLC, available at <https://www.ictlc.com/personal-data-protection-in-the-metaverse-operation-challenges-and-regulatory-uncertainties/?lang=en>

48. Shelly Kramer, Metaverse Privacy Concerns: Are We Thinking About Our Data?, Forbes, 1 June 2022, available at <https://www.forbes.com/sites/forbestechcouncil/2022/06/01/metaverse-privacy-concerns-are-we-thinking-about-our-data/?sh=659426bbff8>

49. Page 252 of Baily Martin, Privacy In A Programmed Platform: How The General Data Protection Regulation Applies To The Metaverse, Harvard Journal of Law & Technology Volume 36, Number 1 Fall 2022, available at <https://jolt.law.harvard.edu/assets/articlePDFs/v36/Martin-Privacy-in-a-Programmed-Platform.pdf>

## (iv) Significant Data Fiduciaries in Online Gaming

Finally, it should also be noted that all three categories of Gaming Data Fiduciaries discussed above (F2P, RMG and Web3) may potentially qualify as Significant Data Fiduciaries under the DPDP Act and may be notified under this category by the Central Government.<sup>50</sup> Once notified as a Significant Data Fiduciary, a range of additional data protection obligations would be applicable to such a gaming entity, which would include, among others:

- Appointment of a Data Protection Officer based in India
- Appointment of an independent data auditor
- Conduct of periodic data impact assessment
- Such other obligations as the Central Government may specify

While notification would carry additional compliance burden for gaming data fiduciaries, the nature of this additional compliance does not appear to present any unique operational challenges for the gaming sector. However, this is open to change in the future on the basis of future prescriptions of the Central Government.

---

50. Section 10 of the DPDP Act enables the Central Government to notify specific or entire classes of data fiduciaries as Significant Data Fiduciaries after assessing factors such as volume of personal data processed, risks to the data principal, impact on sovereignty, security, and public order etc.







# Chapter IV: Summary and Recommendations







## (i) Summary of Issues







While the gaming industry in India continues to expand, there remain significant regulatory challenges ahead, which will need to be addressed. This remains especially true for the implementation of the newly enacted DPDP Act. Based on the discussion of the implementation challenges above, the following table has been compiled to help summarize some of the key privacy law concerns that are anticipated to confront the country’s gaming industry, and its three core sub-categories: F2P, RMG and Web3 gaming (provided that they qualify as Data Fiduciaries under the DPDP Act).




**Table: Observations on Expected Impact of Key DPDP Act Provisions on Gaming Data Fiduciaries**

Legal Provision of DPDP Act	Key Elements of Provision	Observations for Gaming Data Fiduciaries	Expected Impact		
			F2P	RMG	Web3
<b>Notice (Section 5)</b>	(1) Request for consent shall be preceded by a notice informing the user of (a) purpose for which data will be processed; (b) manner of exercise of rights of data principal; (c) manner for complaints to data protection board  (2) Language of notice may be either English or any language of Eighth Schedule of the Constitution of India.	The DPDP Act regulates the collection and processing of digital personal data by entities qualifying as data fiduciaries. The need to acquire explicit and informed consent is one of the key obligations under the DPDP Act, that would be applicable for all Gaming Data Fiduciaries. This requirement mandates specific and prior notice. Data Fiduciaries must issue a clear and plain-language notice, detailing what data will be collected and why. The notice should also guide users on how to exercise their rights or file complaints.  In a departure from previous drafts of the law, the DPDP Act is less explicit about the types of information that should be included in user notices which had detailed requirements for data retention periods and third-party sharing. The current version only mandates that entities show what data is collected and for what specific purpose. However, a scope remains for additional requirements to be prescribed later.	●	●	●

<p><b>Consent (Section 6)</b></p>	<p>(1) Consent in relation to personal data must be free, specific, informed, unconditional, and unambiguous with clear affirmative action to signify agreement do data processing for specified purpose.</p> <p>(2) Any consent that constitutes an infringement under this act, rules, or any other law in force shall be invalid to the extent of the infringement.</p> <p>(3) Every request for consent shall by a data fiduciary should be presented in clear and plain language with the option to access the request in either English or any language in the Eighth Schedule.</p>	<p>Users will be able to manage their consent via 'Consent Managers', who must be registered with the Data Protection Board of India. Failure to comply with the requirements under DPDP Act can potentially result in fines up to INR 250 crores, contingent on the severity of non-compliance.</p>			
<p><b>General obligations of Data Fiduciary (Section 8)</b></p>	<p>(1) Data fiduciary must comply with the act and all rules.</p> <p>(2) Data fiduciary may appoint a data processor to process data on its behalf under a valid contract.</p> <p>(3) In case personal data will affect a decision made by data principal or be disclosed to another data fiduciary, the data fiduciary shall ensure its completeness, accuracy, and consistency.</p> <p>(4) Data fiduciary shall undertake appropriate measures to comply with the DPDP Act and rules.</p> <p>(5) Data fiduciary shall protect personal data in its possession or under its control, including any processing by it or on its behalf by a data processor.</p> <p>(6) In case of data breach, a data fiduciary must inform data protection board and each affected data principal in the prescribed form.</p>	<p>Appointment of data processor pursuant to a valid contract is a well-established industry practice and an effective mechanism for gaming data fiduciaries to ensure the sanctity of any digital personal data transfers to processors.</p> <p>Data fiduciaries (including online gaming entities) are also obligated to prevent data breaches and notify affected parties and the Data Protection Board if breaches occur. Personal data must be erased once the purpose is fulfilled, subject to legal compliance requirements. Greater clarity on what may be deemed as the end of the 'purpose' is awaited under prescribed rules that will be notified by the Central Government to implement the law.</p>			

	<p>(7) Data fiduciary shall (unless its retention is necessary for any law for the time being in force) erase personal data upon data principal withdrawing her consent or when the specified purpose is served (whichever is earlier).</p>				
<p><b>Processing of Children's Data (Section 9)</b></p>	<p>(1) Before processing the data of any minor or person with disability, the data fiduciary (under the age of 18) must obtain verifiable consent of the parent / lawful guardian of such child.</p> <p>(2) Data fiduciary cannot undertake processing of personal data that is likely to cause any detrimental effect on the well-being of a child.</p> <p>(3) Data fiduciary cannot undertake tracking or behavioural monitoring of children or targeted advertising directed at children.</p>	<p>The processing of children's data become a major concern for any games offered to players below the age of 18 (particularly F2P Gaming Data Fiduciaries). However, such issues may also affect some Web3 games, depending on their business model. Systems to distinguish and verify age of players will be necessary to comply with such obligations. Even so, any user-facing complications arising from implementing these changes may affect engagement among players under the age of 18 years.</p> <p>Further, as discussed in the report, restrictions on certain kinds of processing, profiling and targeted advertising may fundamentally affect how F2P Data Fiduciaries structure their offerings towards minors. The DPDP Act's provision regarding well-being of children remains ambiguous and does not enumerate specific actions that are considered harmful. Unlike earlier versions, the enacted law omits the term 'harm' thus broadening the potential scope for legal action. The large potential fine that may be imposed for non-compliance may become a significant source of concern for F2P games.</p>			
<p><b>Significant Data Fiduciary and their Obligations (Section 10)</b></p>	<p>(1) Central Government may notify a data fiduciary or a class of data fiduciaries as significant data fiduciaries on factors, including: (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.</p> <p>(2) Additional obligations for significant data fiduciaries include the appointment of a data protection office, appointment of an independent data auditor, and undertaking periodic Data Protection Impact Assessments.</p>	<p>The actual implementation challenges for Gaming Data Fiduciaries will depending on notification under this category. Till such point, these obligations remain non-applicable.</p> <p>At this stage, it is difficult to assess the precise risk of notification as significant data fiduciaries beyond the factors enumerated. However, once notified, even Gaming Data Fiduciaries offering services in India without significant physical presence within the country would have to comply with the added compliance requirement of appointing an India-based data protection officer. Similar compliance risks as applicable to entities from other digital sectors would also affect gaming entities notified under this category.</p>			

<p><b>Rights of Data Principal</b> (Sections 11, 12, 13, &amp; 14)</p>	<p>(1) The DPDP Act bestows certain rights upon and assigns certain duties to data principals: (a) Right to access information about personal data; (b) Right to correction and erasure of personal data; (c) Right of grievance redressal; (d) Right to nominate in event of death or incapacity.</p> <p>(2) Data fiduciaries are obligated to help Data Principals in the realisation of these rights in a timely manner.</p>	<p>Data Principals can request a summary of personal data, its processing activities, identities of other fiduciaries and processors, and any other related information. This may present a potential challenge for Web3 Gaming Data Fiduciaries, due to the large volumes of digital personal data generated. Providing detailed summaries on-demand could be a resource-intensive and cumbersome task for game operators.</p> <p>The Data Principal also have the right to request corrections, completion, or updating of personal data. Implementing real-time systems to handle these corrections, especially in blockchain-based games where data is immutable by nature, could prove to be technically challenging.</p> <p>Further, in terms of grievance redressal, dedicated resources may be necessary for Gaming Data Fiduciaries to deploy in complying with their obligations.</p>			
<p><b>Data Localisation</b> (Section 16)</p>	<p>(1) The Central Government may restrict the processing of data in certain notified countries or territories outside India.</p> <p>(2) This provision does not restrict the applicability of any laws that provide for a higher degree of protection</p>	<p>The restrictions on digital personal data processing (which includes storage) in other jurisdictions may be published as a 'negative list' of restricted countries by the Central Government. Restricted country names may only be finalized post the implementation of the DPDP Act.</p> <p>Compared to other kind of games, compliance challenges to the RMG gaming Data Fiduciaries may be somewhat reduced owing to the largely domestic nature of the sub-sector. Compliance concerns would be enhanced for Gaming Data Fiduciaries based in jurisdictions which may be potentially restricted from processing personal data.</p>			

<p><b>Power to Notify Rules (Section 40)</b></p>	<p>(1) The DPDP Act is a principle-based law and the gives the Central Government considerable power to make rules that give effect to the principles.</p> <p>(2) At least 25 specific subject-matters are listed under the DPDP Act for prescription of rules in the future.</p>	<p>Due to the large scope for rule-making to give effect to the provisions of the DPDP Act, a full understanding of the standards of compliance necessary for Gaming Data Fiduciaries will evolve only once the relevant rules are notified on a range of subject matters, including some of the issues discussed in this report. This may also significantly alter the estimated compliance risk assessments for various kinds of Gaming Data Fiduciaries.</p>			
--	---	---	---	---	---



## (ii) Recommendations to the Central Government on Rules under the DPDP Act

The DPDP Act is intended to function as a ‘base document’ which will be supplemented by a large volume of delegated legislation<sup>51</sup> to guide the conduct of Data Fiduciaries across various categories of Digital India. A range of issues underscored the above analysis may be either resolved by the notification of balanced rules and regulations under the DPDP Act which are able to offer clarity and guide compliance. At the same time, the notification of prescribed rules carries the risk of enhancing compliance requirements or creating additional operational challenges for different subcategories of Gaming Data Fiduciaries.

Provided below are the key recommendations to the Central Government on utilizing its subordinate legislative powers under the DPDP Act to address the concerns flagged for India’s nascent online gaming industry.

### *Clarifications and Exemptions Regarding Parental Consent for Online Gaming*

- To alleviate concerns for F2P offerings, Central Government should ensure that there is adequate flexibility for a seamless and integration of Parental Consent mechanisms without over-prescriptions (obtaining, storing, and revoking consent), where players may not be as invested in the specific platform of the Gaming Data Fiduciary.
- Subject to such conditions that adequately ensure the wellbeing of minors in relation to the processing of their data, the Central Government may consider granting relevant exemptions to F2P Data Fiduciaries, as a class, from the applicability of behavioral tracking or targeted advertising obligations for minors under the DPDP Act. This may be implemented using powers available to the Central Government under Section 9(5) of the DPDP Act, and may include factors relating to age-appropriateness of gaming content. Where necessary.
- Clarifications should also be notified on what constitutes ‘processing of personal data that is likely to cause any detrimental effect on the well-being of a child’.

---

51 Section 40 of the Digital Personal Data Protection Act, 2023 enables the notification of Central Government rules on a number of subject items, including the manner of obtaining verifiable consent, manner of notice given to Data Principals, and the classes of data fiduciaries for processing children’s personal data.

### *Clarifications on Personal Data Processing*

- The Central Government may consider issuing FAQs or clarifications which may help gaming companies identify the scope, and granularity of digital personal data obligations, such as notice and consent, which is especially relevant for Web3 Gaming Data Fiduciaries, where large volumes of pseudonymous data or psychophysical data can be generated.
- Clarifications may also address the scope of exercise of rights of modification or erasure of digital personal data by the Data Principal in relation to information stored using immutable digital technologies like blockchain, for the benefit of Web3 gaming.
- Alternatively, industry-driven codes (which may be exemplary but not prescriptive) for various sectors, including gaming may be developed to help guide compliance for companies on these aspects.

### *Timelines for Personal Data Processing Restrictions*

- Rules should specify reasonable transition timelines for complying with restrictions on processing of digital personal data in specific countries that are notified under Section 16 of the DPDP Act.

---

## WHAT IS AIGDF ?

The All India Game Developers' Forum (AIGDF) is a not-for-profit collective representing the interests of Indian game developers.

AIGDF is committed to greater representation of Indian game developers as a key stakeholder of the AVGC sector. AIGDF endeavors to be an active contributor in shaping centers of excellence, technology labs and hubs, and dedicated coursework for game development. It also aims to be active in creating a healthy ecosystem of game developers and enablers.

## WHAT IS IGAP ?

The Indian Governance And Policy Project (IGAP) is an emerging think tank focused on driving growth, innovation, and development in India's digital landscape. Specializing in areas like AI, Data Protection, FinTech, and Sustainability, IGAP promotes evidence-based policymaking through interdisciplinary research. By working closely with industry bodies in the digital sector, IGAP provides valuable insights and supports informed decision-making. Core work streams include policy monitoring, knowledge dissemination, capacity development, dialogue and collaboration,