IMPLICATIONS OF THE NEW DATA PROTECTION LAW ON M&E INDUSTRY

18.09.2023

By Gowree Gokhale, Aparna Gaur and Karishma Karthik

Creative First

On August 11, 2023, the Digital Personal Data Protection Act, 2023 ("**DPDPA**") became law. The provisions of the DPDPA are yet to come into effect. The government is in the process of rolling out rules and regulations to operationalize DPDPA. The DPDPA ushers in obligations, restrictions and compliance requirements for all entities processing personal data in digital form. In this article, we discuss the impact of some of the provisions of the DPDPA on the media and entertainment industry in relation to data of consumers.

What constitutes "personal data"?

"Personal data" has been defined as "any data about an individual who is identifiable by or in relation to such data". Such data is not limited to objective identifiers such as name, age, location, identification numbers etc. but may also include subjective factors such as opinions and interests. Personal data of a user of any B2C media service could include likes/dislikes, comments, reviews, ratings, search and watch history, including genres and other categories of content, interactions with recommendations and other

engagement metrics etc. In the context of gaming, profile pictures or personalized avatars, game progress and achievements, game settings such as preferred modes/genres or achievements, customizations (skins, outfits, accessories etc.) and even internet speeds help paint a picture of an individual's identity. Therefore, the provisions of the DPDPA will apply to all such types of data.

Processing data to improve user experiences: do you have adequate consent?

The DPDPA requires data fiduciaries (any person who determines the purpose of processing of personal data) to obtain consent from the data principal and provide notice listing out, among other things, the specific purposes for which consent is sought. The business can only collect personal data which is *necessary* for the specified purpose mentioned in the notice. With this requirement, in addition to listing current services as part of the "specified purpose", businesses will need to ensure adequate language is inserted to enable processing of data for analytics to provide services that enhance user experiences such as new product features, marketing campaigns and so on. The examples provided in the DPDPA will also have to be carefully examined, to determine if allied services offered by a data fiduciary, which are not part of the primary services forming part of the specified purpose for which consent is sought, shall also be covered. For instance, if an OTT platform which begins offering delivery services may process data for such delivery services, under the umbrella of a broader purpose set out in the consent notice, not directly connected to the primary streaming services.

Sharing of data with group entities

Given that the definition of "processing" under the DPDPA includes *sharing* of such personal data, consent and the associated notice requirement remain applicable to sharing of data by the data fiduciaries to its parent or group entities, service providers, consultant etc. For example, if a gaming company collecting gameplay data in the nature of step count, heart rate, health metrics and other physical health tracking through integration with wearable devices, shares such data sets with its associate company engaged in the insurance industry, such information could potentially be used to drive up or customize health insurance premiums. Under the new law, a data principal needs to explicitly consent to the gaming company sharing such information with its associate companies and such sharing needs to be in line with the specified purpose.

Platform level changes: Data fiduciary compliances and rights of data principals

The DPDPA requires a data fiduciary to comply with several new obligations that may necessitate changes to their platform. For instance, entities will be

required to provide users the option to access the consent request in English or any language specified in the Eighth Schedule. Clarity is required if such a requirement shall only be applicable for platforms that support such a language. The DPDPA also provides for several rights of data principals including the right to withdraw her consent for processing personal data. The DPDPA requires that the process of withdrawing consent should be of comparable ease to the ease with which consent was obtained. The data fiduciary will accordingly be required to incorporate a withdrawal mechanism into their platform. The DPDPA also mandates a grievance redressal mechanism, which most entities would likely already have established either under the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 ("**Intermediary Guidelines**"), Consumer Protection (E-Commerce) Rules, 2020 or other relevant sectoral laws. However, entities that do not have existing mechanisms will need to implement such mechanisms.

Content takedown

The Central Government has the power to block access to content (or even the whole platform, in its entirety) of a data fiduciary, including an intermediary. In case of two or more violations by the data fiduciary of the DPDPA and upon recommendation by the Data Protection Board – a body also constituted by the Central Government – the government may block such access in the "interests of the general public". A similar power exists under Section 69A of the Information Technology Act, 2000 and Rule 3(1)(d) of the Intermediary Guidelines, however under separate grounds such as sovereignty, integrity of India, security of the State etc. The Information Technology (Procedure and Safeguards for Blocking for Access of Information by Public) Rules, 2009 sets out the procedure to be followed by the government for takedown orders under Section 69A. However, the DPDPA does not similarly provide for rules to be framed to regulate the procedure for takedown of content. In the absence of the same, this provision offers the Central Government a broader power to issue takedown orders, which presents the possibility of abuse.

Data processors and required contractual safeguards

The DPDPA defines a data processor as one who processes data on behalf of a data fiduciary. The responsibility for ensuring compliance with the obligations under the DPDPA remains with the data fiduciary even in relation to processing by the data processor. Therefore, entities should put in place comprehensive and robust contractual safeguards backed by suitable indemnities to ensure risk mitigation against non-compliances by the data processor. Such agreements should inter alia prescribe security safeguards to prevent personal data breaches, restrictions on sub-processing, audits, inspections and other technical and organizational measures to ensure compliance with the requirements of the DPDPA etc.

Age-gating and parental consent

Another contentious issue is the age of consent being 18 years. As the manner of procuring such *verifiable* parental consent is yet to be prescribed, it remains unclear whether this provision will be enforced through mandatory KYC norms. However, the Central Government may exempt certain categories of data fiduciaries from the consent requirement if they process data in a "verifiably safe" manner.

Content for children

The DPDPA prohibits data fiduciaries from undertaking targeted advertisements directed at children. Safeguards in relation to targeted ads for children have already been built into the Guidelines for Prevention of Misleading Advertisements and Endorsements for Misleading Advertisements, 2022 issued by the Central Consumer Protection Authority under the Consumer Protection Act, 2019. Additionally, the Government of India (Allocation of Business) Rules, 1961 have recently undergone amendment to bring online advertising under the purview of the Ministry of Information and Broadcasting. Online gaming ads are also already regulated

under the Intermediary Guidelines by the Ministry of Electronics and Information Technology. The intent of the provision under the DPDPA appears to be to prevent use of personal data of children to serve targeted ads to them. However, the wording of the provision appears to completely prohibit targeted ads. Despite this prohibition, the Central Government may notify the age above which certain data fiduciaries, that process data in a verifiably safe manner, may be exempt from such requirement. In an interview < https://indianexpress.com/article/business/economy/concerns-around-contentious-provisions-of-data-protection-law-mos-it-8889933/> , the Minister of State for Electronics and IT clarified that this exemption is likely to be applicable only against platforms whose users are entirely youngsters, as opposed to general social media platforms like Meta. Industry members should seek further clarity on this exemption in the stakeholder consultations for the rules to be notified under the DPDPA.

The DPDPA represents a new take on data protection law and is a product of an extensive consultation process, however, many of its key provisions remain to be addressed through delegated legislation and judicial interpretation.

ABOUT THE AUTHOR

Gowree Gokhale

A practicing lawyer over 27 years, Gowree Gokhale leads the IP, Technology, Media and Entertainment, Cybersecurity and Data Protection, Pharma and Medical devices practices of research and strategy driven international law firm, Nishith Desai Associates. She is an expert in various tech industries such as fintech, medtech, and edtech. She has assisted several international businesses in India strategy, regulatory advice, corporate and strategic deals, litigation and arbitration in TMT and Pharma sector. She has spearheaded several policy initiatives for the TMT and Pharma industry including for intermediaries, social media companies, online content companies, gaming industry, IT industry as also for privacy and data protection and cyber security laws. She has also been consistently working on high tech industry aspects. She has been named in several legal directories, including in the Hall of Fame (TMT) in Legal 500 for consecutive 2 years (2022 & 2023), top 100 Indian lawyers by Indian Business Law Journal.

Aparna Gaur

Aparna is a senior member of the Technology and Media Practice at Nishith Desai Associates. Her expertise lies in providing legal and strategic advice to modern digital businesses on a range of legal issues. She specializes in e-commerce, data protection, cybersecurity, intermediary liability, digital advertising, consumer protection, digital competition and issues pertaining to adoption of AI, among others. She also advises clients on defending

against IP infringement actions, ensuring comprehensive protection of their intellectual property rights.

Karishma Karthik

Karishma Karthik is a member of the IP, Data Protection, Media and Technology Practices at Nishith Desai Associates at Nishith Desai Associates. She regularly advises organizations across sectors on transactions involving data protection, media and entertainment laws and gaming and emerging technology laws.