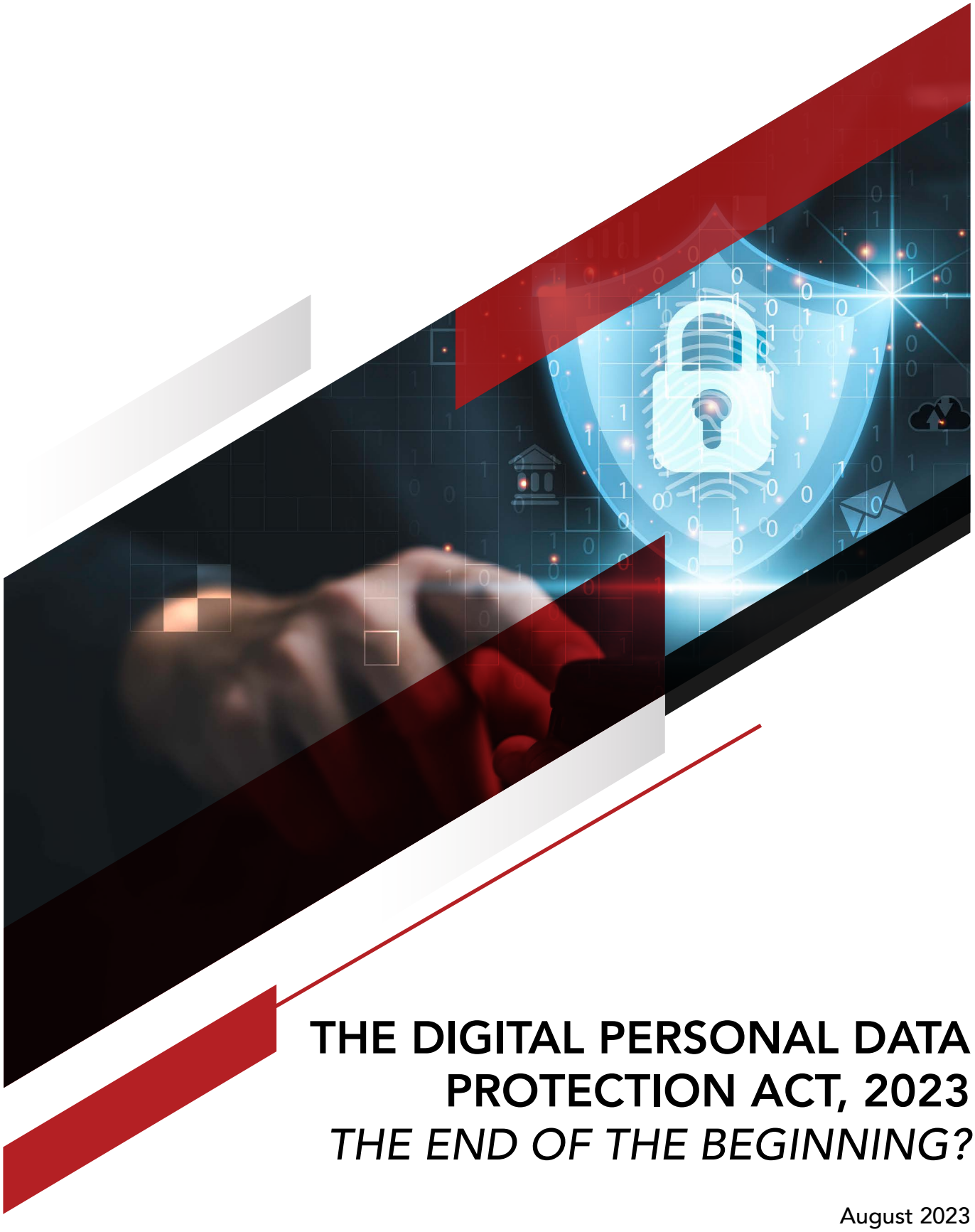
INDUSLAW
THOUGHT LEADERSHIP ... APPLIED



THE DIGITAL PERSONAL DATA PROTECTION ACT, 2023

THE END OF THE BEGINNING?

August 2023

Authors: Namita Viswanath | Shreya Suri | Naqeeb Ahmed Kazia
Nikhil Vijayanambi | Ruhi Kanakia

1. INTRODUCTION

On 11 August 2023, the Digital Personal Data Protection Act, 2023 ("**DPDP Act**") received the President of India's assent after being passed by both houses of the Indian Parliament, and was subsequently notified by the Central Government in the Official Gazette. The DPDP Act builds on its antecedent released in November 2022 ("**2022 Bill**"), implementing some tactical modifications while retaining all core concepts. With smaller key modifications made across the board, the more significant changes include the formation and constitution of the Data Protection Board ("**Board**") (which was earlier to be constituted *'as may be prescribed'* by the Central Government), the power of the Central Government to make rules, and the circumstances under which entities can be exempted from the applicability of its provisions. Through this recent rendition, the law has set out robust notice and consent obligations, 'legitimate uses' for processing personal data without consent, the establishment of an 'Appellate Tribunal', and augmented obligations on data fiduciaries while handling children's data, among others.

The DPDP Act narrows its focus to the protection of 'digital' personal data. A key concern lies in the numerous provisions of the DPDP Act which remain subject to determination by the Central Government, raising apprehensions about the potential for unguided and arbitrary rule-making.

2. KEY TAKEAWAYS

2.1. Key definitions.

2.1.1. Data principal: The DPDP Act has expanded the scope of 'data principal', which not only includes the individual as well as the parent/lawful guardian of a child to whom the personal data relates, but now also includes a lawful guardian of a 'person with disability'. It, however, does not define who a 'person with disability' is. In India, the Rights of Persons with Disabilities Act, 2016, is the primary legislation that recognizes the rights of persons with disabilities. It defines a 'person with disability', as a *'person with long term physical, mental, intellectual or sensory impairment which, in interaction with barriers, hinders his full and effective participation in society equally with others'*.[1] If inference were to be drawn from this definition, it would appear that certain classes of 'persons with disabilities' (for instance, people with physical disabilities) may not always require the assistance of their lawful guardian when it comes to matters involving their personal data. However, it is yet to be seen how the Central Government construes the term 'persons with disabilities' under the rules adopted under the DPDP Act.

2.1.2. Processing of personal data: The DPDP Act defines 'processing' to mean a *'wholly or partly automated operation or set of operations performed on digital personal data, and includes operations such as collection, recording, organisation, structuring, storage, adaptation, retrieval, use, alignment or combination, indexing, sharing, disclosure by transmission, dissemination or otherwise making available, restriction, erasure or destruction'*. This definition is largely in-line with the definition of 'processing' under the European Union's General Data Protection Regulation ("**GDPR**"). However, while the definition under the GDPR envisions automated and certain non-automated operations, the DPDP Act limits the scope of processing to only 'automated' operations.

2.1.3. Digital personal data: The definition of 'digital personal data'[2] has been introduced, to mean 'personal data' in a 'digital form'.

2.2. Applicability. The DPDP Act applies to the processing of digital personal data within India when collected from data principals (i) in digital form; or (ii) in non-digital form and then digitized. It has also extended its applicability to the processing of digital personal data outside India if it relates to offering of goods or services to data principals located in India. However, the DPDP Act remains silent on whether its provisions will apply to the processing of personal data of data principals situated outside India. Unlike the GDPR, which limits its applicability to processing of personal information of all persons resident in the European Union ("**EU**"), or EU citizens, the DPDP Act does not limit the definition of 'data principal' *(captured below)* to persons situated in India, or to Indian citizens, alone. This may create a lacuna in understanding the full extent of the DPDP Act. It is to be seen how the Central Government will interpret this ambiguity in the DPDP Act's extra-territorial application.

The 2022 Bill had introduced certain types of personal data processing that would be exempt from its provisions. The DPDP Act does away with the exemptions introduced by the 2022 Bill, except the exemption in relation to personal data processed by an individual for any personal or domestic purpose. In addition, it now also exempts from its ambit, personal data made publicly available by the data principal or any other person who is under an obligation under any Indian law to make such personal data publicly available.

2.3. Personal data. The DPDP Act covers processing of 'personal data' only, i.e., *'any data about an individual who is identifiable by or in relation to such data'*. The erstwhile classification of personal data into 'sensitive personal data' and 'critical personal data' (which found its way in all iterations till the 2022 Bill) has been done away with in the DPDP Act.

1. Section 2(s) of the Rights of Persons with Disabilities Act, 2016.
2. Section 2(n) of the DPDP Act.

2.4. Notice requirement. A data fiduciary is required to give an itemized notice to the data principal, either at the time of making or preceding a request for consent, (i) describing the personal data sought to be collected and the purpose for its processing; (ii) the manner in which the data principal may exercise his/her/their rights (including the right to correction, withdrawal of consent, etc.); and (iii) the manner in which the data principal may make a complaint to the Board. If the data principals have already provided his/her/their consent for processing their personal data prior to the commencement of the DPDP Act, the data fiduciary must provide him/her/them with such notice *'as soon as it is reasonably practicable'*. The notice must be presented in clear and plain language, by way of a separate document or in an electronic form, or in a form *'as may be prescribed'*. Further, the data fiduciary must give the data principal the option to access the contents of the notice in English or any of the 22 (twenty-two) languages specified in the Eighth Schedule to the Constitution of India.[3]

2.5. Consent.

2.5.1. Concept of consent: Data Fiduciaries will be required to process personal data for lawful purposes for which the data principal has given consent. Consent entails any *'free, specific, informed, unconditional and unambiguous indication of the data principal's wishes by which she, by way of a clear affirmative action, signifies agreement to the processing of her personal data for the specified purpose as is necessary.'*[4] Therefore, a data fiduciary can only process such personal data of a data principal when it is required for the specific purpose for which consent has been sought, and nothing further.

2.5.2. Request for consent: Every request for consent should be provided to the data principal in the following manner:

(i) It must be presented in clear and plain language with an option to access the request in English or any of the 22 languages specified in the Eighth Schedule to the Constitution of India;[5] and

(ii) It must contain the contact details of the data protection officer (for a significant data fiduciary), or a person authorised by the data fiduciary to respond to any communication from the data principal.

2.5.3. Consent manager: The data principal can give, manage, review, or withdraw the consent given to the data fiduciary through a 'consent manager',[6] i.e., a person registered with the Board who enables a data principal to give, manage, review and withdraw his/her/their consent through an accessible, transparent and interoperable platform.[7] However, there is lack of clarity on the role such consent managers will play. Currently, it is not clear if all data fiduciaries are expected to connect with the consent managers to seek consent of the data principals. Additionally, clarity is required on the manner or system that needs to be put in place to enable consent managers to perform their functions.

2.5.4. Consent of parents: The term 'consent of the parent' has also been introduced. It includes the consent of a lawful guardian, wherever applicable.

2.5.5. Legitimate use: The DPDP Act provides for certain 'legitimate uses' for which a data fiduciary may process the personal data of data principals, without obtaining the specific consent of the data principal. One

3. The Eighth Schedule to the Constitution of India consists of the following 22 (twenty-two) languages: (1) Assamese, (2) Bengali, (3) Gujarati, (4) Hindi, (5) Kannada, (6) Kashmiri, (7) Konkani, (8) Malayalam, (9) Manipuri, (10) Marathi, (11) Nepali, (12) Oriya, (13) Punjabi, (14) Sanskrit, (15) Sindhi, (16) Tamil, (17) Telugu, (18) Urdu (19) Bodo, (20) Santhali, (21) Maithili and (22) Dogri.
4. Section 6(1) of the DPDP Act.
5. Section 6(3) of the DPDP Act.
6. Section 6(7) of the DPDP Act.
7. A 'consent manager' means a "data fiduciary which enables a data principal to give, manage, review and withdraw her consent through an accessible, transparent and interoperable platform".

such legitimate use is if the data principal has voluntarily provided his/her/their personal data to the data fiduciary, while availing/ seeking out a specific service and for a specific purpose, has not indicated that he/ she/they do not consent to the use of his/ her/their personal data. Legitimate use also extends to the processing of personal data to comply with any judgment, decree, or order issued under any Indian law, and any judgment, decree or order relating to claims of a contractual or civil nature under any law in force outside India as well.

2.5.6. Withdrawal of consent: The data principal has a right to withdraw consent at any time, and the consequences of such withdrawal will be borne by the data principal without affecting the lawfulness of the processing of personal data based on consent before its withdrawal. In the event a data principal withdraws his/her/their consent to the processing of personal data, the data fiduciary must erase,[8] and cease the processing, and cause its data processors to erase and cease the processing of the personal data of such data principal, unless the retention is prescribed under any applicable laws.

2.6. Personal data breach. The DPDP Act obligates data fiduciaries to protect personal data in its possession by implementing reasonable security safeguards to prevent personal data breaches. In case of a data breach, the data fiduciary is required to notify the same to the Board, as well as to the concerned data principals, in such manner *'as may be prescribed'*.[9] The DPDP Act, however, does not prescribe the standard of reasonable security measures to be implemented by a data fiduciary, as is currently prescribed under the *Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules, 2011*, although a hefty penalty (discussed in paragraph 2.17 below) has been prescribed for non-compliance resulting in a personal data breach.

2.7. Data retention. The data fiduciaries must cease to retain personal data as soon as it is reasonable to assume that: (i) the purpose for which personal data was collected is no longer being served; and (ii) its retention is no longer necessary for legal or business purposes.

2.8. Processing of children's data. The data fiduciary is required to obtain verifiable parental consent before processing any personal data of a child,[10] in such a manner *'as may be prescribed'*[11]. The DPDP Act, however, does not define what 'verifiable' consent means. Additionally, the Central Government can exempt certain data fiduciaries from complying with this obligation by reducing the age limit for seeking parental consent, subject to a determination by the Central Government that the processing is being carried out in a verifiably safe manner. Further, a data fiduciary must not undertake any processing of personal data that is likely to have a detrimental effect on the well-being of a child.

2.9. Targeted advertising. The DPDP Act requires data fiduciaries to not undertake tracking or behavioral monitoring of children or targeted advertising directed at children. The obligation stems from the first iteration of the DPDP Act in 2018, which had restricted only 'guardian' data fiduciaries from undertaking tracking and behavioral monitoring of children -- this has now been extended to all classes of data fiduciaries. By doing this, the DPDP Act aims to ensure that no entity handling personal data of children can engage in practices that compromise their privacy or exploit them for commercial gain. The incorporation of this measure underscores the DPDP Act's commitment to safeguarding the privacy

8. Section 8(7) of the DPDP Act.
9. The Schedule (2), the penalty for failure to notify the Board and affected data principals in the event of a personal data breach, is up to INR 200 (two hundred) Crore under Schedule of the DPDP Act.
10. 'Child' means an individual who has not completed eighteen years of age.
11. Section 9(1) of the DPDP Act.

and digital well-being of children, recognizing their vulnerability in the online environment. By implementing these safeguards, the DPDP Act aims to create a safer and more secure digital space for the younger generation, promoting their right to privacy and protecting them from potential risks associated with targeted advertising and intrusive data tracking practices. However, on the contrary, this obligation may seem detrimental for digital platforms that cater specifically to child audiences, such as ed-tech platforms, video gaming platforms or e-commerce platforms selling products targeted towards children. Restricting such platforms from targeting advertisements to children may deeply impact their outreach, ultimately affecting their revenue streams. That said, the DPDP Act also gives the Central Government the power to notify the age above which a specific data fiduciary can be exempted from complying with the above-mentioned obligation for a data principal, if it is satisfied that the data fiduciary has ensured that its processing of personal data of children is done in a verifiably safe manner.

2.10. Significant data fiduciaries. The Central Government will notify any data fiduciary or class of data fiduciaries as significant data fiduciaries.[12] The said classification would be based on the assessment of factors such as the volume and sensitivity of personal data processed, risk of harm to data principals, the risk to electoral democracy, security of the state, etc. The DPDP Act imposes certain additional obligations on such significant data fiduciaries *viz.*, the need to (i) appoint a data protection officer[13] based in India; (ii) appoint an independent data auditor to evaluate the compliance by the significant data fiduciary with the provisions of the DPDP Act; (iii) undertake a data protection impact assessment;[14] and (iv) undertake periodic compliance audits. The monetary penalty for the non-fulfilment of aforesaid additional obligations by such significant data fiduciaries may extend up to INR 150 (one hundred and fifty) crore.

12. Section 10(1) of the DPDP Act. The Central Government may notify any data fiduciary or class of data fiduciaries as significant data fiduciary, on the basis of an assessment of relevant factors, including: (a) the volume and sensitivity of personal data processed; (b) risk of harm to the data principal; (c) potential impact on the sovereignty and integrity of India; (d) risk to electoral democracy; (e) security of the state; (f) public order; and (g) such other factors as it may consider necessary.
13. A 'data protection officer' means an individual appointed as such by a significant data fiduciary under the provisions of this Act under Section 2(l) of the DPDP Act.
14. 'Data Protection Impact Assessment' means a process comprising description, purpose, assessment of harm, measures for managing risk of harm and such other matters with respect to processing of personal data, as may be prescribed.

2.11. Rights of data principals. *(i) Right to information about personal data:* A data principal has the right to know the summary of the personal data that is/was processed, as well as the identities of all those with whom the data principal's personal data has been shared, along with the categories of personal data shared; *(ii) Right to correction and erasure of personal data:* A data principal has the right to request for the correction, completion, updation or erasure of their personal data processed by a data fiduciary, in such a manner *'as may be prescribed'*. Upon receiving such a request, the data fiduciary must accordingly correct the inaccurate or misleading personal data, complete the incomplete personal data, and update such personal data. Erasure requests can be denied by the data fiduciary if such data is required to be retained to comply with applicable laws; *(iii) Right of grievance redressal:* Data principals also have the right to grievance redressal against any non-compliance of the DPDP Act provisions by the data fiduciary; *(iv) Right to nominate:* Data principals have been given the right to nominate any other individual, who shall exercise the rights of the data principal in the event of their death or incapacity.

2.12. Duties of a data principal. Straying from GDPR and the California Consumer Privacy Act, 2018 ("**CCPA**"), the DPDP Act imposes certain duties on data principals, including the duty not to (i) impersonate another person; (ii) suppress any material information while applying for any document, unique identifier, proof of identity or address issued by the State or any of its instrumentalities; and (iii) register a false or frivolous grievance or complaint with a data fiduciary or the Board. Failure to comply with such duties may attract a penalty of up to INR 10,000 (ten thousand) on the data principal.[15]

2.13. Processing of personal data outside India. The DPDP Act permits transfer of personal data to any country outside India unless specifically restricted by the Central Government (unlike the first iteration of the DPDP Act in 2018 and the 2022 Bill, which permitted transfers only to countries specifically permitted by the Central Government).[16]

2.14. Exemptions. Like the 2022 Bill, the DPDP Act grants discretionary powers to the Central Government to exempt certain data fiduciaries or classes of data fiduciaries[17], including startups and any *'instrumentality of the state'* from certain provisions.[18] Additionally, the DPDP Act allows the Central Government, within 5 (five) years from the commencement of the DPDP Act, to exempt any data fiduciaries or classes of data fiduciaries from any provision of the DPDP Act for such a period as the Central Government may specify[19]. The DPDP Act also exempts data fiduciaries from their obligations while processing personal data in certain instances, with the exception of implementing reasonable security safeguards to protect personal data – . One such instance is the processing of personal data of data principals not within the territory of India, in furtherance of a contract entered with persons outside India[20]. Thus, the DPDP Act seems to reduce the compliance burden of entities engaged in business process outsourcing.

2.15 Government access. TThe DPDP Act continues to allow the instrumentalities of the state to retain personal data for an unlimited period of time regardless of whether the purpose for which such data was collected has been served[21]. Additionally, the Central Government has also been conferred the power to call for any information from data fiduciaries and the Board, as it may specify[22].

15. Section 15 of the DPDP Act.
16. Section 16(1) of the DPDP Act.
17. Section 17(3) of the DPDP Act.
18. Instrumentality of the State can be exempted in the interests of sovereignty and integrity of India, security of the State, friendly relations with foreign States, maintenance of public order or preventing incitement to any cognizable offence relating to any of these; and if necessary for research, archiving or statistical purposes if the personal data is not to be used to take any decision specific to a data principal and such processing is carried on in accordance with standards specified by the Board under Section 18 (2)(a) of the DPDP Act.
19. Section 17(5) of the DPDP Act.
20. Section 17(1)(d) of the DPDP Act.
21. Section 17(4) of the DPDP Act.
22. Section 36 of the DPDP Act.

2.16. Data Protection Board. The DPDP Act seeks to establish the Board, whose functions shall be 'digital by design'. While the DPDP Act envisions the Board to be an independent body, it comprises of a 'chairman' and other members that are to be appointed by the Central Government for a term of 2 (two) years[23]. This is in contrast to the California Data Privacy Agency ("**CDPA**") established under the CCPA which adopts a more autonomous structure as the members of the CDPA are appointed by the Governor, the Attorney General, Senate President Pro Tem, and the Speaker of the Assembly[24]. The members of the Board must possess special knowledge or practical experience in a field useful to the Board and are eligible for reappointment. The Board has been given the power to issue directions, determine non-compliance with the DPDP Act, and in the event of a personal data breach, it can direct the data fiduciary to adopt any urgent measures to remedy such personal data breach. The Board can also accept voluntary undertakings from entities in respect of any matter related to compliance with its provisions. If accepted, any ongoing relevant proceedings against the concerned entity (as regards content of such voluntary undertaking) would be barred, unless the terms of the undertaking are not complied with. While the 2022 Bill conferred the Board with the power to refer complaints to any alternative means of dispute resolution, the DPDP Act has limited this to mediation. It is pertinent to note that an appeal against any order of the Board shall lie to the Telecom Disputes Settlement and Appellate Tribunal ("**TDSAT**"), and the DPDP Act restricts civil courts from entertaining any suit in respect of any matter under the Board. This is unprecedented, given that the TDSAT derives its authority from the Department of Telecommunications, and that the DPDP Act is under the purview of the Ministry of Electronics and Information Technology ("**MeitY**"). Moreover, the TDSAT was originally empowered to handle disputes pertaining to telecommunications and information technology, in contrast to the Board which was constituted purely to regulate the processing of personal data. Hence, it remains to be seen if the TDSAT will be equipped to adjudicate matters pertaining to personal data.

2.17. Penalties. Penalties of up to INR 250 (two hundred and fifty)Crores may be imposed for offences such as failure to take reasonable security safeguards to prevent a personal data breach as obligated under Section 8(5) of the DPDP Act. Moreover, the DPDP Act has removed the INR 500 (five hundred) Crores cap on the penalty for a single instance, thereby exposing data fiduciaries and data processors to a higher penalty. The data principal's right to receive compensation for a breach of the data fiduciary's personal data protection obligations has been done away with. Additionally, the DPDP Act allows the Board to levy a penalty of up to INR 10,000 (ten thousand) if a data principal fails to perform their duties as specified therein[25].

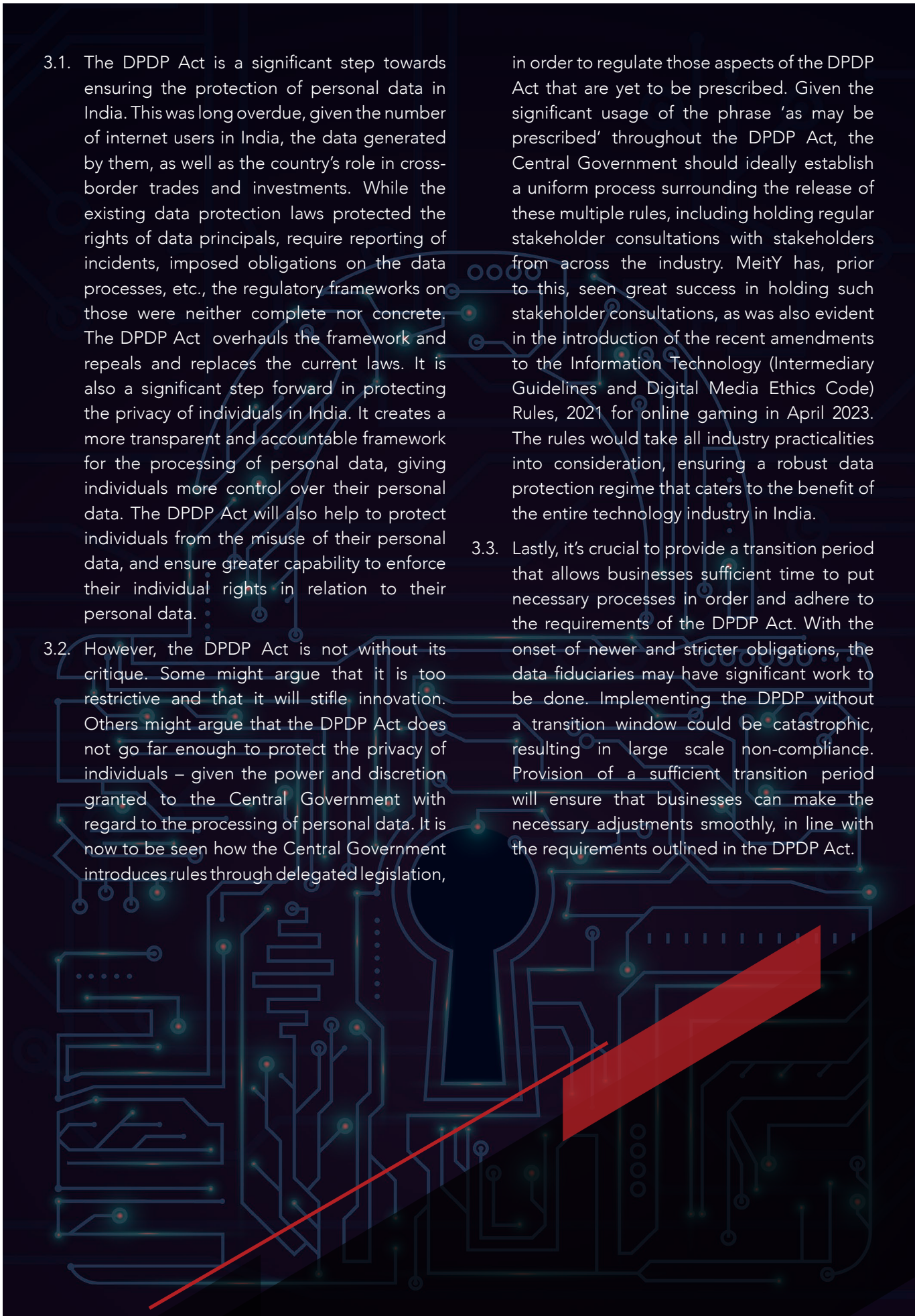
23. Section 20(2) of the DPDP Act.
24. Section 23 of the California Consumer Privacy Act, 2020, can be accessed at https://oag.ca.gov/system/files/initiatives/pdfs/19-0017%20%28Consumer%20Privacy%20%29.pdf.
25. The Schedule (5) of the DPDP Act.

3. CONCLUSION

3.1. The DPDP Act is a significant step towards ensuring the protection of personal data in India. This was long overdue, given the number of internet users in India, the data generated by them, as well as the country's role in cross-border trades and investments. While the existing data protection laws protected the rights of data principals, require reporting of incidents, imposed obligations on the data processes, etc., the regulatory frameworks on those were neither complete nor concrete. The DPDP Act overhauls the framework and repeals and replaces the current laws. It is also a significant step forward in protecting the privacy of individuals in India. It creates a more transparent and accountable framework for the processing of personal data, giving individuals more control over their personal data. The DPDP Act will also help to protect individuals from the misuse of their personal data, and ensure greater capability to enforce their individual rights in relation to their personal data.

3.2. However, the DPDP Act is not without its critique. Some might argue that it is too restrictive and that it will stifle innovation. Others might argue that the DPDP Act does not go far enough to protect the privacy of individuals – given the power and discretion granted to the Central Government with regard to the processing of personal data. It is now to be seen how the Central Government introduces rules through delegated legislation, in order to regulate those aspects of the DPDP Act that are yet to be prescribed. Given the significant usage of the phrase 'as may be prescribed' throughout the DPDP Act, the Central Government should ideally establish a uniform process surrounding the release of these multiple rules, including holding regular stakeholder consultations with stakeholders from across the industry. MeitY has, prior to this, seen great success in holding such stakeholder consultations, as was also evident in the introduction of the recent amendments to the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 for online gaming in April 2023. The rules would take all industry practicalities into consideration, ensuring a robust data protection regime that caters to the benefit of the entire technology industry in India.

3.3. Lastly, it's crucial to provide a transition period that allows businesses sufficient time to put necessary processes in order and adhere to the requirements of the DPDP Act. With the onset of newer and stricter obligations, the data fiduciaries may have significant work to be done. Implementing the DPDP without a transition window could be catastrophic, resulting in large scale non-compliance. Provision of a sufficient transition period will ensure that businesses can make the necessary adjustments smoothly, in line with the requirements outlined in the DPDP Act.



INDUSLAW
THOUGHT LEADERSHIP ... APPLIED

www.induslaw.com

OUR OFFICES

BENGALURU
101, 1st Floor, "Embassy Classic"# 11
Vittal Mallya Road
Bengaluru 560 001
T: +91 80 4072 6600
F: +91 80 4072 6666
E: bangalore@induslaw.com

HYDERABAD
204, Ashoka Capitol, Road No. 2
Banjarahills
Hyderabad 500 034
T: +91 40 4026 4624
F: +91 40 4004 0979
E: hyderabad@induslaw.com

CHENNAI
#11, Venkatraman Street, T Nagar,
Chennai - 600017 India
T: +91 44 4354 6600
F: +91 44 4354 6600
E: chennai@induslaw.com

DELHI & NCR
2nd Floor, Block D
The MIRA, Mathura Road, Ishwar Nagar
New Delhi 110 065
T: +91 11 4782 1000
F: +91 11 4782 1097
E: delhi@induslaw.com

9th Floor, Block-B
DLF Cyber Park
Udyog Vihar Phase - 3
Sector - 20
Gurugram 122 008
T: +91 12 4673 1000
E: gurugram@induslaw.com

MUMBAI
1502B, 15th Floor
Tower – 1C, One Indiabulls Centre
Senapati Bapat Marg, Lower Parel
Mumbai – 400013
T: +91 22 4920 7200
F: +91 22 4920 7299
E: mumbai@induslaw.com

#81-83, 8th Floor
A Wing, Mittal Court
Jamnalal Bajaj Marg
Nariman Point
Mumbai – 400021
T: +91 22 4007 4400
E: mumbai@induslaw.com

DISCLAIMER

This article is for information purposes only. Nothing contained herein is, purports to be, or is intended as legal advice and you should seek legal advice before you act on any information or view expressed herein.

Although we have endeavored to accurately reflect the subject matter of this article, we make no representation or warranty, express or implied, in any manner whatsoever in connection with the contents of this article.

No recipient or reader of this article should construe it as an attempt to solicit business in any manner whatsoever.