Data Privacy in India Post-DPDP Act: Compliance, loopholes, and enforcement challenges

[1]Kanika Khandelwal and [2]Abhay Singhal
[1]Arg city, Block-N, Flat number 103, Ajmer (Rajasthan)
[2]3F12 Mahaveer Nagar Extension, Kota, Rajasthan 324009
Email: [1]knika.Khandelwal@gmail.com and [2]advabhaysinghall@gmail.com

Abstract: India's Digital Personal Data Protection Bill was tabled in 2022, and was finalized as India's Digital Personal Data Protection Act (DPDP Act) when it received approval from both houses of Parliament and the assent of the President in August 2023. The law came into effect August 11, 2023 and covers personal data collected in digital format, or collected by other means and later digitized. The law is intended to protect personal information for citizens in the world's most populous country, and increase accountability for organizations that handle a lot of such data, including those with online operations and that run mobile apps. The law is in line with the standards of many global data privacy regulations, taking influence from China's Personal Information Protection Law (PIPL) and the European Union's General Data Protection Regulation (GDPR). We look at important requirements of the DPDP Act, key definitions, enforcement, and more. (Note: the state-level Delaware Personal Data Privacy Act in the United States also uses the initialism "DPDPA", so we will mostly use "the DPDP Act".)

[Khandelwal, K. and Singhal, A. **Data Privacy in India Post-DPDP Act: Compliance, loopholes, and enforcement challenges** . *The International Journal of Interpretation, Observation and Analysis*, 2025; Volume 3, Issue 1:203-209 (July-September). ISSN 2349-0713, Peer-reviewed (online/offline), Refereed, Indexed and International Journal (Since 2013), Global Impact Factor: 5.776

Key words: Data Privacy, Law, India, Compliance, Challenges

Introduction: Personal data refers to any data about an individual who is identifiable by or in relation to such data. The personal data can be collected and processed in digital format, or collected in another format and later digitized. The Act does not provide a list of examples of personal data (e.g. name, phone number, financial information, etc.) like some data privacy laws do.

In early August 2023, the Indian Parliament passed the Digital Personal Data Protection (DPDP) Act, 2023.[1] The new law is the first cross-sectoral law on personal data protection in India and has been enacted after more than half a decade of deliberations.[2] The key question this paper discusses is whether this seemingly interminable period of deliberations resulted in a "good" law—whether the law protects personal data adequately, and in addition, whether it properly balances, as the preamble to the law states, "the right of individuals to protect their personal data" on one hand and "the need to process such personal data for lawful purposes" on the other.

To answer this question, the paper first details the key features of the law and compares it to earlier versions, especially the previous official bill introduced by the government in Parliament in 2019.[3] The second part of the paper then examines the DPDP Act from two perspectives. First, it highlights certain potentially problematic features of this law to understand its consequences for consumers and businesses as well as the Indian state. Second, it places the act in context of the developments and deliberations that have taken place over the last five years or so. The third part speculates on the key factors that will influence the development of data protection regulation in India in the next few years.

The 2023 act is the second version of the bill introduced in Parliament, and fourth overall. An initial version was prepared by a committee of experts and circulated for public feedback in 2018.[4] This was followed by the government's version of the bill that was introduced in Parliament in 2019—the Personal Data Protection Bill, 2019. This version was studied by a parliamentary committee that published its report in December 2021.[5] The government, however, withdrew this bill, and in November 2022, published a fresh draft for public consultations—the draft Digital Personal Data Protection Bill, 2022.[6] This draft was quite different compared to the previous versions. The 2023 law is based, in significant part, on this draft. However, it has some new provisions that are consequential for the questions this paper seeks to answer.

These four drafts were preceded by a landmark 2017 judgment by India's Supreme Court in *Justice K.S. Puttaswamy and Anr. v. Union of India and Ors.*[7] The judgment declared that the right to privacy is part of the fundamental right to life in India and that the right to informational privacy is part of this right. The judgment, however, did not describe the specific contours of the right to informational privacy, and it also did not lay down

specific mechanisms through which this right was to be protected.

Following this, the first government version of the law, the Personal Data Protection Bill, 2019, was introduced in Parliament in December 2019. This version was expansive in scope and proposed cross-sectoral, economy-wide data protection regulation to be overseen by an all-powerful data protection regulator—the Data Protection Authority (DPA). The 2019 bill provided for a preventive framework.[8] It imposed a number of obligations on entities collecting personal data—to provide notice and take consent from individuals, to store accurate data in a secure manner, and to use it only for purposes listed in the notice. Businesses were also required to delete data once the purpose was satisfied and to provide consumers rights to access, erase, and port their data. Businesses were required to maintain security safeguards and transparency requirements, implement "privacy by design" requirements, and create grievance redress systems. Finally, this bill introduced an entity known as "consent managers," who were intermediaries for collecting and providing consent to businesses on behalf of individuals.[9]

The bill grouped personal data into different categories and required elevated levels of protection for "sensitive" and "critical" personal data. Certain businesses were also to be categorized as "significant data fiduciaries," and additional obligations were proposed for them—registration in India, data audits, and data impact assessments. In addition, the bill imposed localization restrictions on the cross-border flows of certain categories of data. The DPA was empowered to impose penalties on businesses for violating these requirements. The bill also proposed to criminalize activities related to the deanonymization of individuals from anonymized datasets.

The 2019 bill exempted certain entities and businesses from notice and consent requirements under certain circumstances—for lawful state functions, medical and health services during emergencies or epidemics, breakdown of public order, employment-related data processing, the prevention and detection of unlawful activity, whistleblowing, and credit recovery, among others.

The 2019 bill also had a provision to empower the government to regulate nonpersonal data. It allowed the government to require private entities to hand over specific nonpersonal data that the government asked for as per conditions it prescribed. In short, the 2019 bill proposed a comprehensive, cross-sectoral framework based on preventive requirements for businesses (defined as "data fiduciaries") and rights for individuals or consumers ("data principals").

This regulatory structure was based mostly on the 2018 draft bill proposed by the Srikrishna Committee—the committee, chaired by Justice B.N. Srikrishna, a retired Supreme Court judge, was set up by the Ministry of Electronics & Information Technology in July 2017 to help frame data protection norms. The recommendations of this committee, in turn, were based on major regulatory developments that were popular while the work of the committee was proceeding. Primary among these was the European Union's (EU's) General Data Protection Regulation (GDPR).[10] While the general preventive framework of the 2019 bill was welcome, its expansive scope was problematic. It created a number of significant compliance requirements that would have affected both big and small firms in the economy. It also proposed the creation of a DPA that had significant regulation-making and supervisory powers. These regulations would have further detailed the already significant compliance requirements in the bill. The novelty of the law and the lack of prior experience in implementing a data protection law of this nature would have created serious risks of overregulation or under-regulation.[11]

The DPDP Act is a federal law in India that regulates the processing of the digital personal data of its citizens. The law aims to strike a balance between the recognized need to process personal data for various purposes, and individuals' right to control and protect it.

Like many data privacy laws around the world, the DPDP Act is extraterritorial, and so applies to organizations operating both inside and outside of India, if they are offering goods or services to Indian citizens, and in doing so processing personal data. The Act does allow for legal bases for data processing in addition to consent of the data principal, but consent is required for many processing purposes.

Key definitions in the Indian Personal Data Privacy Law

The definitions of key terms outlined in the DPDP Act are consistent with many data privacy laws, though some of the terms are different, e.g. "data fiduciary" instead of "data controller". The definition of a person is also quite broad, as it can include the Indian State, a family, or a firm, for example.

What is a person under the DPDP Act?

A person covers a variety of entities, not just individual people, and refers to:

- an individual
- a Hindu undivided family
- a company

- a firm
- an association of persons or a body of individuals, whether incorporated or not
- the State
- every artificial juristic person, not falling within any of the preceding sub-clauses

What is processing under the DPDP Act?

Processing in the context of personal data means *"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".*

What is the definition of consent under the DPDP Act?

A data principal's consent must be: *"free, specific, informed, unconditional and unambiguous with a clear affirmative action, and shall signify an agreement to the processing of her personal data for the specified purpose and be limited to such personal data as is necessary for such specified purpose".*

Who is defined as a child under the DPDP Act?

A child is defined as a person who is 18 years old or younger.

Who is a data principal under the DPDP Act?

This term refers to any individual to whom personal data being processed relates, and includes an individual who is a child (also, then, including the child's parents or lawful guardians) or an individual who has a disability (also, then, including the person's lawful guardian, acting on their behalf). Also known as a data subject under some other laws.

Who is a data fiduciary under the DPDP Act?

"Data fiduciary" means any person who, alone or in conjunction with other persons, determines the purpose and means of processing of personal data. Also known as a data controller under some other laws.

A "Significant Data Fiduciary" refers to any data fiduciary or class of data fiduciaries as may be notified by the Central Government.

Who is a data processor under the DPDP Act?

A data processor is any person who processes personal data on behalf of a data fiduciary.

What is a consent manager under the DPDP Act?

For the purposes of the Act, "Consent Manager" does not refer to software such as a consent management platform, but instead refers to a person or organization registered with the Data Protection Board. This entity acts as the point of contact to enable an individual, here the "data principal", to provide, manage, review, and/or withdraw her consent via a platform that is "accessible, transparent and interoperable". A consent manager serves as a middleman for businesses to help facilitate compliance with the DPDP Act.

Key Features of the DPDP Act, 2023

Compared to the 2019 version of the bill, the DPDP Act, 2023 is more modest—it has reduced obligations for businesses and protections for consumers. On the one hand, the regulatory structure is simpler, but on the other, it vests the central government with unguided discretionary powers in some cases.

Applicability to Nonresidents

The DPDP Act applies to Indian residents and businesses collecting the data of Indian residents. Interestingly, it also applies to non-citizens living in India whose data processing "in connection with any activity related to offering of goods or services" happens outside India.[13] This has implications for, say, a U.S. citizen residing in India being provided digital goods or services within India by a provider based outside India.

Purposes of Data Collection and Processing

The 2023 act allows personal data to be processed for any lawful purpose.[14] The entity processing data can do so either by taking the concerned individual's consent or for "legitimate uses," a term that has been explained in the law.

Consent must be "free, specific, informed, unconditional and unambiguous with a clear affirmative action" and for a specific purpose. The data collected has to be limited to that necessary for the specified purpose. A clear notice containing these details has to be provided to consumers, including the rights of the concerned individual and the grievance redress mechanism. Individuals have the right to withdraw consent if consent is the ground on which data is being processed.

Legitimate uses are defined as: (a) a situation where an individual has voluntarily provided personal data for a specified purpose; (b) the provisioning of any subsidy, benefit, service, license, certificate, or permit by any agency or department of the Indian state, if the individual has previously consented to receiving any other such service from the state (this is a potential issue since it enables different government agencies providing these services to access personal data stored with other agencies of the government);[15] (c) sovereignty or security; (d) fulfilling a legal obligation to disclose information to the state; (e) compliance with judgments, decrees, or orders; (f) medical emergency or threat to life or epidemics or threat to public health; and (g) disaster or breakdown of public order.[16]

Rights of Users/Consumers of Data-Related Products and Services

The DPDP Act also creates rights and obligations for individuals.[17] These include the right to get a summary of all the collected data and to know the identities of all other data fiduciaries and data processors with whom the personal data has been shared, along with a description of the data shared. Individuals also have the right to correction, completion, updating, and erasure of their data. Besides, they have a right to obtain redress for their grievances and a right to nominate persons who will receive their data.

Obligations on Data Fiduciaries

Entities responsible for collecting, storing, and processing digital personal data are defined as data fiduciaries and have defined obligations. These include: (a) maintaining security safeguards; (b) ensuring completeness, accuracy, and consistency of personal data; (c) intimation of data breach in a prescribed manner to the Data Protection Board of India (DPB); (d) data erasure on consent withdrawal or on the expiry of the specified purpose; (e) the data fiduciary having to appoint a data protection officer and set up grievance redress mechanisms; and (f) the consent of the parent/guardian being mandatory in the case of children/minors (those under eighteen years of age). The DPDP Act also states that any processing that is likely to have a detrimental effect on a child is not permitted. The law prohibits tracking, behavioral monitoring, and targeted advertising directed at children.[18] The government can prescribe exemptions from these requirements for specified purposes. This is potentially a problem since the powers to exempt are broad and without any guidelines.

While the 2023 act retains the broad categories of obligations for the most part, the key difference from the 2019 bill is the absence of the scope for the regulator, the DPA, to make detailed regulations on these obligations. In addition, the substantive requirements under each of these categories have been reduced.

There is an additional category of data fiduciaries known as significant data fiduciaries (SDFs). The government will designate data fiduciaries as SDFs based on certain criteria—volume and sensitivity of data and risks to data protection rights, sovereignty and integrity, electoral democracy, security, and public order.[19]

SDFs will have additional obligations that include: (a) appointing a data protection officer based in India who will be answerable to the board of directors or the governing body of the SDF and will also serve as the point of contact for grievance redressal; and (b) conducting data protection impact assessments and audits and taking other measures as prescribed by the government. The 2019 bill required that SDFs register in India. This requirement has been removed from the 2023 act.

Moderation of Data Localization Requirements

The 2023 law reverses course on the issue of data localization. While the 2019 bill restricted certain data flows, the 2023 law only states that the government may restrict flows to certain countries by notification. While this is not explicit, the power to restrict data flows seems to be to provide the government necessary legal powers for national security purposes. The law also states that this will not impact measures taken by sector-specific agencies that have or may impose localization requirements. For example, the Reserve Bank of India's localization requirements will continue to be legally valid.

Exemptions From Obligations Under the Law

The law provides exemptions from consent and notice requirements as well as most obligations of data fiduciaries and related requirements in certain cases: (a) where processing is necessary for enforcing any legal right or claim; (b) personal data has to be processed by courts or tribunals, or for the prevention, detection, investigation, or prosecution of any offenses; (c) where the personal data of non-Indian residents is being processed within India; and so on.[20]

In addition, the law exempts certain purposes and entities completely from its purview.[21] These include:

1. Processing in the interests of the sovereignty and integrity of India, security of the state, friendly relations with foreign states, maintenance of public order, or preventing incitement to any cognizable offense. This will allow investigative and security agencies to remain outside the purview of this law.
2. Data processing 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.
3. The government can exempt certain classes of data fiduciaries, including startups, from some provisions—notice, completeness, accuracy, consistency, and erasure.
4. One problematic provision allows the government to, "before expiry of five years from the date of commencement of this Act," declare that any provision of this law shall not apply to such data fiduciary or classes of data fiduciaries for such period as may be specified in the notification. This is a significant and wide discretionary power and is not circumscribed by any guidance on the basis for such

exemption, the categories that may be exempted, and the time period for which such exemptions can operate.

New Regulatory Structure for Regulating Data Privacy

The 2023 law completely changes the proposed regulatory institutional design. The 2019 bill proposed an independent regulatory agency. The DPA was proposed on the lines of similar government agencies in many EU countries that function independently of government and implement the GDPR. The proposed Indian DPA was arguably more powerful since it was proposed to have much more extensive regulation-making powers than DPAs under the GDPR. In addition to framing regulations, the DPA would have been responsible for framing codes of conduct for businesses, investigating cases of noncompliance, collecting supervisory information, and imposing penalties on businesses.

In contrast, the 2023 law establishes the DPB.[22] The board is not a regulatory entity and is very different from the DPA. Compared to the latter, the board has a limited mandate to oversee the prevention of data breaches and direct remedial action and to conduct inquiries and issue penalties for noncompliance with the law.[23] The board does not have any powers to frame regulations or codes of conduct or to call for information to supervise the workings of businesses.

Data protection laws in India

Until 2023, India did not have a standalone law or framework to govern data protection. The Information Technology Act, 2000 (**IT Act**) and rules notified thereunder formed the basis around which the data protection framework revolved. This included the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011 (**Privacy Rules**).

In 2017, a constitutional bench of nine judges of the Supreme Court of India in *Justice K. S. Puttaswamy (Retd.) v. Union of India* [Writ Petition No. 494/ 2012] upheld that privacy is a fundamental right, which is entrenched in Article 21 [Right to Life & Liberty] of the Constitution of India. This led to the process of formulation of a comprehensive data protection framework for India. After releasing different draft versions of a data protection legislation and considering the recommendations from different stakeholders, the Ministry of Electronics and Information Technology (**MeitY**), Government of India, released the draft of the Digital Personal Data Protection Bill in 2022 (**DPDP Bill**).

It can only do so during the process of conducting inquiries.

The members of the board will be appointed by the government, and the terms and conditions of their service will be prescribed in rules made by the government.[24] The law states that these terms and conditions cannot be varied to a member's disadvantage during their tenure.

The law allows the board to impose monetary penalties of up to 250 crore rupees (approximately $30.5 million).[25] Appeals from the board's orders will go to an existing tribunal— the Telecom Disputes Settlement and Appellate Tribunal (TDSAT). In addition to monetary penalties, the bill allows data fiduciaries to provide voluntary undertakings to the board as a form of settlement of any complaints against them.[26] Therefore, the board is a very different institution in design compared to the DPA.

Finally, the 2023 law contains a novel provision not included or discussed in any previous version. This is Section 37, which allows the government, based on a reference from the board, to block the public's access to any information that enables a data fiduciary to provide goods or services in India. This has to be based on two criteria: (a) the board has imposed penalties against such data fiduciaries on two or more prior occasions, and (b) the board has recommended a blockage. The government has to provide the data fiduciary an opportunity to be heard before taking such action.

The version of the DPDP Bill which was eventually passed by both houses of the Indian Parliament marked a few significant changes to the original draft of the DPDP Bill. On August 11, 2023, the Government of India published that version as the Digital Personal Data Protection Act, 2023 (**DPDP Act**), which will form the personal data protection and regulatory regime in India. The DPDP Act introduces several compliances with respect to the collection, processing, storage and transfer of digital personal data. However, further actions on behalf of the Government are required to make the DPDP Act effective, including notifying the sections of the DPDP Act itself, repealing the Privacy Rules and notifying the rules and regulations required for effective implementation and enforcement of the DPDP Act. The DPDP Act is applicable only to personal data in digital form and does not regulate non-personal and non-digital data. Considering this, collection and handling of non-personal data is currently unregulated in India.

To clarify, the current privacy regime is contained within the IT Act and the Privacy Rules. While the Government of India (see below) has released a draft of the rules under the DPDP Act, the

provisions of the Act itself have not yet come into force.

Rules

On January 3, 2025, MeitY released a draft of the Digital Personal Data Protection Rules, 2025 (**Draft Rules**), inviting comments from the public and stakeholders till February 18, 2025. The feedback received by the government will be taken into consideration after this date.

Rules related to the establishment and functioning of the Data Protection Board of India are likely to come into effect immediately upon the publication of the rules in the Official Gazette (after the DPDP Act is implemented). For the remaining rules, an extended period may be provided for entities to comply with after which these rules will come into effect. The timeline has not been specified in the Draft Rules.

Note

The DPDP Act has been drafted on the following principles:

- usage of personal data by an organization is to be done in a manner that is lawful, fair and transparent to the individuals concerned;
- usage of personal data is to be limited to the purpose for which it was collected;
- only those items of personal data that are required for attaining a specific purpose are to be collected;
- reasonable efforts should be made to ensure that the personal data of the individual is accurate and kept up to date;
- storage of data is required to be limited to such duration as is necessary for the stated purpose for which personal data was collected;
- reasonable safeguards are to be undertaken to ensure that there is no unauthorised collection or processing of personal data. This is intended to prevent personal data breach; and
- the person who decides the purpose and means of processing of personal data i.e. Data Fiduciary is accountable for such processing.

Scope and Applicability

The DPDP Act pertains to the processing of digital personal data within India, encompassing situations where the personal data is either (i) collected in a digital form or (ii) collected in a non-digitized form and subsequently converted into digital form. Consequently, the DPDP Act does not apply to the processing of personal data in its non-digitized state. The DPDP Act defines 'personal data' broadly to include any data about an individual who is identifiable by or in relation to such data. It also defines 'digital personal data' as personal data in digital form.

While the DPDP Act is applicable to Indian entities which engage in the processing of personal data, it also has extra-territorial applicability, applying to foreign entities who offer goods and services to Data Principals (as defined below) located within the territory of India and process personal data in connection to such activities. The DPDP Act does not apply to (i) personal data utilized by an individual for personal or domestic purposes or (ii) personal data deliberately made publicly accessible by either the Data Principal to whom the personal data relates or any other individual or entity mandated by law to disclose personal data to the public.

Key Challenges:

- **Compliance Complexity and Increased Regulatory Burden:**

The DPDP Act necessitates obtaining consent for data processing, appointing Data Protection Officers (DPOs), maintaining audit logs, and establishing grievance redressal mechanisms. For smaller businesses, these requirements can be costly and resource-intensive.

- **Data Localization:**

The act mandates that certain types of data be stored and processed within India, which can create operational challenges for companies with global operations and increase costs.

- **Potential Conflicts with Other Laws:**

The DPDP Act's data localization requirements may conflict with international data transfer laws and regulations.

- **Enforcement and Monitoring:**

Ensuring the effective functioning of the Data Protection Board (DPB) and providing it with the necessary authority and resources to enforce the law is crucial for its success.

- **General Awareness and Compliance:**

Many individuals and businesses, particularly small and medium-sized enterprises, may lack awareness about the DPDP Act and its implications.

- **Technological Challenges:**

The act may necessitate investments in new data infrastructure and security measures, which can be

challenging for businesses lacking the necessary expertise or resources.

- **Absence of Provisions for Emerging Technologies:**

  The act doesn't explicitly address the privacy implications of emerging technologies like AI and machine learning, which can raise concerns about algorithmic bias and data manipulation.

- **Dilution of RTI Act:**

  There are concerns that the DPDP Act could be used to limit access to information under the Right to Information (RTI) Act, hindering transparency and accountability.

- **User Rights:**

  While the DPDP Act grants rights to access, correct, and erase personal data, it lacks provisions for data portability and the right to object to automated decision-making.

References

[1] The Digital Personal Data Protection Act, 2023 (No. 22 of 2023), *Gazette of India*, August 11, 2023, https://www.meity.gov.in/writereaddata/files/Digital%20Personal%20Data%20Protection%20Act%202023.pdf.

[2] Starting with the Supreme Court's judgment declaring privacy to be a fundamental right in *Justice K.S. Puttaswamy and Anr. v. Union of India and Ors.* (10 SCC 1, Supreme Court of India, 2017). .

[3] The Personal Data Protection Bill, 2019 (Bill No. 373 of 2019), accessed December 16, 2019, http://164.100.47.4/BillsTexts/LSBillTexts/Asintroduced/373_2019_LS_Eng.pdf.

[4] The Personal Data Protection Bill, 2018, accessed March 8, 2019, https://www.thehinducentre.com/resources/article24561526.ece/binary/Personal_Data_Protection_Bill,2018_0.

[5] "Report of the Joint Committee on the Personal Data Protection Bill, 2019," 17th Lok Sabha Secretariat, December 16, 2021, https://eparlib.nic.in/bitstream/123456789/835465/1/17_Joint_Committee_on_the_Personal_Data_Protection_Bill_2019_1.pdf.

[6] The Digital Personal Data Protection Bill, 2022, Ministry of Electronics & Information Technology, Government of India, accessed August 9, 2023, https://www.meity.gov.in/writereaddata/files/The%20Digital%20Personal%20Data%20Potection%20Bill%2C%202022_0.pdf.

[7] *Justice K.S. Puttaswamy and Anr. v. Union of India and Ors.*

[8] Anirudh Burman, "Will India's Proposed Data Protection Law Protect Privacy and Promote Growth?," Carnegie India, March 9, 2020, https://carnegieindia.org/2020/03/09/will-india-s-proposed-data-protection-law-protect-privacy-and-promote-growth-pub-81217.

[9] Ibid.

[10] "Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)," *Official Journal of the European Union*, May 4, 2016, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679.

11 Anirudh Burman, "The Withdrawal of the Proposed Data Protection Law Is a Pragmatic Move," Carnegie India, August 22, 2022, https://carnegieindia.org/2022/08/22/withdrawal-of-proposed-data-protection-law-is-pragmatic-move-pub-87710.

12 The Digital Personal Data Protection Bill, 2022.

[13] Ibid., Section 3.

14 The Digital Personal Data Protection Act, 2023, Section 4.

15 Ibid., Section 7(b).

[16] Ibid., Section 7.

[17] See ibid., Sections 11–14.

[18] Ibid., Sections 8 and 9.

[19] Ibid., Section 10.

[20] Ibid., Section 17(1).

[21] Ibid., Section 17(2).

[22] Ibid., Section 18.

[23] Ibid., Sections 27 and 28.

[24] Ibid., Sections 19 and 20.