VOLUME 4 | ISSUE 3

INTERNATIONAL JOURNAL OF ADVANCED LEGAL RESEARCH

ANALYSING THE DIGITAL PERSONAL DATA PROTECTION (DPDP) BILL, 2023

- Ananya Yadav & Dr Rajeev Kumar Singh[1]

Abstract

The Digital Personal Data Protection (DPDP) Bill of 2023 presents a comprehensive framework aimed at safeguarding the privacy rights of individuals in the digital realm. This paper highlights key provisions and modifications in the bill compared to previous iterations, focusing on its scope, consent mechanisms, legitimate uses, responsibilities of data fiduciaries, access to information, cross-border data transfer, exemptions, conflict resolution, regulatory aspects, and enforcement measures.

The bill expands its scope to cover personal data processed in digital format within India's territorial boundaries and data digitized after public dissemination, even if processed outside India but associated with providing goods or services to individuals in India. However, data processed for personal or domestic purposes is exempt, as is publicly disseminated personal data. Notice and consent form the foundation of data processing, requiring explicit, informed, voluntary consent from data subjects for specific purposes, with an emphasis on minimal data collection. Certain legitimate uses allow data processing without consent in specified situations, including state activities like medical emergencies or natural disasters, though concerns arise regarding privacy rights.

Data fiduciaries are tasked with implementing streamlined complaint resolution procedures, appointing data protection officers, conducting regular assessments, and ensuring due diligence in data processing. Concerns regarding harm to data principals, particularly

[1] Student & Assistant Professor at Amity University Lucknow

children, are addressed through waivers of additional obligations if data processing is secure and verifiable.

The bill also addresses access to information, with limitations on individuals' right to access information about their personal data processing, particularly when related to preventing wrongdoing. Notably, the bill introduces modifications to the Right to Information Act, potentially hindering transparency and accountability.

Regarding cross-border data transfer, the bill facilitates international data flow unless restricted by the central government, prioritizing data localization but allowing for exceptions. Exemptions from certain provisions are granted to startups and government entities, raising concerns about privacy violations and abuse of power.

Enforcement mechanisms include monetary sanctions for violations, with reduced penalties compared to previous versions. The bill emphasizes conflict resolution through mediation and voluntary adherence to legal requirements.

Despite incorporating several recommendations, the bill faces criticisms regarding state exemptions, lack of clarity in enforcement procedures, and potential infringement of privacy rights. Balancing privacy with national security concerns remains a challenge, necessitating robust oversight mechanisms.

Digital Personal Data Protection (DPDP) Bill, 2023

The introduction of the Digital Personal Data Protection (DPDP) Bill for 2023 has resulted in notable revisions compared to the previous draft that was made available for public feedback in the previous year. DeepStrat provided input on the draft in January 2023, and subsequently, specific ideas have been included.

Significant modifications have been implemented to the ultimate Bill that has been submitted to the legislative body. A number of these modifications would have a substantial effect on the privacy rights of individuals, beyond the limitations established by the landmark Puttaswamy vs. Union of India[2] decision in August 2017.

[2]Justice K.S. Puttaswamy (Retd) vs. Union of India, W.P. (Civil) No 494 of 2012, Supreme Court of India, August 24, 2017

The Bill aims to guarantee that the handling of digital personal data upholds persons' rights and is carried out for legitimate purposes.

Since Puttaswamy, there have been four distinct iterations of the legislation, and the process of establishing a privacy law commenced with a committee led by Justice AP Shah in 2012. Subsequently, four further amendments to the legislation have been implemented. The current iteration is the fifth.

Concerning the Act's Applicability

The scope of this legislation includes personal data that is gathered in digital format inside the territorial boundaries of India, as well as data that has been digitized subsequent to its public dissemination. The legislation would encompass the processing of digital personal data that occurs outside of India, if there is any association with the provision of goods and services to persons in India.[3]

The requirements of the Act do not apply to data that is processed for domestic or personal purposes. It is important to acknowledge that the newly implemented policy does not encompass personal data that has already been publicly disseminated by the relevant individual or by another party with a legal obligation to do so. This is a thrilling and innovative advancement. It is important to acknowledge that the legislation in question may not provide protection for personal information disclosed on social media platforms or in accordance with other legal requirements.

A system built on notice and consent

In relation to the Bill, there are three primary stakeholders. The data subject refers to the individual whose personal information is being requested for processing. A data fiduciary is an individual or entity that, either autonomously or in collaboration with a data processor, determines the manner and objectives for processing personal data. Furthermore, the state possesses the capacity to scrutinize data for certain objectives. In general, it is customary for a data fiduciary to engage in the processing of personal data just upon notifying the data principal and acquiring her explicit agreement. Consent must not only be voluntary, explicit,

[3]Report of the Joint Committee on the Personal Data Protection Bill, 2019, December 2021

well-informed, absolute, and unequivocal, but it should also be clearly demonstrated via a definitive affirmative action. Fulfilling this condition is crucial. This iteration of the Bill highlights the need of acquiring consent for a particular objective and guaranteeing that just the essential personal information is gathered. Furthermore, the law adeptly incorporates the crucial concepts of need and purpose constrained.[4]

Nevertheless, the fundamental foundation for processing personal data extends beyond the context of notice and authorization. Data can be processed for particular legal applications, even in the absence of the data principal's authorization.

Appropriate Uses

The provision that was previously a source of contention has been reissued under the name "certain legitimate uses," which permits the use of personal data in nine overarching situations without the need for consent from the individuals concerned. Similar to businesses, data fiduciaries may only process information with the consent of the principal for particular purposes. In certain circumstances, the state may nevertheless process data without the consent of the principal. These consist of the provision of services, subsidies, certificates, licenses, and permits, among others. In situations involving medical emergencies, natural disasters, or a breakdown in public order, the state may also process data. Thankfully, the most recent iteration of the legislation has eliminated two use cases that exhibited an excessively narrow focus. These use cases were motivated by a just and rational intention and served the public interest. The potential for data to be processed without the consent of individuals in a variety of situations gives rise to apprehensions regarding the fundamental right to privacy of citizens of India.

The Responsibilities of "Data Fiduciaries"

Data fiduciaries must ensure that the procedures for mediating and resolving complaints are streamlined and effective. The appointment of a data protection officer is imperative in order to address any inquiries or apprehensions pertaining to the management of personal data. It is compulsory for organizations that manage significant volumes of data to designate Data

[4] 'A Free and Fair Digital Economy Protecting Privacy, Empowering Indians', Committee of Experts under the Chairmanship of Justice B.N. Srikrishna, July 2018.

Protection Officers situated in India, who are answerable directly to the Board of Directors. Furthermore, additional responsibilities pertaining to due diligence must be fulfilled. These encompass the selection of an autonomous data auditor, the execution of routine data protection impact assessments, the completion of periodic audits, and the fulfillment of analogous obligations.

We have effectively resolved the issue of harm in connection with a data principle in this iteration. In the capacity of an education specialist, it is critical to contemplate the potential adverse ramifications of the Bill on children and devise strategies to protect their welfare. However, additional obligations may be waived if a data fiduciary can guarantee that the processing of children's data is secure and verifiable independently.[5]

Appreciating the opportunity to access information

Additionally, the revised manuscript includes a modification to the provision pertaining to the right of access to information. The right of individuals to access information is contingent upon the consent that has been obtained from the data subject. Individuals typically lack the authority to request information pertaining to the processing and dissemination of their personal data. This occurs in the event that data is exchanged. When information is disclosed to prevent, detect, investigate, prosecute, or sanction wrongdoing, individuals will not be entitled to access the identity of the data fiduciaries responsible for handling the shared data. The Puttaswamy ruling of 2017 established a precedent by recognizing the right to information privacy as a critical component of the fundamental right to privacy. This significantly restricts the capacity of individuals to uphold their privacy with respect to information.[6]

Access to Information

The objective of the Draft Bill of 2022 was to eliminate Section 8(1)(j) and the proviso to Section 8(1) of the 2005-enacted Right to Information Act. Frequently, Section 8 is invoked to exempt information pertaining to public activities from being made public to Indian

[5]Yashraj Bais, Privacy and Data Protection in India: An Analysis, International Journal of law and Management and Humanities, Volume 4 issue 5, 2021

[6]Shanaz, Asifullah Samim and Mohammad Edris Abdurahim Zai, Navigating Data Protection in India: Key Laws and Regulations for Protecting Personal Information, Trinity Law Review, Volume-3, Issue-2, 2023

citizens. Section 8(1)(j) prohibits the disclosure of information that is irrelevant to public interest or activity, or that would unreasonably infringe upon the privacy of an individual. However, such publication may be justified if it serves a greater public interest. We had previously issued a warning regarding this amendment, reasoning that it might impede the overarching goal of the RTI Act.

The provision in subsection (j) of subsection 8(1) is not entirely eliminated from the 2023 bill. Conversely, it is substituted with a straightforward expression that reads, "(j) information pertaining to personal information." This ostensibly minor modification will yield substantial ramifications within the domain of the RTI regime. It is crucial to acknowledge that personal information will not be subject to public surveillance, even if it is associated with public activity or possesses a significant public interest. In light of these conditions, the legislation that advocates for accountability and openness will encounter a hindrance. The provision in section 8(1) of the RTI Act is only applicable to clause (j), per the Bill.[7]

An additional enticing facet warrants contemplation. Any information that is not subject to denial by the Parliament or State legislatures is obligated to be disclosed to any individual in accordance with this provision. This provision has been interpreted by a number of courts as applying to every exemption granted in Section 8(1). Nonetheless, this bill deems the proviso to be exclusively associated with clause (j); therefore, by substituting it, this vital safeguard is eliminated. The aforementioned modifications will have an effect on every exemption specified in Section 8(1) of the RTI Act. Even information that ought to be accessible to the legislative bodies of the state or parliament may be denied access under these exemptions. The Constitution of India designates the right to information and the right to privacy as fundamental rights of equal significance. Ensuring the alignment of both laws in a way that prevents one law from superseding the other is of utmost importance.

Understanding the movement of data across borders and the concept of data localization

To facilitate international data flow, the Bill allows data processing outside India unless the Central government has issued a notification prohibiting it. This would facilitate foreign trade

[7] Nivedita Baraily, An Analysis of Data Protection and Privacy Law in India

and help India become a trillion-dollar digital economy. The previous measure required notification to every nation before sending data across borders via whitelisting. The new plan encourages data interchange with all nations rather than restricting it. However, if another Indian law raises the bar for personal data communication, it will take precedence over the DPDP. Sectoral laws with a big impact, like the Reserve Bank of India's Storage of Payment System Data directive, are crucial in this circumstance. Priority is given to storing all payment system data in India under this order.[8]

The exceptions

The phrase that sparked disagreement and enabled large Bill exclusions has been kept, with minor revisions. For instance, firms reorganizing or considering debt failure have certain exclusions. This updated proposal includes several more justifications for state exclusions, which still threatens private rights.

Startups may be excluded from notification, data completeness, correctness, consistency, data deletion, substantial data fiduciaries' extra requirements, and the right to access personal data. The Central Government exempts. Additionally, the Central Government might exempt data fiduciaries from some Bill provisions for five years after passage.

In Justice K.S. Puttaswamy v. Union of India, the Supreme Court of India said that legality, need, and proportionality underpin privacy. Justice S.K. Kaul further added a fourth criteria stressing procedural safeguards to prevent intervention abuse. The Joint Parliamentary Committee report stresses using a just, fair, reasonable, and equitable exemption system. Most exemptions in this law are at danger of misuse due to the lack of a well-defined methodology. In India, there is no post-independence surveillance legislation, thus the Bill must incorporate monitoring mechanisms over the exclusions clause to defend the basic right to privacy.

Addressing Complaints and Concerns

[8] Yashraj Bais, Privacy and Data Protection in India: An Analysis, International Journal of law and Management and Humanities, Volume 4 issue 5, 2021

A good plan has been made to handle privacy regulatory complaints. Consent managers and data fiduciaries can file complaints through a specified method. After the Data Protection Board, the Telecom Disputes Settlement and Appellate Tribunal is next.[9]

The Bureau of Data Protection

No modifications have been implemented to the definition of the Data Protection Board. It has been converted into a body corporate, which grants it, among other privileges, the capacity to engage in legal proceedings, maintain an ongoing existence, and possess a common seal. This legislation comprises a multitude of complexities that regulate the framework, capacity, prerequisites, duration, remuneration, dismissal, and resignation, among other pertinent aspects. Furthermore, initiatives have been implemented to deter retirees from seeking employment. Nonetheless, the Central Government retains the authority to appoint members of the Board of Directors.[10]

In the advocacy and preliminary report of the Justice Srikrishna Committee, an autonomous entity comprising a Selection Committee was suggested. It would be the responsibility of this organization to designate candidates for appointment. In addition, the composition of the Selection Committee was meticulous, comprising individuals from diverse sectors including the executive branch, judiciary, civil society, and industry. Subsequently, the Joint Parliamentary Committee observed that the 2019 Draft Selection Committee was composed exclusively of bureaucrats holding the rank of secretary. They suggested that the Committee be comprised of professionals from diverse disciplines, including academic, legal, and technical, in order to guarantee a thorough, formidable, and impartial composition. All of these recommendations are entirely disregarded in the current draft.

Concerns

In accordance with the Telecom Regulatory Authority of India Act, 1997, the Telecom Disputes Settlement and Appellate Tribunal shall now hear appeals against decisions or

[9] M. R Konvitz, Privacy and the Law: a Philosophical Prelude. Law and Contemporary Problems Vol 31, No. 2. (1966) p. 272

[10] Nikhil Pahwa, The Problem with India's Proposed Intermediary Liability Rules, Quartz India (Dec. 28, 2018)

orders of the Data Protection Board. The Appellate Tribunal maintains a steadfast determination to expedite the appeal's resolution within a prescribed period of six months. In accordance with the Telecom Regulatory Authority of India Act, 1997, individuals are granted the opportunity to petition the Supreme Court for review of Appellate Tribunal orders or decisions within a ninety-day timeframe. Digital offices will be established for the Data Protection Board and the Appellate Tribunal to facilitate the submission of complaints and appeals, case deliberations, and the dissemination of rulings.[11]

Exploring Different Approaches to Conflict Resolution and Encouraging Active Involvement

To effectively manage the substantial volume of grievances that may emerge in relation to this legislation, the Bill additionally integrates provisions for the resolution of complaints via mediation. This measure would effectively mitigate the workload of the regulatory bodies tasked with handling grievances, consequently alleviating pressure. Moreover, the provision permitting voluntary adherence to legal requirements has been upheld, enabling individuals to voluntarily acknowledge accountability at any juncture throughout an adversarial proceeding. This clause was initially included in the document.[12]

The Impact of Inflation

As per the provisions of the measure, those found in violation of the legislation shall be subject to monetary sanctions exclusively, devoid of any criminal consequences. In addition, the maximum penalties have been reduced from INR 500 crore (equivalent to INR 5 billion) to INR 250 crore (equivalent to INR 2.5 billion), for a grand total of INR 250 crore. Many data fiduciaries, particularly small organizations and start-ups, may find this reassuring, given that rigorous regulations may be imposed upon them upon the passage of this measure. This measure contains both positive and negative provisions. A number of the recommendations put forth during the public consultation have been integrated into the novel legislation, whereas others have been omitted. In light of the 2017 landmark decision that

[11] Upasana Sharma & Aniket Singhania, The Personal Data Protection Bill, 2019: An Overview, Mondaq (Jan. 13, 2020)

[12] Vijay Pal Dalmia and Rajat Jain, Compliances by an Intermediary Under Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 - social media - India, Mondaq (May 9, 2022)

established the right to privacy as a fundamental right by the Supreme Court of India, it is clear that this measure has been the subject of considerable anticipation and anticipation.[13]

Comparison of various drafts of the Data Protection Law

"The Draft Personal Data Protection Bill, 2018"	**"The Personal Data Protection Bill, 2019"**	**"Recommendations of the Joint Parliamentary Committee"**	**"The Digital Personal Data Protection Bill, 2023"**
SCOPE AND APPLICABILITY			
Processing of personal data can occur either within India or outside of India, depending on the specificcircumstances. If the processing is related to business activities, the offering of goods and services, or profiling individuals in India, it may also take place outside of the country.	Extends the reach of the 2018 Bill to include specific anonymized personal data	Expands the scope under the 2018 Bill to include the processing of non-personal data and anonymized personal data.	Does not address offline personal data and non-automated processing.

[13] Upasana Sharma & Aniket Singhania, The Personal Data Protection Bill, 2019: An Overview, Mondaq (Jan. 13, 2020)

REPORTING OF DATA BREACHES			
When a breach occurs that may result in harm, it is important for the fiduciary to inform the Data Protection Authority. The Authority will then determine whether the data principals should be notified or not.	Just like the 2018 Bill	It is mandatory to report all breaches to the Authority within 72 hours, regardless of the potential harm they may cause.	It is essential to report every personal data breach to the Data Protection Board of India and notify each affected data principal in the prescribed manner.
Exclusions from provisions of the Bill for the purpose of ensuring the security of the state, maintaining public order, and preventing offenses, among other reasons.			
Processing must be authorized by law and carried out in accordance with the established legal procedure. It should also be necessary and proportionate.	The central government has the authority to grant exemptions to agencies when processing is deemed necessary or expedient. However, this is subject to specific procedures, safeguards, and	Emphasizes the importance of including a well-defined procedure in the order, one that is fair, just, and reasonable	The central government has the authority to grant exemptions through a notification, without the need for any specific procedures or safeguards to be mentioned.

	oversight.		
Understanding the concepts of data portability and the right to be forgotten is crucial.			
The data principal will be entitled to data portability, allowing them to obtain their data in a format that can be easily used with other systems. Additionally, they will have the right to be forgotten, which means they can request that their personal data be restricted from being disclosed over the internet.	Ensured equal access to both rights	Ensured equal access to both rights	**NA**
Potential negative consequences of personal data processing			
• Harm can encompass various negative consequences	Just like the 2018 Bill	It would be beneficial for the central government to have the authority to	**NA**

such as financial loss, identity theft, damage to one's reputation, and invasive surveillance. • Data fiduciaries should implement measures to minimize and mitigate potential risks of harm. • If harm occurs, the data principal has the right to seek compensation.		designate and address additional negative impacts.	
REGULATOR			
It would be beneficial for the central government to have the authority to designate and address additional negative	Just like the 2018 Bill	Just like the 2018 Bill	• Supports the Data Protection Board of India, which plays a crucial role in

impacts.			resolving non-compliance issues; • TDSAT has been designated as the Appellate Tribunal.
Transferring personal data outside of India			
• It is necessary for every entity to maintain at least one duplicate of personal data in India. • May be transferred to certain permitted countries or under contracts approved by the Authority, if consent is	• It is important to ensure that sensitive personal data is kept within India. • Explicit consent is required for the transfer of certain sensitive personal data, while there are no restrictions on the transfer of other	Emphasizes that personal data will only be shared with foreign agencies or government after receiving prior approval from the central government, ensuring the protection of sensitive information.	• Eliminates the classification of sensitive and critical personal data • The central government has the authority to limit the transfer of personal data to specific countries by issuing a notification.

provided, even outside India. • Some specific data can only be processed in India.	personal data. • Regarding sensitive personal information, it is similar to the 2018 Bill.		

PRIORITIES AND ANALYSATION

State exemptions might have a negative impact on privacy

The State receives exemptions for processing personal data under the Bill. According to Article 12 of the Constitution, the state includes the federal government, state governments, municipal organizations, and government-established institutions and corporations. These exclusions might cause issues.

The Bill may empower the State to process data without scrutiny, violating private rights. Privacy intrusion must be justified by necessity, according to a 2017 Supreme Court judgment. Exemptions allow the state to acquire, analyze, and store more data than necessary. This may violate privacy.

The Bill allows the federal government to waive processing rules for government entities to safeguard public order and state security. In cases when processing is required to avoid, discover, and prosecute violations, data fiduciaries and data principals have no obligations or rights other than data security. The Bill does not require government agencies to delete personal data after processing. Under the exceptions, a government agency may collect personal data to create a 360-degree profile for national security surveillance. Several government departments' files might be used. This calls into question whether these exemptions are proportionate.
On national security concerns, the Supreme Court (1996) required need, purpose limitation, and storage limitation for communication interception. The exemption Bill's data fiduciary obligations are similar. According to the Srikrishna Committee (2018), processing for

national security and crime prevention and prosecution should not require obligations other than fair and appropriate processing and security measures. It said a new legislation would define purpose and set storage limitations if needed. This legal structure is absent in India. UK data privacy law 2018 provides similar exceptions for national security and military. However, the Investigatory Powers Act, 2016, controls government agencies' widespread processing of personal data for intelligence and law enforcement. The Secretary of State or Home Minister issues a warrant for such action with judicial commissioner approval. We must examine the need and proportionality of such activities. Data retention beyond warrant expiration is restricted. Additionally, this act creates parliamentary oversight. Can consent for licenses, certificates, subsidies, and perks be overridden?

The Bill supersedes consent when the State processes personal data for a benefit, service, license, permit, or certificate. It explicitly allows reusing information processed for one usage. It also allows the use of State-held personal data for these purposes. It eliminates purpose restriction, a basic privacy principle. Information should only be collected and used for its intended purpose. Whether exemptions are justified is the question.

Profiling people may be achieved by combining data from several sources. If consent were required, people would have control over data collection and dissemination.[14]

The Bill does not regulate personal data processing damage.

The Bill does not address personal data processing injury hazards. Personal data processing may harm, according to the Srikrishna Committee (2018). Harm might include financial loss and reduced perks or services. Other examples include identity theft, reputational harm, prejudice, and illogical surveillance and profiling. It recommended data privacy laws cover damages.

The Personal Data Protection Bill, 2019 defined harm as psychological suffering, identity theft, monetary loss, reputation damage, unjust treatment, and monitoring or surveillance that the data principle did not reasonably foresee. The 2019 Bill required data fiduciaries to prevent, mitigate, and reduce harm. These included audits and impact assessments to assess

[14] National Institution for Transforming India. (2020). Data Empowerment and Protection Architecture (DEPA): A Policy Framework for Empowering Residents with Control over their Personal Data. New Delhi: NITI Aayog"

hazards. If affected, the data principal might sue a data processor or fiduciary for damages. The Joint Parliamentary Committee recommended preserving personal data processing damage clauses in the 2019 Bill. The EU's General Data Protection Regulation (GDPR) addresses harm risks and data principal compensation.

The right to be forgotten and data portability are denied.

The measure does not include data portability or the right to be forgotten. These rights were in the 2018 Draft Bill and 2019 Parliamentary Bill. After analyzing the 2019 Bill, the Joint Parliamentary Committee advised preserving these rights. GDPR acknowledges these rights. Data protection legislation must provide strong data primary rights, according to the Srikrishna Committee (2018). These rights provide people data control based on accountability, transparency, and autonomy.

Data portability rights: Data principals can use data fiduciaries' machine-readable data for their own purposes under this legal protection. Data principals have more control over their data. It may simplify data fiduciary transfers. Some worried it might reveal the data fiduciary's trade secrets. According to the Srikrishna Committee (2018), the right should be protected as far as possible without divulging trade secrets. The Joint Parliamentary Committee states that trade secrets can only be used to deny right-to-right data portability if it is technologically feasible.
Right to be Forgotten: People can limit their online personal information. The freedom to be forgotten limits memory in the digital environment, according to the Srikrishna Committee (2018). The Committee noted that this right may need to be balanced against other rights and interests. This right may violate another's freedom of expression and information. The data principal's role in public life, the sensitivity of the personal information to be controlled, and the public interest in it may decide its use.

A shorter appointment term may harm board independence.

The Bill gives Indian Data Protection Board members autonomy. After two years, members can be reappointed. A short tenure with reappointment may impair the Board's independence. Compliance enforcement, investigations, and fines are the Board's main duties. The Supreme Court of 2019 highlighted that short-term tribunals with re-appointment processes give the

Executive more discretion. Adjudicatory regulatory agencies like the Central Electricity Regulatory Commission and the Competition Commission of India have five-year terms under their Acts. TRAI appointments last three years. Regulations limit SEBI appointments to five years.

Extra child protections

There are additional standards for handling child data. We discuss many issues with these clauses below.

Kids are defined differently by each country.

While it is generally agreed that children' data should be protected, different countries have differing definitions of minors and when they can consent to data processing. The Bill defines a kid as under 18. US and UK residents over 13 can consent to data processing. The GDPR establishes this age at 16, although member states can lower it to 13. The Srikrishna Committee (2018) advised considering many factors when determining if a child can consent. These include a 13-year-old minimum and 18-year-old maximum age, and a single criterion for realistic implementation. It also suggested that 18 may be too old for a child's full autonomy. The existing legal framework requires a consenting age of 18. The Indian Contract Act, 1872, requires 18-year-olds to sign contracts.

For confirmed parental authorization, digital platforms may need age verification.

Data fiduciaries must have legal guardian approval before processing a child's personal data under the Bill. To comply, data fiduciaries must verify the age of each new customer. You must determine if the person is a child to seek authorization from their legal guardian. The risk of youngsters making up comments may decrease. However, this may make online anonymity tougher.

Definition of child damage is lacking.

Data fiduciaries cannot process child-harming information, under the measure. Bill does not specify harm. No instructions are provided for calculating this consequence.

Conclusion

In conclusion, the Digital Personal Data Protection (DPDP) Bill, 2023, represents a significant step towards enhancing the protection of individuals' privacy rights in the digital sphere. Through multiple iterations and extensive consultation processes, the Bill has evolved to address various concerns and considerations.

The Bill establishes a comprehensive framework for the handling of digital personal data, emphasizing the importance of notice, consent, and purpose limitation in data processing activities. It delineates the roles and responsibilities of data fiduciaries, outlines mechanisms for addressing complaints and breaches, and establishes regulatory oversight through the Data Protection Board.

Key provisions of the Bill include the recognition of individuals' rights to access and control their personal data, mechanisms for reporting data breaches, and measures to regulate the transfer of personal data across borders. Additionally, the Bill addresses concerns related to the processing of personal data by the state, ensuring that such activities are authorized by law and subject to necessary safeguards.

However, certain aspects of the Bill have sparked debates and raised concerns, particularly regarding the scope of exemptions granted to the state, the balance between privacy rights and national security interests, and the adequacy of provisions for addressing harm resulting from data processing activities.

Overall, while the DPDP Bill, 2023, represents a significant advancement in India's data protection landscape, it is imperative for stakeholders to continue engaging in dialogue and scrutiny to ensure that the legislation effectively balances privacy rights with legitimate interests and safeguards against potential abuses of personal data.