KING STUBB & KASIVA
ADVOCATES AND ATTORNEYS

NEW DELHI | MUMBAI | BANGALORE | HYDERABAD | CHENNAI | KOCHI | PUNE | MANGALORE

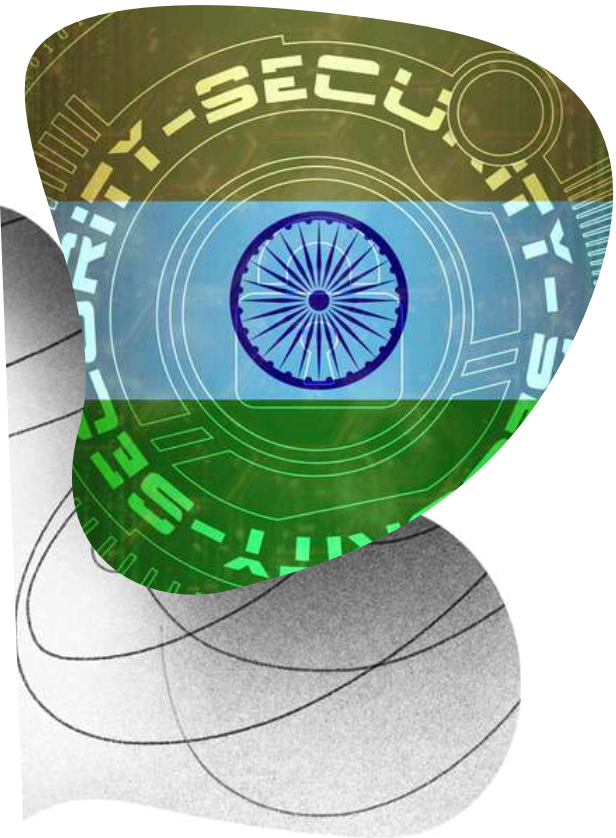
DIGITAL PERSONAL DATA PROTECTION ACT, 2023

A DAWN OF A NEW ERA FOR DATA PROTECTION IN INDIA: AN IN-DEPTH ANALYSIS OF THE DIGITAL PERSONAL DATA PROTECTION ACT, 2023

INTRODUCTION

India has ushered in a new era in the context of data protection. Thus far, we have had to rely on the Information Technology Act, 2000 ("IT Act") and Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules, 2011 ("SPDI Rules") as the only legislations for the interpretation of all things data-related. However, there were various limitations to these laws, and in a digital age where concerns about one's personal data are on the rise, the arrival of the Digital Personal Data Protection Act, 2023 provides much relief.

While 2017 gave a glimpse of what the future of privacy looked like with the historic Justice K. S. Puttaswamy v. Union of India case decided by the Supreme Court of India,*[1]* the country lacked a comprehensive and updated legislation that could be relied upon for interpreting cases involving data protection. What India did not have, and sorely missed, was an equivalent to the General Data Protection Regulation ("**GDPR**") of the European Union.



Since 2018, there have been efforts made by the Indian Government to introduce and implement a central legislation that could prove to be the successor to the SPDI Rules, and act as a standalone data protection law. After releasing multiple drafts of the proposed data protection bill over the years, 2023 finally saw the latest iteration of the legislation, titled the 'Digital Personal Data Protection Bill, 2023' ("**DPDP Bill**"), approved by the Lok Sabha on August 3, 2023. This was followed by the Rajya Sabha passing the DPDP Bill on August 9, 2023. Finally, on August 11, 2023, the President of India granted her assent to the same, and the Digital Personal Data Protection Act, 2023 ("**DPDP Act**") was notified and published in the Official Gazette of India.

ANALYSIS

Building upon previous versions:

The DPDP Act builds upon its predecessor, which was the 'Digital Personal Data Protection Bill, 2022' released in November, 2022 ("2022 Bill"). While preserving its core concepts, the DPDP Act introduces strategic adjustments, some of which are minor, yet others are more substantial.

The DPDP Act introduces robust provisions concerning notice and consent obligations, delineates the permissible 'legitimate uses' for processing personal data without explicit consent, establishes an 'Appellate Tribunal' for grievance redressal, and imposes enhanced responsibilities upon data fiduciaries when handling the data of children, among other changes.

It is also noteworthy that the DPDP Act's focus has been deliberately narrowed to the safeguarding of 'digital' personal data, reflecting an evolution from its earlier scope in the 2022 Bill.

Government interface with existing data protection framework:

At the outset, it seems as if the DPDP Act establishes a mutual connection with the Government of India's broader information technology regulations. The dimension of information solicitation reflects an interface with the IT Act *[2]* and the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, empowering the Central Government to request information from the Data Protection Board ("Board"), fiduciaries, or intermediaries.*[3]* However, the absence of specific details indicates an exploration into the scope, purpose, and safeguards associated with this information solicitation, necessitating alignment with the legal principles elucidated in the Puttaswamy judgment.

Furthermore, there seems to be evidence of interlinking between the DPDP Act and the Information Technology (Procedure and Safeguards for Blocking for Access of Information by Public) Rules, 2009, converging data protection concerns with the regulation of access to computer resources. This arrangement appears as the government, following due process and the right to be heard, *[4]* gains authority to instruct agencies or intermediaries to block information, safeguarding public interests. *[5]* This confluence of mechanisms offers a robust avenue to mitigate risks linked to non-compliance, while warranting a detailed roadmap for operational execution.

KEY PROVISIONS

1. **Applicability and Scope:**

The DPDP Act governs the processing of digital personal data within India in two scenarios: (i) when such data is collected from data principals in digital format; or (ii) when initially collected in

non-digital form and subsequently digitized. Thus, the DPDP Act shall not apply to processing of personal data in non-digitized form. It is clearer and narrower than the 2022 Bill, which did not apply to 'non-automated' processing and 'offline' data.

Moreover, the scope of the law has been extended. It now has an extra-territorial application, to encompass the processing of digital personal data beyond India's borders if it pertains to the provision of goods or services to data principals located within India. Notably, the DPDP Act does not explicitly address whether its provisions are applicable to the processing of personal data belonging to data principals situated outside India.

Unlike the GDPR, which confines its applicability to the processing of personal information of individuals physically present within the European Union or EU citizens, the DPDP Act adopts a broader approach. It does not limit the definition of 'data principal' to individuals within India's boundaries or solely to Indian citizens. This could potentially lead to ambiguity regarding the full scope of the DPDP Act's jurisdiction. The resolution of this ambiguity concerning the DPDP Act's extraterritorial application hinges on the interpretation that the Central Government eventually provides, most likely in the rules that would be framed under the DPDP Act.

2. Exemptions for Startups and Transitory Provisions:

Within the outlines of the DPDP Act, a distinct focus emerges on accommodating the dynamic landscape of startups. In addition to exemptions granted to the state, its instrumentalities, research, and statistical purposes, the DPDP Act introduces a tailored approach, proposing certain provisions for potential exemption for startups. *[6]* This strategic measure recognizes the distinct challenges and evolving nature of startups, with the intent to nurture innovation while upholding robust data protection principles.

3. Personal Data:

A novel term, 'digital personal data,' has been introduced within the DPDP Act, signifying 'personal data' presented in a 'digital form.' *[7]* This helps clarify the scope of the impending Act to be passed, and distinguishes it from personal data that is otherwise defined.

The DPDP Act confines its coverage to the processing of 'personal data,' defined as 'any data

pertaining to an identifiable individual.' Notably, the distinction between 'sensitive personal data' and 'critical personal data,' present in all prior iterations of the draft bills up to the 2022 version, has been discarded in the DPDP Act. This shift signifies a departure from the previous framework and merits close examination in terms of its implications for data protection and privacy concerns.

An obligation has been placed on data fiduciaries by the DPDP Act to safeguard the personal data in their possession by implementing ‘reasonable security measures’ to prevent breaches. In the event of a data breach, the data fiduciary is mandated to notify both the Board and the affected data principals. However, the specific manner of notification is left to be prescribed. *[8]*

It is worth noting that the DPDP Act does not specify the exact standard for 'reasonable security measures,' which although, is currently covered under the SPDI Rules and Section 43A of the IT Act. Despite this, significant penalties are imposed for non-compliance resulting in a personal data breach.

4. Processing of Personal Data:

The DPDP Act meticulously outlines the scope of 'processing' by denoting it as a 'wholly or partly automated operation or a series of operations conducted on digital personal data'. This encompassing definition encompasses various actions, including collection, recording, organization, structuring, storage, adaptation, retrieval, utilization, alignment, combination, indexing, sharing, and disclosure through transmission or other means. Furthermore, the concept extends to encompass operations such as restriction, erasure, or destruction of data.

When it comes to processing the personal data of a child, the DPDP Act requires verifiable parental consent, although it doesn't explicitly define 'verifiable' consent. The Central Government has the authority to exempt certain data fiduciaries from this requirement by lowering the age limit for parental consent, provided that the processing is considered safe. Additionally, data fiduciaries must avoid processing personal data likely to have a detrimental impact on a child's well-being.

The transfer of personal data to countries outside India is also permitted under the DPDP Act, unless explicitly restricted by the Central Government. *[9]*

It is noteworthy that the definition of 'processing' closely mirrors the definition of 'processing' outlined in the GDPR. However, a subtle divergence exists in the fact that while the GDPR's definition encapsulates both automated and specific non-automated operations, the DPDP Act confines the scope of processing exclusively to 'automated' operations. This distinction, while seemingly subtle, could have consequential ramifications for the data processing landscape, necessitating a comprehensive analysis of the potential effects in practice.

The 2022 Bill outlined certain categories of personal data processing exempt from its purview. In contrast, the DPDP Act eliminates most exemptions introduced by the 2022 Bill, save for the exemption related to personal data processed by an individual for personal or domestic purposes. Furthermore, the DPDP Act introduces an additional exemption, excluding from its scope personal data that has been publicly disclosed by the data principal or any other party obligated by Indian law to make such personal data accessible to the public.

5. Data Principal:

The concept of 'data principal' has undergone a substantial expansion. It not only encompasses individuals but also includes parents or lawful guardians of children to whom the personal data pertains. Moreover, the definition has been extended to incorporate lawful guardians of 'persons with disabilities'.

While the term 'person with disability' lacks a precise explication within the DPDPB, it is notable that the Rights of Persons with Disabilities Act, 2016, forms the foundational legislation in India for recognizing the entitlements of individuals with disabilities. Under it, a 'person with disability' is defined as someone possessing enduring physical, mental, intellectual, or sensory impairments that, when compounded by societal barriers, impede their equitable participation in society, akin to their peers. *[10]*

Under the DPDP Act, certain rights of data principals may be highlighted: (i) Right to Information about Personal Data; (ii) Right to Correction and Erasure; (iii) Right of Grievance Redressal; and (iv) Right to Nominate. As such, data principals have the right to know a summary of the personal data processed, the identities of entities with whom their data has been shared, and the categories of personal data shared. Additionally, data principals can request correction, completion, updating, or erasure of their personal data processed by a data fiduciary.

The data fiduciary must make necessary corrections and updates. Erasure can be denied if retention is required by law. The DPDP Act also casts responsibility on the data principal to not impersonate

another person or suppress information when applying for any document or proof from the state, and to provide only authentic information while exercising their right to data erasure.

Data principals shall have the right to have readily available means of grievance redressal provided by a data fiduciary in respect of any act or omission of such data fiduciary, regarding the performance of its obligations in relation to the personal data of such data principal or the exercise of her rights. *[11]* They can also nominate an individual to exercise their rights upon their death or incapacity.

6. Data Fiduciary:

Data fiduciaries are defined as any person who alone or in conjunction with other persons determines the purpose and means of processing personal data, under the DPDP Act.

The DPDP Act outlines specific 'legitimate uses' that permit data fiduciaries to process personal data without explicit consent. One instance is when a data principal voluntarily provides personal data while availing or seeking a service and has not indicated non-consent. Legitimate use also extends to processing data to comply with Indian laws or foreign laws in cases involving contractual or civil claims.

Data fiduciaries are also required to cease retaining personal data when it becomes reasonable to assume that the purpose for which the data was collected is no longer being served, and its retention is no longer necessary for legal or business reasons.

The DPDP Act prohibits data fiduciaries from engaging in tracking, behavioural monitoring of children, or targeted advertising directed at children. Originally applying only to 'guardian' data fiduciaries, this prohibition now extends to all types of data fiduciaries. This measure safeguards children's privacy and prevents their exploitation for commercial gain, emphasizing the DPDP Act's dedication to protecting children's digital well-being.

7. Significant Data Fiduciaries:

The DPDP Act allows the Central Government to have the authority to classify certain data fiduciaries or classes of them as ‘significant data fiduciaries.’*[12]* This classification is based on factors such as data volume, sensitivity, risk to data principals, electoral democracy, and state security. The 2022 Bill allowed the government to also consider ‘other factors’, but this has been

removed. Significant data fiduciaries must fulfil 'additional' obligations, including appointing a data protection officer based in India, engaging an independent data auditor for compliance evaluation, conducting data protection impact assessments, and undergoing periodic compliance audits. *[13]* Non-compliance with these obligations can result in substantial penalties, extending up to INR 250 crore.

8. Consent:

a) *Data fiduciary*

Data fiduciaries are authorized to process personal data only for lawful purposes, contingent upon obtaining consent. This consent must be characterized by being free, specific, informed, unconditional, and unambiguous. It necessitates a clear affirmative action on the part of the data principal to signify agreement for the processing of their personal data for the specified and necessary purpose. *[14]*

The request for consent must adhere to the following criteria:

- It must be presented in a clear and understandable manner, providing the option to access the request in English or any of the 22 languages listed in the Eighth Schedule to the Indian Constitution. *[15]*
- The request must include contact details for the data protection officer or an authorized representative to handle communications from the data principal.

Additionally, a data fiduciary must provide a detailed notice to the data principal either during or before seeking consent. This notice should encompass several key elements: (i) Explanation of the personal data to be collected and the purpose of its processing; (ii) Description of the data principal's rights, including correction, withdrawal of consent, and the procedure for filing complaints with the Board; and (iii) Clarity on how a complaint can be lodged with the Board.
In cases where consent was given prior to the DPDP Act's enactment, the data fiduciary must furnish such notice "*as soon as it is reasonably practicable.*" The notice must be presented in straightforward language, through a separate document, electronically, or in a manner as prescribed.

b) Data principals

When it comes to data principals, the DPDP Act mandates that they can provide, manage, review, or withdraw their consent through a 'consent manager.' *[16]* These consent managers, registered with the Board, facilitate accessible, transparent, and interoperable platforms for managing consent. However, the exact role and obligations of consent managers remain unclear, including whether all data fiduciaries are required to engage with them for seeking consent and the mechanisms they

employ for performing their functions. Data principals also retain the right to withdraw consent at any time. Such withdrawal does not impact the legality of prior data processing based on consent. Upon withdrawal, the data fiduciary and its processors must erase and cease processing the personal data, unless retention is required by applicable laws. *[17]*

c) Parental consent

It is also noteworthy that the DPDP Act introduces the concept of 'consent of the parent,' which encompasses the consent of a lawful guardian where applicable.

9. Data Protection Board:

Among the notable changes in the DPDP Act, the most significant pertains to the establishment and composition of the Board. In the 2022 Bill, the formation of the Board was contingent upon future regulations prescribed by the Central Government. However, in this recent rendition, the framework for the Board's constitution is explicitly outlined. Additionally, the authority of the Central Government to establish rules, as well as the specific scenarios under which entities can be exempted from complying with the bill's provisions, have undergone significant alteration.

10. Evolving Dispute Adjudication:

The DPDP Act aids in a paradigm shift in the arena of dispute resolution, reflecting a nuanced interplay between the legislative framework and established legal mechanisms.

A noteworthy departure lies in the empowerment of the Board to levy monetary penalties as specified in the Schedule. It omits a prior reference to a maximum penalty ceiling of Rs. 500 crores, which was present in the 2022 Bill,*[18]* signifying a deliberate recalibration in penalty imposition. This recalibration highlights a meticulous approach that brings into line penalties with the gravity of breaches, embodying a principle of proportionality.

The appellate process, too, witnesses a transformative shift as it finds its recourse in the Telecom Disputes Settlement and Appellate Tribunal.*[19]* This change instils the process with efficiency, outlining a defined window of 60 days *[20]* for appeals from the Board's decisions.

11. Penalties:

Penalties of up to INR 250 crore can be imposed for certain offenses, including failure to prevent a personal data breach. The DPDP Act removed the INR 500 crore cap on penalties for a single instance. Unlike the previous drafts, the DPDP Act does not enable affected data principals to seek compensation for breaches by data fiduciaries. Instead, the Board can now levy penalties of up to INR 10,000 for data principals not fulfilling their duties.*[21]*

CONCERNS

While there has been praise reserved for the DPDP Act in terms of acting as an able standalone data protection framework, not everything is as rosy as it seems. Concerns arise from the fact that several provisions within the DPDP Act are still subject to determinations made by the Central Government. This aspect raises valid concerns about the potential for unchecked and arbitrary rule-making, which could lead to uncertainties and potential gaps in the regulatory framework. Furthermore, for a legislation that is intended to protect the rights of data principals, it seems ironic that the DPDP Act imposes duties on data principals.

Similar to the 2022 Bill, the DPDP Act also possesses the capability to provide exemptions to the Central Government. However, in this iteration, these exemptions have been extended even more, perpetuating the absence of substantial criteria to counter excessive surveillance practices. The Central Government also retains the provision to exempt certain fiduciaries or classes of data fiduciaries from particular provisions, specifically including start-ups. The Act defines startup to mean “a private limited company or a partnership firm or a limited liability partnership incorporated in India, which is eligible to be and is recognised as such in accordance with the criteria and process notified by the department to which matters relating to startups are allocated in the Central Government.”*[22]*

fThe 2022 Bill allowed the Central Government to assume the consent of data principals in certain situations, with no way for them to opt-out through its deemed consent clause. The DPDP Act has retained this provision, rebranding it to "certain legitimate uses."

The introduction of a transition period is vital to facilitate a smooth adaptation for businesses. The DPDP Act introduces new and stringent obligations, which could require significant adjustments rom data fiduciaries. Implementing the DPDP Act without a transition period could lead to widespread non-compliance. Providing an ample transition window allows businesses the time needed to align processes and adhere to DPDP Act requirements, mitigating potential disruptions and ensuring a seamless transition to the new data protection landscape.

CONCLUSION

The DPDP Act marks a distinctive approach by India to safeguard personal data, reflecting the culmination of thorough discussions after its initial draft. This data protection law represents a crucial step in safeguarding personal data, addressing longstanding needs in the context of increasing internet users, data generation, and cross-border trade.

In its entirety, the DPDP Act signifies India's unique stance on modern data protection, enriched by extensive post-draft consultations. While its provisions are less detailed than standards like GDPR, it mandates a significant shift in how Indian businesses approach privacy and personal data.

However, the DPDP Act is not immune from criticism. Some argue it could hinder innovation due to perceived strictness, while others contend that it might not go far enough to ensure individual privacy, primarily considering the discretionary power granted to the Central Government in personal data processing. The forthcoming rules through delegated legislation will play a vital role in shaping these aspects. A standardized process for rule release, coupled with industry consultations as seen in amendments to Information Technology Rules for online gaming, would establish a robust data protection framework benefiting entire technology sector in India.

[1]Justice K. S. Puttaswamy v. Union of India, (2017) 10 SCC 1.
[2] Section 2(1)(w), Information Technology Act, 2000.
[3] Section 36, Digital Personal Data Protection Act, 2023.
[4]Section 37, Digital Personal Data Protection Act, 2023.
[5]Section 37(2), Digital Personal Data Protection Act, 2023.
[6]Explanation to Clause 17(3), Digital Personal Data Protection Bill, 2022.
[7]Section 2(n), Digital Personal Data Protection Act, 2023.
[8] Schedule 2, Digital Personal Data Protection Act, 2023.
[9]Section 16(1), Digital Personal Data Protection Act, 2023.
[10]Section 2(s), The Rights of Persons with Disabilities Act, 2016.
[11] Section 13, Digital Personal Data Protection Act, 2023.
[12] Section 10(1), Digital Personal Data Protection Act, 2023.
[13] Section 2(l), Digital Personal Data Protection Act, 2023.
[14] Section 6(1), Digital Personal Data Protection Act, 2023.
[15] Section 6(3), Digital Personal Data Protection Act, 2023.
[16] Section 6(7), Digital Personal Data Protection Act, 2023.
[17] Section 8(7), Digital Personal Data Protection Act, 2023.
[18] Clause 25(1), Digital Personal Data Protection Bill, 2022.
[19] Section 29(1), Digital Personal Data Protection Act, 2023.
[20] Section 29(2), Digital Personal Data Protection Act, 2023.
[21] Schedule 5, Digital Personal Data Protection Act, 2023.
[22] Explanation to Section 17(3), Digital Personal Data Protection Act, 2023.

CONTRIBUTED BY

Vatsal Gaur
Partner
Vatsal@ksandk.com

Krishnan Sreekumar
Associate
krishnan@ksandk.com

NEW DELHI
Unit-14, Ground Floor, DLF Tower-A, Jasola, New Delhi
Tel: +911141318190/41032969
Email: delhi@ksandk.com

BANGALORE
1A & 1B, Lavelle Mansion, 1/2, Lavelle Road, Bangalore
Tel: +91 80 41179111/41179222,
Email: bangalore@ksandk.com

CHENNAI
211, Alpha Wing, Second Floor, Raheja Towers, #177, An / na Salai, Chennai
Tel: +91 44 28605955/28606955
Email: chennai@ksandk.com

MUMBAI
61, Atlanta Building, Jamnalal Bajaj Road, Nariman Point, Mumbai
Tel: +91 22 62372076/22020080
Email: mumbai@ksandk.com

HYDERABAD
404, Shangrila Plaza, Road no. 2, Banjara Hills, Hyderabad, Telangana
Tel: +91 40 48516011/+91 40 48506011
Email: hyderabad@ksandk.com

KOCHI
1st Floor, Manavalan Building, Banerji Road, Ernakulam, Kochi
Tel: +91 484-3592950
Email: kochi@ksandk.com

PUNE
Bootstart Cowork, 1st Floor, Arcadian Building Plot No 12, Lane 5A, Koregaon Park, Pune
Tel: +91 9952966619
Email: pune@ksandk.com

MANGALORE
Office No. 406, 4th Floor, Ajanta Business Center, Kapikad, Bejai, Mangalore- 575004
Tel: +91 9844093300
Email: mangalore@ksandk.com