The Digital Personal Data Protection Bill, 2023 ("Bill")
tabled before Parliament on August 3, 2023 is the
culmination of a decade long process for evolving general
data protection regime for India.

By withdrawing an elaborate, prescriptive draft which
was under consideration by Parliament until 2021,
to introducing a new, lean, principles based draft for
consultation on November 18, 2022 ("Draft"), and then
engaging an extensive consultation process which
reportedly involved in excess of 20,000 submissions, and
several dozen discussions involving personal participation
at the highest levels of the Ministry, the Ministry of
Electronics and Information Technology has set the
stage for the evolution and adoption of a customized and
Indian legislation that seeks to find a balance between
enabling ease of doing business, and protecting sovereign
imperatives and citizens' rights, which has proved elusive
globally.

As a concise 33 -page document, written in simple
language with several illustrations, the Bill is a
significant, almost anachronistic, departure from dense,
and prescriptive approaches to personal data protection
legislation which occupied centre stage till date:

a. setting broad ground rules, several of which, like
    consent, purpose limitation and data minimization, have
    been sharpened through the consultation process;

b. providing for some guidance through delegated
    legislation on concepts such as manner of parental
    consent and privacy notices, but leaving open concepts
    like "reasonable" security practices and technical and
    organizational measures for interpretation by entities;

c. establishing a dedicated body, the Data Protection Board
to address unresolved grievances, and potentially hand
    down material fines (ranging up to Rs. 250 Crores) along
    with recommendations to ban applications and
    services of repeat offenders; and

---

1 The Digital Data Protection Bill, 2023 ("Bill") accessible here.
2 Notice - Public Consultation on DPDP 2022_1.pdf (meity.gov.in); The Digital Personal Data Protection Bill, 2022 ("Draft"), available here.
3 The Hindustan Times, Over 20k suggestions sent on data privacy law: Officials; May 1, 2023, available here.
5 Read our analysis on the 2019 Bill here.
6 Sections 5, 6, 7 and 8, Bill.
7 Sections 5(1), 9(1), Bill; Clause 40(2), Bill.
8 Sections 8(4) and 8(5), Bill.
9 Sections 18(1) and 29(1), Bill.
10 Schedule, Bill.
d. Creating a mechanism of appeals to the Telecom Disputes Settlement and Appellate Tribunal, and thereafter, the Supreme Court, the Bill provides for the creation of a rich vein of jurisprudence around privacy which is, at its core, a constitutional, fundamental right.

the Bill represents the possibility for a new start for the data ecosystem in India, and the exciting possibility of setting a new, global approach for personal data protection for innovation focussed economies.

As the first paper of our series on the Bill, we now examine the key aspects in which the Bill has evolved, as against the Draft and some global frameworks.

a. Extent of application and exclusions

The Bill continues to apply to processing of personal data i.e., any data about an individual who is identifiable by, or in relation to such data (the “Data Principal”) in digital form or personal data which may be digitized later. The Bill also applies both in India and, as is the case with other global frameworks, to processing outside India, where it is done in connection with activity related to offering goods or services to Data Principals in India. The Bill removes several proposed exclusions and proposes only two exclusions:

(a) The first for processing for personal or domestic purposes, is also common globally; and

(b) The second, with much more far-reaching consequences, is a blanket exclusion for any and all personal information that a Data Principal makes (or causes to be made) public, or is made public pursuant to a legal obligation.

While this second exclusion has the potential to enable unrestricted and widespread use of public information by businesses, and encourage AI solutions and search engines, it also means that that information, once made public, is irrevocably excluded from the ambit of any and all forms of protection, including principles like fair processing, storage or purpose limitation as well as rights like erasure and correction.

These changes on the extent and the applicability of the Bill are helpful and remove some confusing and ambiguous language. The removal of ‘profiling’ (i.e., predicting behaviour of) Data Principals in India, as an express ground for extra territorial application, along with the broad exclusion for public information, makes the Bill more permissive than global regimes.

Despite much debate, the Bill continues to treat all personal data as monolithic category rather than classifying into sensitive categories as is the case under current law and in much of the world. That said, based on criteria including volume and sensitivity of personal data processed, and its impact, entities who process such personal data on their own account, who continue to be referred to as data fiduciaries (“Data Fiduciaries”), can be classified as ‘significant’ and be subject to materially higher compliance obligations including appointing resident data protection officers, conducting data impact assessments, independent data audits and other requirements that may be specified.

b. Consent framework

While the operational consent framework largely remains the same as the Draft, there are certain differences. The Bill no longer requires notice to be provided in an ‘itemized’ manner. However, it also states

---

11 Section 30, Bill.
12 Right to Privacy has been recognized as a fundamental right under Article 21 by the Supreme Court in Justice K.S. Puttaswamy and Ors. v. Union of India (UOI) and Ors., (2019) 1 SCC 1 (“Puttaswamy Judgment”).
13 Section 3(a)(ii), Bill.
14 Article 3, GDPR; Section 4, Personal Information Protection and Electronic Documents Act, available here [read with Office of the Privacy Commissioner of Canada, 411Numbers ceases practice of removing information for a fee, March 25, 2019, available here].
15 Section 3(b), Bill.
16 Section 3(c), Bill. For similar exclusions globally, see Recital 18, GDPR; Section 4(1)(a), Personal Data Protection Act, 2012 (“PDPA”), available here.
17 Section 3(c), Bill.
18 Refer to our analysis on the Draft here and here.
19 Recital 71, GDPR.
20 The Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules, 2011 provide substantive protection only to a narrowly defined category of passwords; financial data (such as bank account or credit card or debit card or other payment instrument details); physical, physiological and mental health condition; sexual orientation; medical records and history; and biometric information.
21 Article 9, GDPR.
22 Section10, Bill.
23 Section 5(1), Bill. See also Section 6(1) of the Draft.
that the format for notice may be prescribed through delegated legislation24 and further requirements may be spelt out in such legislation. Perhaps to crystallize the principles of right to privacy under the Puttaswamy Judgment25, the additional language requiring consent for personal data to be ‘limited to such personal data that is necessary for the specified purpose’26 and the new illustration28 at the end of the clause have codified and emphasized the principles of data minimization and purpose limitation in the Bill.

While “specified purposes” may be drafted widely by the Data Fiduciaries in notices, rules that may be formulated with respect to consent and notice will provide additional guidance on what grounds in the consent notices may pass muster under the Bill.

Under the Bill, notice much be given each time consent is sought, and fresh notice must be provided where processing has been consented to previously.28 Allowing these notices to be received, and consents managed through the framework of consent managers which has been retained in the Bill, may help solve for some of the consent fatigue that may result from the above.

Data Fiduciaries can continue to process Data for whose processing consent was collected prior to enactment of the Bill29, by providing notice is prescribed form30, and in a move that will be welcomed by businesses, the Bill clarifies that Data Fiduciaries may continue to process personal data until the Data Principal withdraws consent31.

c. Legitimate Use

i. The concept of ‘deemed consent’, a novel basis for processing introduced in the Draft,32 perhaps taking inspiration from Singapore PDPA,33 has been replaced with the concept of ‘Legitimate Use’.34

While voluntary submission of personal data is still a basis for processing on grounds of legitimate use35 the requirement of a “reasonable expectation”36 of processing is gone. While the illustration to Section 7(a)37 alludes to the Data Principal withdrawing consent, how this will be done in cases where information is submitted on a one-off basis is unclear.

ii. The provision enabling processing by State has been made subject to compliance with applicable law or policy issued by the Central Government. Given that there were concerns raised during the consultation process on certain exceptions, this is a welcome move and may be a step towards data adequacy decision on data transfer across jurisdictions.38 Somewhat confusingly, there is also a requirement for such processing having been previously consented to for availing any subsidy39, or, somewhat contrarily “being available in any government register”40.

iii. Significantly, limited public interest exceptions and the reasonable purpose exceptions have retained as

---

24 Sections 5(1) and 40(2)(a), Bill.
25 Puttaswamy Judgment; Clause 8, Bill.
26 Section 6(1), Bill.
27 Illustration under Section 6(1) of the Bill.
28 Section 5(2), Bill.
29 Section 5(2), Bill.
30 Sections 5(2) and 40(2)(b), Bill.
31 Section 5(2)(b), Bill.
32 Section 8, Draft.
33 Section 15, PDPA.
34 Section 7, Bill.
35 Section 8(a), Bill.
36 Section 8(1), Draft.
37 Illustration b of Section 7(a), Bill.
38 Section 7(b), Bill.
39 Section 7(b)(i), Bill.
40 Section 7(b)(ii), Bill.
a separate clause in Chapter IV (Special Provisions) and other grounds, like mergers and acquisitions, and loan recovery have been substantially narrowed.\(^{41}\)

d. Retention and other Obligations of Data Fiduciaries

While the obligations largely remain the same, the Bill has sharpened the focus on data retention.

Unlike the Draft that had enabling language on ceasing to retain personal data (including by way of anonymization) and retain personal data as required for business purposes, the Bill imposes a hard obligation to erase (and cause processors to erase) personal data (other than where required for compliance with law), upon withdrawal of consent, or where the specified purpose of retention is no longer being served.\(^{42}\)

Importantly, the Bill deems that the purpose of retention is no longer being served where the Data Principal has not approached the Data Fiduciary for the particular purpose or exercising their rights for specific period which will be prescribed. Depending on the time period specified, this standard may prove too onerous for several types of Data Fiduciaries who have no direct contact with the Data Principal.

e. Processing of Children’s personal data

In a significant deviation from the Draft, the restrictions on processing personal data of children may be exempted for a class of Data Fiduciaries that are notified by the Government and subject to regulations that may be prescribed.\(^{43}\)

Further, subject to rules that may be formulated and demonstration of verifiably safe manner of processing personal data of children by the Data Fiduciary, the Central Government may exempt operation of some or all provisions of Clause 9 (Additional Obligations in relation to processing of personal data of children) for processing the personal data of children below the age of majority.\(^{44}\)

While the rules are yet to be formulated, this is a welcome move especially for the online education sector and organizations working with children from vulnerable background or who require support for mental or physical challenges.

f. Cross border transfer of personal data

Arguably, in the most significant change from the Draft Bill, Data Fiduciaries now have the ability to transfer personal data to any country other than countries of territories that may be notified\(^{45}\).

The Bill is also now clear that more restrictive sectoral norms on localization will continue to apply and closes the door firmly on a more permissive interpretation.\(^{46}\)

g. Exemptions

As indicated above, certain processing activities that had been included under the deemed consent exception in the Draft Bill have been moved to Chapter IV, which provides more broad-based exception to operative provisions of the Bill. While actions such as processing for judicial proceedings, court-based scheme and mergers and prevention and detection of offences have been added, in a material change, the exception for search engines has been removed.

However, very interestingly, along with the existing power to exempt applicability of certain provisions to certain Data Fiduciaries,\(^{47}\) the Central Government also has the power to notify certain Data Fiduciaries who may be exempt from operation of the Bill for a specified period of time. The exemption may be very beneficial to the start-up community and many new age technology innovators who will need time to realign their business processes.

h. Data Protection Board and power of Central Government

The provisions with respect to constitution and operation of Data Protection Board (“DPB”) have been significantly expanded in the Bill. The DPB now has the

\(^{41}\) Section 8(8) of the Draft Bill had exempted mergers and acquisitions, business transfers or corporate transactions, however Section 17(1)(e) of the Bill provides exemption only for court-based schemes
\(^{42}\) Section 8(7), Bill.
\(^{43}\) Section 9, Bill.
\(^{44}\) Section 10(1), Bill.
\(^{45}\) Section 16(1), Bill.
\(^{46}\) Section 16(2), Bill.
\(^{47}\) Section 18(1), Bill.
power to direct urgent or remedial mitigation measures in the event of a personal data breach. Very interestingly, even if the DPB powers appear to have been expanded, it is restricted from preventing entry into premises or taking any equipment into custody or otherwise adversely impacting the day to day operations of the person.48

The practical manner of implementation has to be seen,49 given that the DPB has the powers of a civil court to enforce attendance of persons, inspect books or document and require services of the police to conduct its investigation50. Further, expanding on the appeal process, the Bill prescribes that appeal against decisions of the DPB will lie with the TDSAT that has been designated as the appellate authority51.

Significantly, for repeat offenders, based on the recommendations of the DPB, the Central Government has the power to takedown offending applications or services52. This is a significant power and along with the high penalty thresholds, leaves Data Fiduciaries facing the spectre of significant business disruption for repeated non-compliance.

All in all, the Bill represents a uniquely Indian take on a modern data protection regime, which has benefitted significantly from the extensive consultations that followed the Draft. While the provisions are less prescriptive than some standards like the GDPR, it represents the requirement for a significant shift in current “state of the art” and indeed mindset of businesses in India surrounding privacy and personal data. In the next article in our series, we examine the key changes for Indian businesses, and how they can go about complying with the Bill, upon its enactment.

48 Section 28(8), Bill.
49 Section 28(9), Bill.
50 Section 28(7), Bill.
51 Section 29(1), Bill.
52 Section 37(1), Bill.
client alert

August 03, 2023

Key Contacts:

Cyril Shroff
Managing Partner
cyril.shroff@cyrilshroff.com

Arun Prabhu
Partner (Head - Technology & Telecommunications)
arun.prabhu@cyrilshroff.com

Arjun Goswami
Director - Public Policy
arjun.goswami@cyrilshroff.com

Contributors:

Arun Prabhu
Partner (Head - Technology & Telecommunications)

Arjun Goswami
Director - Public Policy

Anirban Mohapatra
Partner

Varun Mehta
Principal Associate

Arpita Sengupta
Senior Associate

Mahim Sharma
Senior Associate Designate

Anoushka Soni
Associate

Sabreen Hussain
Associate

Soumya Tiwari
Associate

Disclaimer

All information given in this alert has been compiled from credible, reliable sources. Although reasonable care has been taken to ensure that the information contained in this alert is true and accurate, such information is provided ‘as is’, without any warranty, express or implied as to the accuracy or completeness of any such information.

Cyril Amarchand Mangaldas shall not be liable for any losses incurred by any person from any use of this publication or its contents. This alert does not constitute legal or any other form of advice from Cyril Amarchand Mangaldas.

Should you have any queries in relation to the alert or on other areas of law, please feel free to contact us on cam.publications@cyrilshroff.com

Cyril Amarchand Mangaldas
Advocates & Solicitors

100+ years of legacy 1000 Lawyers Over 170 Partners

Peninsula Chambers, Peninsula Corporate Park, GK Marg, Lower Parel, Mumbai 400 013, India
T +91 22 2496 4455 E cam.mumbai@cyrilshroff.com W www.cyrilshroff.com
Presence also in Delhi-NCR | Bengaluru | Ahmedabad | Hyderabad | Chennai | GIFT City | Singapore