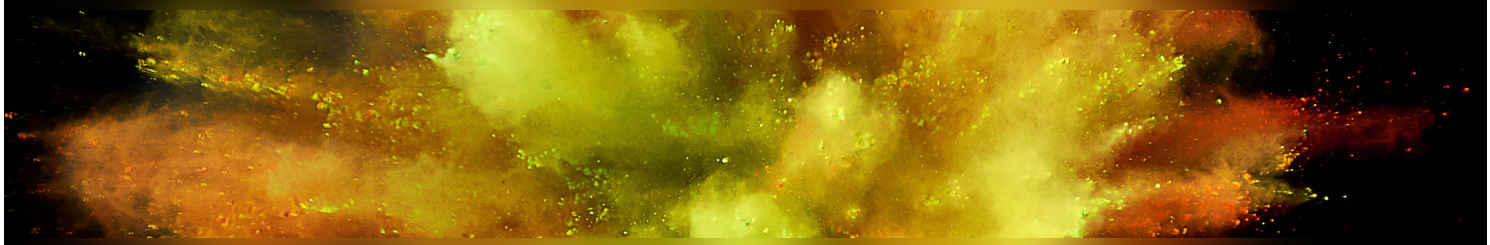
CLIFFORD
CHANCE

jsa
advocates & solicitors



DIGITAL PERSONAL DATA PROTECTION ACT:
INDIA'S NEW DATA PROTECTION FRAMEWORK

DIGITAL PERSONAL DATA PROTECTION ACT: INDIA'S NEW DATA PROTECTION FRAMEWORK

The Indian Parliament recently passed the long-awaited Digital Personal Data Protection Act, 2023 (the "**DPDPA**") into law.[1] The DPDPA, which was notified in the Official Gazette of India on 11 August 2023, is India's first comprehensive data protection law. It will overhaul the existing patchwork of rules on personal data privacy.

The DPDPA applies to any processing of digital personal data within India and, like the EU General Data Protection Regulation (the "**GDPR**"), also has extraterritorial reach in certain circumstances.

The DPDPA will sit alongside other new digital policy initiatives, including the Indian Telecommunications Act, the Digital India Act and the National Data Governance Policy.

Although it does not set out a defined transition period, the DPDPA's provisions are expected to become effective in a phased manner. India's Minister for Electronics and Information Technology has indicated in recent media interviews that the Indian government will prioritize the implementation of this law by larger technology companies and will offer more time to smaller entities and start-ups. However, no official indication has been given of the likely timetable for its overall implementation.

What is the DPDPA?

The DPDPA is a horizontal law that applies to businesses across all sectors. The past few years have seen an increase in data privacy laws being introduced across the Asia-Pacific ("**APAC**") region, and frequently lawmakers are taking inspiration from the GDPR. The DPDPA follows this trend by incorporating the seven key principles of data protection in the GDPR and, like recent legislative developments in Vietnam and Indonesia, is expected to trigger a sea-change in the way Indian businesses collect and handle personal data.

The statute introduces a broad definition of "personal information", creates transparent disclosure requirements for data controllers (referred to as "Data Fiduciaries" in the DPDPA) with an emphasis on notice and consent, establishes fairly strong data subject rights, provides for the possibility of limitations on cross-border data transfers, and places various obligations on data controllers to safeguard personal data.

Although inspired by the GDPR in terms of its basic principles, the final version of the law is far more concise. As a result, the DPDPA sets out compliance requirements and restrictions at a high level and delegates substantial rule-making powers to the Indian

1 Clifford Chance and J. Sagar Associates (JSA) are independent law firms that have collaborated to co-author this briefing. The firms are not affiliated or associated with each other.

government and a yet to be established Data Protection Board of India (the "**Board**"). These powers are not unlimited, however, and it is possible that the DPDPA's relatively simple approach, with only limited exceptions to general principles and a strong emphasis on data subject consent (*see discussion below*), may prove problematic for in-scope organizations.

What is the scope of the DPDPA?

The DPDPA applies – with limited exceptions – to any processing of digital personal data within India. It also applies to processing carried out by organizations outside India in connection with the offering of goods or services in India.

The term "personal data" is defined broadly and covers any data about an individual who is identifiable by or in relation to such data. Interestingly, the DPDPA does not create subcategories of personal data, and its provisions apply uniformly irrespective of the sensitivity of datasets being processed. Statutes in other jurisdictions, such as Singapore and Hong Kong, have taken this approach, although regulators have subsequently implemented guidance notes and codes of practice highlighting certain categories of information that may be considered sensitive and stating that, where appropriate, personal data of a sensitive nature should be subject to a higher standard of protection.

"Processing" under the DPDPA is limited to an operation (such as collection, use, storage, transfer, etc.) performed on digital personal data that is *wholly* or *partly automated*. Therefore, unlike the GDPR, the DPDPA does not seek to regulate a processing operation or activity that is wholly manual or non-automated.

The DPDPA exempts the processing of publicly available personal data. However, the exemption is limited to data made publicly available by the data subjects themselves or pursuant to a legal requirement to publish. Businesses that rely on public information, such as web crawlers and telemarketing agencies, will therefore not be able to assume that their activities are exempt but will need to carefully consider the scope and application of the DPDPA. On the other hand, note the very broad scope of the exemption by international standards. For example, the GDPR provides a similar exemption, but only to its specific restrictions on the processing of particularly sensitive personal data; and Singapore law exempts publicly available information only from its consent requirements but not from the law as a whole.

Finally, the DPDPA also excludes from its territorial scope the processing of personal data belonging to offshore individuals, when such processing is undertaken in India pursuant to a contract between any person located in India and a person located outside India. This exemption seeks to benefit Indian outsourcing companies that routinely process data belonging to persons located outside of India, although it will likely also remove the possibility of the EU and similar jurisdictions treating India as providing adequate protection for personal data transferred to such companies.

What are the key requirements and restrictions for data processing?

Grounds for processing

As in many jurisdictions in the APAC region, consent is the primary ground for processing personal data under the DPDPA. Consent of a data subject is mandatory unless processing is carried out for one of the "legitimate uses" described in the DPDPA (*discussed below*). Such consent must be free, specific, informed, express and limited to the personal data necessary for fulfilling the specific purposes. This, in effect, introduces a 'purpose limitation' for the collection of personal data, and suggests that opt-in is the preferred approach.

The DPDPA does permit processing without consent for certain "legitimate uses". These are limited, but they include the processing of information for employment purposes, and where information is voluntarily disclosed by a data subject for a specific purpose. They also include processing in response to a medical emergency. Although these will be helpful to bridge the gap between the consent requirement and the wide range of processing operations which should reasonably be expected to go ahead irrespective of consent, the pre-GDPR European experience suggests that the absence of a relatively broad "legitimate interests" concept to justify processing without consent is likely to prove problematic for Indian businesses building DPDPA compliance programmes. It appears, for example, that all processing of personal data for direct marketing purposes will require prior opt-in consent, even in a B2B context.

Consent notice

While obtaining consent, a controller must provide data subjects with a notice that describes (a) the types of personal data processed; (b) the purposes of processing; (c) the method to be used to exercise data subject rights and make complaints to the regulator; and (d) contact details of the data protection officer (where required) or a contact person for individuals to contact to exercise their data subject rights.
The requirement to give notice is built into the process of obtaining consent and does not arise where processing is based on "legitimate use". The DPDPA requires controllers to translate consent notices into each of India's 22 national languages and empowers the Indian government to impose further requirements under rules for implementation. For instance, a recent Parliamentary Committee Report on the DPDPA suggests that organizations may be required to provide videos and animations to help individuals understand the notice and consent form.

Data Security and Breach Reporting

A data controller must implement reasonable security safeguards and appropriate technical and organizational measures to ensure compliance with the DPDPA and prevent personal data breaches. Upon the occurrence of a data breach, the law requires a controller to notify the Board and *each affected data subject* of the incident. The form and manner of such reporting must comply with the implementing rules that are to be issued by the Indian government.

Notably, unlike the GDPR and many data privacy laws in the APAC region, the DPDPA does not create a threshold of risk or harm for breach reporting. This suggests that, at least in theory, it may be necessary to report very large numbers of minor personal data

breaches – which has been a problem in Europe under the GDPR even with the inclusion of limited thresholds. On the other hand, there is no specific timeline for reporting – a 2021 draft, based (in this respect) on the GDPR, required data breaches to be reported within 72 hours of the data controller becoming aware of them.

It should also be noted that all data controllers already have an obligation to report data breaches and other specified cyber incidents (of all kinds, regardless of materiality) to a nodal agency, namely CERT-In (Computer Emergency Response Team – India). The DPDPA does not seek to discontinue this obligation, and, as a result, controllers will have to file at least two reports for each breach. Interestingly, many controllers have adopted a risk-based approach to reporting incidents to CERT-In and are in practice choosing only to report incidents that are material or are also reportable under sector-specific laws to other regulators (for instance, the Reserve Bank of India).

Data Erasure and Retention Periods

The DPDPA requires data controllers to erase personal data when consent is withdrawn or when it is reasonable to assume that the specified purpose is no longer being served.

Crucially, the DPDPA also empowers the Indian government to prescribe maximum retention periods for personal data. In other words, the government may prescribe the period within which personal data must be purged in certain circumstances, such as when the data subject does not contact the data controller for the performance of the specified purpose. The government may set different retention periods for different classes of controllers and for different purposes of processing. This provision will require controllers to formulate their data retention schedules in a manner consistent with the prescribed periods and to ensure that personal data is periodically purged or de-identified.

Relationship with Processors

Like the GDPR, the DPDPA recognizes the difference between controllers (or Data Fiduciaries) – who determine the purposes and means of processing of personal data – and processors, who merely process personal data on their behalf, both in terms of responsibilities and liability for contraventions. It allows controllers to engage third-party processors through written agreements but places the compliance burden solely on controllers. Controllers must, for instance, ensure that processors implement safeguards to protect personal data and erase such data when required to do so under the law. Unlike under the GDPR, for example, processors themselves have no obligations or responsibilities under the DPDPA, and, barring the requirement to have a valid contract, no specific conditions are prescribed with respect to the sharing of personal data between controllers and processors.

What are Significant Data Fiduciaries?

The DPDPA empowers the Indian government to identify a data controller or a class of data controllers as "Significant Data Fiduciaries" based on factors such as the volume and sensitivity of data being processed, and the level of risk presented to the rights of data subjects. This concept is broadly equivalent to the various tests in the GDPR for the application of some of its "accountability" requirements, but with a greater degree of discretion in the hands of government.

Significant Data Fiduciaries have specific obligations over and above those applicable to general data controllers. These include appointing a Data Protection Officer based in India, appointing an independent data auditor, and conducting periodic Data Protection Impact Assessments (DPIAs) and data audits.

Note that the Indian government recently carried out a similar risk-based classification exercise for social media platforms under India's intermediary rules. These rules classify any social media platform that has more than five million registered users as a "Significant Social Media Intermediary" (SSMI) and subjects them to additional obligations.

Can personal data be transferred outside of India?

The transfer of personal data for processing outside India is generally permitted under the DPDPA. However, the law empowers the Indian government to identify specific countries or territories to which data transfers are prohibited. At present, the government has not given any indication of the countries that may feature on this list.

Although earlier iterations of the law contemplated a 'white-list' approach, i.e., allowing transfer only to a specific list of pre-approved territories, the government has yielded to industry pressure, and the current version of the DPDPA provides a more favourable 'blacklist' approach. This, of course, contrasts with the strict requirements under the GDPR. Some other APAC jurisdictions, including Indonesia and Singapore, have taken a broadly similar, although more flexible, approach than that of the GDPR, imposing a requirement on organizations transferring personal data overseas to ensure the recipient complies with adequate standards (for example, that it is subject to legally binding obligations that contain the same or a higher level of protection as is afforded under the local law).

The DPDPA also clarifies that, if its provisions on international data transfer conflict with other Indian laws, the law which provides a higher degree of protection or restriction on cross-border transfers will prevail. Consequently, sector-specific regulations, such as the RBI's data localization mandate with respect to payment system data, will continue to apply notwithstanding the liberal position contained in the DPDPA.

How should personal data of children be handled?

Data controllers can only process a child's (*i.e., any individual below 18 years of age*) data after obtaining the verifiable consent of a parent or a guardian. Moreover, any tracking and behavioural monitoring of children or targeted advertising towards children is prohibited. Notably, this restriction applies to all controllers and is not specifically applicable to controllers that focus on processing children's data or are otherwise aware that they are collecting and processing children's data. Consequently, controllers that do not target children do not enjoy any plausible deniability and must, presumably, act as though they are likely to collect and process children's data unless they have a high degree of confidence that this will not, in fact, be the case.

The law does not explain how a data controller is expected to obtain "verifiable consent", and such guidance will likely be provided by the government through implementing rules.

Notably, the government may exempt certain data controllers from these additional obligations based on the type of processing or controller involved. For instance, where an Ed-Tech platform caters to children's education, parental consent may be made mandatory for data subjects below 15 (rather than 18) years of age. However, in order to rely on this exemption, a controller would need to demonstrate to the government that its processing is verifiably safe.

What rights do data subjects have?

Data subjects have the following key rights under the DPDPA:

- A right to access information regarding the personal data being processed.
- A right to withdraw consent.
- A right to correct, erase or update personal data.
- A right to redress for grievances.
- A right to appoint a nominee to exercise rights in case of death or incapacity.

Data controllers will need to revisit existing mechanisms (if any) to deal with data subject access requests. Controllers will also have to be more proactive and transparent in dealing with grievances or complaints with respect to their data processing activities.

What is the regulatory body's role?

The Board will be an independent body established by the Indian government to oversee regulatory compliance with the DPDPA. The Board will act as the forum for a fully 'digital by design' online complaint resolution mechanism for data subjects. It will also act as a supervisory body in the event of any data breaches or any other non-compliance with the DPDPA and impose penalties under the DPDPA as it may deem fit.

Notably, any appeals from the Board's decisions must be directed to the Telecom Disputes Settlement and Appellate Tribunal, This was a surprising choice given that processing of digital personal data is governed by the Ministry of Electronics and Information Technology, not the government's telecommunications department.

What are the consequences of non-compliance?

Non-compliance with the provisions of the DPDPA may lead to the imposition of significant penalties. Failure by a data controller to take reasonable security measures may lead to a penalty of up to INR 250 crores (approximately USD 30 million), whereas failure to notify a personal data breach or comply with children's data protection requirements may lead to penalties of up to INR 200 crores (approximately USD 24 million). Penalties for any other non-compliance may range from INR 50 crores (approximately USD 6 million) to INR 150 crores (approximately USD 18 million). The procedure for imposition of these penalties is to be separately prescribed.

When will the law be implemented?

The DPDPA is expected to be brought into force in a phased manner, and the Indian government is expected to notify specific chapters or sections of the law for commencement over a period.

Media reports suggest that implementation will begin with Big Tech companies, while smaller entities will be given a longer transition period. This suggests that, as part of the initial implementation plan, the government may identify large global conglomerates with a significant presence in India as Significant Data Fiduciaries.

What are the next steps for businesses?

Data controllers will need to move swiftly to evaluate their current data processing practices to assess gaps in compliance with the DPDPA, with a view to implementing necessary changes before the relevant requirements take effect. They will need to adopt a flexible approach in the short term, however, taking account of the accompanying rules and guidance that are yet to be published by the Indian government and the Board. Below are a few key matters for data controllers to consider:

- **Data flows and tracking personal data:** Data controllers should map their personal data flows and understand their current processing activities with respect to Indian personal data.
- **Consent requirements:** Except in limited circumstances where it can rely on a "legitimate use" exception, a data controller will need to either obtain opt-in consent from a data subject or rely on existing consent to process personal data. Therefore, controllers should immediately examine existing grounds for the processing of personal data and evaluate whether fresh consent from data subjects will be required once the law takes effect.
- **Revise privacy notices and policies:** Data controllers should consider amending the form and content of privacy policies and consent notices to conform with the provisions of the new legislation. Consent notices must contain the requisite information and should be translated into local languages to comply with the provisions of the new law.
- **Breach reporting:** The new law requires mandatory reporting of incidents to impacted data subjects regardless of their magnitude or risk of harm. This may be a significant departure from the existing policies of companies, where breach reporting is limited to large-scale incidents. These policies will need to be re-evaluated by data controllers and modified.
- **Children's data:** Data controllers will need to evaluate their current practices with respect to the data of children (customers / users below 18 years of age) and ensure that verifiable parental consent has been obtained for such processing. Data controllers compliant with foreign laws will need to re-examine their practices in India given the difference in the age thresholds applicable.

Of course, many international businesses with operations in India, or that will otherwise be subject to the DPDPA, have already developed sophisticated compliance arrangements designed to address the requirements of the GDPR and/or other data protection laws. These businesses will need to conduct a careful gap analysis to identify the respects in which these arrangements can / need to be rolled out to their Indian operations to facilitate DPDPA compliance. GDPR compliance arrangements, in particular, may need to be adjusted to take account of the DPDPA's consent-based approach, which is alien to the GDPR compliance culture. For these purposes compliance approaches developed in the APAC region, where a consent-based approach to data protection is more common, may provide a helpful model.

AUTHORS

J. SAGAR ASSOCIATES (JSA)

Probir Roy Chowdhury
Partner
T: +91 80 4350 3618
E: probir@
jsalaw.com

Yajas Setlur
Partner
T: +91 80 4350 3638
E: yajas.setlur@
jsalaw.com

Pranavi Pera
Senior Associate
T: +91 80 4350 3639
E: pranavi.pera@
jsalaw.com

CLIFFORD CHANCE

Arnav Joshi
Senior Associate
London
T: +44 207006 1303
E: arnav.joshi@
cliffordchance.com

Sian Smith
Senior Associate
Singapore
T: +81 3 6632 6320
E: sian.smith@
cliffordchance.com

Richard Jones
Senior Associate
Knowledge Lawyer
London
T: x+44 207006 8238
E: richard.jones@
cliffordchance.com

CLIFFORD CHANCE DATA PROTECTION CONTACTS

APAC

Stella Cramer
Partner
Singapore
T: +65 6410 2208
E: stella.cramer@cliffordchance.com

Lena Ng
Partner
Singapore
T: +65 6410 2215
E: lena.ng@cliffordchance.com

Ling Ho
Partner
Hong Kong
T: +852 2826 3479
E: ling.ho@cliffordchance.com

Terry Yang
Partner
Hong Kong
T: +852 2825 8863
E: terry.yang@cliffordchance.com

Clarice Yue
Counsel
Hong Kong
T: +852 2825 8956
E: clarice.yue@cliffordchance.com

Natsuko Sugihara
Partner
Tokyo
T: +81 3 6632 6681
E: natsuko.sugihara@cliffordchance.com

Michihiro Nishi
Partner
Tokyo
T: +81 3 6632 6622
E: michihiro.nishi@cliffordchance.com

Tim Grave
Partner
Sydney
T: +61 2 8922 8028
E: tim.grave@cliffordchance.com

USA

Devika Kornbacher
Partner
Houston
T: +1 713 821 2818
E: devika.kornbacher@cliffordchance.com

Megan Gordon
Partner
Washington DC
T: +1 202 912 5021
E: megan.gordon@cliffordchance.com

EMEA

Daniel Silver
Partner
New York
T: +1 212 878 4919
E: daniel.silver@cliffordchance.com

Jonathan Kewley
Partner
London
T: +44 207 006 3629
E: jonathan.kewley@cliffordchance.com

Simon Persoff
Partner
London
T: +44 207 006 3060
E: simon.persoff@cliffordchance.com

Dessislava Savova
Partner
Paris
T: +33 1 4405 5483
E: dessislava.savova@cliffordchance.com

Holger Lutz
Partner
Frankfurt
T: +49 69 7199 1670
E: holger.lutz@cliffordchance.com

Fernando Irurzun
Partner
Madrid
T: +34 91 590 4120
E: fernando.irurzun@cliffordchance.com

Jack Hardman
Partner
Dubai
T: +971 4503 2712
E: jack.hardman@cliffordchance.com

Jaap Tempelman
Senior Counsel, Amsterdam Tech Group Co-Head
T: +31 20 711 9192
E: jaap.tempelman@cliffordchance.com

Andrei Mikes
Counsel
Amsterdam
T: +31 20 711 9507
E: andrei.mikes@cliffordchance.com

Andrea Tuninetti Ferrari
Counsel
Milan
T: +39 02 8063 4435
E: andrea.tuninettiferrari@cliffordchance.com

CLIFFORD
CHANCE

jsa
advocates & solicitors

www.cliffordchance.com

Clifford Chance, 10 Upper Bank Street, London, E14 5JJ

2308-007534