Baker McKenzie.

September 2023

India: India's Digital Personal Data Protection Act - What should United States companies do now?

In brief

Following a five-year legislative process, India's **Digital Personal Data Protection Act** (DPDP) received presidential assent on 11 August 2023. Practically speaking, the DPDP is not yet enforceable as the government still needs to establish the Data Protection Board of India (Board), which will serve as the enforcement authority for the law. The Board, in turn, must implement certain legally binding rules before the DPDP becomes fully operational. This process is expected to unfold over the next 8-12 months, although it could take longer and the national elections in 2024 may further delay the DPDP's implementation.

For now, US companies doing business in India should continue to comply with current privacy laws in India, which consist largely of the Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules, 2011 (**SPDI Rules**). In parallel, companies should monitor implementation developments and, when more concrete details emerge, consider how they will leverage existing **GPDR** and **CCPA** compliance mechanisms to help gear up for when the DPDP formally replaces and supersedes the SPDI Rules.

Following is a look at some of the main rules and requirements under the DPDP.

Who & what data is protected?

The DPDP uses different terminology than the GDPR, but its scope is quite similar. The DPDP protects the "digital personal data" of a "data principal"—i.e., the individual to whom certain personal data relates. "Personal data" includes any data about an individual who is identifiable by or in relation to such data, as under the GDPR, and the DPDP is focused on personal data in digital form. For simplicity, we refer to "personal data" instead of "digital personal data" throughout this article.

A "data principal" can be any person anywhere in the world, as under the GDPR—whereas the CCPA only protects California residents. The term includes the parent of a child under the age of 18, or the lawful guardian of a disabled individual acting on their behalf, where the personal data relates to the child or disabled individual.

The DPDP applies to the processing of personal data within the territory of India. Like the GDPR does with respect to the EU, the DPDP also expressly applies to processing of personal data outside of India where such processing is in connection with any activity related to offering of goods or services to data principals in India. But unlike the GDPR, the DPDP does not expressly apply to persons outside of India that monitor the behavior of individuals in the country.

The DPDP does not apply to processing of personal data by an individual for personal or domestic purposes—which is similar to the GDPR and CCPA—or to personal data that the data principal made publicly available—which is similar to the CCPA but different from the GDPR. The DPDP also does not apply to personal data that was made publicly available by someone who was legally obliged to make it publicly available.

The Federal Government of India (Federal Government) has the authority to exempt certain government agencies and data processing activities from the DPDP's requirements, such as for research, national security, and other public policy purposes. The Federal Government may also exempt certain types of entities, such as start-ups, from the DPDP's application.

Who must comply?

Persons that act as a "data fiduciary" must comply with the DPDP. A data fiduciary is a person who, alone or in conjunction with other persons, determines the purpose and means of processing of personal data, similar to a "controller" under the GDPR. The DPDP defines "data processor" as a person who processes personal data on behalf of a data fiduciary.

The DPDP does not impose any obligations directly on data processors, except for a certain type of processor called a "consent manager." A consent manager is a person registered with the Board who acts as a single point of contact on behalf of a data fiduciary to enable a data principal to give, manage, review, and withdraw their consent with respect to that data fiduciary through an accessible, transparent, and interoperable platform. Consent managers are accountable to the data principal and required to act on the data principal's behalf.

The DPDP also refers to "intermediaries," which include telecoms, network, and web-hosting service providers, search engines, and online payment sites. The DPDP authorizes the Federal Government to block access to certain online information that a data fiduciary makes available in the interest of the public—after giving the data fiduciary an opportunity to be heard—and order intermediaries to block access to such information as well.

How to comply?

Data fiduciaries

Notice & legal basis.
In general, a data fiduciary must provide notice and obtain consent from a data principal before processing their personal data. The notice is required to inform the data principal of:

- The personal data to be processed and purpose for which such data is to be processed
- The manner in which the data principal may exercise rights under the DPDP
- The manner in which the data principal may make a complaint to the Board

Consent must be free, specific, informed, unconditional and unambiguous, and given with clear affirmative action. The DPDP's consent requirements also include a data minimization concept: Consent signifies an agreement to the processing of the data principal's personal data for the specified purpose and is limited to personal data that is necessary for such specified purpose.

A data principal has the right to withdraw consent given for processing of their personal data. On withdrawal of consent, the data fiduciary may no longer process personal data and must cause its data processors to cease processing the personal data within "a reasonable time."

There are a number of exemptions to the notice and consent requirements. A data fiduciary does not have to obtain consent where the processing is for certain "legitimate uses." One such "legitimate use" contemplates a sort of implied consent scenario though the statute does not use this term. In particular, the law does not require a data fiduciary to obtain consent where the processing is for a purpose that has been specified to the data principal, the data principal voluntarily provided their personal data to the data fiduciary, and the data principal has not indicated to the data fiduciary that the data principal does not consent to the use of their personal data. The law lists a number of illustrations that suggest this "implied consent" concept may be narrowly interpreted.

The law lists other legitimate uses, including the processing of personal data for employment purposes, to comply with Indian laws, and to respond to medical emergencies and disasters. A data fiduciary is also not required to provide notice or obtain consent in certain limited scenarios, including as necessary to enforce legal rights and claims, and to prevent contraventions of the law. One of the scenarios listed that is interesting is where a company in India processes the personal data of individuals outside of India as part of a contractual arrangement with a company outside of India.

Data pincipal rghts

Data fiduciaries must observe specific requirements with regard to data principals' rights under the DPDP, which include the following:

- **Access Right.** A data principal may obtain (a) a summary of personal data being processed by the data fiduciary and the processing activities undertaken by the data fiduciary with respect to personal data, (b) identities of all data fiduciaries and data processors with whom the personal data has been shared by the data fiduciary along with the description of the personal data so shared and; (c) any other information related to the personal data and its processing as may be prescribed by the Federal Government.
- **Correction Right.** The data principal may correct, complete, and update their personal data.
- **Right of Erasure.** The data principal may request for erasure of their personal data which is incorrect or no longer necessary for the purpose for which it was processed unless retention is necessary for a legal purpose. On receipt of such a request of erasure, the data fiduciary must erase the personal data unless retention of the same is necessary for the specified purpose or for compliance with law.
- **Consent Withdrawal.** As noted earlier, a data fiduciary that processes personal data according to the data principal's consent must honor their withdrawal of consent. Unlike the right of erasure, the data principal must honor a withdrawal even if retention is necessary to fulfill a purpose that was specified to the data principal.
- **Grievance Redressal Right.** Data principals have the right to have readily available means of grievance redressal provided by a data fiduciary with respect to privacy matters, and the data fiduciary must respond within timelines to be prescribed. A data principal must exhaust the right to grievance redressal before approaching the Board on any grievance / issue of theirs.
- **Nomination Right.** A data principal may nominate any other individual to exercise their rights under the DPDP in the event of their death or incapacity (unsoundness of mind or infirmity of body).

Additional Obligations

Data fiduciaries are further subjected to the below requirements:

- **Accuracy.** The data fiduciary is required to ensure the accuracy, completeness, and consistency of the personal data when such personal data is processed, including when it needs to make a decision that affects the data principal or if the personal data is likely to be disclosed to another data fiduciary.
- **Reasonable Security Practices & Procedures.** The data fiduciary needs to protect personal

data in its possession or under its control by taking reasonable security safeguards to prevent a personal data breach.

The DPDP defines “personal data breach” to mean any unauthorized processing, disclosure, use, alteration, or loss of personal data that compromises the confidentiality, integrity, or availability of the data.

- **Breach Notification.** In the event of a personal data breach, the data fiduciary must notify the Board and each affected data principal. This requirement does not alter potential obligations to report under the Information Technology (The Indian Computer Emergency Response Team and Manner of Performing Functions and Duties) Rules, 2013 and the CERT-In's direction relating to information security practices, procedures, prevention, response, and reporting of cyber incidents for a Safe & Trusted Internet.
- **Significant Data Fiduciaries Duties.** It is up to the Federal Government to classify a data fiduciary or class of data fiduciary as a Significant Data Fiduciary (SDF) based on certain factors such as the volume and sensitivity of the data they process, the risk of harm to data principals, potential impact on the sovereignty and integrity of India, and similar issues. An SDF is subject to additional obligations including to appoint a DPO in India, appoint an independent data auditor and undertake a data protection impact assessment in certain circumstances.
- **Ultimate Responsibility.** The data fiduciary has the ultimate responsibility of complying with the DPDP irrespective of whether processing is undertaken by a processor. This includes the requirement to Implement appropriate technical and organizational measures to ensure effective adherence with the provisions of the DPDP.
- **Cross-Border Data Transfers.** The DPDP currently allows free cross-border transfers of data. However, the law contemplates that the Federal Government may blacklist countries or territories and restrict transfers of personal data to them based on how thy protect personal data. The PDPD does not contain data residency requirements, like the GDPR and CCPA, but unlike earlier versions of the draft Indian Personal Data Protection Law of 2018.
- **Children's Data.** Data fiduciaries are required to obtain verifiable consent prior to processing a child's personal data from their parent, or personal data of a disabled person from their lawful guardian. A “child” is an individual under 18. The DPDP does not prescribe any requirements on how to ascertain whether a data principal is a child or a person with disabilities. In addition, there are prohibitions on processing children's personal data in a manner that is likely to cause a detrimental effect to the child, tracking and behavioral monitoring of children, and directing targeted advertising at children. Keeping in mind the booming education tech industry in India, the Federal Government may exempt a data fiduciary from some or all of the above restrictions, in respect of children above a certain age, if it is satisfied that the data fiduciary has ensured that processing of personal data of such children is done in a manner that is verifiably safe.
- **Translations.** The DPDP recognizes the 22 official languages of India, listed in the eighth schedule of the Indian Constitution. The data fiduciary is required to give an option to the data principal to access a request for consent and privacy notice in English or any of India's official languages.

Data Principals

Under the DPDP, data principals must:

- Not impersonate another person while providing personal data
- Not suppress any material information while providing personal data for any document, unique identifier, proof of identity or proof of address issued by the State or any of its agencies
- Not register a false or frivolous grievance or complaint with a data fiduciary
- Furnish only such information as is verifiably authentic, while exercising the right to correction or erasure.

Sanctions & Remedies

Once the Board has been established, it will have exclusive authority to enforce the DPDP. There is no private right of action and civil courts in India do not have jurisdiction to enforce the DPDP. The DPDP excludes the jurisdiction of civil courts to entertain any suit or proceeding relating to any matter for which the Board is empowered. Thus, the Board is supreme in terms of sanctions and remedies.

If the Board finds that there has been a "significant" violation of the DPDP—the law does not define "significant"—the Board may impose a monetary penalty. Different penalties are prescribed for different types of non-violations, with the maximum penalty of INR 2.5 Billion (approx. USD 300 million) reserved for failure by a data fiduciary to take reasonable security safeguards to prevent personal data breach.

When determining the amount of a monetary penalty, the Board may consider:

- The nature, gravity and duration of the breach
- The type and nature of personal data affected by the breach
- The repetitive nature of the breach
- Whether a person has realized a gain or avoided a loss as a result of the breach
- Whether a person has taken any action to mitigate the effects of the breach, and the effectiveness of such steps
- The likely impact of the penalty on the data fiduciary subject to the penalty.

Parties who may be liable for penalties under the DPDP include:

- A data fiduciary with respect to a personal data breach or a breach of its obligations with respect to personal data and data principal rights
- A consent manager with respect to a breach in observance of its obligations in relation to a data principal's personal data, or breach of any condition of registration of the consent manager
- An intermediary, for breach of its obligation to block access to information when directed to do so by the Federal Government
- A data principal, who may be subject to a penalty of up to INR 10,000 if they contravene the DPDP.

A data principal may seek compensation for DPDP breaches from parties that breached their duties, but there is no private right of action. Data principals may complain to the Board, which has discretion on whether to take action against the relevant party. The Board is allowed to accept a voluntary undertaking in respect of any matter related to compliance with provisions of DPDP from any person at any stage of complaint proceedings. The Board may vary the terms of the voluntary undertaking if it deems fit. This voluntary undertaking may take the form of the person taking or refraining from taking certain actions.

On filing of a voluntary undertaking, there would be a bar on proceedings pertaining to the subject matter of the undertaking, unless the relevant party fails to adhere to its terms. The Board may require the undertaking to be made public. If the party does not adhere to the terms of the undertaking, such breach would be treated as a breach of the DPDP, and the Board has a right to impose a penalty for such breach.

Contact Us

Lothar Determann
Partner
lothar.determann
@bakermckenzie.com

Helena Engfeldt
Partner
helena.engfeldt
@bakermckenzie.com

Jonathan Tam
Partner
jonathan.tam
@bakermckenzie.com