S&R

Data+

India's New Data Protection Regime: Tracking Updates and Preparing for Compliance

Introduction

The Digital Personal Data Protection Act, 2023 (the "**DPDP Act**" or the "**Act**"), published in India's official gazette last year, is a new law regulating the collection, storage, use and processing of personal data. The DPDP Act will take effect from the date(s) notified by the Indian Government ("**Government**"), and different dates may be notified for different provisions of the Act. Further, several provisions of the Act require specific rules which are yet to be notified.

According to a recent statement made by the new union minister of the Ministry of Electronics and Information Technology ("**MeitY**"), the new rules are in advanced stages of drafting and are expected to be released for industry wide consultation in the near future. These reports also suggest that the Government is in the process of creating a "digital-by-design" platform in order to facilitate smooth implementation of the DPDP Act.

In general, the DPDP Act seeks to establish a regulatory framework for the purpose of protecting the digital personal data of 'data principals'. To this end, it imposes obligations and limitations on data processing by 'data fiduciaries' (see below for a discussion on data principals and data fiduciaries, respectively). The published version of the DPDP Act contains certain incremental changes relative to the draft released in 2022 (the "**2022 Draft**"). For a comparison of the DPDP Act with the 2022 Draft, see our note here.

Applicability and Overview of the DPDP Act

The DPDP Act seeks to overhaul the current legal framework governing personal data in India (such current framework, the "**Existing Regime**"). For a broad overview of the Existing Regime and India's legislative trajectory with respect to governing personal data, see our notes here and here.

All entities need to check whether and to what extent the DPDP Act applies to them and their operations. Other than certain types of start-ups, no other organizational category has been explicitly referred to as qualified for exemption under the Act. Further, such exemptions may be subject to governmental discretion and extend to some, but not all, of the Act's provisions.

Accordingly, data fiduciaries need to comply with the Act's requirements unless they have been expressly exempted pursuant to a governmental notification. Further, the DPDP Act provides for extra-territorial application with certain exemptions – for a discussion in this regard, see here. Given the indicative financial penalties, non-compliance and/or breaching obligations under the DPDP Act may be costly. For a discussion on the wide applicability of the DPDP Act, see our note here.

Personal Data

The DPDP Act defines both 'personal data' and 'processing' broadly. As a result, various automated operations that companies routinely perform on, or with respect to, digitized data are likely to come under the ambit of the Act. For a discussion on what 'digital personal data' entails and an overview of the various types of information that may constitute 'personal data', see our notes here and here.

For the purpose of preparing for, and complying with, obligations under the Act, it would be advisable for all organizations to undertake data mapping exercises and data audits *inter alia* in order to facilitate the identification and determination of 'personal' information from mixed or legacy databases and/or organizational datasets. For further discussion in this regard, see our note here.

Main Entities under the Act

The key entities identified under the DPDP Act are as follows:

1. A "**data principal**" is an individual to whom the personal data relates and includes the parents or lawful guardian of such individual if the individual is a 'child' or a person with disability. Certain additional obligations apply for the processing of children's data. In this regard, see our notes here and here.

2. A "**data fiduciary**" is a person that determines the purpose and means of processing digital personal data by itself or in conjunction with other persons. In addition, the Government may notify any data fiduciary (or a class thereof) as a "**significant data fiduciary**" ("**SDF**"). For a discussion on SDFs and their additional obligations in the context of the 2022 Draft, see our note here. To read our analyses on key evaluative parameters for making SDF classifications under the 2022 Draft, see here and here.

3. A "**data processor**" is any person who processes personal data on behalf of a data fiduciary.

4. In addition, data principals will be allowed to give, manage, review or withdraw their consent through a "**consent manager**". For a discussion on the potential use of consent managers through India's digital public infrastructure, see our notes here and here.

Taking Stock: Transfer of Data; Notice and Consent Requirements

Consent is identified as one of the grounds for processing personal data under the DPDP Act. The Act sets forth specific requirements related to obtaining valid consent, including requirements for such consent to be informed and specific. With respect to notice and consent requirements, organizations should be prepared to go back to individuals once the Act becomes effective. Organizations that collect, process and monetize personal data need to ascertain where, how and whose personal information is lodged within their systems.

For an overview on organizational planning for managing consents under the DPDP Act, see our note here.

Unlike the General Data Protection Regulation ("**GDPR**") of the European Union, the DPDP Act does *not* classify data into 'sensitive' or 'special' categories. Accordingly, a wide variety of entities and data

processing activities may fall under the ambit of the Act. For a discussion on 'sensitive' personal information, see our note here.

Importantly, a transfer of personal data outside India is allowed subject to certain qualifications. However, organizations will need to monitor entities in their supply chains, such as suppliers and vendors, about data processing obligations, and review existing contractual arrangements. In this regard, for a discussion on contractual arrangements with data processors, including in terms of due diligence, risk assessment, transferring liability, indemnification, confidentiality, data security, business continuity and disaster recovery, see our note here.

Relatedly, organizations may need to consider improving their information technology and cybersecurity systems to meet new compliance requirements under the DPDP Act, including in respect of a breach.

*This insight has been authored by **Dr. Deborshi Barat** (Counsel) and **Reshma (Vaidya) Gupte** (Counsel). They can be reached at dbarat@snrlaw.in and rgupte@snrlaw.in, respectively, for any questions. This insight is intended only as a general discussion of issues and is not intended for any solicitation of work. It should not be regarded as legal advice and no legal or business decision should be based on its content.*

S&R ASSOCIATES ADVOCATES

NEW DELHI
Max House
Tower C, 4th Floor
Okhla Industrial Estate Phase III
New Delhi 110 020
Tel: +91 11 4069 8000

MUMBAI
One World Center
1403 Tower 2 B
841 Senapati Bapat Marg, Lower Parel
Mumbai 400 013
Tel: +91 22 4302 8000