

All Aboard: Getting Ready for India's New Data Protection Journey

The Digital Personal Data Protection Act, 2023 (the “DPDP”) is ready to (re)define the legal framework governing personal data in India.

But are companies and firms ready?

Which Companies/Firms?

All organizations need to check whether and to what extent the DPDP applies to them and their operations, as mentioned in our previous [note](#). Other than certain kinds of start-ups – *i.e.*, eligible India-incorporated private limited companies, partnership firms or limited liability partnerships which are recognized start-ups pursuant to government-notified criteria and processes – no other organizational category has been explicitly referred to as qualified for exemption under the DPDP. Further, even such exemptions will be subject to governmental discretion and extend to some – but not all – of the DPDP's provisions.

While certain prior iterations of the new law had sought to exempt ‘small’ entities in a limited set of circumstances (based on criteria such as turnover and purpose of data collection), the DPDP appears to make no significant exception in that regard. Accordingly, the new regime is poised to be an overarching one, and all ‘data fiduciaries’ will need to comply with its requirements unless they have been expressly exempted via governmental notification.

Who are ‘Data Fiduciaries’?

DPDP defines this term broadly. Any individual, company, firm, association of persons/body of individuals (even if unincorporated), the State itself (as defined in the Indian constitution), as well as any other artificial juristic person can be a ‘data fiduciary’ – as long as it determines the purpose and means of processing digital personal data. Further, such determination may be made by an entity itself or in conjunction with other entities.

The DPDP seeks to establish a regulatory framework for the purpose of protecting the digital personal data of individuals (“**data principals**”). To this end, it imposes obligations and limitations on data processing by data fiduciaries. Accordingly, a wide variety of actors in the Indian economy will need to comply with the DPDP.

The Scope of ‘Digital’ Personal Data

We have previously explained what the term ‘personal data’ means (see [here](#)), including with reference to the proposed regime under the DPDP (see [here](#)). Obviously, not all data may be considered personal. For

an overview of the distinctions between personal and non-personal data, respectively, please refer to our previous notes available [here](#), [here](#), [here](#) and [here](#).

The DPDP will only apply to the processing of personal data when such data is in digital form. However, if personal information is collected in non-digital form (e.g., manually) and digitized later, DPDP's provisions will nevertheless apply.

In general, digitization refers to the process of converting physical or analog information (such as paper documents or images) into digital, machine-readable formats – which, in turn, may be accessed, stored and/or manipulated using computers and digital technologies. Since most modern commercial operations and business processes deal with digitized data, the DPDP will have extensive coverage.

The Scope of 'Processing'

Like the EU's General Data Protection Regulation (the "GDPR"), the DPDP defines the term 'processing' broadly. For instance, it involves any activity among a wide range of operations that businesses routinely perform on data, including the collection, storage, use and sharing of information. It also includes things that entities may often take for granted, such as the organization, structuring or retrieval of data. In addition, processes involving transmission, dissemination, making available – or even erasing or destroying data – will be subsumed under the DPDP.

In essence, 'processing' under the DPDP involves automated operations. Importantly, such operations may even be partially automated. Any digital process that is capable of operating automatically in response to instructions given (or otherwise) for the purpose of processing data can be considered 'automated'. Thus, even those business operations which involve some amount of human intervention and/or stem from human prompts will be covered under the DPDP's definition of 'processing'.

Timelines

Since both the Lok Sabha (lower house) and the Rajya Sabha (upper house), respectively, have cleared the DPDP during the Indian parliament's monsoon session – the last day of which (August 11) coincided with the President's assent followed by publication in India's official gazette (for general information) – the only thing that remains for the new law to become enforceable is the identification of date(s) on which relevant sections of the DPDP will come into force. Given the pace at which both houses of India's bicameral legislature approved the underlying bill, it seems that the government is keen to put the DPDP into effect as soon as possible. Accordingly, the last stage – procedural formality as it is – will likely be completed quickly.

However, different dates may be appointed for different provisions. The DPDP is a framework document enshrining broad principles and norms. Accordingly, several discrete provisions still require granular rules which are yet to be prescribed by the central government. As of date, there exists no clarity about when such provisions will be put into effect through delegated legislation – although recent ministerial [statements](#) reported in the media suggest a six-month transitional timeline.

It is possible that the proposed Data Protection Board of India (the "DPBI") will be set up first, before various [templates](#) (e.g., for notices), [procedures](#) (e.g., with respect to data breach notifications; obtaining verifiable parental consent for processing children's data; grievance redressal; etc.), [processes](#) (e.g., to conduct data protection impact assessments ("DPIAs")), and various [other details](#) (e.g., relevant time

periods; registration conditions; accountability mechanisms; specific obligations, etc.) are notified through government-made rules under the DPDP's overall framework.

In past versions of the DPDP, a data protection authority was proposed to be vested with regulatory powers such that it could: (i) certify data auditors based on pre-notified qualifications, (ii) prescribe clear DPIA methodologies, (iii) monitor technological developments, (iv) raise awareness with respect to new corporate responsibilities, etc. However, based on the DPDP's text, the DPBI will be restricted by and large to adjudicatory (and certain registration) functions. Accordingly, entities that seek to get the scope of their statutory obligations and/or new requirements clarified may not have recourse to a formal mechanism, including for the purpose of obtaining authoritative interpretive guidance. The central government alone may decide how various rules get formulated and rolled out, respectively.

Prior Familiarity

GDPR and CCPA

Mainly on account of the GDPR and the California Consumer Privacy Act (“**CCPA**”), entities with a presence or involvement in Europe and/or in the US may have managed to orient their international business practices over time for the purpose of complying with such data protection regimes. However, even these entities may need to make certain processual adjustments to comply with the DPDP. Although the DPDP has largely been modeled on a global template spawned by the GDPR, it nevertheless contains provisions that are unique to India.

For instance, the DPDP is more consent-based than the GDPR: while the GDPR allows non-consensual data processing by private entities under various circumstances – ranging from contractual necessity to the pursuit of legitimate/vital interests of various parties – such grounds are either absent or have now been purged from the DPDP (relative to its prior iterations). Accordingly, a working familiarity with GDPR requirements may *not* be enough for DPDP compliance. For an overview of the changes made to the DPDP's final form compared to its previous draft (released in November 2022 for public comments), see our summary [here](#).

SPDI Rules

Further, certain entities – especially those dealing with sensitive personal data/information (“**SPDI**”) – may have learnt by now how best to adjust their respective business operations for the purpose of complying with the existing data protection framework in India (the “**Existing Regime**”). The Existing Regime stems from Section 43A of the Information Technology Act, 2000, as amended (the “**IT Act**”), along with its subordinate rules, *viz.*, the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011 (the “**SPDI Rules**”).

To be sure, the DPDP will *not* replace the IT Act (although the proposed ‘Digital India Act’ might – given that a draft bill in this regard is expected to be released [soon](#)). However, the DPDP does seek to *amend* the IT Act, including by omitting the latter's Section 43A. Accordingly, entities will have to comply with such obligations as spelled out afresh under the new law.

RSPP

Provisions under the SPDI Rules relate to privacy policies; data collection, disclosure and transfer; reasonable security practices and procedures (“**RSPPs**”), etc. – each of which addresses a specific set of requirements. However, the Existing Regime will soon be rendered obsolete. Instead, concerns about RSPPs will be dealt with under the DPDP directly (after it comes into force). To the extent that the DPDP and its subsequent rules may deviate from the Existing Regime, such differences need to be accounted for.

‘Personal data’

Although references to ‘personal data’ may suggest that only private information, *i.e.*, data about individuals in their personal capacity, will be covered – the DPDP, like the EU’s GDPR, extends the scope of this term to all those who are *identifiable* by or in relation to such data.

In general terms, information can be considered to ‘relate’ to an individual when it is *about* that person. While personal data may involve any kind of information about an individual, it could cover both objective and subjective information (including opinions, estimates or assessments related to such person). However, in some situations, the information conveyed by a piece of data may involve something or someone else, and not a specific individual as such. Even in these cases, the information may relate to an individual indirectly.

In this regard, the SPDI Rules define personal information as information relating to a natural person which, either directly or indirectly, in combination with other information available or likely to be available with a body corporate, is capable of identifying such person. It is possible that this understanding will persist with respect to the DPDP in the future.

However, under the DPDP, entities which process any digital personal data are required to implement appropriate technical and organizational measures to ensure effective compliance. In addition, contrary to the Existing Regime, entities will remain responsible for protecting such data even when it is not ‘sensitive’ – as long as it remains in their possession or under their control, including in respect of separate processing tasks undertaken by data processors on their behalf. These overarching responsibilities will extend to taking RSPP-like precautions to prevent data breaches, as well as complying with prescribed steps if and when a breach does occur.

Importantly, compared to its immediate predecessor, the DPDP appears to attribute sole responsibility upon the main custodians of data, *i.e.*, data fiduciaries (as opposed to shared responsibility with data processors), based on the principle that an entity which decides the purpose and means of data processing should be held accountable. Such liability may also be invoked when a data breach and/or an event of non-compliance arises entirely on account of a negligent data processor. Further, while processing tasks *can* be delegated to a third party, such delegation and/or outsourcing must only be under a valid contract when the processing is in respect of an activity related to the offering of goods or services to data principals. Accordingly, these contracts need to be negotiated carefully, given the quantum of penalty involved. Nevertheless, irrespective of any agreement to the contrary, a data fiduciary will be responsible for complying with the provisions of the DPDP and its rules with respect to any processing undertaken on its behalf by a data processor.

New safeguards?

Unlike the SPDI Rules, the DPDP does *not* prescribe exact standards (e.g., ISO/IEC 27001) that ought to be implemented with respect to handling SPDI. In fact, the DPDP eschews data categorizations altogether. Further, the erstwhile power of the central government to make rules with respect to RSPPs and SPDI under the IT Act (under the Existing Regime) will be retracted once the DPDP enters into force. Although the government may frame bespoke rules with respect to several of DPDP's provisions, RSPPs have not been explicitly earmarked for delegated legislation under the new regime.

Nevertheless, in the absence of specified technical measures and/or prescriptive safeguards, industry-specific paradigms related to data processing may develop over time, including in connection with standards based on parameters such as informational sensitivity, the volume of data processed, the risk to individual rights, etc. Some such parameters have already been provided under the DPDP; however, as of now, those are solely for the government's consideration when it chooses to assess an entity's status in terms of how onerous the latter's obligations should be – based on the nature and scale of its data processing. For a discussion on such entities (called 'significant data fiduciaries' ("**SDFs**")), see our note [here](#). To read our analyses about the prescribed evaluative parameters for making SDF classifications, see [here](#) and [here](#).

Penalty vs. compensation

Section 43A of the IT Act provides for the payment of compensation on account of failures to protect data. Accordingly, under the Existing Regime, if the negligent implementation of RSPPs while handling SPDI leads to wrongful loss or gain, such negligent entity can be held liable to pay compensatory damages to the affected person. Partly on account of poor implementation with regard to this provision, the DPDP moves away from a damages-based mechanism to a framework of financial penalties – some of which can go up to (approx.) USD 30 million.

According to a recent [report](#) of the parliamentary standing committee on communications and information technology with respect to citizens' data security and privacy – an individual who suffers a civil wrong (on account of rights violations or non-compliance with obligations) can invoke liability before a civil court for damages under tort law. Such aggrieved individual may also cite penalties imposed by the DPBI in support of their claim.

Conflict with other laws

The DPDP will apply in addition to (and *not* in derogation of) other laws. Thus, if a sector-specific law or a regulatory body mandates additional data protection and/or data processing obligations, those will apply over and above the general requirements under the DPDP. For instance, recent obligations imposed under the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Amendment Rules, 2022 – which amended the preceding 2021 rules – will continue to apply in parallel, such as with respect to requiring 'intermediaries' (as defined in the IT Act) to publish their privacy policy and user agreement on websites and/or mobile based apps. However, if there is a direct conflict with any other law, the DPDP's provisions will prevail.

SPDI Rules vs. DPDP

Since the DPDP does not separately deal with or refer to SPDI (although the government can consider data 'sensitivity' as a ground for imposing additional obligations upon SDFs), even those entities that are familiar with the SPDI Rules (along with its corresponding compliance regime) need to remain alert with respect to processing digitized data – including each and every kind of personal data in their possession or control – because all of such information may come under the DPDP's ambit.

Conclusion

While provisions of the new law are likely to come into force soon, several details are yet to be specified. In that regard, enforcement may take some time, since most granular rules will need to be formulated, including through stakeholder consultation. The DPBI is likely to be constituted on a priority basis, while regulations may be rolled out by the government over a staggered period.

*This insight has been authored by **Rajat Sethi** (Partner) and **Deborshi Barat** (Counsel). They can be reached at rsethi@snrlaw.in and d Barat@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.*

© 2023 S&R Associates



NEW DELHI
64 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