S&R

Data+

Navigating Data Minimization Requirements under India's DPDP Act

Background

While the notification of provisions and rules under India's Digital Personal Data Protection Act, 2023 (the "**DPDP Act**") is awaited, organizations need to plan ahead (for an update on the DPDP Act and a roadmap for planning a long-term compliance strategy, see our notes here and here). Compliance planning strategies will need to consider the principles of legality, purpose/use limitation, data minimization, accuracy and storage limitation.

Data Minimization

The principle of data minimization involves limiting the collection, storage, processing and retention of personal data only to what is relevant and necessary for a specific purpose. A few practical examples of practices which may be contrary to principles of data minimization may include a recruitment agency seeking detailed information about the physical fitness of potential applicants, while inviting applications for an office/ desk job or a food delivery application retaining a customer's contact information for marketing purposes after completion of the delivery, if such purposes were not disclosed at the point of collection of information. In both these cases, the collection or retention of the information may not be considered necessary for the purpose disclosed at the point of collection, thus violating data minimization requirements.

A 2017 white paper (the "**White Paper**") drafted by a government-constituted committee of experts ("**Srikrishna Committee**") for the purpose of inviting public comments on the shape of India's data protection law had stated that 'data that is processed ought to be minimal and necessary for the purposes for which such data is sought and other compatible purposes beneficial for the data subject'. In its final report, the Srikrishna Committee adopted the standard prescribed in the White Paper. The underlying rationale for the data minimization principle is to limit the risks associated with collection and storage of personal information including data theft and leakage.

Relevant Laws in India

Data privacy laws

The principle of data minimization is embodied in section 6 of the DPDP Act. Any consent for processing digital personal data needs to be free, specified, informed, unconditional and unambiguous with a clear

affirmative action (for a discussion on consent management, see our note here). Consent can only be sought for the processing of personal data for the specified purpose (*i.e.*, 'purpose limitation') and must be limited to such personal data as is necessary for that specified purpose (*i.e.*, 'data minimization'). The principles of data minimization and purpose limitation are closely related and have also been built into the draft Digital Personal Data Protection Rules, 2025, which were published by the Indian government on January 3, 2025. Specifically, the draft rules provide that the notice which is to be provided to a data principal along with the consent request should clearly set out the specific purposes of processing and an itemized list of goods and services to be provided using the personal information collected (for an update on the draft rules, see our note here).

Through an illustration about a telemedicine app, the DPDP Act clarifies that even if individuals provide consent for such app to access their 'contact list', the consent will be invalid since access to contact list data is not required for providing telemedicine services. Any breach of the data minimization principle may lead to a penalty of INR 500 million.

At present, under the existing Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011, this principle has been applied to a certain extent in relation to collection of sensitive personal data or information ("**SPDI**") inasmuch as companies are prohibited from collecting SPDI unless a) it is collected for a lawful purpose connected with a function or activity of such body corporate or any person on its behalf; and b) such collection is considered necessary for that purpose.

Consumer protection laws

The data minimization principle also appears to be integrated within India's consumer protection framework. For instance, in May 2023, the Ministry of Consumer Affairs issued a notice to retailers restricting them from imposing a mandatory requirement on customers to provide personal information (including mobile numbers) as a condition of purchase. The ministry had characterized such practices as 'unfair contracts' and 'unfair trade practices' under the Consumer Protection Act, 2019 ("**CP Act**"). Further, state consumer disputes redressal commissions have imposed penalties for compulsory enrolment in 'loyalty programs' as a condition of sale.

In addition, the Guidelines for Prevention and Regulation of Dark Patterns, 2023 ("**Dark Pattern Guidelines**") were notified under the CP Act in November 2023. Broadly, the Dark Pattern Guidelines seek to prevent all 'platforms' that systematically offer goods or services in India (note that the Consumer Protection (E-Commerce) Rules, 2020 define a 'platform' to mean "an online interface in the form of any software including a website or a part thereof and applications including mobile applications"), as well as all advertisers and sellers, from engaging in any patterns or processes in their user interface or user experience interaction which can mislead or trick users. Accordingly, requiring a user to share personal information to facilitate a purchase or subscription (i.e., a 'forced action') has been characterized as a dark pattern under the Dark Pattern Guidelines.

Data Minimization under the GDPR

Globally, data protection regimes incorporate the data minimization principle within their respective regulatory frameworks with varying levels of stringency. For instance, under the European Union's General Data Protection Regulation ("**GDPR**"), the principle of data minimization requires the processing of personal data to be 'adequate, relevant, and limited to what is necessary in relation to the purpose for which they are processed'. Further, the principle's dimensions include the amount of personal data collected, the extent of its processing, the period of storage, and accessibility. The Guidelines on Data Protection by Design and by Default ("**EU Guidelines**") adopted by the European Data Protection Board ("**EDPB**") clarifies that controllers (the equivalent of 'data fiduciaries' under the DPDP Act) should:

- first, determine whether they need to process personal data for the relevant purposes;
- verify whether the relevant purposes can be achieved by processing less personal data, or having less detailed or aggregated personal data, or without having to process personal data at all (such verification should take place before any processing takes place, but could also be carried out at any point during the processing lifecycle);
- periodically consider whether processed personal data is still adequate, relevant and necessary, or if the data should be deleted or anonymized.

Further, the EU Guidelines explain that data minimization can also refer to the degree of identification. If, for instance, the purpose of processing does not require the final dataset to refer to an identified or identifiable individual (such as in statistics), but the initial processing does (*e.g.*, before data aggregation), then the controller should delete or anonymize personal data as soon as identification is no longer needed. On the other hand, if continued identification is needed for other processing activities, the personal data should be pseudonymized to mitigate risks.

Pending future clarifications or interpretation under the GDPR, the standard appears to be more restrictive than that of the DPDP Act. However, cases under the GDPR may be instructive in the Indian context, including for the purpose of understanding how the principle may be applied by courts and regulatory bodies in the future. Under the GDPR, fines have been imposed, among other instances, for (i) collection of excessive medical data for processing insurance claims and (ii) collection of identity cards for entry into concerts and other events. Insurance companies have also been reprimanded for collecting additional data directly from health service providers.

While considering video camera surveillance, the Court of Justice of the European Union has held that the necessity of a processing operation must be examined in conjunction with the data minimization principle. Further, the controller must examine whether it is sufficient if video surveillance operates only at certain hours of the day and blocks or obscures the images taken in areas where surveillance is unnecessary.

Implementing Data Minimization

To ensure compliance with the 'data minimization' framework under the DPDP Act, businesses can look to implement the principles provided under the EU Guidelines. Further, businesses can look to identify the personal data that they already possess, how it is used, how it is stored, and streamline data collection and processing practices accordingly. Organizations can also look to review their data retention policies.

Data Minimization and Big Data Analytics

The principle of data minimization does not translate into a bar on processing of large quantities of data. In some cases, a data fiduciary may need to process large amounts of data for achieving the business goal. For businesses engaged in big data analytics, the principle of data minimization may be difficult to implement. However, such businesses can rely on anonymized data which cannot be later used to re-identify the individual. Globally, regulators have recommended that such businesses should be transparent about their data processing practices and provide meaningful privacy notices at appropriate stages throughout a big data project.

The Srikrishna Committee had recommended that big data processing which is used to improve the provision of services or purposes reasonably expected by the data principal should be permitted to continue.

Data Minimization and AI/ML

Similar to Big Data businesses, businesses focusing on artificial intelligence and machine learning ("**AI - ML**") rely upon large datasets, specifically those looking to build large language models ("**LLMs**"). Common techniques used to implement the principles of data minimization in the context of LLMs include:

At the training stage:

- perturbation (i.e., adding 'noise'),
- use of synthetic data (we have written about this here), and
- federated learning (i.e., by combining patterns identified by several local models into a unified global model without sharing training data with each other).

At the inference stage:

- conversion of personal data into feature vectors (i.e., a series of numbers),
- making inferences locally (*e.g.*, on the user's device), and
- privacy-preserving techniques (*e.g.*, rendering personal data pseudonymous or anonymous).

AI-ML businesses may also evaluate the features included in a dataset which will necessarily be relevant to their purpose.

Conclusion

As discussed in our previous note, organizations need to check whether and to what extent the DPDP Act applies to them and their operations. Most organizations may need to improve their existing data collection and processing practices to meet new compliance obligations, especially with respect to data minimization (for a discussion on the wide applicability of the DPDP Act, see our note here). Regulatory decisions and developments in other jurisdictions may prove useful in this regard, including for the purpose of formulating internal policies and practices. Implementing data minimization practices may help reduce data storage costs and limit risk. In some cases, it may also lead to cleaner and higher quality datasets. Preparedness for compliance may help avoid litigation and penalties.

*This insight has been authored by **Dr. Deborshi Barat** (Counsel), **Reshma (Vaidya) Gupte** (Counsel) and **Prakriti Anand** (Associate). They can be reached at dbarat@snrlaw.in, rgupte@snrlaw.in and panand@snrlaw.in, respectively, for any questions.*

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