DATA PRIVACY SPOTLIGHT

INTRODUCTION

We are pleased to present the latest edition of our Data Privacy newsletter, highlighting key updates and practical insights on India's new data protection regime. Curated by our Technology and Data Privacy Practice Group, this edition provides a clear overview of the 18-month implementation roadmap and the major features of the DPDPA—helping businesses stay informed and prepared for this important shift in India's data privacy landscape.

INDIA NOTIFIES NEW DATA PRIVACY LAW

Introduction

More than 2 years after its enactment, the Indian government has notified India's new data privacy law, the Digital Personal Data Protection Act, 2023 ("DPDPA"). The statute required the government to bring the law into force by publishing its effective date in the official gazette. The government has now done so, setting out an 18 month roadmap for implementation.

With this notification, India, the 5th largest economy in the world will finally have a dedicated data privacy legislation. Even though it is simpler and less comprehensive than GDPR, it has some of the toughest levels of compliance seen globally.

Timelines

The government has prescribed three timelines for implementation of the law:

Provisions	Date of enforcement
Provisions relating to the Data Protection Board of India	November 13, 2025 (now in force)
Provisions relating to registration of Consent Managers	November 13, 2026 (one year from now)
All other provisions	May 13, 2027 (18 months from now)

Businesses have 18 months to prepare for compliance with the new law. Given how pervasive the use of personal data is for businesses and the steps required for them to comply with the new law, this period is justified. It may be noted however, that the concerned Minister announced soon after that the government may shorten the implementation period to 1 year, but that has not been finalized.

DPDPA Rules

The government also finalized the Rules under the DPDPA, called the Digital Personal Data Protection Rules, 2025 ("Rules") with the timeframe for enforcement of these Rules being in alignment with the timeframe for enforcement of the statute.

The Rules are similar to the draft rules that were circulated earlier with a few changes.

KEY ASPECTS OF THE DPDPA

The following are some of the key aspects of the new law:

1. Lack of Legitimate Interest

Unlike the GDPR, the DPDPA does not include legitimate interest as a ground for processing personal data. There are exemptions to the applicability of the law and exemptions to the requirement to obtain consent. However, by and large, the main ground for processing of personal data is consent. This comes with its own problems, including the high standard of consent and the right of data principals (akin to data subjects) to withdraw consent.

2.Standard of Consent

The standard of consent is the same as under the GDPR. The law prescribes that consent must be free, informed, specific, unambiguous and unconditional and it needs to involve an affirmative action. As the language is the same

as under the GDPR, one would assume that the jurisprudence that has developed in the EU would apply similarly. This would be of concern to businesses who largely avoid using consent in the EU. In addition, the Rules prescribe that the privacy notice must include an itemized list of (a) the services or goods being provided; (b) the personal data being processed; and (c) the purposes for which the personal data is processed. This means that GDPR compliant privacy policies/notices based on legitimate interest would very likely not work in India.

3.Four stages of breach notifications

The new law, along with existing cybersecurity regulations, prescribes four separate notifications for a personal data breach. There is also no threshold for when a personal data breach needs to be notified. The following are the four stages:

(a) Within 6 hours – to the cyber security authority, the CERT
(b) On becoming aware and without delay – to the data principal
(c) On becoming aware and without delay – to the DPBI
(d) Within 72 hours – to the DPBI with more detailed information.

In addition, the CERT has also been known to ask for additional information including forensic reports. These requirements are among the toughest in the world relating to data breach notifications.

4.Data Localization

Businesses can breathe easy here as data localization provisions are largely absent from the statute. The government can prescribe a blacklist of countries to which personal data transfer can be restricted. We expect it would be either countries which do not have sufficient data privacy protection or countries which have hostile relations with India. It is very likely that Pakistan and China will be on that list.It is possible that when the government notifies these countries, it may include some exceptions or workarounds, such as standard contractual clauses or similar arrangements. The government can prescribe conditions for the transfer of personal data to a "foreign state or to a person or entity under the control of the foreign state". The government can also prevent certain personal data and traffic data held by significant data fiduciaries from being transferred outside India

5.Cross Border Applicability

The law does have cross border application in the following manner:

Type of Personal Data and Location of Processing	Applicability
Personal data of Indian citizens processed outside India	The law would apply in connection with any activity related to offering goods or services to data principals within the territory of India.
Personal data of non-Indian citizens processed in India	Most of the law would not apply.

It is not entirely clear what is meant by "offering goods or services". We believe any systematic and intentional effort to target Indian customers would trigger applicability. This is not dissimilar to provisions in GDPR and other Indian laws, including India's e-commerce regulations under consumer law.

It is also important to note that the law will largely not apply to personal data of people outside India that is being processed by India's huge offshore and outsourcing industry. Only the provisions on reasonable safeguards and procedures would apply.

6.Data Protection Standards

The law requires businesses to use reasonable security measures to prevent breaches. The statute empowers the government to prescribe minimum standards. The Rules prescribe reasonable safeguards which must include "at a minimum" – encryption, obfuscation or masking of PI, use of virtual tokens, restrictions on access, visibility on access through maintaining logs, requirement of maintaining logs for a period of 1 year, etc. By prescribing that reasonable security safeguards must include the above "at a minimum", there is some concern as to the extent to which a business must employ all of these methods.

7.Applicability to AI

The law is reasonably friendly to AI. To start with, the law does not include a data minimization requirement. There are no standards relating to what purposes the personal data can be used.The only requirement is that the personal data must be used for purposes that are mentioned in the privacy notice.This gives room for businesses to draft purposes broadly. Individuals may however refuse consent to use of personal data for training AI models.Further, there is no right not to be subject to automated decision making without a human element. The law does however states that where personal information is processed in order to take a decision that affects a person, the data fiduciary (akin to data controller) must ensure completeness, accuracy, and consistency of personal data.

8.Liability and penalties

One key aspect of the law is that it does not directly regulate data processors. The only requirement is that there

must be a contract between the data fiduciary and the data processor. The law also states that the data fiduciary would be responsible for processing by the data processor. This means that data fiduciaries must review carefully indemnity and limitation of liability provisions in their contracts with data processors so that they can pass through penalties imposed on them due to the fault of the data processor.There is a schedule which prescribes penalties for different violations with the highest penalties being INR 2.5 billion (about USD 28 million).

The Way Forward

With the enactment of the new law and the time frame for enforcement being finalized by the government, the roadmap is now set for businesses to comply with the new law. Businesses must go through a detailed process, commencing with data mapping – understanding what data is being collected, for what purpose and for what services/goods. Businesses then need to determine what changes they wish to make to their current data processing – it is likely that the more data that is collected, the more the level of compliance with the new law. Businesses then need to prepare a new data privacy policy/notice that complies with the new law. Finally, businesses need to implement technology measures so that practically, they comply with the new law and with their own privacy notice. This is a fairly long process and accordingly, businesses should commence work on this as soon as possible.

OUR TEAM

STEPHEN MATHIAS
Senior Partner and Co-Chair Technology
stephen.mathias@bgl.kochhar.com

GAYATHRI POTI
Senior Associate
gayathri.poti@bgl.kochhar.com