THOMSON REUTERS
PRACTICAL LAW™

# Expert Q&A: AI and India's Digital Personal Data Protection Act (DPDPA)

**by Practical Law Data Privacy & Cybersecurity**

Status: **Published on 24 Apr 2024** | Jurisdiction: **India**

This document is published by Practical Law and can be found at: **content.next.westlaw.com/w-042-9380**
Request a free trial and demonstration at: **tr.com/practicallaw-home**

An expert Q&A with Arun Babu, a Partner with Kochhar & Co., discussing India's Digital Personal Data Protection Act 2023 (DPDPA) and its effect on AI governance. This Q&A addresses the intersection of the DPDPA and AI, consent as a legal basis for processing personal data for AI, complying with data subject rights provisions, AI-related cybersecurity concerns, challenges the DPDPA poses, and compliance measures organizations using AI systems can take to prepare for the DPDPA.

Practical Law asked Arun Babu from Kochhar & Co. to discuss how organizations developing and using AI systems can navigate processing personal data using AI under India's Digital Personal Data Protection Act 2023 (DPDPA). The DPDPA is India's first comprehensive data protection legislation and will regulate the collection, use, and disclosure of personal data. It was published in the Official Gazette on August 11, 2023, and will come into force as notified by the Indian Government in the Official Gazette.

Arun Babu is a Partner in the Bangalore office of Kochhar & Co. and specializes in Indian data privacy laws and cybersecurity regulations.

## What data and businesses does the DPDPA regulate?

The DPDPA regulates the processing of personal data collected in digital form, or in non-digital form and digitized subsequently. The law defines personal data as any data about an individual who is identifiable by or in relation to that data. The DPDPA does not apply to personal data:

- An individual processes for personal or domestic purposes.
- Made publicly available by the data principal or a person with a legal obligation to make it publicly available.

The DPDPA applies to the processing of digital personal data in India and outside India where the processing is in connection with any activity related to offering goods or services to individuals in India.

The DPDPA protects the personal data of data principals, defined as individuals to whom the personal data relates. It applies to personal data that the following parties process:

- Data fiduciaries, defined as any person who alone or in conjunction with others determines the purposes and means of processing personal data.
- Data processors, defined as any person who processes personal data on behalf of a data fiduciary, and sub-processors who process personal data on behalf of a data processor.

The DPDPA also applies to consent managers, defined as persons registered with the Data Protection Board of India (DPBI) that act as a single point of contact to enable a data principal to give, manage, review, and withdraw their consent through an accessible, transparent, and interoperable platform.

The DPDPA does not impose any specific compliance obligations or penalties on data processors. Instead, the DPDPA gives data fiduciaries responsibility for overall compliance, including for activities of the data processors they engage. The law requires data fiduciaries to engage data processors under a valid contract.

For more information about the DPDPA and its requirements, see Country Q&As, Data Protection in India: Overview and Data Protection Authority Registration and Data Protection Officer Requirements for Data Controllers: India. For more

information on data privacy and cybersecurity in India, see Data Protection Toolkit (India).

## Does the DPDPA regulate AI?

Organizations configure and train AI systems and algorithms to perform various tasks and make decisions that would otherwise require human intelligence. AI systems typically process large amounts of data for training, testing, deployment, and monitoring. Depending on the AI system's end use, this data could include personal data, for example:

- AI systems enabling targeted advertising are generally developed using data pertaining to consumers' online behavior and characteristics such as purchase history, web browsing, gender, age, and geolocation.
- AI-based facial recognition algorithms are developed and used by continuously feeding them an exceedingly large number of facial images.

Although the DPDPA does not specifically refer to AI, it applies to AI systems' processing of personal data. The DPDPA does contain certain exemptions, however, that may apply to AI systems, one of which exempts processing personal data that the data principal or any person with a legal obligation makes publicly available. This exclusion is relevant for many AI systems and services because publicly available personal data scraped from the internet using automated tools is a major source of their training data. However, other sources exist for personal data that AI systems process, including personal data that data principals directly provide or input. The DPDPA applies to this personal data.

The DPDPA also contains an exemption for processing personal data necessary for research, archiving, or statistical purposes if both:

- The personal data is not used to make a decision specific to a data principal.
- The processing complies with prescribed standards.

Although this exemption does not explicitly refer to AI, using personal data to conduct research for AI system development could potentially fall under this exemption, including developing training models for AI-based text generator tools.

Further, unlike one of its previous draft versions, the DPDPA does not govern the processing of anonymized personal data. The DPDPA does not define this term, but anonymization generally means the irreversible transformation of personal data into a form where it is impossible to associate or identify an individual from that data. Where appropriate, a business can use anonymized data to develop AI systems without complying with the DPDPA's requirements.

Except for the above exemptions, the DPDPA applies to all personal data processing by AI systems. Organizations must establish a legal basis under the DPDPA for this processing as discussed below.

Does the DPDPA require valid data principal consent to process personal data?

The DPDPA requires data fiduciaries to establish a legal basis for processing a data principal's personal data. Consent is the primary legal basis for processing personal data under the DPDPA. However, the law also permits processing personal data for several uses without obtaining data principal consent, including:

- For employment-related purposes or to protect an employer from loss or liability.
- Responding to medical emergencies.
- Performing state functions.
- Disaster management.

Processing personal data to train, deploy, and monitor AI systems would likely not constitute a legitimate use under the DPDPA and consequently, almost all processing scenarios would require the data fiduciary to obtain data principal consent.

## What are the challenges to using data principal consent for AI-related personal data processing?

The DPDPA requires valid consent to be:

- Free.
- Specific.
- Informed.
- Unconditional and unambiguous.
- Restricted to the personal data necessary for a specified purpose.
- Indicated with a clear affirmative action, signifying the data principal's agreement to the processing of their personal data for a specified purpose.

Data fiduciaries must present every request for consent to the data principal in clear and plain language that

explains why they are collecting the personal data. They must also give the data principal the option to access the request in English or any of the 22 languages the Eighth Schedule to the Constitution specifies.

This is a high standard to meet and is similar to the valid consent requirements under the General Data Protection Regulation (GDPR), the EU's comprehensive data protection law. However, in contrast to the GDPR, the DPDPA does not include other alternative and broad legal bases for processing such as processing for the data fiduciary's legitimate interest, which would be more suitable for AI-related personal data processing. Legitimate interest is generally considered the most flexible legal basis for processing personal data under the GDPR and can, in principle, enable its processing for most reasonable and lawful purposes.

Unfortunately, most data fiduciaries in India must rely on consent as their legal basis for processing personal data for AI purposes. They generally receive a vast amount of the personal data they process for training and developing AI systems from third-party data brokers, who have likely obtained and aggregated the data from various sources other than data principals themselves. It would therefore be practically difficult to ensure compliance with the DPDPA's onerous consent requirements as there is often no direct relationship between the data principal and the data fiduciary.

Adding to this challenge is AI systems' capability to deduce patterns and correlations between data, which can result in:

- Additional, unforeseen processing purposes for personal data after the data fiduciary has already collected it.
- Generation of new personal data.

In these cases, data fiduciaries cannot rely on the consent they obtained for the initial processing purposes. They must obtain an additional data principal consent for each purpose for which they will process the already collected or newly generated personal data.

Additionally, the law requires data fiduciaries to provide data principals with a privacy notice with certain information before or at the time they obtain consent. The privacy notice must include, for example, the types of personal data collected, the processing purposes for the personal data, how to withdraw consent for processing, and how data principals can redress grievances. Data fiduciaries that use AI must update their privacy notices to reflect each new processing purpose and any newly generated personal data and ensure they are made available for data principals to access in English and the 22 languages set out in the Eighth Schedule to the Constitution.

## What are the challenges to complying with data subject rights requests under the DPDPA for data used in AI systems?

The DPDPA grants data principals certain rights regarding their personal data, including the rights of access, correction, erasure, grievance redressal, and withdrawal of consent. The law requires data fiduciaries to enable data principals to withdraw their consent as easily as they provided it. Further, once a data principal withdraws their consent, the data fiduciary must erase the relevant personal data and stop any further processing, unless a retention obligation exists under any other law. Due to the sheer volume of data that AI systems process, tracking and identifying the relevant personal data would be like finding a needle in a haystack, unless data fiduciaries exercise robust data governance processes from the very beginning. Data fiduciaries will likely encounter similar difficulties while responding to other data principal rights requests such as correction and deletion of personal data. In addition, erasure or modification of personal data used in training AI models may require resetting and retraining the models.

Notably, the DPDPA does not include the right to opt out of automated decision making. However, the law requires data fiduciaries to ensure the completeness, accuracy, and consistency of personal data they use to make decisions affecting a data principal. This essentially flows from the popular phrase in computer science "garbage in, garbage out." Use of biased, incomplete, or inaccurate personal data to develop AI systems and algorithms will invariably affect their output and behavior, resulting in inaccurate and discriminatory algorithmic decisions, reproduction of human biases, and introduction of new ones.

On a related note, the Ministry of Electronics and Information Technology recently issued an advisory to all intermediaries directing them to ensure their use of AI models does not result in any bias or discrimination. An intermediary is an entity which receives, stores, or transmits data on behalf of another person, or provides any service with respect to that data. AI will continue to be an area of regulatory focus that organizations should monitor.

For more information on data subject rights under the DPDPA, see Country Q&A, Data Protection in India: Overview: Rights of Individuals.

## What cybersecurity risks do AI systems present, and does the DPDPA address them?

The massive amounts of data that AI systems process result in an increased risk of cybersecurity attacks, data theft and loss, financial and reputational damage, and regulatory attention. While the DPDPA does not require data fiduciaries to implement any particular security standard, it will require them to implement reasonable security safeguards to protect personal data in their possession or control from any breach, including for processing that data processors conduct on their behalf. The DPDPA also requires data fiduciaries to report personal data breaches to the DPBI and each affected individual in a manner to be prescribed.

The DPDPA imposes a steep penalty of up to INR250 crores (approximately USD30 million and EUR28 million) for data fiduciaries that fail to implement reasonable security safeguards to prevent a personal data breach. Since the DPDPA does not define reasonable security safeguards, data fiduciaries should look to information security mechanisms that are industry best practices and appropriate to the nature and scope of their processing. The DPDPA also does not establish a threshold for reporting data breaches based on the number of affected individuals.

For more information on information security best practices in India, see Practice Notes, Information Security Considerations (India) and Cyber Incident Response and Data Breach Notification (India).

## Looking ahead, what are some open issues that the DPBI or legislature could clarify or address?

The DPDPA is reasonably friendly to data fiduciaries involved in AI system development, as it exempts processing of publicly available personal data and does not grant data principals the right to opt out of automated decisionmaking. However, several DPDPA requirements may prove difficult for all businesses, including those developing or using AI, to comply with in practice, including:

- Obtaining valid data principal consent for processing personal data other than publicly available personal data, especially for personal data that a data fiduciary obtains from another source.
- Facilitating data principals' rights requests, especially requests to delete and correct personal data that a data fiduciary has used to train an AI system.
- Providing data principals access to a privacy notice and consent request in English and 22 other languages that the Indian Constitution sets out.
- Reporting every data breach, no matter how small, to every affected data subject and the DPBI since the DPDPA does not set out a reporting threshold.

Data fiduciaries and data processors should closely monitor how these issues unfold once the new law takes effect. The government may take note of AI-related concerns and industry feedback, provide guidance, or even amend the law, for example, to introduce a legitimate interest legal basis for processing.

In addition, the DPDPA only grants the DPBI adjudicatory powers and tasks the Indian government with all rulemaking authority. Considering the rapid pace of technological advancement and the dynamic nature of privacy law, the DPBI would have been a more natural and streamlined choice for clarifying privacy related issues, liaising with stakeholders, publishing consultation and recommendation papers, and issuing guidance notes.

## What should organizations do to prepare for the DPDPA taking effect?

Although the DPDPA does not yet have an effective date set, organizations should start taking steps now to comply with the new law, especially those who need to build a privacy program from the ground up. These steps include, among others:

- Performing data mapping exercises to ascertain the categories of personal data they collect, the processing purposes for the collected data, including for use in AI system development and training, where and how they store the data, and third parties with whom they share it.
- Determining the processing purposes for which data principal consent is required and taking measures to obtain and record valid consent and withdrawal of consent.
- Determining if any DPDPA exemptions will apply to the organization's processing.
- Preparing compliant privacy notices.
- Implementing measures to delete or anonymize personal data once the collection purpose is fulfilled.

- Adopting reasonable information security practices in line with industry best practices.
- Developing a plan to identify, respond to, and remediate personal data breaches.
- Developing a process for receiving and responding to data principals' rights requests.
- Identifying relevant data processors and executing appropriate data processing agreements.

Importantly, the DPDPA relies heavily on delegated legislation and empowers the government to prescribe rules at a future date in 26 areas. Until the rules are finalized, it may not be practically possible for organizations to ensure compliance with every aspect of the DPDPA, but creating a framework based on the bullets above will provide a solid foundation to build on.