Insights, News & Events

# 9 SWEEPING CHANGES PROPOSED IN INDIA'S LATEST DATA PROTECTION DRAFT RULES: WHAT U.S. EMPLOYERS CAN DO TO PREPARE

Insights
Jan 29, 2025

India just released a landmark draft of new rules to refine and implement the Digital Personal Data Protection Act (DPDP Act) – which is India's first comprehensive data privacy legislation regulating digital personal data processing. If adopted, the rules would apply to processing digital personal data within the territory of India – and outside of the country if such processing relates to offering goods or services to individuals within India. You should recognize, however, that the DPDP Act is not yet in force and an effective date has yet to be set – but impacted businesses should consider having an action plan ready for when the time comes. Here's what you need to know about the new DPDP Act and rules and what you can do to prepare.

**Key Proposed Changes**

The DPDP Act (which was passed in August 2023) and the new Digital Personal Data Protection Rules propose a number of updates to India's current data privacy framework. Below are the nine most significant:

1. **Consent:** Explicit written consent is required for the collection of an individual's sensitive personal data or information. This individual (referred to as a data principal) must be informed, in clear and plain language, about all personal data being processed, the processing purpose, and each service that will be enabled by the data processing.

## Related People

**Nan Sato, CIPP/E, CIPP/C**
Partner

610.230.2148

## Service Focus

International

Privacy and Cyber

Copyright © 2026 Fisher Phillips LLP. All Rights Reserved.

2. **Security Measures:** Companies are required to implement security measures, programs, and policies aiming to protect personal data and prevent breaches. The new rules lay out several detailed security measures and safeguards that must be adopted. In addition, security provisions must be included in contracts between data fiduciaries (data controllers under the DPDP Act) and data processors.

3. **Data Breach Notice:** In the event of a data breach, the data fiduciary is required to give notice to India's enforcement authority (the Data Protection Board) and to affected data principals. Unless an extended deadline is granted by the authority, details on the breach must be given in up to 72 hours from discovery of the breach.

4. **Data Deletion:** Personal data must be deleted either upon the data principal's consent withdrawal or when the legal purpose for the collection is no longer served. In any event, the data fiduciary is required to give a 48-hour notice to the data principal before deleting the data.

5. **Officers:** Specific requirements are set out for the appointment of a data protection officer by the companies, including that the officer must be based in India. Companies that are not required to have a data protection officer need to, at least, appoint a professional responsible for addressing data principals concerns on their personal data. All companies need to display on their website information on the appointed individuals.

6. **Children's Personal Data:** When processing a child's personal data, companies need to obtain verifiable consent from the parent or legal guardian. Also, it is forbidden to process personal data that is likely to cause any detrimental effect to the well-being of a child, as well as tracking or engaging in behavioral monitoring of children, or using targeted advertising directed at children.

7. **Individuals With Disabilities:** When processing the personal data of an individual with a disability, companies need to obtain verifiable consent from the parent or legal guardian.

8. **Cross-Border Transfer:** India's government may impose restrictions and additional requirements to the transfer of personal data for processing outside India.

Copyright © 2026 Fisher Phillips LLP. All Rights Reserved.

9. **Consent Managers:** Consent managers are entities registered with India's Data Protection Board that assist companies and data principals with obtaining, managing, and withdrawing consent for personal data processing. There are several requirements for companies to act as consent managers, including being incorporated in India and having a net worth of at least 2 crore Indian rupees (approximately USD 230,000).

**What's Next?**

The DPDP Act is not yet in force and no date has been set for it to take effect. Likewise, the DPDP rules are currently open to public comment until February 18. As a result, the proposed changes listed above may not become final or may be revised before being finalized.

In addition, implementation of the DPDP Act and rules is expected to take place in stages. Therefore, employers will have time to prepare once the new rules come into force.

**What Should You Do?**

Should the proposed changes take effect, U.S. and international companies that process digital personal data within the territory of India – or outside if such processing relates to offering goods or services to individuals within India – should revise their data privacy policies. Our International Practice Group can help your business navigate these changes.

**Conclusion**

We will continue to monitor developments related to data privacy law changes in India, and specifically, the approval of the new DPDP rules. Make sure you are subscribed to Fisher Phillips' Insight System to get the most up-to-date information. If you have questions, contact your Fisher Phillips attorney, the authors of this Insight, or any attorney in our International Practice Group.

Copyright © 2026 Fisher Phillips LLP. All Rights Reserved.