Insights, News & Events

INDIA'S NEW DATA PRIVACY RULES ARE HERE: 8 STEPS FOR BUSINESSES AS KEY COMPLIANCE DEADLINES APPROACH

Insights
Feb 25, 2026

India's New Data Privacy Rules Are Here: 8 Steps for Businesses as Key Compliance Deadlines Approach

Many businesses will feel the impact on their data privacy compliance practices as India's robust new rules are rolled out. India's Digital Personal Data Protection (DPDP) Act of 2023, and the DPDP Rules – which were finalized in November 2025 – create India's first comprehensive framework governing the collection, processing, storage, and transfer of digital personal data. While some provisions took effect immediately, most day-to-day employer compliance obligations, such as notice and consent operations, breach notification, and individual rights handling, will become enforceable during an 18-month implementation phase, with full compliance required by mid-May 2027. Several key deadlines come into effect later this year, making 2026 a critical "build year" for employers with Indian operations or India-linked data flows. Here is what you need to know about the DPDP Act and new DPDP Rules, the steep penalties for noncompliance, and your eight-step plan to stay ahead of key deadlines.

Overview of India's New Privacy Framework

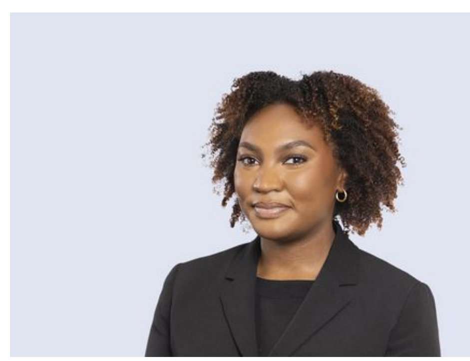
The DPDP Act established the statutory framework, while the DPDP Rules provide operational details, including requirements relating to notice, security safeguards, breach reporting, grievance handling, and processor contracting obligations. Enforcement authority rests with the Data

Related People

Gustavo José Villaça Borin Gavião De Almeida

Visiting Legal Professional

484.581.2494



Vivian Isaboke, CIPP/US, CIPM

Associate

Protection Board of India, which has the power to investigate complaints, require remedial measures, and impose significant monetary penalties, making day-to-day compliance and documentation critical for employers and businesses.

Together, the act and rules establish a stringent data protection regime that, like the EU's General Data Protection Regulation (GDPR), is grounded in principles of purpose limitation, consent, transparency, and accountability.

However, the DPDP framework includes structural and operational differences from the GDPR that are tailored to India's regulatory and economic context, particularly in how organizations are expected to operationalize notices, vendor oversight, and internal grievance handling processes. Unlike the GDPR, the DPDP framework relies primarily on consent and limited legitimate uses, rather than multiple lawful bases for processing.

Scope and Territorial Reach

The DPDP Act applies broadly to businesses that:

- Process digital personal data related to goods or services offered to individuals in India, regardless of the business location; or
- Process digital personal data within India, including data initially collected in non-digital form and later digitized.

Broad Reach: The scope and territorial reach are not limited by a business's physical location, so US and other multinational employers may be subject to the law even without a legal entity in India.

Roles and Responsibilities

While the DPDP framework is similar to other global data protection regimes, there are several key differences to keep in mind:

- **Data Fiduciary**: The entity that determines the purpose and means of processing personal data (analogous to a controller).
- **Data Processor**: An entity that processes personal data on behalf of a Data Fiduciary (analogous to a processor).

908.516.1028

Service Focus

International

Privacy and Cyber

- **Data Principal:** The individual to whom the data relates, including employees, applicants, contractors, and consumers (analogous to a data subject).

Importantly, compliance responsibility rests with the Data Fiduciary, even where processing is carried out by a Data Processor. The DPDP Act expects valid contracts with processors, and the DPDP Rules expressly require appropriate security provisions in Data Fiduciary-Data Processor agreements.

Phased Implementation Timeline

India opted for a phased implementation to allow organizations time to prepare:

- **November 2025 (Immediate):** The Data Protection Board ("DPB") was established to handle administrative duties and oversight.
- **November 13, 2026:** The Consent Manager Framework becomes operational. Organizations may register as third-party intermediaries to manage user consent and permissions. The DPB will handle registration.
- **May 13, 2027:** Full compliance deadline. All covered businesses must comply with the DPDP Act and Rules, including core obligations applicable to Data Fiduciaries.

Key Compliance Aspects

This is just an overview of key requirements that covered businesses will need to address before enforcement begins in May 2027. It's a good idea to reach out to your FP legal counsel as soon as possible to develop your compliance game plan, particularly given the high penalties described below.

As most operational compliance duties are scheduled to become enforceable during the 18-month phase starting in November 2025 – and finishing in mid-May 2027 – businesses should treat 2026 as the primary planning, implementation, and testing period, with rollout and refinement continuing into early 2027. The following requirements will be central to organizational compliance efforts as enforcement approaches:

- **Standalone Privacy Notices:** Create clear, itemized notices that are separate from standard terms of service and explain what data you collect and why. Where processing is based on consent, notices must include a dedicated communication mechanism allowing Data Principals to withdraw consent, exercise rights, or submit grievances, with withdrawal being as easy as giving consent.

- **Breach Notification:** If a breach occurs, you should promptly notify the Data Protection Board and all affected individuals and follow up with a detailed report to the DPB within 72 hours. These obligations align closely with India's broader cybersecurity incident reporting expectations and should be coordinated accordingly.

- **Security Measures:** Take steps to protect data, such as encrypting information, controlling access to information, and monitoring for all personal data processed or controlled. You should generally keep logs for at least one year unless another rule requires longer retention.

- **Contractual Requirements:** Processor contracts must reflect these safeguards and clearly allocate security and breach-response responsibilities.

- **Grievance Procedures:** Establish a channel for complaints and ensure data-related grievances are resolved within 90 days. Certain organizations will be required to appoint a Data Protection Officer, while for others it will be a best practice.

- **Children's Data:** Establish a system to verify parental consent before processing data for children under age 18. This is a higher age threshold than in many other jurisdictions.

- **Data Minimization, Deletion, and Retention:** Delete personal data as soon as the specific purpose for collecting it is complete, or the individual withdraws their consent.

Penalties for Violations Will Be Steep: A Data Fiduciary may be fined up to **₹250 crore** (about **$30 million USD**) for failing to maintain reasonable security safeguards. Failure to notify the DPB or affected individuals of a personal data breach or violations of minor-related rules can result in penalties of up to **₹200 crore** (about **$25 million USD**). Any other violation by a Data Fiduciary may be penalized up to **₹50 crore** (about **$6 million USD**).

Does an Exception Apply to Your Operations?

While India's new law focuses on consent to process digital personal data, the government recognizes that asking for permission in every instance is impractical. The law includes some carveouts for specific legitimate uses, as well as some broad exemptions, such as the following:

- **Employment "Legitimate Use" Exception:** You generally will not need to obtain explicit consent for standard HR activities when processing data for recruitment, onboarding, payroll, and benefits. However, the exception will not apply if you want to use employee data for something unrelated.
- **Publicly Available Data and Legal Mandates:** The DPDP Act won't apply if an individual has voluntarily made their personal data public (like on social media) or if the data is required to be public by law. You are also exempt from the consent requirement if you are processing data under certain legal mandates.
- **Outsourcing Exemption:** In good news to businesses that outsource operations to India, if you contract with an entity in India that processes data of individuals located outside India, certain privacy obligations may not apply.

What Should Covered Employers Do Now: Your 8-Step Action Plan

You shouldn't wait until 2027 to develop your compliance strategy, as you will need time to plan. Here is your eight-step action plan to stay ahead:

1. **Conduct a Comprehensive Audit.** Inventory the HR lifecycle and systems. Map where data is processed (India versus outside India), which entities act as Data Fiduciaries, and which vendors act as Data Processors.
2. **Create Privacy Notices and Consent Forms.** Create standalone, plain-language notices that explain what data you are collecting and why. These should be made available in English and any of the 22 official Indian languages.
3. **Review Vendor Contracts and Data Processing Agreements.** Vendor contracts and processor agreements should be reviewed, and where necessary, updated to incorporate DPDP-mandated obligations

relating to data security, breach reporting, and processor accountability.

4. **Align Security Controls and Incident Response.** Be sure you are taking appropriate measures under the act to safeguard information and comply with the 72-hour breach reporting and other requirements.

5. **Establish a Grievance Process.** Appoint a Data Protection Officer (which will be required for certain businesses and a best practice for others) and be prepared to resolve grievances within 90 days.

6. **Perform DPIAs for Higher-Risk HR Technologies.** Conduct impact assessments for biometrics, AI-driven screening tools, continuous monitoring, psychometric profiling, geolocation tracking, and large-scale global data sharing.

7. **Create a Crisis Management Plan and Train Key Employees.** Develop a plan to deal with breaches or lapses in protocol quickly and effectively, should they occur – and conduct regular trainings to ensure key managers and employees are apprised of the rules and know what to do.

8. **Consult Legal Counsel.** The DPDP Act and Rules contain very detailed requirements and significant penalties for noncompliance. It's a good idea to develop your compliance strategy with your FP legal counsel to ensure you are building a plan that works for your business.

Conclusion

We will continue to monitor developments in this area. 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 or Privacy and Cyber Practice Group.