India's Data Privacy Law: The Digital Personal Data Protection Act

Late last year, India passed the Digital Personal Data Protection Act (DPDPA) and joined the growing number of countries to pass a broad consumer protection law. After years of amendments and debates, the DPDPA will replace India's current piecemeal data protection regime. The purpose of the DPDPA is to establish transparency and accountability regarding the collection and processing of personal data of India residents. Currently, the law is not in effect and will not be until the government finalizes and passes detailed rules required for implementation. However, it is expected that the DPDPA will go into effect sometime this year.

Who does DPDPA apply to?

The DPDPA applies to organizations that process personal data of India residents both within and outside of India. The extra-territorial reach of DPDPA applies when an organization located outside of India is engaged in the processing of personal data in connection with any activity related to the offering of goods or services to residents of India.

What does DPDPA do?

As with most consumer privacy laws, the DPDPA grants data principals (defined as the individuals to whom the personal data relates) the right to know, correct and erase their data. Personal data is broadly defined under the law to be any data about an individual who is identifiable by or in relation to such data. Such a broad definition of personal data means that many data points, even an email address, would be considered personal data under the act. Unlike the European Union Data Protection Regulation (GDPR), DPDPA does not have a distinction for sensitive personal data, meaning that all personal data is expected to be collected and processed in the same manner and with the same protections.

Of particular note, DPDPA does not restrict the transfer of personal data outside of India. However, DPDPA does enable the government of India to restrict the transfer of personal data to certain countries or territories outside India by way of a notification. It is unclear under the current version of the act what such transfer restrictions could be, but the implementing regulations may provide further clarity, as well as other government guidance.

Like GDPR and China's Personal Information Protection Law, covered organizations are required to have legal bases for processing information. Covered organizations under DPDPA can process personal data for a lawful purpose for which individuals have consented or for certain "legitimate purposes" such as to respond to a medical emergency, or to fulfill the purpose for which the individuals have voluntarily provided the information and have not indicated that they do not consent to the use of their personal data.

Moreover, DPDPA places numerous additional obligations onto covered organizations including, but not limited to, providing notice to individuals concerning the entities' collection and processing practices, designating data protection officers, preparing for and responding to data breaches and performing data protection impact assessments, along with other duties.

Notably, unlike GDPR and U.S. consumer privacy laws, the DPDPA places obligations on the data principal. The duties of the data principal include compliance with all applicable laws when exercising their rights, not impersonating another individual while providing personal data, not suppressing material information when providing personal data, not filing a false or frivolous grievance or complaint; and furnishing verifiable authentic information when exercising their right to correct or erase their personal data.

What are the enforcement mechanisms?

The soon-to-be-created Data Protection Board will have enforcement power over noncompliance and data breaches. Data breaches have steep fines under the act. Covered organizations that experience a data breach and are unable to fulfill required breach reporting obligations could see a fine up to RS250 crore (approximately $30 million U.S. dollars).

What does this mean for your organization?

Organizations who do business, recruit or employ residents of India should begin to assess their policies and procedures. Although the DPDPA shares many similarities with the GDPR and U.S. consumer privacy laws, there are notable differences, and thus, a gap analysis should be conducted to ensure compliance to all consumer privacy laws. For example, businesses should implement a policy that addresses the consent requirements for processing of India resident personal data.

Bond attorneys regularly assist and advise clients on an array of data privacy and cybersecurity matters. For more information regarding India's Digital Personal Data Protection Act and to discuss compliance efforts businesses should be taking, contact Shannon Knapp, CIPP/US & CIPP/A, Victoria Okraszewski or any attorney in the cybersecurity and data privacy practice.

BOND SCHOENECK & KING ATTORNEYS