THOMSON REUTERS
PRACTICAL LAW™

Data Protection Authority Registration and Data Protection Officer Requirements for Data Controllers: India

by Supratim Chakraborty, Sumantra Bose, and Shramana Dwibedi, Khaitan & Co LLP, with Practical Law Data Privacy & Cybersecurity

Status: **Law stated as of 25 May 2023** | Jurisdiction: **India**

This document is published by Practical Law and can be found at: **content.next.westlaw.com/w-026-5386**
Request a free trial and demonstration at: **tr.com/practicallaw-home**

This Q&A discussing obligations for private-sector data controllers in India to notify, register with, or obtain authorization from the data protection authority under India's comprehensive data protection law before processing personal data. It also discusses any requirements for data controllers to appoint a data protection officer (DPO) and any applicable notification or registration obligations relating to DPO appointments. This Q&A does not cover notification, registration, or authorization requirements for data processors or arising under sectoral laws. For an overview of the data protection law in India, see Country Q&A, Data Protection in India: Overview.

Data Protection Authority

1. What is the name and contact information of the country's data protection authority or supervisory authority responsible for data protection?

Name

The Digital Personal Data Protection Act 2023 (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. The DPDPA will establish the Data Protection Board of India as the data protection authority, but no contact information is available as of the date of this Q&A.

The Ministry of Electronics and Information Technology (MeitY) issues rules under the Information Technology Act 2000, which the Information Technology (Amendment) Act 2008 amended, such as the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules 2011, and acts as an enforcement authority.

Additionally, sectoral regulators issue data protection related regulations and standards, such as Telecom Regulatory Authority of India for telecom service providers and the Reserve Bank of India for banking and finance.

DPA Contact Information

W: meity.gov.in/cyber-security

E: mljoffice@gov.in

Ministry People Directory

Agency Contact Webpage

Notification or Registration

2. Does the country's comprehensive data protection law require private-sector data controllers to notify or register with the data protection authority before processing personal data?

The Digital Personal Data Protection Act 2023 (DPDPA) will not require data fiduciaries (similar to data controllers) to notify or register with the Data Protection Board of India before processing personal data. However, the DPDPA introduces the concept of consent managers, defined as persons registered with the Data Protection Board of India that acts 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 (Section 2(g), DPDPA). The DPDPA will require consent managers to register with the Data Protection Board of India (Section 6(9), DPDPA).

There are no requirements in the Information Technology Act 2000, which the Information Technology (Amendment) Act 2008 amended, or the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules 2011 for corporations, proprietorships, or other associations engaged in professional or commercial activities, known as body corporates, to register with or notify or register with any authority before processing personal data. Practitioners understand body corporate to exclude organizations that are not classified as engaging in professional or commercial activities.

Authorization

3. Does the country's comprehensive data protection law require private-sector data controllers to seek authorization from the data protection authority before processing personal data?

The Digital Personal Data Protection Act 2023 (DPDPA) will not require data fiduciaries (similar to data controllers) to seek authorization from the Data Protection Board of India before processing personal data.

There are no requirements in the Information Technology Act 2000, which the Information Technology (Amendment) Act 2008 amended, or the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules 2011 requiring individuals or body corporates that handle personal data to obtain authorization from any authority before processing personal data.

Data Protection Officers

4. Does the country's comprehensive data protection law require private-sector data controllers to appoint a data protection officer?

The Digital Personal Data Protection Act 2023 (DPDPA) will require significant data fiduciaries to appoint a data protection officer (DPO) based in India that reports to the company board of directors and serves as a contact for the grievance redressal mechanism. The DPDPA permits the Indian government to classify certain data fiduciaries as significant data fiduciaries, considering factors including:

- The volume and sensitivity of personal data they process.
- Risk to data principals' rights.
- Potential impact on India's sovereignty and integrity India.
- Risk to electoral democracy.
- Security of the state.
- Public order.

(Section 10, DPDPA.)

The DPDPA will also require non-significant data fiduciaries to designate an individual to handle inquiries from data principals regarding their personal data (Section 8(9), DPDPA).

The Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules 2011 (Privacy Rules) require a body corporate that handles sensitive personal data or information (SPDI) to appoint a grievance officer to address data subject grievances (Rule 5(9), Privacy Rules). SPDI consists of information relating to a person's:

- Passwords.
- Financial information, including information relating to bank accounts, credit cards, debit cards, and other payment instrument details.
- Physical, physiological, and mental health condition.
- Sexual orientation.
- Medical records and history.
- Biometric information.

SPDI also includes any details relating to the above even if the body corporate receives the data in connection with providing a service or under a lawful contract. (Section 3, Privacy Rules.)

Unlike a data protection officer (DPO) under the EU's General Data Protection Regulation (Regulation (EU) 2016/679) (GDPR), who has several responsibilities like cooperating with supervisory authorities or monitoring compliance, body corporates appoint a grievance officer only to ensure that they address grievances in a timely manner. For more on other responsibilities that

apply when processing personal information or SPDI, see Country Q&A, Data Protection in India: Overview: Question 8.

5. If the comprehensive data protection law requires private-sector data controllers to appoint a data protection officer (DPO), do data controllers have any obligations to notify or communicate the DPO's contact details to the data protection authority or register with the data protection authority?

The Digital Personal Data Protection Act 2023 (DPDPA) will not require significant data fiduciaries to notify or communicate the data protection officer's (DPO) contact details to the Data Protection Board of India or register.

If a body corporate must appoint a grievance officer (see Question 4), it must publish the name of the grievance officer and contact details on its website (Rule 5(9), Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules 2011). There is no need to register with the Ministry of Electronics and Information Technology, which enforces the data protection laws in India.

For the Ministry of Electronics and Information Technology's contact information, see Question 1.

Contributor Profile

Supratim Chakraborty, Partner

Khaitan & Co LLP

T +91 33 2248 7000

F +91 33 2248 7656

E supratim.chakraborty@khaitanco.com

W http://www.khaitanco.com/people/supratim-chakraborty

Professional qualifications. India, Attorney, 2008

Areas of practice. Data protection; cybersecurity; IT contracts; mergers and acquisitions.

Sumantra Bose, Principal Associate

Khaitan & Co LLP

T +91 33 2248 7000

F +91 33 2248 7656

E sumantra.bose@khaitanco.com

W www.khaitanco.com

Professional qualifications. India, Attorney, 2012

Areas of practice. Data protection; cybersecurity; IT contracts; mergers and acquisitions.

Shramana Dwibedi, Associate

Khaitan & Co LLP

T +91 33 2248 7000

F +91 33 2248 7656

E shramana.dwibedi@khaitanco.com

W www.khaitanco.com

Professional qualifications. India, Attorney, 2020

Areas of practice. Data protection; cybersecurity; IT contracts.