October 31, 2026

MINISTRY OF ELECTRONICS AND INFORMATION TECHNOLOGY

Cross-border data transfer under India's DPDP Act

Cross-border data transfer under India's Digital Personal Data Protection (DPDP) Act is allowed unless the government restricts a country by notification (section 16(1)). No restriction was among the documents read to October 31, 2026. Rule 15 of the DPDP Rules lets the government set requirements, by order, on making data available to foreign States. Both start about May 13, 2027.

YES. A DATA FIDUCIARY, whoever decides why and how personal data is processed, may send it to a parent, a cloud or an AI service abroad. The government may restrict transfers to a country or territory by notification (section 16(1)). Rule 15 lets data leave India, subject to any requirements set on making it available to foreign States.

KEY FACTS

DATA PROTECTION

Digital Personal Data Protection Act, 2023

DATA RULES

Digital Personal Data Protection Rules, 2025

IT LAW

Information Technology Act, 2000

UPDATED

October 31, 2026

Cross-border data transfer under India's DPDP Act

Ministry of Electronics and Information Technology · October 31, 2026

Cross-border data transfer under India's Digital Personal Data Protection (DPDP) Act is allowed unless the government restricts a country by notification (section 16(1)). No restriction was among the documents read to October 31, 2026. Rule 15 of the DPDP Rules lets the government set requirements, by order, on making data available to foreign States. Both start about May 13, 2027.

Is cross-border data transfer allowed under the DPDP Act?

Yes. A Data Fiduciary, whoever decides why and how personal data is processed, may send it to a parent, a cloud or an AI service abroad. The government may restrict transfers to a country or territory by notification (section 16(1)). Rule 15 lets data leave India, subject to any requirements set on making it available to foreign States.

Rule 15 of the DPDP Rules, 2025 is sometimes read as setting country-by-country conditions on every transfer. It doesn't. Under the Digital Personal Data Protection Act, 2023, country restrictions come only by a notification under section 16, and none was among the documents read to October 31, 2026.

Neither provision is in force yet. Section 16 and rule 15 start at the third step, about May 13, 2027 (eighteen months after the Gazette of November 13, 2025). Neither notification prints that date (G.S.R. 843(E), para (c); DPDP Rules, rule 1(4)). For the other rules of MeitY, the Ministry of Electronics and Information Technology, see MeitY: India's data, platform, cyber security and electronics rules.

Where must data or logs stay in India?

CERT-In, the Indian Computer Emergency Response Team, makes companies and other bodies keep their ICT (information and communication technology) logs within Indian jurisdiction now. MeitY's cloud empanelment keeps government cloud data in India. From about May 13, 2027, a Significant Data Fiduciary, one the government notifies as such, keeps in India only the data the government specifies (rule 13(4)).

Rules that keep data in India

Rule	Who it binds	What stays in India	Status on October 31, 2026	Source
DPDP Act, section 16(1)	Any Data Fiduciary	Personal data bound for a country or territory the government notifies	Starts about May 13, 2027. No restriction among the documents read	DPDP Act, 2023
DPDP Rules, rule 13(4)	Significant Data Fiduciaries only	Personal data the government specifies, with the traffic data on its flow	Starts about May 13, 2027. No such fiduciary notified in the documents read	G.S.R. 846(E)
CERT-In directions, direction (iv)	Service providers, intermediaries, data centers, companies and other businesses, and government bodies	Logs of all their ICT systems, for a rolling 180 days	In force: took effect 60 days after April 28, 2022, and for MSMEs on September 25, 2022	CERT-In directions and June 2022 extension
Cloud empanelment call, section 5.2.4(k), items 37 to 39	Cloud providers MeitY empanels for government buyers	All data, processing and backups	A condition of the July 2026 call	MeitY cloud call
Online Gaming Rules, rule 17	Providers of online social games and e-sports	Traffic data and metadata, for the period a direction sets	In force since May 1, 2026. Applies once a direction sets what is kept and for how long	G.S.R. 303(E)

Rule 13(4) of the DPDP Rules is the localization duty. Rule 13(5), sometimes cited as the localization rule, only defines the committee that recommends which data stays. The government notifies Significant Data Fiduciaries under section 10(1) of the DPDP Act, and a MeitY officer may call for information for that assessment (DPDP Rules, rule 23(1) and Seventh Schedule, item 3).

CERT-In's FAQ reads differently. It says logs may also be stored outside India if they can be produced to CERT-In in reasonable time (Q35). It also says a provider serving users in India keeps logs and records of financial transactions in Indian jurisdiction (Q36). The FAQ says it isn't a legal document, so the direction binds.

The cloud call also bars any legal framework outside Indian law from applying to the service (section 5.2.4(l), legal compliance requirements, item 5). See the CERT-In directions guide and the MeitY cloud empanelment guide.

What if a sector regulator's rules are stricter?

A stricter Indian law on transfers still applies. Section 16(2) of the DPDP Act says nothing in section 16 limits an Indian law that gives more protection, or restricts transfers more, for any personal data or Data Fiduciary. On any other conflict between the Act and another law, the Act prevails to the extent of the conflict (section 38(2)).

The DPDP Act also says it adds to other laws and doesn't take away from them (section 38(1)). Section 38 took effect on publication, in the Gazette of November 13, 2025, and section 16 starts about May 13, 2027 (G.S.R. 843(E), paras (a) and (c)).

What does rule 15 mean for foreign governments' access?

Rule 15 of the DPDP Rules lets personal data leave India on one condition. The Data Fiduciary must meet any requirements the government sets, by general or special order, on making the data available to a foreign State, its agencies, or a person or entity it controls. Rule 15 itself sets no requirement.

The Indian government's own power to call for data is a different rule, rule 23 of the DPDP Rules, in the FAQ below.

What must be in place before a processor abroad handles the data?

A valid contract. A Data Fiduciary may use a Data Processor, anyone who processes personal data on its behalf, in offering goods or services only under a valid contract (section 8(2)). Where applicable, the contract must provide for reasonable security safeguards (rule 6(1)(f)). The Data

Fiduciary stays responsible for the processor's work, whatever any agreement says (section 8(1)).

- **Safeguards at the processor.** The security duty covers processing done on the Data Fiduciary's behalf (DPDP Act, section 8(5)). Its minimum includes measures such as encryption, access controls, logs and monitoring, and backups (DPDP Rules, rule 6(1)(a) to (d)).
- **A year of data and logs.** The Data Fiduciary keeps personal data, traffic data and processing logs for at least a year from the processing, including at its processor (rule 8(3)). In the Rules' own example, a company must make sure its cloud provider keeps the data and logs for a year too (illustration, case 2).
- **Erasure.** When the data must be erased, the Data Fiduciary must have its processor erase it too (section 8(7)(b)).

For the Act's other duties, see the DPDP Act guide.

Does the DPDP Act cover data processed in India for clients abroad?

Only in part. When a person based in India processes the personal data of people outside India under a contract with a person outside India, most of the DPDP Act's duties don't apply to it (section 17(1)(d)). Nor does section 16. Two of the Data Fiduciary's duties still apply: responsibility for compliance and reasonable security safeguards (section 8(1) and (5)).

Section 17(1) of the DPDP Act lifts the Data Fiduciary's duties in Chapter II, except section 8(1) and (5), people's rights in Chapter III, and section 16. Clause (d) has three parts: the person processing is based in India, the contract is with a person outside India, and the people whose data it is are not in India. That can fit a global capability center (GCC) in India working on data of customers outside India under a contract with its parent abroad. If one part fails, clause (d) doesn't apply, and the Act covers data processed in India (section 3(a)).

The exemption starts with the duties it lifts, about May 13, 2027, and covers the DPDP Act only: CERT-In's log rule comes from directions under the Information Technology Act, 2000. For foreign companies, see India's digital laws for foreign companies.

How IndusDesk helps with data transfers

We watch the authorities, tell you what each change means for your products and plans, represent you while a decision is still open, and carry the work through, with every step on record in your workspace.

Regulatory & trade advisory →

Rule exposure audit →

Talk to our desk about cross-border data transfers Message us on WhatsApp

Frequently asked questions

Can the Indian government demand data, and bar the company from telling anyone?

Under the DPDP Rules, yes, once rule 23 starts about May 13, 2027. For purposes the Seventh Schedule lists, such as the security of the State and assessing Significant Data Fiduciaries, the government may require a Data Fiduciary or intermediary to provide information (rule 23(1)). Where disclosure is likely to harm India's sovereignty and integrity or the security of the State, it may bar the company from telling anyone without the authorized person's written permission (rule 23(2)).

What must a contract with a processor abroad say, and is it needed now?

The Act allows a Data Processor to work on the data only under a valid contract (section 8(2)), and the DPDP Rules ask, where applicable, for a clause on reasonable security safeguards (rule 6(1)(f)). Neither is required yet: section 8 and rule 6 start about May 13, 2027, eighteen months after the Gazette of November 13, 2025. The DPDP Act guide has the rest of the duties.

How long must logs be kept: one year under the DPDP Rules or 180 days under CERT-In?

Each applies on its own terms: CERT-In's directions require logs of all ICT systems for a rolling 180 days, within Indian jurisdiction, now (direction (iv)). From about May 13, 2027, the DPDP Rules add a year for the logs needed to investigate unauthorized access, unless another law requires otherwise (rule 6(1)(e)). They also require at least a year for personal data, traffic data and processing logs (rule 8(3)).

Sources

- Ministry of Law and Justice, Act No. 22 of 2023, August 11, 2023: The Digital Personal Data Protection Act, 2023, sections 2(i) and (k), 3, 8, 10(1), 16, 17(1) and 38
- MeitY, G.S.R. 846(E), November 13, 2025: Digital Personal Data Protection Rules, 2025, rules 1, 6, 8(3), 13, 15 and 23 and the Seventh Schedule
- MeitY, G.S.R. 843(E), November 13, 2025: Dates on which the provisions of the Digital Personal Data Protection Act, 2023 come into force, paras (a) and (c)
- CERT-In, No. 20(3)/2022-CERT-In, April 28, 2022: Directions under sub-section (6) of section 70B of the Information Technology Act, 2000, direction (iv) and the closing paragraph
- CERT-In, No. 20(3)/2022-CERT-In, June 27, 2022: Extension of timelines for the Cyber Security Directions of 28.04.2022 for MSMEs and for validation of customer details, para 1
- CERT-In, May 2022: Frequently Asked Questions on the Cyber Security Directions of 28.04.2022, the note on its status, Q35 and Q36
- MeitY, July 2026: Inviting Application for Empanelment of Cloud services of Cloud Service Providers, section 8, section 5.2.4(k), items 37 to 39, and section 5.2.4(l), legal compliance requirements, item 5
- MeitY, G.S.R. 303(E), April 22, 2026: Promotion and Regulation of Online Gaming Rules, 2026, rules 1(2) and 17 (PDF, 2.1 MB)

IndusDesk

hello@indusdesk.com · +91 11 4141 3939

9th Floor, Hemkunt House, Rajendra Place, New Delhi, Delhi 110008, India

Read online: indusdesk.com/meity/cross-border-data-transfer/