October 31, 2026

MINISTRY OF ELECTRONICS AND INFORMATION TECHNOLOGY

Data breach reporting in India: CERT-In's 6 hours and DPDP's 72

Data breach reporting in India runs on two clocks. CERT-In, India's cyber security agency, makes you report listed cyber incidents, breaches included, within 6 hours of noticing them. From about May 13, 2027, the Digital Personal Data Protection (DPDP) Rules add notice to everyone affected and the Data Protection Board without delay, then a detailed Board report within 72 hours.

BOTH, WHEN A LISTED cyber incident compromises personal data and the DPDP duties have started. CERT-In's report applies now, within 6 hours of noticing a listed incident. From about May 13, 2027, any personal data breach goes to the Data Protection Board, without delay and then in detail within 72 hours, and to each affected person.

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

Data breach reporting in India: CERT-In's 6 hours and DPDP's 72

Ministry of Electronics and Information Technology · October 31, 2026

Data breach reporting in India runs on two clocks. CERT-In, India's cyber security agency, makes you report listed cyber incidents, breaches included, within 6 hours of noticing them. From about May 13, 2027, the Digital Personal Data Protection (DPDP) Rules add notice to everyone affected and the Data Protection Board without delay, then a detailed Board report within 72 hours.

Do you report to CERT-In, the Data Protection Board, or both?

Both, when a listed cyber incident compromises personal data and the DPDP duties have started. CERT-In's report applies now, within 6 hours of noticing a listed incident. From about May 13, 2027, any personal data breach goes to the Data Protection Board, without delay and then in detail within 72 hours, and to each affected person.

The two reports side by side: cyber incident reporting to CERT-In, and personal data breach notification under the DPDP Rules

What it asks	CERT-In report	DPDP breach report
Who reports	Service providers, intermediaries, data centers, companies and other businesses, and government organizations (direction (ii); FAQ Q25)	The Data Fiduciary, which decides, alone or with others, why and how the personal data is processed (DPDP Act, sections 2(i) and 8(6))
Reports to	CERT-In	The Data Protection Board and each affected person (section 8(6))
What triggers it	Any of the 20 kinds of incident in Annexure I, data breaches and leaks included	Any personal data breach (rule 7)
Deadline	Within 6 hours of noticing the incident or being told about it (direction (ii))	Without delay to each person and to the Board; then the detailed Board report within 72 hours of becoming aware, or longer if the Board allows it on a written request (rule 7)
In force from	In force now: since 60 days after April 28, 2022 (closing paragraph); for MSMEs, since September 25, 2022 (CERT-In, June 27, 2022)	About May 13, 2027, eighteen months after the Gazette of November 13, 2025 (G.S.R. 843(E), para (c))
Penalty for failing	Up to 1 year in prison, a fine of up to ₹1 crore, or both (Information Technology Act, section 70B(7))	Up to ₹200 crore (DPDP Act, Schedule, item 2)
Source	No. 20(3)/2022-CERT-In, direction (ii) and Annexure I	DPDP Act, 2023, section 8(6); G.S.R. 846(E), rule 7

Among the documents read to October 31, 2026, no official text puts the two reports together. The DPDP Act applies in addition to other laws, not in place of them (section 38(1)), so you plan for both. MeitY's summary of comments on the draft Rules records requests for clarity on how the 72-hour rule sits with other duties, such as CERT-In's 6 hours. The final Rules don't mention CERT-In.

The DPDP Act also reaches processing outside India connected with offering goods or services to people in India (section 3(b)).

CERT-In and the DPDP Rules both sit under MeitY, the Ministry of Electronics and Information Technology.

Which incidents must go to CERT-In within 6 hours?

You must report every incident listed in Annexure I of CERT-In's directions within 6 hours of noticing it or being told about it (direction (ii)). The list has 20 kinds, data breaches and data leaks among them. It binds service providers, intermediaries, data centers, companies and other businesses, and government bodies; individual citizens aren't covered (FAQ Q7).

Among the 20 kinds in Annexure I of the directions:

- Data breach (item xi) and data leak (item xii)
- Unauthorized access to IT systems or data (item iii)
- Malicious code attacks such as ransomware (item v), and identity theft, spoofing and phishing (item vii)
- Denial of service attacks (item viii)
- Attacks on cloud systems (item xviii), digital payment systems (item xiv), IoT devices (item xiii) and AI systems (item xx)

CERT-In's FAQ of May 2022 confirms that the clock runs from noticing, even for an incident that went undetected for a long time (Q24). You don't need every fact by then: report what you know and send the rest later, within reasonable time (Q30).

The FAQ singles out four kinds of listed incident to report inside the 6 hours (Q30):

- Severe incidents, such as denial of service or ransomware, on any part of the public information infrastructure
- Data breaches or data leaks

- Large-scale or most frequent incidents
- Incidents that affect human safety

The direction itself sets 6 hours for every listed incident, and the FAQ says it isn't a legal document (introduction, note).

Who reports when a vendor or cloud provider is breached?

Whoever notices the incident reports it to CERT-In. CERT-In's FAQ says a contract can't transfer, indemnify or dispense with that duty (Q13), and that it overrides any confidentiality clause because of section 81 of the IT Act (Q22). So if you and your vendor both notice it, each of you reports.

CERT-In's FAQ gives the example of an attack on an outsourcing partner's servers that compromises a consumer business's data (Q13). Asked about your data in a third party's systems, it answers that the directions apply to all entities so far as reporting goes (Q31).

Under the DPDP Act, the breach notice falls on the Data Fiduciary, which stays responsible for processing its Data Processor does for it, whatever any agreement says (sections 8(6) and 8(1)). Both duties start about May 13, 2027.

Intermediaries also carry the CERT-In duty in rule 3(1)(l) of the IT Rules, 2021. CERT-In's FAQ adds that they should report kinds of incident that neither the CERT-In Rules, 2013 nor the directions list, weighing their nature, severity and impact (Q10).

How do you report an incident to CERT-In?

You report an incident to CERT-In by email at incident@cert-in.org.in, by phone on 1800-11-4949 or by fax on 1800-11-6969 (direction (ii) and Annexure I). Send your logs with the report, and keep a designated Point of Contact who answers CERT-In's follow-up orders in the time and format it sets.

1. Name a Point of Contact first

Send its details to info@cert-in.org.in in the Annexure II format and keep them current. CERT-In sends its requests and directions there (direction (iii)).

2. Report within 6 hours

Use the email, phone or fax line above. CERT-In publishes its reporting methods and formats at cert-in.org.in (direction (ii)).

3. Send your logs

Keep logs of all your information and communication technology (ICT) systems securely for a rolling 180 days within Indian jurisdiction, and give them to CERT-In with the report or on its order (direction (iv)).

4. Answer CERT-In's orders

Take the action, or give the information or help, it asks for, in the format and time it sets, up to near real-time. Missing the format or the time counts as non-compliance (direction (iii)).

For the clock rule, the logs and the customer records cloud and VPN providers keep, see CERT-In directions: logs, clocks, records and incident reports.

What must you tell affected people under the DPDP Rules?

From about May 13, 2027, a Data Fiduciary that becomes aware of a personal data breach must tell each affected person without delay. It writes to the best of its knowledge, in a concise, clear and plain way, through the person's user account or a contact the person registered with it (rule 7(1)).

Rule 7 covers "any personal data breach". The DPDP Act defines one as any unauthorized processing of personal data, or its accidental disclosure, acquisition, sharing, use, alteration, destruction or loss of access, that compromises its confidentiality, integrity or availability (section 2(u)).

The message must cover (rule 7(1), clauses (a) to (e)):

- A description of the breach: its nature, its extent and when it happened
- The consequences likely to arise for the person
- What the Data Fiduciary has done, and is doing, to reduce the risk, if anything

- The safety steps the person can take to protect their interests
- The business contact of someone who can answer the person's questions for the Data Fiduciary

What goes to the Data Protection Board, and when?

From about May 13, 2027, the Data Protection Board gets two reports. Without delay, the Data Fiduciary sends a description of the breach: its nature, extent, timing, location and likely impact (rule 7(2)(a)). Within 72 hours of becoming aware, it sends a detailed report, unless the Board allows a longer period on a written request (rule 7(2)(b)).

The 72-hour report covers (rule 7(2)(b), items (i) to (vi)):

- Updated and detailed information on the first description
- The broad facts of the events, circumstances and reasons that led to the breach
- The steps taken or proposed, if any, to reduce the risk
- Any findings on the person who caused the breach
- The remedial steps taken to prevent a repeat
- A report on the notices given to affected people

Once it receives a breach intimation, the Board may direct urgent remedial or mitigation steps, inquire into the breach and impose a penalty (DPDP Act, section 27(1)(a)). It works as a digital office (DPDP Rules, rule 20).

What if you don't report a breach?

Not following CERT-In's directions, the 6-hour report included, can bring up to one year in prison, a fine of up to ₹1 crore, or both (IT Act, section 70B(7)). From about May 13, 2027, failing to notify the Data Protection Board or an affected person may cost up to ₹200 crore (DPDP Act, Schedule, item 2).

The fine in section 70B(7) was ₹1 lakh until the Jan Vishwas (Amendment of Provisions) Act, 2023 raised it to ₹1 crore, from November 30, 2023 (Schedule, serial 32, entry (I); S.O. 4745(E)). CERT-In's FAQ of May 2022 still quotes ₹1 lakh (introduction, para 4), so pages that copy it are out of date.

CERT-In says it will use this power reasonably, where non-compliance is deliberate (FAQ Q23). A court can take up the offense only on a complaint from an officer CERT-In authorizes (section 70B(8)).

Under the DPDP Act, failing to take reasonable security safeguards may cost up to ₹250 crore (Schedule, item 1). The Board imposes a penalty only where it finds a breach significant, after an inquiry and a hearing (section 33(1)). See DPDP Act penalties: fines, the Data Protection Board and appeals.

How IndusDesk helps with data breach reporting in India

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 reporting a data breach Message us on WhatsApp

Frequently asked questions

Do the CERT-In directions apply to a foreign company with no office in India?

Yes, on CERT-In's reading: its FAQ says the directions apply to any entity whatsoever in the matter of cyber incidents, citing sections 1 and 75 of the IT Act (Q26). It also says service providers, intermediaries, data centers, companies and other businesses offering services to users in India must designate a Point of Contact, physical presence or not (Q29). The FAQ isn't a legal document, and the CERT-In directions guide has the detail.

Must logs be kept for 180 days, and must they stay in India?

Yes, under direction (iv) of CERT-In's directions: logs of all ICT systems, kept securely for a rolling 180 days within Indian jurisdiction. The FAQ says copies may also be stored abroad if you can produce them in reasonable time (Q35), but that providers serving users in India keep logs in Indian jurisdiction (Q36). Only the direction is binding.

What security safeguards do the DPDP Rules require?

Rule 6(1) of the DPDP Rules sets the minimum: data security such as encryption or masking, access controls, logs and monitoring, backups, safeguard clauses in processor contracts, and technical and organizational measures. It also has you keep the logs and personal data needed to investigate unauthorized access for one year, unless another law requires otherwise. Failing to take reasonable safeguards may cost up to ₹250 crore from about May 13, 2027, and the DPDP Act guide has the rest.

Sources

- 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 relating to information security practices, procedure, prevention, response and reporting of cyber incidents, directions (ii) to (iv), the closing paragraph and Annexures I and II

- CERT-In, May 2022: Frequently Asked Questions on the Cyber Security Directions of 28.04.2022, introduction (para 4 and note) and Questions 7, 8, 10, 13, 22 to 26, 29 to 31, 35 and 36
- CERT-In, No. 20(3)/2022-CERT-In, June 27, 2022: Extension of timelines for enforcement of the Cyber Security Directions of 28th April, 2022 for MSMEs and for validation of subscriber and customer details
- Ministry of Electronics and Information Technology, G.S.R. 846(E), November 13, 2025: Digital Personal Data Protection Rules, 2025, rules 1, 6, 7 and 20
- Ministry of Electronics and Information Technology, G.S.R. 843(E), November 13, 2025: dates on which the provisions of the Digital Personal Data Protection Act, 2023 come into force, para (c)
- Ministry of Electronics and Information Technology: Summary of submissions received on Digital Personal Data Protection Rules 2025 (undated; uploaded January 14, 2026), Rule 7, item 3
- The Digital Personal Data Protection Act, 2023 (Act No. 22 of 2023), August 11, 2023: sections 2(i), 2(u), 3(b), 8(1), 8(6), 27(1)(a), 33(1) and 38(1), and the Schedule, items 1 and 2
- The Information Technology (Amendment) Act, 2008 (Act No. 10 of 2009): section 70B, sub-sections (6) to (8)
- The Jan Vishwas (Amendment of Provisions) Act, 2023 (Act No. 18 of 2023), August 11, 2023: the Schedule, serial 32, entry (I)
- Ministry of Electronics and Information Technology, S.O. 4745(E), October 31, 2023: date of coming into force of the Jan Vishwas Act, 2023 amendments to the Information Technology Act, 2000
- Ministry of Electronics and Information Technology: Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, as updated on February 10, 2026, rule 3(1)(l)

IndusDesk

hello@indusdesk.com · +91 11 4141 3939

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

Read online: indusdesk.com/meity/data-breach-reporting/