MINISTRY OF ELECTRONICS AND INFORMATION TECHNOLOGY

MeitY questions, answered from the official texts

This page answers 159 questions about MeitY, the Ministry of Electronics and Information Technology, from the official texts as of October 31, 2026. Each cites its clause and links a deeper guide. They're grouped by who asks, from privacy, security and platform teams to game publishers, electronics makers and foreign companies. Where the texts stop, the answer says so.

MEITY, THE MINISTRY OF Electronics and Information Technology, is the ministry that administers the IT Rules, 2021 for online intermediaries (rule 2(1)(l)) and made the Digital Personal Data Protection (DPDP) Rules, 2025. CERT-In, the national cyber security incident agency, and the Online Gaming Authority work under it. MeitY also runs the electronics incentives and empanels government cloud.

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

MeitY questions, answered from the official texts

Ministry of Electronics and Information Technology · October 31, 2026

This page answers 159 questions about MeitY, the Ministry of Electronics and Information Technology, from the official texts as of October 31, 2026. Each cites its clause and links a deeper guide. They're grouped by who asks, from privacy, security and platform teams to game publishers, electronics makers and foreign companies. Where the texts stop, the answer says so.

General MeitY questions: its laws and its agencies

What is MeitY, and what does it do?

MeitY, the Ministry of Electronics and Information Technology, is the ministry that administers the IT Rules, 2021 for online intermediaries (rule 2(1)(l)) and made the Digital Personal Data Protection (DPDP) Rules, 2025. CERT-In, the national cyber security incident agency, and the Online Gaming Authority work under it. MeitY also runs the electronics incentives and empanels government cloud.

MeitY: India's data, platform, cyber security and electronics rules → The guide this page belongs to

Which laws and rules does MeitY administer?

MeitY administers the IT Rules, 2021 under the Information Technology Act, 2000, and made the DPDP Rules, 2025 and the Online Gaming Rules, 2026. Under the IT Act, it designates the section 69A blocking officer (S.O. 4769(E)) and declares protected systems under section 70. The Ministry of Information and Broadcasting runs the Rules' part for digital publishers.

What MeitY covers, in our MeitY guide →

Are MeitY's and CERT-In's FAQs legally binding?

Neither is legally binding: MeitY's FAQ of February 10, 2026 on the IT Rules amendments says it is not a legal document, and CERT-In's FAQ of May 2022 says the same of itself. Where an FAQ and its rule differ, as CERT-In's does on the fine for ignoring its directions, follow the rule.

The FAQs and the Rules, in our IT Rules guide →

Is CERT-In still the statutory cyber security agency after October 2026?

Yes. Since October 12, 2026, CERT-In has worked as an attached office under MeitY's administrative control, and MeitY's order of that date keeps it as the agency appointed under

section 70B of the IT Act (para 2). On October 31, 2026, CERT-In's page of section 70B directions still listed its directions of April 28, 2022.

What CERT-In requires, in our CERT-In directions guide →

Companies that handle personal data: the DPDP duties

What is the DPDP Act, and whom does it cover?

The Digital Personal Data Protection Act, 2023 is India's data protection law, given assent on August 11, 2023. It covers digital personal data processed in India, and processing abroad connected with offering goods or services to people in India (section 3). Personal or domestic use, and data made public by the person or under a law, fall outside it.

What the Act covers, in our DPDP Act guide →

Does the DPDP Act apply to startups and small businesses, or are they exempt?

The DPDP Act applies to startups and small businesses: section 3 sets no size test. Section 17(3) lets the government exempt some Data Fiduciaries, startups included, from the notice, accuracy, erasure, access and Significant Data Fiduciary duties by notification. No such notification was among the documents read to October 31, 2026.

Who the duties bind, in our DPDP Act guide →

Is a SaaS provider or a web developer a Data Fiduciary or a Data Processor?

Either, depending on who decides. A Data Fiduciary decides why and how personal data is processed, and a Data Processor processes it on a Data Fiduciary's behalf (DPDP Act, section 2(i) and (k)). A SaaS provider or developer handling a client's data for the client is its processor, but a Data Fiduciary for any purpose it decides itself.

Fiduciaries and processors, in our DPDP Act guide →

What must a contract with a Data Processor say, and is it needed now?

To offer goods or services, a Data Fiduciary may use a Data Processor only under a valid contract (DPDP Act, section 8(2)), and the contract must provide for reasonable security safeguards (DPDP Rules, rule 6(1)(f)). The fiduciary stays responsible whatever the contract says, and has its processor erase data too (section 8(7)). Both duties start about May 13, 2027.

Contracts with processors, in our DPDP Act guide →

What must a DPDP notice contain, and in which languages?

A DPDP notice must stand on its own in clear, plain language. It itemizes the personal data, states the specific purpose, and links to the company's site or app to withdraw consent, use rights and complain to the Board (DPDP Rules, rule 3). The person may read it in English or any Eighth Schedule language (DPDP Act, section 5(3)).

Notices, in our DPDP Act guide →

Must you send a fresh notice to customers who consented before the Act?

Yes. Where people consented before the Act started, the Data Fiduciary must send them a notice as soon as reasonably practicable (DPDP Act, section 5(2)), and may keep processing their data until they withdraw consent. Section 5 starts about May 13, 2027, eighteen months after the Gazette of November 13, 2025.

Notices for earlier consent, in our DPDP Act guide →

Is a cookie banner enough under the DPDP Act?

None of the official texts read to October 31, 2026 mentions cookies or banners. Their tests apply however personal data is collected: a notice that stands on its own and itemizes the data and purpose (DPDP Rules, rule 3). Consent must be free, specific, informed, unconditional and unambiguous, by a clear affirmative action (DPDP Act, section 6(1)).

Notice and consent, in our DPDP Act guide →

What makes consent valid, and can you reward users for giving it?

Valid consent is free, specific, informed, unconditional and unambiguous, given by a clear affirmative action, and limited to the data the stated purpose needs (DPDP Act, section 6(1)). The person may withdraw it as easily as it was given (section 6(4)). Whether a reward makes consent conditional isn't settled by any official text read to October 31, 2026.

Consent, in our DPDP Act guide →

Is there a GDPR-style legitimate interest basis, or do you always need consent?

The DPDP Act gives two grounds only: consent, or one of the legitimate uses in section 7 (section 4(1)). The list covers data a person gave voluntarily for a purpose without objecting, State benefits and functions, legal duties to disclose, court orders, medical emergencies, epidemics, disasters and employment. Outside that list and the Act's exemptions (section 17), you need consent.

Legitimate uses, in our DPDP Act guide →

Do employers need consent to process employee data?

Not for employment purposes. Section 7(i) of the DPDP Act makes processing for employment, or to safeguard the employer from loss or liability, a legitimate use that needs no consent. The employer still owes the other duties of a Data Fiduciary, such as reasonable security safeguards (section 8(5)) and erasure once the purpose is served (section 8(7)).

Legitimate uses, in our DPDP Act guide →

Do you need consent for CCTV footage, emergency contacts, or details customers give about other people?

Digital footage or details that identify a person are personal data (DPDP Act, section 2(t)), so they need consent, a legitimate use such as a medical emergency (section 7(f)), or a section 17 exemption. None of the official texts read to October 31, 2026 deals with CCTV or with details given about third parties as such.

Personal data and its legitimate uses, in our DPDP Act guide →

Do you need a Data Protection Officer, and can the CTO or CISO be one?

Only a Significant Data Fiduciary must appoint a Data Protection Officer: an individual based in India who represents it and answers to its board (DPDP Act, section 10(2)(a)). Other Data Fiduciaries publish a business contact for questions, their officer's if they have one (DPDP Rules, rule 9). The texts set no other qualifications and don't mention a CTO or CISO.

Data Protection Officers, in our DPDP Act guide →

Do you have to use a Consent Manager?

The choice is the person's. Section 6(7) of the DPDP Act says a person may give, manage, review or withdraw consent to a Data Fiduciary through a Consent Manager, which must be registered with the Data Protection Board (section 6(9)). Consent Manager registration starts about November 13, 2026, one year after the Gazette of November 13, 2025.

Consent Managers, in our DPDP Act guide →

Who can register as a Consent Manager, and from when?

A company incorporated in India with a net worth of at least ₹2 crore, whose platform is independently certified against the Board's data protection standards (DPDP Rules, First Schedule, Part A). A Consent Manager can't read the data it passes on, and keeps consent records for seven years or more (Part B). Registration opens about November 13, 2026.

Consent Managers, in our DPDP Act guide →

Can a foreign company be a Consent Manager?

Only through a company incorporated in India, which the DPDP Rules require of every Consent Manager (First Schedule, Part A, item 1). Once registered, its control may change only with the Data Protection Board's prior approval (Part B, item 13), and it may not subcontract or assign its duties (Part B, item 6).

Consent Managers, in our DPDP Act guide →

How is a Consent Manager different from a consent management platform?

A Consent Manager is a legal role, a company registered with the Data Protection Board through which people give, manage, review or withdraw consent (DPDP Act, section 6(7) and (9)). It acts in a fiduciary capacity for them (DPDP Rules, First Schedule, Part B). A consent management platform, the software some companies run, isn't a term in the texts read.

Consent Managers, in our DPDP Act guide →

What security safeguards do the DPDP Rules require?

At the minimum, the DPDP Rules require data security measures such as encryption, masking or tokens; access controls; logs and monitoring, kept a year; and backups. They add processor contract clauses and technical and organizational measures (rule 6(1)). Failing to take reasonable security safeguards (DPDP Act, section 8(5)) can cost up to ₹250 crore from about May 13, 2027.

Security safeguards, in our DPDP Act guide →

An app stores Aadhaar and PAN copies without encryption. What is its exposure?

The DPDP Rules name encryption as one example of a data security measure, beside masking and tokens (rule 6(1)(a)). The test is whether the app took reasonable security safeguards, and failing it can cost up to ₹250 crore from about May 13, 2027 (DPDP Act, Schedule, item 1). The Aadhaar Act's own limits weren't among the texts read.

Security safeguards, in our DPDP Act guide →

How long must you keep personal data and logs, and when must you erase them?

From about May 13, 2027, keep personal data, traffic data and processing logs at least a year, for the Seventh Schedule's purposes, and logs needed to investigate unauthorized access for a year (rules 8(3) and 6(1)(e)). Erase personal data once consent is withdrawn or the purpose is served, unless a law requires keeping it (DPDP Act, section 8(7)).

Retention and erasure, in our DPDP Act guide →

How do you erase data on request when tax or banking rules say keep it?

Keep what the other law requires and erase the rest. The DPDP Act's erasure duty gives way where retention is needed to comply with a law (section 8(7)), and so does an erasure request

(section 12(3)). The Act's own example is a bank that keeps a closed account's identity records for ten years because banking law requires it.

Retention and erasure, in our DPDP Act guide →

How do you verify a parent's consent, and who counts as a child?

A child is anyone under 18 (DPDP Act, section 2(f)), and before processing a child's data the Data Fiduciary checks that the parent is an identifiable adult (DPDP Rules, rule 10). It may rely on identity and age details it holds, or a token from an authorized entity such as Digital Locker. No text read gives a check's cost.

Children's data, in our DPDP Act guide →

Which businesses are exempt from parental consent and the tracking ban?

The DPDP Rules exempt health professionals and clinics, educational institutions, creches and child day care centers, and school transport providers, each for set purposes such as health and safety (rule 12 and Fourth Schedule, Part A). Part B's exempt purposes include checking that a user isn't a child, keeping harmful content from a child, and creating an email-only account.

Children's data, in our DPDP Act guide →

Can you show targeted ads to users under 18?

No: a Data Fiduciary may not track or behaviorally monitor children, or direct targeted advertising at them, and anyone under 18 is a child (DPDP Act, sections 9(3) and 2(f)). It may also not process children's data in a way likely to harm their well-being (section 9(2)). The bar starts about May 13, 2027, subject to the Rules' exemptions.

Children's data, in our DPDP Act guide →

How does the DPDP Act affect ads and marketing by WhatsApp, SMS and email?

Marketing that uses personal data needs consent or a legitimate use (DPDP Act, section 4(1)), and the person may withdraw consent as easily as it was given (section 6(4)). Children can't be the target of such ads (section 9(3)). The telecom regulator's rules on commercial messages weren't among the texts read, so this answer doesn't cover them.

Consent, in our DPDP Act guide →

How does consent work for a person with a disability who has a lawful guardian?

The lawful guardian gives verifiable consent before the person's data is processed, as a parent does for a child (DPDP Act, section 9(1)). The Data Fiduciary checks that a court, a designated authority or a local level committee appointed the guardian (DPDP Rules, rule 11). The Removal of Difficulties Order of October 5, 2026 tidied the section's wording.

Children's and guardians' consent, in our DPDP Act guide →

Will your company be a Significant Data Fiduciary, and is there a user threshold?

Only if the government notifies it, alone or in a class (DPDP Act, section 10(1)), weighing data volume and sensitivity, risk to people's rights, sovereignty, elections, state security and public order. The Act sets no user count, and none had been notified among the documents read to October 31, 2026. The DPDP Rules' user counts are erasure thresholds.

Significant Data Fiduciaries, in our DPDP Act guide →

What extra duties does a Significant Data Fiduciary have?

A Significant Data Fiduciary appoints a Data Protection Officer based in India and an independent data auditor (DPDP Act, section 10(2)). Every twelve months it runs an impact assessment and an audit and reports significant findings to the Board. It checks its algorithmic software and keeps specified data in India (DPDP Rules, rule 13).

Significant Data Fiduciaries, in our DPDP Act guide →

Is there a DPDP compliance certificate you must get?

No certificate for ordinary Data Fiduciaries appears in the texts read to October 31, 2026. The texts set two narrower checks. A Significant Data Fiduciary appoints an independent data auditor (DPDP Act, section 10(2)(b)), and a Consent Manager's platform must be independently certified (DPDP Rules, First Schedule, Part A).

Audits and certification, in our DPDP Act guide →

What rights do people have, and how fast must you answer them?

People may ask for a summary of their data, its processing and who else received it (DPDP Act, section 11), and have it corrected, completed, updated or erased (section 12). They use your grievance system before the Board, and you answer within the period you publish, at most 90 days (DPDP Rules, rule 14(3)).

People's rights, in our DPDP Act guide →

Is processing for research, archiving or statistics exempt?

Yes, with two conditions. The DPDP Act doesn't apply to processing necessary for research, archiving or statistics if the data isn't used for a decision about a particular person (section 17(2)(b)). The processing must also follow the standards in the Rules' Second Schedule (DPDP Rules, rule 16).

Exemptions, in our DPDP Act guide →

Can the government demand personal data from a company, and bar it from telling anyone?

Yes. For purposes listed in the Seventh Schedule, such as state security and assessing Significant Data Fiduciaries, authorized officers may require a Data Fiduciary or intermediary to provide information (DPDP Rules, rule 23(1)). Where disclosure could harm sovereignty or state security, the company may be barred from telling anyone without written permission (rule 23(2)), from about May 13, 2027.

Government requests, in our DPDP Act guide →

Does the DPDP Act weaken the Right to Information Act?

Section 44(3) of the DPDP Act rewrites the Right to Information Act's privacy exemption, section 8(1)(j), to cover any information which relates to personal information. That change took effect on publication of G.S.R. 843(E), dated November 13, 2025. The RTI Act's public-interest override wasn't among the texts read, so this answer doesn't weigh it.

The Right to Information change, in our DPDP Act guide →

Planning for the DPDP dates, the Board and penalties

When do the DPDP duties and penalties start, and is there a soft enforcement period?

Most DPDP duties and all penalties start about May 13, 2027, eighteen months after the Gazette of November 13, 2025 (G.S.R. 843(E), para (c)). The Board started on publication, and Consent Manager registration starts about November 13, 2026. No notification among the documents read sets a soft enforcement period: the eighteen months are the transition.

Every step and its date, in our DPDP Act timeline →

Has the government cut the 18-month DPDP window to 12 months?

No, among the documents read to October 31, 2026. The only 2026 change to the Act is the Removal of Difficulties Order of October 5, 2026, which fixed two wordings and left the dates alone. On August 12, 2026, the government still told the Lok Sabha of an eighteen-month transition (Unstarred Question 3943).

What hasn't changed, in our DPDP Act timeline →

Do the DPDP deadlines run from November 13 or November 14, 2025?

G.S.R. 843(E) counts from Gazette publication and prints no dates. The Gazette issue is dated Thursday, November 13, 2025, but its ID and digital signature carry November 14, as does the government's press backgrounder. So the steps fall about November 13 or 14, 2026 and May 13 or 14, 2027, and this page says about November 13 and May 13.

How the dates are counted, in our DPDP Act timeline →

What did the Removal of Difficulties Order of October 2026 change?

Two wordings, and no dates. The Digital Personal Data Protection (Removal of Difficulties) Order, 2026 (S.O. 5458(E), October 5, 2026) added a missing "of" in section 9(1), so it reads "child or of a person with disability". It also turned "audit" into "data audit" in section 10(2)(c)(ii), on a Significant Data Fiduciary's periodic audit.

The 2026 order, in our DPDP Act timeline →

What happens to IT Act section 43A until the DPDP duties start?

Section 43A stays in force until about May 13, 2027, when the DPDP Act's section 44(2) deletes it (G.S.R. 843(E), para (c)). Until then, a company, firm or other business handling sensitive personal data pays compensation if negligent in maintaining reasonable security practices, causing wrongful loss or gain (IT Act, section 43A). The 2011 rules under it weren't read.

Section 43A, in our DPDP Act timeline →

What are the DPDP penalties?

Up to ₹250 crore for failing to take reasonable security safeguards, and up to ₹200 crore each for not reporting a breach and for breaking the children's data duties (DPDP Act, Schedule). Significant Data Fiduciary duties carry up to ₹150 crore, and other breaches up to ₹50 crore. The Board imposes them only for significant breaches, after a hearing.

Penalties, in our DPDP penalties guide →

Is each DPDP penalty per breach, or capped per inquiry?

The DPDP Act's Schedule sets a ceiling for each kind of breach, and the Board fixes the amount by weighing the breach's nature, gravity and duration, any gain, mitigation and proportionality (section 33(2)). Neither the Act nor the Rules read say how ceilings combine when one inquiry finds several breaches.

How penalties are set, in our DPDP penalties guide →

Has the Data Protection Board been set up, and who sits on it?

The Data Protection Board was set up by G.S.R. 844(E) of November 13, 2025, with its head office in the National Capital Region. Its size reads two ways: G.S.R. 845(E) says four members,

while MeitY's call of May 6, 2026 lists a Chairperson and four Members. The government's Lok Sabha answer of August 12, 2026 named no appointee.

The Board, in our DPDP penalties guide →

Can the Data Protection Board hear complaints or fine companies today?

Not yet. The Board's powers to inquire into breaches and complaints and to impose penalties start about May 13, 2027 (G.S.R. 843(E), para (c)), and its power over Consent Managers about November 13, 2026. The government's Lok Sabha answer of August 12, 2026 named no appointee.

What the Board can do, and when, in our DPDP penalties guide →

How long does a Board inquiry take, and where do appeals go?

The Board is to finish an inquiry within six months, extendable three months at a time with reasons recorded (DPDP Rules, rule 19(9)). Appeals go to the Telecom Disputes Settlement and Appellate Tribunal within 60 days (DPDP Act, section 29), and it is to try to decide them within six months. The six-month periods are the texts' own targets.

Inquiries and appeals, in our DPDP penalties guide →

Can India block a company's service for breaking the DPDP Act?

Yes, after repeated penalties. Once the Board has penalized a Data Fiduciary in two or more instances, the government may act on the Board's advice. After a hearing, it may have public access blocked to what lets the company offer goods or services in India (DPDP Act, section 37(1)), from about May 13, 2027.

Blocking, in our DPDP penalties guide →

Global groups moving data in and out of India

Can personal data be sent outside India, for example to a parent company, cloud or AI service abroad?

Yes. Personal data may go abroad unless the government restricts a country or territory by notification (DPDP Act, section 16(1)), and none had been notified among the documents read to October 31, 2026. The Data Fiduciary must meet any requirements the government sets by order on making data available to a foreign State (DPDP Rules, rule 15).

Transfers abroad, in our cross-border data transfer guide →

Has India restricted transfers to any country yet?

No, among the documents read to October 31, 2026. Section 16(1) of the DPDP Act lets the government restrict transfers to a country or territory outside India by notification, and none had been issued, so the Act names no restricted country. Section 16 itself starts about May 13, 2027.

Restricted countries, in our cross-border data transfer guide →

Will India force companies to keep personal data in India?

Not across the board, but some rules keep some data in India. They cover data the government specifies for a Significant Data Fiduciary (DPDP Rules, rule 13(4)), 180 days of CERT-In logs, and all data on empaneled government cloud. Online gaming directions may require traffic data kept in India (Online Gaming Rules, rule 17).

Data that stays in India, in our cross-border data transfer guide →

What does rule 15 require about foreign governments' access to Indian data?

Rule 15 of the DPDP Rules lets personal data leave India, subject to any requirements the government sets by general or special order on making it available to a foreign State or an entity it controls. No such order was among the documents read to October 31, 2026. The Rules don't address foreign laws such as the US CLOUD Act.

Rule 15, in our cross-border data transfer guide →

If RBI, SEBI or another regulator has stricter data rules, which wins?

For sending data abroad, the stricter Indian law: section 16(2) of the DPDP Act keeps any law that gives a higher degree of protection or restriction on transfers. More generally, the Act adds to other laws rather than replacing them (section 38(1)), and where it conflicts with one, the Act prevails to the extent of the conflict (section 38(2)).

Sector rules, in our cross-border data transfer guide →

Does the DPDP Act apply to data an Indian company or GCC processes for clients abroad?

Mostly not. Where a person based in India, such as a global capability center (GCC), processes data of people outside India under a contract with someone abroad, section 17(1)(d) of the DPDP Act spares most duties. Section 8(1) and (5), on overall responsibility and reasonable security safeguards, still apply.

Work for clients abroad, in our cross-border data transfer guide →

Security and incident teams: breaches and CERT-In

After a breach, do you report to CERT-In in 6 hours, the Data Protection Board in 72 hours, or both?

Both, from about May 13, 2027, when a listed cyber incident compromises personal data. CERT-In needs listed incidents, data breaches included, within 6 hours (CERT-In directions, direction (ii)). The Board will need any personal data breach described without delay and fully reported within 72 hours (DPDP Rules, rule 7(2)); the DPDP Act adds to other laws (section 38(1)).

Both clocks, in our data breach reporting guide →

How fast must a personal data breach be reported under the DPDP Rules, and what must the notices say?

Each affected person is told without delay, in plain words, what happened, the likely consequences, the steps taken, what they can do, and whom to contact (DPDP Rules, rule 7(1)). The Board gets a description without delay, then a full report within 72 hours or a longer period it allows (rule 7(2)). Both start about May 13, 2027.

The DPDP breach notices, in our data breach reporting guide →

Which cyber incidents must go to CERT-In within 6 hours, and when does the clock start?

CERT-In's directions list 20 kinds of incident, including data breaches, ransomware, phishing, and attacks on cloud, IoT, payment and AI systems (Annexure I). The 6 hours run from noticing the incident or being told of it (direction (ii)). CERT-In's FAQ (Q30) singles out severe incidents on public information infrastructure, large-scale or most frequent ones, and those affecting human safety.

CERT-In's 6 hours, in our data breach reporting guide →

What if you don't have all the facts within six hours?

Report what you know within the 6 hours and send the rest later, within reasonable time. CERT-In's FAQ, which isn't legally binding, says entities may give information to the extent available at the time of reporting (Q30). The duty itself, direction (ii) of April 28, 2022, runs 6 hours from noticing the incident or being told of it.

What a first report needs, in our data breach reporting guide →

Who reports when a vendor is breached, and can a confidentiality clause stop the report?

Whoever notices the incident must report it to CERT-In, and CERT-In's FAQ says the duty can't be shifted by contract (Q13). The FAQ also says the duty overrides any confidentiality clause in a contract (Q22), relying on section 81 of the IT Act, which gives the Act effect over any inconsistent law.

Who reports, in our data breach reporting guide →

How do you report an incident to CERT-In?

By email to incident@cert-in.org.in, by phone on 1800-11-4949, or by fax on 1800-11-6969, within 6 hours of noticing the incident (CERT-In directions, direction (ii) and Annexure I). Each entity also names a Point of Contact to deal with CERT-In (direction (iii)), and a service provider serving users in India names one even with no office there (FAQ, Q29).

How to report, in our data breach reporting guide →

What do CERT-In's directions of April 28, 2022 require?

CERT-In's directions, issued under section 70B(6) of the IT Act, require covered entities to sync clocks, report listed incidents within 6 hours and name a Point of Contact. They keep 180 days of information and communication technology (ICT) logs in India. Hosts, virtual private network (VPN) providers and virtual asset firms keep customer records for five years.

The six directions, in our CERT-In directions guide →

Who must follow the CERT-In directions?

Service providers, intermediaries, data centers, companies and other businesses, and government bodies; individual citizens are not covered (CERT-In's FAQ, Q7). The FAQ also reads them as applying to any entity in the matter of cyber incidents, citing IT Act sections 1 and 75 (Q26). Data centers, cloud, virtual private server (VPS) and VPN providers carry extra record duties.

Who the directions bind, in our CERT-In directions guide →

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

Yes, if it serves users in India, by CERT-In's reading. CERT-In's FAQ says providers offering services to users in India must name a Point of Contact, even with no office in India (Q29). It reads the directions as reaching any entity in the matter of cyber incidents, under sections 1 and 75 of the IT Act (Q26).

Foreign providers, in our CERT-In directions guide →

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

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

Logs, in our CERT-In directions guide →

Logs: one year under the DPDP Rules or 180 days under CERT-In?

Both apply, each to its own scope: CERT-In's directions require 180 days of ICT logs today (direction (iv)). From about May 13, 2027, the DPDP Rules add a year for logs and personal data needed to investigate unauthorized access (rule 6(1)(e)). Rule 8(3) adds a year for personal data, traffic data and processing logs, for the Seventh Schedule's purposes.

Logs, in our CERT-In directions guide →

Must your systems sync to Indian government time servers?

Yes, or to a source that matches them. Direction (i) ties ICT clocks to the time servers of the "National Informatics Centre (NIC) or National Physical Laboratory (NPL)", or servers traceable to them (CERT-In directions). CERT-In's FAQ says clocks needn't use Indian Standard Time if the time zone is recorded (Q40).

Clock sync, in our CERT-In directions guide →

Do the CERT-In directions apply to MSMEs, and must they get an annual audit?

Yes: for micro, small and medium enterprises (MSMEs), the directions took effect on September 25, 2022, under CERT-In's extension of June 27, 2022. None of the six directions sets an annual audit. CERT-In's 2025 audit guidelines weren't among the texts read, so this answer can't say what they ask.

Who the directions bind, in our CERT-In directions guide →

What is the penalty for not following CERT-In's directions, and who can demand your logs?

Up to one year in prison, a fine of up to ₹1 crore, or both (IT Act, section 70B(7)), the fine raised from ₹1 lakh from November 30, 2023 by the Jan Vishwas Act, 2023. CERT-In's FAQ still prints ₹1 lakh, and says log requests come from an officer of Deputy Secretary rank or above (Q38).

The penalty, in our CERT-In directions guide →

Must you report vulnerabilities to CERT-In, or patch exploited bugs within set hours?

Under CERT-In's directions, no: reporting a vulnerability on its own, unconnected with an incident, isn't mandatory, CERT-In's FAQ says (Q15). But CERT-In's guidelines of June 10, 2026 ask equipment makers and technology providers to tell CERT-In and affected organizations

immediately about critical and high-severity flaws. They set indicative patch timelines, from an emergency release to 90 days (section 3.1).

Reporting, in our CERT-In directions guide →

Cloud, hosting, data center and VPN providers

What customer records must data centers, cloud, VPS and VPN providers keep, and does it cover company VPNs?

Data centers and VPS, cloud and VPN providers record validated customer names, hire periods, IP addresses, contact details, purpose and ownership (CERT-In directions, direction (v)). They keep them five years after the registration ends, or longer if a law requires. The VPN rule covers providers of internet proxy-like services to the general public, not company VPNs (CERT-In's FAQ, Q34).

Records for hosts and VPN providers, in our CERT-In directions guide →

What did MeitY's April 2026 advisory ask VPN providers and platforms to do?

MeitY's advisory dated April 25, 2026 told VPN providers and other intermediaries that giving access to blocked betting and prediction market platforms may breach their IT Rules due diligence (para 3). That may cost them their section 79 protection (para 7). MeitY's document list dates it April 24; the date written on it reads April 25.

Advisories, in our IT Rules guide →

If you run your own VPN on a rented server, do the CERT-In record rules apply?

CERT-In's FAQ says the VPN record rule covers providers of internet proxy-like services to the general public (Q34), and the directions don't cover individual citizens (Q7). A self-hosted VPN for your own use isn't addressed in the texts read. The server's host, as a data center, VPS or cloud provider, keeps its own customer records (direction (v)).

Records for hosts and VPN providers, in our CERT-In directions guide →

Who can get MeitY cloud empanelment, and how?

An applicant must be incorporated in India and operating there three consecutive years (MeitY's call of July 2026, Annexure 6). It, or one holding company, needs positive net worth and ₹10

crore of Indian cloud or data center revenue over the last two financial years, and cloud infrastructure sold in India at 99.5% uptime. MeitY's testing directorate audits it first.

Eligibility, in our cloud empanelment guide →

Must government data on an empaneled cloud stay in India?

Yes. Empaneled services are hosted in India, with all data, processing and backups inside India, and network and security operations centers in India too (MeitY's cloud call of July 2026, section 5.2.4(h) and (k)). No legal framework outside Indian law may apply to running them, and CERT-In gets complete access to the infrastructure used for government bodies.

Data in India, in our cloud empanelment guide →

How long does empanelment last, and how often is it audited?

Five years, after an audit before empanelment, renewing automatically if the provider declares nothing listed has changed (MeitY's cloud call, section 8). The call reads two ways on timing: renewal after three years (item 9) or in the fifth year (item 8), and a surveillance audit every year (section 2) or after the third (item 8).

Term and audits, in our cloud empanelment guide →

Do private companies need a MeitY-empaneled cloud?

MeitY empanels the cloud services that government departments may buy, and takes applications all year (MeitY's cloud call, section 8). The call is for services sold to government buyers and sets no duty for private ones. Sector regulators' own rules, such as those for banks, weren't among the documents read, so this answer doesn't cover them.

Who empanelment is for, in our cloud empanelment guide →

Platforms, apps and websites: the IT Rules

What are the IT Rules, 2021, and who must follow them?

The IT Rules, 2021 (G.S.R. 139(E), last amended February 10, 2026) set the due diligence an intermediary follows to keep its section 79 protection (rule 3(1)). An intermediary receives, stores or transmits a record for someone else, such as internet providers, hosts, search engines, payment sites and marketplaces (IT Act, section 2(1)(w)).

Who the Rules cover, in our IT Rules guide →

Is your website, SaaS or AI chatbot an intermediary that can claim safe harbor?

The answer turns on what the service does. An intermediary receives, stores or transmits a record on behalf of another person, or provides a service for that record (IT Act, section 2(1)(w)). The government told the Lok Sabha on July 29, 2026 that an AI service's status depends on the nature of the service (answer 1647), and gave no list.

Intermediaries and safe harbor, in our IT Rules guide →

Does a small platform or foreign SaaS need a grievance officer, and must that officer live in India?

Every intermediary, whatever its size, must publish its Grievance Officer's name, contact details and a way to complain (IT Rules, rule 3(2)(a)). A significant social media intermediary, one with over 50 lakh registered users in India, must appoint three officers resident in India, including a Resident Grievance Officer (rule 4(1)). MeitY may order others to do the same (rule 6(1)).

Grievance officers, in our IT Rules guide →

When does a platform lose its section 79 safe harbor?

When it took part in the unlawful act, or fails to remove material quickly once it has actual knowledge or a government notice (IT Act, section 79(3)). The shield also needs due diligence, and a role limited to giving access or no hand in starting, addressing or changing the transmission (section 79(2)). Failing the IT Rules removes it (rule 7).

Safe harbor, in our IT Rules guide →

How fast must a platform remove content now: 3 hours, 2 hours or 36?

All three apply since February 20, 2026, to different things (G.S.R. 120(E)). Three hours follow a court order or an authorized officer's reasoned intimation (rule 3(1)(d)), two hours a person's complaint of intimate or morphed images (rule 3(2)(b)). Complaints asking to remove most listed content get 36 hours; MeitY's 2021 FAQ still prints the old limits.

Time limits, in our IT Rules guide →

Who can send a platform a takedown intimation under rule 3(1)(d)?

Officers of Joint Secretary rank or above, or a Director where none is appointed, authorized by written order; for police, Deputy Inspector General rank or above (IT Rules, rule 3(1)(d)(ii)). Intimations give the legal basis, the unlawful act and the exact URL. G.S.R. 775(E) set these from November 15, 2025; G.S.R. 120(E) added the written order from February 20, 2026.

Takedown intimations, in our IT Rules guide →

What did the February 2026 amendment to the IT Rules change?

G.S.R. 120(E) of February 10, 2026, in force from February 20, cut takedowns on orders from 36 hours to three and grievances from 15 days to seven. Removal complaints fell from 72 hours to 36, and intimate-image complaints from 24 hours to two. It also brought in rules on synthetic content and a reminder to users every three months.

The 2026 changes, in our IT Rules guide →

What are the grievance timelines for intermediaries now?

The Grievance Officer acknowledges a complaint within 24 hours and resolves it within 7 days, down from 15 (IT Rules, rule 3(2)(a)(i)). A complaint asking to remove most listed content is resolved within 36 hours, down from 72, and intimate or morphed images come down within two hours. The new limits apply since February 20, 2026.

Time limits, in our IT Rules guide →

When is a platform a significant social media intermediary, and what must it do?

A social media intermediary with more than 50 lakh registered users in India is significant (S.O. 942(E)). It appoints a Chief Compliance Officer, a round-the-clock nodal contact for law enforcement and a Resident Grievance Officer, all living in India. It publishes a compliance report every month and keeps a physical contact address in India (IT Rules, rule 4).

Significant platforms, in our IT Rules guide →

Which officers must a significant social media intermediary appoint, and can they be held personally liable?

Three, all resident in India: a Chief Compliance Officer, a nodal contact for law enforcement around the clock, and a Resident Grievance Officer (IT Rules, rule 4(1)). The Chief Compliance Officer is liable in proceedings over third-party content if the officer fails to ensure the platform observes due diligence. Rule 4(1)(a)'s proviso bars liability on the platform without a hearing.

Significant platforms, in our IT Rules guide →

What must a significant social media intermediary's monthly compliance report contain?

The details of complaints received and action taken, and the number of links or items the platform removed through proactive monitoring with automated tools (IT Rules, rule 4(1)(d)). The rule adds any other relevant information as may be specified. MeitY's 2021 FAQ answer on the report's format isn't covered here.

Significant platforms, in our IT Rules guide →

Must messaging apps trace the first originator of a message?

A messaging service that is a significant social media intermediary must be able to identify a message's first originator when a court, or an order under IT Act section 69, requires it (IT Rules, rule 4(2)). Orders are limited to listed offenses punishable with five years or more. The court challenge wasn't among the texts read.

Messaging services, in our IT Rules guide →

Is the fact check unit rule in force?

MeitY's consolidated IT Rules of February 10, 2026 still print the fact check unit rule, in rule 3(1)(b)(v). No court ruling on it was among the documents read to October 31, 2026, so this page can't say whether it can be applied today.

What the Rules still print, in our IT Rules guide →

How fast must a platform give information to a government agency?

As soon as possible, and within 72 hours of a written order from an authorized agency, for identity checks, offenses or cyber security incidents (IT Rules, rule 3(1)(j)). Removed information and its records are kept 180 days, or longer if required, and a user's registration details 180 days after the account closes (rule 3(1)(g) and (h)).

Government requests, in our IT Rules guide →

What must a platform do when someone reports intimate images shared without consent?

The platform must remove or disable the content within two hours of the complaint, down from 24 since February 20, 2026 (IT Rules, rule 3(2)(b); G.S.R. 120(E)). The rule covers content exposing a person's private area, nudity or sexual acts, or impersonating them with morphed images. The person, or anyone on their behalf, may complain.

Intimate images, in our IT Rules guide →

How often must a platform remind users of its rules?

At least once every three months, since February 20, 2026 (IT Rules, rule 3(1)(c)). The reminder tells users that breaking the platform's rules can lead to suspension or termination of access, or removal of the content. Rule 3(1)(f) still asks platforms to tell users of their rules, or changes to them, at least once a year.

User duties, in our IT Rules guide →

Are MeitY's advisories binding on platforms, and what would the April 2026 draft change?

The draft amendment would make them binding: intermediaries would follow MeitY's written clarifications, advisories, orders and guidelines, as part of their section 79 due diligence

(proposed rule 3(4)). Each would state its legal basis and whom it covers. The draft leaves its start date blank and is a proposal, not law.

The April 2026 draft, in our IT Rules guide →

Draft IT Rules would make MeitY advisories part of due diligence →

Where can you read the draft IT Rules amendment, and can you still comment?

MeitY first posted the draft on March 30, 2026, and its notice of April 21, 2026 added a change to the synthetic content label and set May 7, 2026 for comments, so the window has closed. Our files server holds the April 2026 draft, which leaves its start date blank.

The April 2026 draft, in our IT Rules guide →

Would news posted by ordinary users come under the Part III oversight rules?

Under the April 2026 draft amendment, yes: Part III's oversight rules, rules 14 to 16, would also apply to news and current affairs content that users who aren't publishers post on intermediaries (para 5). Today Part III covers digital news publishers and streaming services (rule 8). The draft is a proposal, not law.

The April 2026 draft, in our IT Rules guide →

Does Part III, the Digital Media Ethics Code, apply to a news or streaming service?

Yes: Part III of the IT Rules applies a code of ethics to digital news publishers and streaming services that operate in India or do systematic business there (IT Rules, rule 8(2)). The Ministry of Information and Broadcasting administers it (rule 8(1)). Who counts as a publisher, and the court challenges, aren't covered by the texts read here.

Part III, in our IT Rules guide →

Are WhatsApp group admins liable under the IT Rules?

The IT Rules set duties for intermediaries (rule 3), and none of the texts read names group admins. An intermediary is one who receives, stores or transmits a record for another person, or provides a service for it (IT Act, section 2(1)(w)). Whether running a group, or its members' posts, creates liability isn't addressed in the texts read.

Who the Rules cover, in our IT Rules guide →

How does the government block a website or app, and can you see the order?

Under section 69A of the IT Act, the central government may order an intermediary to block public access to information for reasons such as sovereignty, security or public order. Failing to comply carries up to seven years in prison and a fine. MeitY designates the officer who handles requests (S.O. 4769(E)), and the blocking procedure rules weren't read.

The IT Act's powers, in our MeitY guide →

AI developers, platforms and creators

What counts as synthetically generated information?

Synthetically generated information is audio, images or video created or altered by computer so that it looks real and could pass for a real person or event (IT Rules, rule 2(1)(wa)), regulated since February 20, 2026. Routine editing, accessibility tools, translation, and good-faith documents, slides and training material are excluded, if they don't create false documents or change meaning.

The definition, in our AI-generated content guide →

Does the AI label rule cover AI-written text, or content posted before February 20, 2026?

Text on its own isn't synthetically generated information, MeitY's FAQ of February 10, 2026 says (Q8), though unlawful text is still covered by the general rules. The definition covers audio, images and video (rule 2(1)(wa)). The texts read don't say whether the rule reaches content posted before it started on February 20, 2026.

What the rule covers, in our AI-generated content guide →

Which services must follow the synthetic content rules, and do they cover enterprise AI tools?

An intermediary whose service lets users create or share synthetic content must use reasonable technical measures against unlawful kinds and label the rest (IT Rules, rule 3(3)). Whether an AI service is an intermediary depends on the service, the government told the Lok Sabha (answer 1647). No text read addresses enterprise tools as such.

Which services, in our AI-generated content guide →

Do creators have to label the AI videos, voices or images they post?

The labeling duty is the platform's (IT Rules, rule 3(3)(a)(ii)), but on a significant social media platform, one with over 50 lakh registered users in India, you must declare whether content is synthetic (rule 4(1A)(a)). Platforms warn users that misuse can bring penalties under the IT Act, the Bharatiya Nyaya Sanhita and other laws (rule 3(1)(ca)).

Labels and declarations, in our AI-generated content guide →

How must AI-generated content be labeled, and must the label cover 10% of the screen?

With a prominent label that is easily noticeable and adequately perceivable, or a spoken disclosure at the start of audio (IT Rules, rule 3(3)(a)(ii)). Permanent metadata with a unique identifier goes in too, where technically feasible. The rule sets no share of the screen, and the April 2026 draft would keep the label visible throughout.

Labels, in our AI-generated content guide →

Must large platforms check whether uploaded content is AI-generated?

Yes, a significant social media intermediary must. Before content goes up, it asks users to declare whether it is synthetic, checks the declaration with appropriate technical measures, and labels content confirmed as synthetic (IT Rules, rule 4(1A)). If it knowingly lets unlabeled synthetic content through, it is deemed to have failed its due diligence.

Large platforms, in our AI-generated content guide →

What happens if a platform or user ignores the AI content rules?

A platform that fails the IT Rules loses its section 79 shield and is liable under the IT Act and the Bharatiya Nyaya Sanhita (IT Rules, rule 7). On learning of a violation, it acts quickly, for example by removing content and suspending the account (rule 3(1)(cb)). The Rules name users' penalties under other laws without setting them.

Enforcement, in our AI-generated content guide →

Does removing content with automated tools cost a platform its safe harbor?

No. Removing or disabling content in line with the IT Rules, including with automated tools or other reasonable technical measures, doesn't break the section 79 conditions (IT Rules, rule 2(1B)). That clarification came with the February 2026 amendment that added the synthetic content duties (G.S.R. 120(E)).

Removal and safe harbor, in our AI-generated content guide →

Does India have an AI law?

Not a separate one. The India AI Governance Guidelines, released on November 5, 2025, say a separate AI law isn't needed at this stage. They expect existing laws on IT, data protection, consumer protection, civil and criminal law to govern AI uses, and the government points to the 2026 synthetic content rules for deepfakes.

The guidelines, in our AI governance guide →

Do you need government permission to launch an AI model or chatbot in India?

No approval regime appears in the texts read to October 31, 2026. The India AI Governance Guidelines advise regulators to avoid mandatory approvals unless needed. MeitY's advisory of

March 15, 2024, replacing one of March 1, 2024, asks for labels on under-tested or unreliable AI models. A chatbot making realistic audio, images or video must meet the synthetic content rules.

What a launch needs, in our AI governance guide →

Who steers AI governance in the government?

MeitY leads: a committee it set up in July 2025 wrote the India AI Governance Guidelines. On April 13, 2026, it formed the AI Governance and Economic Group, chaired by the Minister of Electronics and IT, to issue guidelines and study regulatory gaps. The government also has an expert committee and an AI Safety Institute.

Who decides, in our AI governance guide →

Is there an Indian certification for AI systems?

The certification the government points to is to ISO/IEC 42001:2023, the AI management system standard. NABCB, the National Accreditation Board for Certification Bodies, accredits the bodies that certify AI developers, producers and users to it, the government told the Lok Sabha on August 5, 2026 (answer 2988).

Certification, in our AI governance guide →

Can you train AI models on personal data or publicly available content?

From about May 13, 2027, personal data needs consent or a legitimate use (DPDP Act, section 4(1)) unless an exemption applies. The Act doesn't cover data the person made public, or that a law required to be made public (section 3(c)). MeitY's discussion draft, posted October 29, 2026, covers a data architecture for AI training. Copyright law wasn't read.

Training data, in our AI governance guide →

Game publishers, platforms and players

What does the Online Gaming Act ban, and since when?

The Promotion and Regulation of Online Gaming Act, 2025 bans offering online money games, advertising them and handling payments for them (sections 5 to 7), whether the game rests on skill, chance or both. The ban took effect on May 1, 2026, with the Online Gaming Rules, 2026 (S.O. 1994(E)), not on October 1, 2025.

The bans, in our Online Gaming Act guide →

Online gaming rules take effect with the Act on May 1, 2026 →

What are the penalties under the Online Gaming Act?

Offering an online money game, or handling its payments, carries up to three years in prison, a fine of up to ₹1 crore, or both (Online Gaming Act, section 9). Advertising one: up to two years, ₹50 lakh, or both. Repeat offenses bring minimum terms and fines up to ₹2 crore; ignoring a direction, up to ₹10 lakh (section 12).

Penalties, in our Online Gaming Act guide →

Can a player be jailed or fined for playing online money games?

None of the Online Gaming Act's penalty sections names a user who only plays. Section 9 punishes those who offer, advertise or handle payments for online money games (Online Gaming Act, section 9), and section 12's penalty is for failing a direction of the government or the Authority. The texts read say nothing more about players.

Players, in our Online Gaming Act guide →

If you played before May 1, 2026, can you still get into trouble?

The Online Gaming Act came into force on May 1, 2026 (S.O. 1994(E)). Its penalty sections reach those who offer, advertise or handle payments for online money games, not a user who only plays (section 9). The texts read don't address play before the start date.

Players, in our Online Gaming Act guide →

Are free contests with cash prizes, in-game purchases or loot boxes online money games?

An online money game is played by paying fees or staking money or other stakes, such as coins bought with money, hoping to win (Online Gaming Act, section 2(1)(g) and (j)). The Authority decides each game on its own facts and revenue model (rules 9 and 10). No decision on these models was among the documents read.

What a money game is, in our Online Gaming Act guide →

Must every online game register with the Online Gaming Authority?

No. A game must be registered only where the government notifies it or its category, where it is offered as an e-sport, or where the Authority so decides on an application (Online Gaming Rules, rule 12). In notifying games, the government may weigh the provider's country of origin, risk, scale and payments.

Registration, in our Online Gaming Act guide →

How does the Authority decide whether a game is an online money game?

The Online Gaming Authority weighs fees and deposits, the hope of winnings, the revenue model, and whether rewards can be redeemed outside the game (Online Gaming Rules, rule 9). A

decision covers only that game from that provider (rule 10(2)), due within 90 days as far as practicable. Money games go on a published list (rule 26).

How games are decided, in our Online Gaming Act guide →

How long do decisions and registration take, and how long is a certificate valid?

The Rules set 90 days from a complete application for deciding whether a game is a money game, as far as practicable (Online Gaming Rules, rule 10(3)(a)), and 90 days to register an e-sport (rule 13(3)). A certificate lasts up to ten years, not five, for the period the provider names (rule 14(2)).

Time limits, in our Online Gaming Act guide →

Which games are legal now, and does the law name titles?

The Online Gaming Act and Rules set categories, not titles. E-sports and online social games are promoted, and the government may recognize and register them (sections 3 and 4), while online money games are banned. The Authority publishes a list of the games it finds to be money games (rule 26), but that list wasn't among the documents read.

What is allowed, in our Online Gaming Act guide →

Does registration let real-money games operate again?

No. Registration under the Online Gaming Rules is for e-sports and online social games (rule 12), which the Act promotes. Section 5 of the Online Gaming Act bars anyone from offering an online money game, whether of skill, chance or both, and registration of an e-sport or social game doesn't change that.

Registration, in our Online Gaming Act guide →

What is the difference between an e-sport and a money game, and must a tournament register?

An e-sport is a recognized competition at multi-sports events, decided solely by skill, with entry fees and prize money allowed but no bets or stakes (Online Gaming Act, section 2(1)(c)); a money game involves stakes. A game offered as an e-sport must be registered (rule 12(1)(b)), and the Authority is to register it within 90 days of a complete application.

E-sports, in our Online Gaming Act guide →

Are app stores, banks, cloud providers, social media and ad agencies liable under the gaming law?

Yes, they can be. The Online Gaming Act bars aiding the offering of money games, taking part in their advertising and handling their payments (sections 5 to 7). The Authority's advisory of July 29, 2026 names app stores, cloud, telecom and payment firms, social media, OTT streaming platforms and ad agencies, and tells them to disable such apps.

Intermediaries and payment firms, in our Online Gaming Act guide →

Does the gaming law reach offshore operators and foreign game publishers?

Yes. The Online Gaming Act applies to online money gaming services offered in India or run from outside India (section 1(2)). Information about a service that breaks its bans may be blocked under the IT Act (section 14), and the government may weigh a provider's country of origin in notifying games (rule 12(1)(a)(v)).

Offshore services, in our Online Gaming Act guide →

Can directors of a gaming company be prosecuted?

Yes. Whoever was in charge of the company's business can be prosecuted with the company, unless they prove the offense happened without their knowledge or that they took all due care (Online Gaming Act, section 11). A director whose consent, connivance or neglect is proved is liable, unless independent or non-executive and not involved in the decisions (section 11(3)).

Companies and directors, in our Online Gaming Act guide →

Where do gaming users complain, and who hears appeals?

First to the provider, as providers of online social games and e-sports must run a grievance system (Online Gaming Rules, rule 20). A user may then appeal to the Online Gaming Authority within 30 days, and then to the MeitY Secretary as Appellate Authority. The Rules set a 30-day target for deciding each of the two appeals.

Complaints and appeals, in our Online Gaming Act guide →

Who regulates online gaming, and who sits on the Online Gaming Authority?

MeitY regulates it through the Online Gaming Authority of India, an attached office of MeitY (Online Gaming Rules, rule 3). An Additional Secretary of MeitY chairs the Authority, with Joint Secretaries from five other ministries or departments as members (S.O. 1992(E)). It decides which games are money games, registers games where required, hears appeals and issues directions.

The Authority, in our Online Gaming Act guide →

Who investigates offenses under the gaming law?

Police officers in charge of state and union territory cyber cells are authorized to investigate offenses under the Online Gaming Act (S.O. 1993(E)). Officers authorized under the Act may enter any place, physical or digital, to search it, and may arrest without a warrant anyone there reasonably suspected of an offense (section 16(1)).

Enforcement, in our Online Gaming Act guide →

Must gaming companies keep data in India or route payments through India?

Only where a direction says so. Directions under the Act may require providers to keep traffic data and metadata on computer resources in India, and may set how user payments are routed and settled (Online Gaming Rules, rules 17 and 18). Banks and payment firms follow the Authority's directions on checking a game's registration before handling its payments (rule 19).

Data and payments, in our Online Gaming Act guide →

How is MeitY acting against offshore betting sites, and how many has it blocked?

Information about a money gaming service that breaks sections 5 to 7 may be blocked under the IT Act's procedure (Online Gaming Act, section 14). On April 25, 2026, MeitY advised VPN providers and other intermediaries that giving access to blocked betting and prediction platforms may breach their due diligence. Block counts weren't among the texts read.

Blocking, in our Online Gaming Act guide →

Do the 2023 IT Rules on permissible real money games still matter?

MeitY's consolidated IT Rules of February 10, 2026 still print the 2023 rules on verifying permissible online real money games through self-regulatory bodies (rules 4A to 4C). Since May 1, 2026, the Online Gaming Act bans offering online money games, whether of skill, chance or both (section 5), so read the Act, not those rules.

The older rules, in our Online Gaming Act guide →

Electronics and chip makers: schemes and government buying

What did the PLI scheme for mobile phones deliver, and has it ended?

The Production Linked Incentive (PLI) scheme for large-scale electronics, for mobile phones and parts, was notified on April 1, 2020. It drew ₹20,587 crore of investment against a ₹7,000 crore target and paid ₹19,091 crore by March 2026, by the government's figures (Lok Sabha answer 1695). Its end date isn't in the texts read.

The schemes, in our electronics schemes guide →

Can you still apply for PLI 2.0 for IT hardware, and is it paying out?

Not now. Applications closed on August 30, 2023, though MeitY may reopen the scheme at any time before it ends on March 31, 2031 (PLI 2.0 notification, paras 6.2 and 6.3). MeitY lists 27

approved companies, and the IT hardware PLI schemes had paid ₹97.85 crore by June 2026, by the government's figures (Lok Sabha answer 1695).

PLI 2.0, in our electronics schemes guide →

What does ECMS cover, and can you still apply?

The Electronics Component Manufacturing Scheme (ECMS) supports display and camera modules, passive and electro-mechanical components, printed circuit boards, lithium-ion cells for digital devices and enclosures (ECMS, para 4), and optical transceivers since July 7, 2025. Only segment D, supply chain and capital equipment, still takes applications, until April 30, 2027. Budget 2026 raised the outlay to ₹40,000 crore.

ECMS, in our electronics schemes guide →

Can a company with a Chinese partner get ECMS or MPMS support?

Under the Mobile Phone Manufacturing Scheme (MPMS), an applicant or brand owned or controlled from a country sharing a land border with India faces the same checks as foreign direct investment (guidelines, para 3.2). The ECMS texts read say nothing on it. Our Press Note 3 guide sets out the investment rule.

Who may apply, in our electronics schemes guide →

Press Note 3: India's land-border investment rule in 2026 →

What is the Mobile Phone Manufacturing Scheme, and when can you apply?

The Mobile Phone Manufacturing Scheme is MeitY's incentive on phone sales from 2026-27 to 2030-31, notified on August 21, 2026 with a ₹62,500 crore budget (paras 4 and 6). Target Segment 1, for makers with ₹10,000 crore turnover, takes applications from October 15, 2026 to March 31, 2029. Those filed after March 31, 2027 earn only from approval (para 14.2).

MPMS, in our electronics schemes guide →

Mobile phone makers can apply for incentives from October 15 →

What does Semicon 2.0 offer, and how does it differ from the first program?

Semicon 2.0, approved on July 15, 2026 with ₹1.27 lakh crore (Lok Sabha answer 246) and notified on August 31, covers six pillars, from chip design to talent (para 3). It pays 40% of eligible capital cost for a 300 mm silicon wafer fab and 35% for other fabs. The texts read don't give the first program's rates.

What Semicon 2.0 pays, in our Semicon 2.0 guide →

Semicon 2.0 applications for fabs and ATMP open for three years →

Which semiconductor projects has India approved?

By the government's figures of August 5, 2026, 12 manufacturing projects in six states were approved under the first Semicon India program, with about ₹1.64 lakh crore committed (Lok Sabha answer 246). Three plants had started commercial production. This page doesn't list the projects, and Semicon 2.0 takes new applications for three years.

Projects and applications, in our Semicon 2.0 guide →

How can a chip design startup or engineer join India's semiconductor program?

A chip design company qualifies if incorporated and headquartered in India, with significant operations there, and owned and controlled by Indian citizens, or Overseas Citizens of India for commercial chips (Semicon 2.0, paras 3.1.3 and 3.2.3). New chips can earn 9% of net sales for five years, within set caps. Support for individual engineers isn't in the texts read.

Chip design support, in our Semicon 2.0 guide →

Must laptops sold in India be made in India, and do imports need a licence?

The rule here is on imports. Laptops, tablets, all-in-one PCs, ultra small form factor computers and servers under HSN 8471 are restricted imports, and importers apply in the Import Management System of DGFT, the Directorate General of Foreign Trade (Policy Circular 08/2025-26). Our DGFT import authorization guide covers it.

DGFT import authorization: how to import a restricted item →

Do electronics need BIS registration before sale or import?

Listed electronics do. Under MeitY's Compulsory Registration Order of 2021 (S.O. 1248(E)), they must meet an Indian Standard and carry the Standard Mark under a licence from the Bureau of Indian Standards (BIS), which certifies and enforces it. Our MeitY tracker lists the products covered, MeitY's notices and the BIS and MeitY guidance.

The MeitY tracker: products, notices and guidance →

What security testing must CCTV cameras pass?

STQC (Standardization Testing and Quality Certification), a MeitY directorate, issues the security test reports CCTV cameras need, valid for three years (MeitY clarification of February 4, 2026, para 2). Since that date, one STQC security report against the essential requirements serves both registration and public procurement, and it has no bearing on local value addition (para 4).

Government buying of electronics, in our MeitY guide →

Does the government prefer Indian-made electronics and cyber security products in its purchases?

Yes for electronics. Central buyers apply the Make in India procurement order of DPIIT, India's industry department, to electronics (MeitY circular of December 3, 2025), and MeitY lists it among its measures (Rajya Sabha answer 2472). MeitY added CCTV cameras from June 7, 2024; its own order for cyber security products wasn't among the documents read.

Government buying of electronics, in our MeitY guide →

Make in India procurement order: local content and bidding rules →

Will government buyers check that supplied electronics meet the regulations?

Yes. Goods bought under the Make in India order must meet every Indian technical regulation that applies, including telecom testing and quality control orders (MeitY circular of December 3, 2025, para 2). Buyers may test supplies through third parties and add penalty clauses, and should report non-compliant goods to the nodal ministry (para 3).

Government buying of electronics, in our MeitY guide →

Foreign companies new to India's digital rules

Does the DPDP Act apply to a foreign company with no office in India?

Yes, where its processing is connected with offering goods or services to people in India (DPDP Act, section 3(b)), from about May 13, 2027. It needs a representative in India only if notified as a Significant Data Fiduciary, whose Data Protection Officer represents it and is based in India (section 10(2)(a)).

What applies abroad, in our guide for foreign companies →

Does a foreign company need an office, representative or officer in India?

Only in set cases. A Significant Data Fiduciary's Data Protection Officer must be based in India (DPDP Act, section 10(2)(a)). So must a significant social media intermediary's three officers and a news or streaming publisher's Grievance Officer (IT Rules, rules 4(1) and 11(2)(a)). Every intermediary publishes a Grievance Officer; CERT-In's FAQ asks for a Point of Contact, office or not.

Officers and contacts, in our guide for foreign companies →

Do you need to register with the Data Protection Board to process Indian personal data?

No such registration for ordinary Data Fiduciaries was found among the texts read to October 31, 2026. The DPDP Act and Rules set Board registration for Consent Managers (section 6(9); DPDP Rules, rule 4), which must be companies incorporated in India with a net worth of at least ₹2 crore.

Registration, in our guide for foreign companies →

Do Indian laws apply to apps owned by foreign or offshore companies?

Yes. The government told the Rajya Sabha on July 24, 2026 that entities incorporated outside India, or with foreign owners, must follow India's laws when they offer digital services to users in India (answer 718). The IT Act also reaches offenses and contraventions outside India, by anyone of any nationality, involving a computer, system or network in India (section 75).

What applies abroad, in our guide for foreign companies →

Which ministry handles what: MeitY, the Ministry of Information and Broadcasting, DGFT or DPIIT?

MeitY handles data protection, intermediaries, CERT-In, online gaming, electronics schemes and government cloud. The Ministry of Information and Broadcasting runs the IT Rules' part for digital news and streaming (rule 8(1)). DGFT runs restricted IT hardware imports and DPIIT the Make in India procurement order, while the telecom department's remit isn't covered here.

Who does what, in our guide for foreign companies →

DGFT import authorization: how to import a restricted item →

Does a GDPR program cover the DPDP Act?

No text read compares the two, so check India's rules one by one. A child is anyone under 18 (DPDP Act, section 2(f)), and consent is needed unless section 7 or 17 applies. The Board gets a full breach report within 72 hours (DPDP Rules, rule 7(2)), and logs for investigating unauthorized access are kept a year (rule 6(1)(e)).

India's own rules, in our guide for foreign companies →

What counts as offering goods or services to people in India?

The DPDP Act reaches processing outside India when it is in connection with any activity related to offering goods or services to people in India (section 3(b)). The Act doesn't define offering, and no rule or notification read does. The government says foreign-owned entities offering digital services to users in India must follow India's laws (Rajya Sabha answer 718).

What applies abroad, in our guide for foreign companies →

Can a foreign company claim MeitY's incentives directly, or must it set up in India?

Through a company in India. PLI 2.0 for IT hardware (para 10.1) and the Mobile Phone Manufacturing Scheme's Target Segment 1 (para 7.1) take makers registered in India. Semicon 2.0's chip design pillar is for companies owned and controlled by Indian citizens, or Overseas Citizens of India for commercial chips, and cloud empanelment needs a provider incorporated in India.

Incentives, in our guide for foreign companies →

People using their data and platform rights

How do you complain to the Data Protection Board, and must you go to the company first?

Yes, the company first: you use the Data Fiduciary's grievance system before going to the Board (DPDP Act, section 13(3)), and it answers within its published period, at most 90 days (DPDP Rules, rule 14(3)). Every notice must say how to complain to the Board (rule 3(c)), from about May 13, 2027.

Complaints, in our DPDP penalties guide →

How do you find out which companies hold your data, and make them delete it?

Ask each company for a summary of your data and who else received it (DPDP Act, section 11), and for erasure unless the purpose or a law still needs the data (section 12(3)). Each answers within its published period, at most 90 days (rule 14(3)), from about May 13, 2027. No text read lists who holds a person's data.

People's rights, in our DPDP Act guide →

Can a person nominate someone to use their data rights?

Yes. A person may nominate someone to exercise their DPDP rights in the event of their death or incapacity (DPDP Act, section 14(1)). The DPDP Rules let them nominate one or more people through the Data Fiduciary's own process (rule 14(4)), from about May 13, 2027.

People's rights, in our DPDP Act guide →

Can you still claim compensation under IT Act section 43A for a data breach?

Yes, while section 43A stands. It makes a company, firm or other business handling sensitive personal data pay compensation if negligent in maintaining reasonable security practices,

causing wrongful loss or gain (IT Act, section 43A). Section 44(2) of the DPDP Act deletes it about May 13, 2027, and whether claims for earlier breaches survive isn't addressed in the texts read.

Section 43A, in our DPDP Act timeline →

A platform's grievance officer didn't reply. What can you do next?

Appeal online to a Grievance Appellate Committee within 30 days (IT Rules, rule 3A(3) and (6)). The appeal lies against the Grievance Officer's decision, or where the grievance isn't resolved in time (rule 3(2)). Since February 20, 2026, that's seven days for most complaints, 36 hours for most removal requests and two hours for intimate images.

Appeals, in our IT Rules guide →

Must you go to the grievance officer before a Grievance Appellate Committee, and how long does an appeal take?

Yes: an appeal lies against the Grievance Officer's decision, or an unresolved grievance, within 30 days (IT Rules, rule 3A(3)). The committee is to try to resolve it within 30 calendar days (rule 3A(4)), the rule's own target. Appeals run online, and the platform must follow the order and report that on its website.

Appeals, in our IT Rules guide →

Is using a VPN legal in India?

CERT-In's directions put their VPN duties on providers of internet proxy-like services to the general public, not on users, and individual citizens are not covered (CERT-In's FAQ, Q7 and Q34). MeitY's April 2026 advisory is addressed to providers and intermediaries too. None of the texts read speaks to ordinary users of a VPN.

VPN providers, in our CERT-In directions guide →

Can you use a VPN to reach blocked betting or prediction sites?

MeitY's advisory of April 25, 2026 is addressed to VPN providers and other intermediaries: giving access to blocked betting and prediction market platforms may breach their due diligence and cost them section 79 protection. Offering, advertising and handling payments for money games are punishable (Online Gaming Act, section 9). A user's own position isn't addressed in the texts read.

Blocking, in our Online Gaming Act guide →

Sources

- Act No. 22 of 2023: The Digital Personal Data Protection Act, 2023 (August 11, 2023)
- G.S.R. 843(E): Dates on which the provisions of the Digital Personal Data Protection Act, 2023 come into force (November 13, 2025)
- G.S.R. 844(E): Establishment of the Data Protection Board of India (November 13, 2025)
- G.S.R. 845(E): Number of members of the Data Protection Board of India (November 13, 2025)
- G.S.R. 846(E): Digital Personal Data Protection Rules, 2025 (November 13, 2025)
- S.O. 5458(E): Digital Personal Data Protection (Removal of Difficulties) Order, 2026 (October 5, 2026) (PDF, 642 KB)
- F. No. 2(1)/2026-Pers.I: Appointment to the post of Chairperson and Other Members in the Data Protection Board of India (May 6, 2026)
- PIB backgrounder: Digital Personal Data Protection Rules, 2025 (November 17, 2025)
- Lok Sabha Unstarred Question No. 3943: Implementation of Rules under DPDP Act, 2023 (August 12, 2026)
- Lok Sabha Unstarred Question No. 3960: Appointment of Chairperson and Members of Data Protection Board of India (August 12, 2026)
- Rajya Sabha Unstarred Question No. 718: Measures for regulating apps owned by foreign companies (July 24, 2026)
- Act No. 21 of 2000: The Information Technology Act, 2000 (as enacted) (June 9, 2000)
- Act No. 10 of 2009: The Information Technology (Amendment) Act, 2008 (February 5, 2009)
- Act No. 18 of 2023: The Jan Vishwas (Amendment of Provisions) Act, 2023 (August 11, 2023)
- S.O. 4769(E): Designated Officer under section 69A of the Information Technology Act, 2000 (October 21, 2025)
- G.S.R. 139(E), as amended: Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 (updated as on 10.02.2026)
- G.S.R. 120(E): Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Amendment Rules, 2026 (February 10, 2026)
- G.S.R. 775(E): Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Amendment Rules, 2025 (October 22, 2025)
- S.O. 942(E): Threshold for a significant social media intermediary (February 25, 2021)

- FAQs (10.02.2026): Frequently Asked Questions on the IT (Intermediary Guidelines and Digital Media Ethics Code) Amendment Rules, 2026 (February 10, 2026)
- F. No. 2(5)/2025-CyberLaws: Draft Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Second Amendment Rules, 2026 (April 21, 2026) (PDF, 143 KB)
- No. 2(6)/2024-CL&DG-Part(1): Advisory to VPN service providers and intermediaries on access to illegal and blocked online betting and prediction market platforms (April 25, 2026)
- No. 20(3)/2022-CERT-In: 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 (April 28, 2022)
- FAQs (May 2022): Frequently Asked Questions on the Cyber Security Directions of 28.04.2022
- No. 20(3)/2022-CERT-In: Extension of timelines for the Cyber Security Directions of 28.04.2022 for MSMEs and for validation of customer details (June 27, 2022)
- CISG-2026-03: Guidelines regarding AI-Accelerated Vulnerability Protection and Response Requirements for Original Equipment Manufacturers (OEMs), and Technology Providers, version 1.0 (June 10, 2026)
- F. No. P-1501/3/2020-Personnel: Declaration of the Indian Computer Emergency Response Team (ICERT) as an Attached Office (October 12, 2026)
- Bare Act: The Promotion and Regulation of Online Gaming Act, 2025, bare act with corrigenda (uploaded October 2, 2025)
- S.O. 1994(E): Date of coming into force of the Promotion and Regulation of Online Gaming Act, 2025 (April 22, 2026)
- S.O. 1992(E): Constitution of the Online Gaming Authority of India (April 22, 2026)
- S.O. 1993(E): Officers authorized to investigate offenses under the Online Gaming Act (April 22, 2026)
- G.S.R. 303(E): Promotion and Regulation of Online Gaming Rules, 2026 (April 22, 2026) (PDF, 2.1 MB)
- OGAI advisory: Advisory on compliance with sections 5, 6 and 7 of the Promotion and Regulation of Online Gaming Act, 2025 (July 29, 2026)
- W-17/9/2021-IPHW: Production Linked Incentive Scheme - PLI 2.0 for IT Hardware (May 29, 2023)
- Lok Sabha Unstarred Question No. 1695: PLI scheme for large-scale electronics/IT hardware (July 29, 2026)
- F. No. W/49/2024-IPHW: Electronics Component Manufacturing Scheme (April 8, 2025)
- File No. W/49/2024-IPHW: Addendum-1 to the Electronics Component Manufacturing Scheme notification, adding optical transceivers (July 7, 2025)
- Rajya Sabha Unstarred Question No. 2472: Progress of Electronics Components Manufacturing Scheme (March 13, 2026)

- F. No. W/11/2026-IPHW: Mobile Phone Manufacturing Scheme (MPMS) (August 21, 2026)
- Guidelines for Operation of the Mobile Phone Manufacturing Scheme for Target Segment-1 (October 6, 2026) (PDF, 4.5 MB)
- F. No. W-38/6/2025-IPHW: Semicon 2.0: Scheme for development of Semiconductor Design and Manufacturing Ecosystem in India (August 31, 2026)
- Lok Sabha Starred Question No. 246: Promotion of semiconductor manufacturing and strengthening of electronics ecosystem (August 5, 2026)
- W-18/26/2025-IPHW: Clarification on testing requirements under the Public Procurement (Preference to Make in India) Order for CCTV cameras (February 4, 2026)
- W/56/2025-IPHW: Circular on regulatory compliance of goods procured under the Public Procurement (Preference to Make in India) framework (December 3, 2025)
- Call for applications (July 2026): Inviting Application for Empanelment of Cloud services of Cloud Service Providers
- India AI Governance Guidelines: Enabling Safe and Trusted AI Innovation (released November 5, 2025)
- No. ET/9/2023-ET-(Part 1): Constitution of AI Governance and Economic Group (AIGEG) (April 13, 2026)
- eNo.2(4)/2023-CyberLaws-3: Due diligence by intermediaries and platforms under the Information Technology Act, 2000 and the IT Rules, 2021, replacing the advisory of March 1, 2024 (March 15, 2024)
- Draft for discussion: Data Empowerment and Protection Architecture (DEPA) for AI Training (posted October 29, 2026)
- Lok Sabha Unstarred Question No. 1647: Eligibility of generative artificial systems for safe harbour protection (July 29, 2026)
- Lok Sabha Unstarred Question No. 2988: Institutional framework for auditing artificial intelligence (August 5, 2026)
- S.O. 1248(E): Electronics and Information Technology Goods (Requirement of Compulsory Registration) Order, 2021 (March 18, 2021) (PDF, 1.5 MB)
- Policy Circular No. 08/2025-26: Import Management System for restricted IT hardware in 2026 (December 17, 2025)
- Notice (21.04.2026): Extension of time for comments on the draft amendments to the IT Rules, 2021, with additional amendments in rule 3(3)(a)(ii) (April 21, 2026)

IndusDesk

hello@indusdesk.com · +91 11 4141 3939

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

Read online: indusdesk.com/meity/questions/