DPDP

& Cybersecurity

A plain-language guide for individuals, employees, educators and organisations

BASED ON THE OFFICIAL GAZETTE TEXT

The Digital Personal Data Protection Act, 2023

Act No. 22 of 2023 | Assented on 11 August 2023

Inside this guide

- What the DPDP Act covers and whom it applies to
- Consent, lawful use, organisational duties and individual rights
- Children's data, breach responsibilities and penalties
- 10 DPDP terms explained without legal fog
- 10 cybersecurity terms explained without techno-soup
- A practical readiness checklist and a real-world example

Educational guide | Version 1.0 | 2 August 2026

How to use this guide

This document paraphrases the linked Act. It does not replace the official legal text.

IMPORTANT	The Act leaves several operational details to rules, notifications and prescribed procedures. This guide focuses on the official Gazette PDF supplied for this document and does not claim to incorporate every later rule, notification, sectoral law or regulator direction.

The central idea

The DPDP Act creates a framework for processing digital personal data while recognising two interests at the same time: an individual's right to protect personal data and the need to process that data for lawful purposes.

Topic	Plain-language summary
Who is protected?	The individual to whom personal data relates, called the Data Principal.
Who is responsible?	The person or organisation deciding why and how personal data is processed, called the Data Fiduciary.
What is covered?	Personal data in digital form, including data first collected on paper and later digitised.
What is expected?	Lawful purpose, proper notice, valid consent where required, security safeguards, accountability and mechanisms for individual rights.
What happens after a breach?	The Data Fiduciary must intimate the Board and affected Data Principals in the prescribed form and manner.
What can enforcement involve?	Inquiry, directions, remedial steps, voluntary undertakings and monetary penalties up to the statutory maxima.

Privacy and cybersecurity are connected

Privacy decides whether personal data should be collected, used, shared or retained. Cybersecurity protects that data and the systems holding it from unauthorised access, alteration, loss or disruption. Good privacy without security is a locked diary left in the rain. Good security without privacy is a vault storing things that never needed to be collected.

Act reference: Preamble; sections 2, 3, 8 and the Schedule

1. Scope and key participants

Where the Act applies

Subject to the Act's provisions, it applies to processing digital personal data within India when the data is collected digitally or collected in non-digital form and later digitised. It can also apply to processing outside India when connected with offering goods or services to Data Principals in India.

Main exclusions in the Act

- Personal data processed by an individual for a personal or domestic purpose.
- Personal data made publicly available by the Data Principal.
- Personal data made publicly available by another person who is legally required to publish it.

REMEMBER	An exclusion from this Act does not automatically erase duties under other laws, contracts, professional obligations or cybersecurity requirements.

The people and organisations in the data journey

Topic	Plain-language summary
Data Principal	The individual whose personal data is involved. In specified cases, this includes a parent or lawful guardian acting on behalf of a child or person with disability.
Data Fiduciary	The person or organisation deciding the purpose and means of processing personal data.
Data Processor	A person or organisation processing personal data on behalf of a Data Fiduciary.
Consent Manager	A Board-registered person that helps an individual give, manage, review and withdraw consent through an accessible and interoperable platform.
Data Protection Officer	An individual appointed by a Significant Data Fiduciary with specified responsibilities under the Act.
Data Protection Board of India	The body established under the Act to perform enforcement, inquiry, remedial and penalty-related functions.

Act reference: Sections 2 and 3

2. Lawful processing, notice and consent

Two broad grounds for processing

A person may process a Data Principal's personal data only in accordance with the Act and for a lawful purpose. The Act recognises processing based on consent and processing for certain legitimate uses described in section 7.

What a proper notice should communicate

- The personal data proposed to be processed.
- The purpose for which the data will be processed.
- How the individual may exercise consent-related rights and use grievance redressal.
- How the individual may make a complaint to the Board, in the prescribed manner.

The notice must be available in English or any language listed in the Eighth Schedule to the Constitution. Consent requests must be presented in clear and plain language and provide relevant contact details.

The consent test

VALID CONSENT	Consent should be free, specific, informed, unconditional and unambiguous, shown through a clear affirmative action. It should cover only personal data necessary for the stated purpose.

Withdrawal must not be a maze

Where consent is the basis of processing, the Data Principal may withdraw it at any time. Withdrawing consent should be as easy as giving it. After withdrawal, the Data Fiduciary must stop and cause its processors to stop the consent-based processing within a reasonable time, unless continued processing is required or authorised by law.

Certain legitimate uses, in simple terms

Topic	Plain-language summary
Voluntarily provided data	Using data for the purpose for which the individual voluntarily supplied it, unless the individual indicates otherwise.
Government functions and benefits	Specified processing by the State for benefits, services, licences, legal functions or related purposes.
Legal obligations and orders	Processing needed to meet legal disclosure duties or comply with judgments, decrees or orders.
Emergencies and public safety	Processing for medical emergencies, epidemics, public-health threats, disasters or breakdowns of public order.
Employment-related use	Specified processing for employment purposes or to safeguard an employer from loss or liability.

Act reference: Sections 4 to 7

3. What organisations must do

Core obligations of a Data Fiduciary

Topic	Plain-language summary
Remain accountable	The Data Fiduciary remains responsible for compliance, including processing performed on its behalf by a Data Processor.
Use valid processor contracts	A Data Processor should be engaged for relevant processing under a valid contract.
Maintain data quality where it matters	When data may be used to make a decision affecting the individual or disclosed to another Data Fiduciary, ensure completeness, accuracy and consistency.
Implement governance measures	Put suitable technical and organisational measures in place to support compliance.
Use reasonable security safeguards	Protect personal data in its possession or control against personal data breaches.
Notify breaches	Intimate the Board and each affected Data Principal in the prescribed form and manner.
Erase data when no longer needed	Unless retention is legally necessary, erase data when consent is withdrawn or the stated purpose is no longer served, whichever is earlier.
Provide a contact point	Publish business contact details for the DPO, where applicable, or another authorised person who can answer questions.
Operate grievance redressal	Establish an effective mechanism for resolving Data Principal grievances.

Data minimisation in practice

The Act's consent standard limits processing to data necessary for the specified purpose. A practical test is: "Would the service still work safely and lawfully without this data field?" If yes, collecting it needs closer scrutiny.

Retention is not a digital attic

Keeping data forever "just in case" increases privacy and security risk. Organisations should connect each data category to a purpose, legal retention requirement, review date and secure deletion method.

Act reference: Sections 6 and 8

4. Children, significant organisations and individual rights

Processing children's data

Under the Act, a child is an individual below 18 years of age. Before processing a child's personal data, a Data Fiduciary must obtain verifiable consent of the parent or lawful guardian in the prescribed manner.

- Do not process data in a way likely to cause a detrimental effect on the child's well-being.
- Do not track or behaviourally monitor children, or direct targeted advertising at children, subject to the Act's prescribed exceptions and notifications.

Additional duties of a Significant Data Fiduciary

The Central Government may notify a Data Fiduciary or class of Data Fiduciaries as significant after considering factors such as data volume and sensitivity, risk to rights, security of the State, public order and other listed factors.

- Appoint a Data Protection Officer based in India and responsible to the governing body.
- Appoint an independent data auditor.
- Undertake periodic Data Protection Impact Assessments and audits, along with other prescribed measures.

Rights of a Data Principal

Topic	Plain-language summary
Access	Request a summary of personal data being processed and processing activities, plus specified information about sharing.
Correction and updating	Ask for inaccurate or misleading data to be corrected, incomplete data to be completed and data to be updated.
Erasure	Request erasure, unless retention is needed for the stated purpose or required by law.
Grievance redressal	Use the readily available grievance mechanism before approaching the Board.
Nomination	Nominate another individual to exercise rights in the event of death or incapacity, in the prescribed manner.

Duties of a Data Principal

Individuals must also act honestly and lawfully. The Act prohibits impersonation, suppression of material information in specified identity-related contexts, false or frivolous complaints, and furnishing unverifiable information when seeking correction or erasure.

Act reference: Sections 9 to 15

5. Transfers, exemptions, enforcement and penalties

Transfers outside India

The Central Government may notify countries or territories to which a Data Fiduciary may not transfer personal data for processing. The Act also preserves the effect of other Indian laws that provide a higher degree of protection or stronger restrictions for particular data or organisations.

Exemptions are specific, not a universal escape hatch

Section 17 lists situations in which specified provisions do not apply, including certain legal claims, judicial or regulatory functions, investigation or prosecution, some cross-border contract processing, approved corporate restructuring, specified loan-default processing, notified State instrumentalities and qualifying research, archiving or statistical processing. The exact scope depends on the statutory conditions.

Data Protection Board of India

The Act establishes the Data Protection Board of India as a digital office. Its functions include responding to breach intimations and complaints, directing urgent remedial or mitigation measures, conducting inquiries, accepting voluntary undertakings and imposing penalties under the Act.

Maximum monetary penalties in the Schedule

Type of breach	Statutory maximum
Failure to take reasonable security safeguards	May extend to Rs. 250 crore
Failure to notify the Board or affected Data Principals of a breach	May extend to Rs. 200 crore
Failure to observe obligations relating to children	May extend to Rs. 200 crore
Failure to observe Significant Data Fiduciary obligations	May extend to Rs. 150 crore
Failure by a Data Principal to observe section 15 duties	May extend to Rs. 10,000
Breach of an accepted voluntary undertaking	Up to the applicable amount for the underlying breach
Breach of another provision or rule	May extend to Rs. 50 crore

CAUTION	These are maximum amounts stated in the Schedule, not automatic fines. The Act provides factors for determining the penalty in a proceeding.

Act reference: Sections 16 to 18, 27 to 33 and the Schedule

6. Practical DPDP readiness checklist

A practical implementation aid. This checklist is not a substitute for legal analysis or prescribed requirements.

1	**Map personal data:** List what personal data is collected, where it comes from, where it is stored, who can access it and where it is sent.
2	**Document purposes:** Connect every data field and processing activity to a clear, lawful and understandable purpose.
3	**Identify the processing ground:** Record whether processing relies on consent or a specific legitimate use under the Act.
4	**Improve notices:** Use concise language that explains the data, purpose, rights, grievance route and contact point.
5	**Prove consent:** Retain evidence showing that the notice was provided and consent met the Act's standard.
6	**Make withdrawal easy:** Provide a visible, usable route to withdraw consent and propagate the change to relevant processors.
7	**Review vendors and processors:** Use contracts, due diligence, access controls, incident duties and deletion/return requirements.
8	**Strengthen safeguards:** Apply access control, MFA, patching, encryption where appropriate, logging, secure backups and staff training.
9	**Prepare for breaches:** Define detection, containment, assessment, decision-making, notification and evidence-preservation steps.
10	**Build a rights workflow:** Assign owners and timelines for access, correction, erasure, grievances and nominations.
11	**Control retention:** Create category-wise retention rules and verify deletion from active systems, archives and processors.
12	**Protect children:** Identify age-related processing, parental consent needs, tracking risks and targeted advertising controls.
13	**Audit and improve:** Test controls, review incidents, update records and retain evidence of compliance decisions.

7. A simple example: a training institute registration portal

Imagine a training institute collects a student's name, email address, mobile number, date of birth, photograph, identity document and course preferences through an online portal. The portal is operated by an external LMS provider.

How the roles may look

Topic	Plain-language summary
Student	Data Principal, because the personal data relates to the student.
Training institute	Usually the Data Fiduciary, because it decides why the data is collected and how it will be used.
LMS or cloud provider	Often a Data Processor when it handles the data on the institute's instructions.
Parent or guardian	May act for a child where the Act requires verifiable parental or guardian consent.

Questions the institute should ask

1. Is every field necessary for enrolment, learning delivery, certification or a documented legal requirement?
2. Does the notice clearly explain each purpose instead of hiding everything under a vague phrase such as "for services"?
3. Is optional marketing separate from necessary course administration?
4. Can the student withdraw optional consent without losing unrelated services?
5. Does the LMS contract cover security, breach cooperation, access limits, retention and deletion?
6. Can the institute respond to access, correction, erasure and grievance requests?
7. Are photographs and identity documents protected more carefully because misuse could cause greater harm?

CYBER LINK	A fake login page could steal student credentials through phishing. Malware could then access the LMS. Weak access control could expose records. DPDP governance decides what should be held and why; cybersecurity controls reduce the chance that the data escapes the fence.

Act reference: Illustrative application of sections 2 to 15; not an official statutory illustration

8. Ten DPDP terms for laypersons

The legal concepts are paraphrased from section 2 and related provisions of the Act.

Term	What it means in everyday language	Simple example
1. Personal Data	Any data about an individual who can be identified from that data or in relation to it.	A name linked with a mobile number, customer ID, photograph or account record.
2. Digital Personal Data	Personal data that exists in digital form.	A paper admission form becomes digital personal data after it is scanned or entered into software.
3. Data Principal	The individual whose personal data is being processed. A parent or lawful guardian may act in specified cases.	A patient whose appointment details are stored by a clinic.
4. Data Fiduciary	The person or organisation deciding the purpose and method of processing personal data.	A bank deciding what customer information is needed to open and operate an account.
5. Data Processor	A service provider processing personal data for a Data Fiduciary.	A payroll vendor calculating salaries for an employer.
6. Processing	Almost any automated operation performed on digital personal data, including collecting, storing, using, sharing, altering or deleting it.	Uploading a contact list, searching it, emailing it to a vendor and later erasing it.
7. Consent	A clear, informed and voluntary yes for a specific purpose, limited to necessary data.	Ticking an unticked box to receive optional promotional emails after reading a clear explanation.
8. Consent Manager	A Board-registered service that helps individuals give, manage, review and withdraw consent.	One dashboard showing which organisations have consent and allowing the user to withdraw it.
9. Personal Data Breach	Unauthorised processing or accidental disclosure, loss, alteration, destruction or loss of access that compromises confidentiality, integrity or availability.	A database is exposed online, records are changed without authority, or ransomware makes them unavailable.
10. Significant Data Fiduciary	A Data Fiduciary notified by the Government because of factors such as data volume, sensitivity or risk, and therefore subject to extra duties.	A notified organisation required to appoint a DPO, undergo audits and perform impact assessments.

Quick memory trick: The Data Principal is the person. The Data Fiduciary decides. The Data Processor performs work for the Fiduciary.

9. Ten cybersecurity terms for laypersons

Plain-language explanations informed by CERT-In awareness material and the NIST cybersecurity glossary.

Term	What it means in everyday language	Simple example
1. Phishing	A deceptive message or website designed to trick you into revealing passwords, bank details or other sensitive information.	An email pretending to be your bank asks you to "verify" your account through a fake login page.
2. Malware	Software intentionally designed to harm, spy on, disrupt or gain unauthorised access to a device or data.	A malicious app secretly copies contacts and messages.
3. Ransomware	Malware that locks systems or encrypts files and demands payment for access or recovery.	Office documents become unreadable and a ransom note appears.
4. Vulnerability	A weakness in software, hardware, configuration or procedure that can be exploited or accidentally triggered.	A public server uses outdated software with a known security flaw.
5. Patch / Patching	A software update that fixes security or functionality problems, and sometimes adds capabilities.	Installing an operating-system security update that closes a known flaw.
6. Firewall	A device or program that controls network traffic according to security rules.	The firewall blocks unexpected internet connections to an internal database.
7. Encryption	Transforming readable data into a protected form that requires the correct key or method to read.	A stolen laptop contains encrypted files that cannot be opened without the decryption key.
8. Multi-Factor Authentication	Login protection requiring more than one different factor, such as a password plus a device, code or biometric.	After entering a password, the user must approve the login on a registered phone.
9. Backup	A separate copy of important data kept so information can be restored after deletion, damage, failure or attack.	The organisation restores clean files from an isolated backup after ransomware.
10. Cybersecurity Incident	An event that actually or potentially harms the confidentiality, integrity or availability of information or systems, or violates security rules.	A stolen admin password is used to download customer records.

The three questions behind most security controls

Security question	What it protects
Can unauthorised people see it?	This is the confidentiality question.
Can someone change it improperly?	This is the integrity question.
Can authorised people access it when needed?	This is the availability question.

10. A seven-day starter plan

When	Action
Day 1	Choose one service or department and list the personal data it uses.
Day 2	Write the real purpose beside each data field and mark unnecessary fields.
Day 3	Collect all notices, consent forms, privacy policies and processor contracts.
Day 4	Test one individual request: access, correction, erasure or grievance.
Day 5	Review user access, MFA, patches, backups and encryption for the selected service.
Day 6	Run a tabletop breach exercise: who detects, decides, contains, informs and records?
Day 7	Create a short action register with owner, priority, deadline and evidence required.

Key takeaway

BOTTOM LINE	DPDP compliance is not one privacy policy pasted onto a website. It is a repeatable operating system for lawful purpose, understandable notice, meaningful choice, controlled access, secure processing, limited retention, individual rights and evidence.

Sources

Primary legal source: Government of India, The Digital Personal Data Protection Act, 2023 (No. 22 of 2023), Gazette of India, 11 August 2023. https://www.meity.gov.in/static/uploads/2024/06/2bf1f0e9f04e6fb4f8fef35e82c42aa5.pdf

Cyber awareness source: Indian Computer Emergency Response Team (CERT-In), Cyber Security Awareness Booklet for Digital Nagriks and Organisations. https://www.cert-in.org.in/PDF/CSA_Booklet.pdf

Terminology source: National Institute of Standards and Technology (NIST), Computer Security Resource Center Glossary. https://csrc.nist.gov/glossary

Accessed: 2 August 2026.

Disclaimer

This document is an educational summary written in plain language. It is not legal advice, a compliance certification or a substitute for the official Act, applicable rules, notifications, regulator directions, contractual duties or sector-specific law. Organisations should obtain qualified legal and security advice for their facts, risks and implementation decisions.