

GenzLudo

Ludo with 3D characters and up to 8 players. A first-of-its-kind no-teaming-up feature keeps play fair. Try it - you'll love the difference.

Download on Google Play



Kachu

Too much scrolling straining your neck? Add your addictive apps and complete daily neck exercises to unlock them.

Download on Google Play

DPDP: what founders should know beyond the basics

You already know the usual three: ask for consent when needed, explain your data use, and handle deletion requests. Here are the other parts that can affect a real app.

The Act calls your business a **Data Fiduciary** when it decides why and how personal data is used. The person whose data it is is the **Data Principal**.

Timing: India is bringing the law into force in stages. Most day-to-day duties below are scheduled for 13 May 2027. Some provisions started earlier. Read this as a build-now guide, not a claim that every duty applies today.

When can you use the data?

1. Grounds for processing

You need a lawful ground to use digital personal data: consent or a use allowed by section 7. Example: A shopping app uses an address to deliver the order the customer placed.

Act: sections 4 and 7

2. Certain legitimate uses

The Act lists situations where consent is not the route. They are specific cases, not a general permission to use data however you like. Example: A customer gives an email to receive an order receipt.

Act: section 7

3. General duties of the Data Fiduciary

Your business remains responsible for following the Act, even when another company processes data for you. Example: Your email vendor sends messages, but you still own the compliance decision.

Act: section 8(1)

4. Data processors and contracts

When a vendor processes personal data for you, use a valid contract and cover security in it. Example: Before sending customer records to a cloud provider, check the contract and access controls.

Act: section 8(2); Rules: rule 6(1)(f)

5. Data accuracy

Keep data accurate, complete and consistent when you use it to make a decision about a person or share it with another Data Fiduciary. Example: Fix a wrong address before using it for a credit or eligibility decision.

Act: section 8(3)

Protect the data and prepare for incidents

6. Reasonable security safeguards

Protect personal data against breaches. The Rules name measures such as encryption or masking, access controls, monitoring and backups. Example: Limit who can open your customer database and keep access logs.

Act: section 8(5); Rules: rule 6

7. Technical and organisational measures

Security needs people and processes as well as software. Decide who can access data, review that access and respond to problems. Example: Only support staff who need account details can see them.

Act: section 8(4); Rules: rule 6(1)(g)

8. Personal data breach notification

If a breach happens, tell affected people without delay and notify the Data Protection Board. The Rules call for a more detailed Board update within 72 hours, unless extended. Example: If a database is exposed, prepare user messages and a Board report while you investigate.

Act: section 8(6); Rules: rule 7

9. Retention and purpose

Do not keep personal data forever just because storage is cheap. Erase it when the purpose ends, subject to legal retention duties and the Rules. Example: After an order is complete, check what records you must keep and for how long.

Act: section 8(7); Rules: rule 8

People, children and requests

10. Children's personal data

A child is under 18 under this Act. Processing generally needs verifiable parental consent; tracking, behavioural monitoring and targeted ads to children face restrictions, with stated exemptions. Example: An app for teens needs an age and parent-consent flow before collecting their data.

Act: section 9; Rules: rules 10 and 12

11. Right to access information

A user can ask what personal data you process and for information about how it has been shared, subject to the Act. Example: A user asks which service providers received their profile details.

Act: section 11

12. Grievance redressal

Give people a working way to raise data complaints and publish a response period. The Rules cap that published period at 90 days. Example: Put a clear privacy contact in the app and route requests to someone who can answer.

Act: section 13; Rules: rules 9 and 14(3)

13. Right to nominate

A person can name someone to exercise their data rights if they die or become incapable of doing so. Example: An account settings page could let a user record a nominee.

Act: section 14; Rules: rule 14(4)

14. Consent Manager

This is a registered service that helps people give, manage, review and withdraw consent. A normal startup does not become one just by showing a consent box. Example: A user may manage permissions through a registered Consent Manager.

Act: sections 2(g) and 6(7)-(9); Rules: rule 4

Growth, overseas services and oversight

15. Processing outside India

Cross-border transfers are generally allowed, subject to government restrictions. Some data of Significant Data Fiduciaries may face extra transfer limits. Example: Check where a foreign analytics or cloud provider handles Indian user data.

Act: section 16; Rules: rules 13(4) and 15

16. Significant Data Fiduciary (SDF)

The government can notify certain businesses or classes as SDFs based on factors such as data volume and risk. Extra duties apply only if your business is covered. Example: A fast-growing platform should watch for an SDF notification before assuming the label fits.

Act: section 10

17. Data Protection Officer (DPO)

An SDF must appoint an India-based DPO who is responsible to its board or governing body and is a contact for complaints. Example: If notified as an SDF, name the person who will own this role.

Act: section 10(2)(a)

18. Data Protection Impact Assessment (DPIA)

An SDF must assess the risks of its personal-data processing. The Rules require this once every 12 months. Example: Before expanding a sensitive profiling feature, assess how it could affect users.

Act: section 10(2)(c); Rules: rule 13(1)

19. Independent data audit

An SDF must appoint an independent auditor. The Rules require an audit once every 12 months. Example: Have an outside auditor test whether your stated data controls work in practice.

Act: section 10(2)(b)-(c); Rules: rule 13(1)

20. Data Protection Board of India

The Board handles complaints and breaches under the Act and can decide penalties. The maximum for failing to take reasonable security safeguards is Rs 250 crore; the amount is not automatic. Example: Keep breach facts and decisions documented so you can explain what happened.

Act: sections 18, 27, 33 and Schedule

Read the official text

DPDP Act, 2023 DPDP Rules, 2025 Commencement notification

Plain-English overview for founders. Check the Act, Rules and legal advice for your exact product and launch date.

More things worth exploring

Find more free guides at vikasbuilds.com/resources