

My Clients Signed an NDA. So Why Do I Need DPDP Compliance?



Recently, a founder asked me a question I now hear in some form almost every week: "Why do I need all these compliances? My clients have already signed an NDA."

It's a fair question, and the instinct behind it is reasonable. An NDA feels like protection. It has "confidential" in the title, it has penalty clauses, and a lawyer drafted it. But under the Digital Personal Data Protection Act, 2023, an NDA and compliance are not the same thing, and an NDA is not consent. They answer different questions, involve different people and do different jobs. Treating one as a substitute for the other is a common mistake, and an expensive one.

Who is actually in the room?

Let's understand the difference:

An NDA is a contract between two organisations: a company and a client, a business and a vendor, a startup and an investor. It says: whatever I show you, you will keep secret and use only for the agreed purpose. The two signatories are the ones who benefit.

Consent under the Act comes from someone else entirely i.e. the Data Principal, the individual, whose data is being taken at the first place. This Data Principal can be anyone, a customer, an employee, an app user, a job applicant etc. Section 6 of the Act, requires that consent be free, specific, informed, unconditional and unambiguous, given through a clear affirmative action, and limited to the purpose the person was told about.

So the two documents answer different questions:

- NDA: Will the recipient keep this information confidential?
- Consent: Did the person this data belongs to agree to this use of it?

A perfectly drafted NDA answers the first question and says nothing about the second. The individual was never at the table.

So the two documents answer different questions:

- NDA: Will the recipient keep this information confidential?
- Consent: Did the person this data belongs to agree to this use of it?

A perfectly drafted NDA answers the first question and says nothing about the second. The individual was never at the table.

A scenario worth sitting with

Picture a business that provides a service to other companies. To do its job, it receives personal data from those clients: names, phone numbers, identification details, transaction records of the clients' own customers. Before work begins, the client and the service provider sign a thorough NDA. Everyone feels covered.

Now ask what the individuals in that dataset agreed to. They dealt with the client, for a specific purpose. They have probably never heard of the service provider. Nothing they were told covers the provider receiving, storing or analysing their data.

Is the provider bound to secrecy? Yes. Is the processing lawful under the Act? That depends on whether the client had a valid basis to share the data in the first place, whether the provider is acting strictly on the client's instructions, and whether the contract between them says the things the Act expects it to say. The NDA answers none of these questions.

The same pattern shows up everywhere: an employer sharing staff records with a payroll vendor, a platform passing user data to an ad partner, an institution sending student details to an outside service. The sector changes and the gap stays the same.

Why the NDA doesn't fill the gap

There are several reasons, and it helps to separate them.

1. An NDA does not create a lawful basis.

Section 4 says personal data may be processed only for a lawful purpose, meaning either with the Data Principal's consent or for one of the "certain legitimate uses" in Section 7. A confidentiality contract between two companies is not on that list. It is not a ground for processing. At best it is a safeguard placed around processing that is already lawful.

2. The individual is not a party to it.

Under ordinary contract law, only the parties can enforce an agreement. A customer cannot sue on your NDA. If her records leak, her remedies come from the statute: grievance redressal with the Data Fiduciary, and a complaint to the Data Protection Board if that fails. The NDA is irrelevant to her. It also gives you no shield against the Board, because Section 8(1) makes the Data Fiduciary responsible for compliance, including for processing carried out on its behalf by a Data Processor. A private contract does not move that responsibility elsewhere.

3. The NDA is the wrong shape.

NDAs are built around "Confidential Information" and carry familiar carve-outs: information already public, independently developed, or disclosed under legal compulsion. Personal data does not work that way. A phone number that is publicly available may sit outside your NDA's definition, but it can still be personal data that you need a basis to process. The categories do not line up.

4. Requirement of consent under the Act is for far greater purpose

When a Data Fiduciary engages a processor, Section 8(2) requires that it does so under a valid contract. That contract has to do more than promise secrecy. In practice it should deal with purpose limitation, security safeguards, breach notification, control over sub-processors, deletion or return of data when the engagement ends, and cooperation when an individual exercises her rights. A standard NDA covers almost none of that. What you need is a proper data processing agreement. The NDA can sit beside it, but it cannot replace it.

5. Consent has features an NDA cannot copy.

Consent must be tied to a purpose. It must be withdrawable, and the Act says withdrawal should be as easy as giving consent. The notice that goes with it must describe what data is collected, why, and how the person can exercise her rights. An NDA has no counterpart to any of this. It does not know the individual exists, so it cannot honour her choices.

"But we have an NDA and a consent form. sn't that enough?"

Sometimes, but only if the two match each other. This is where the second layer of mistakes appears.

A company may collect consent for "order processing and related services," then share data with an NDA-bound vendor for behavioural profiling. Two documents exist, and neither covers the activity that is actually happening. The consent was for one purpose and the NDA protects a different one. The space between them is exactly where regulatory risk sits.

The way to close it is to map your data. For every flow of personal data in or out of your organisation, you should be able to answer three questions:

1. What is my basis for this processing?
2. Is the purpose described in the notice wide enough to cover it?
3. What contract governs how the recipient handles the data?

An NDA answers none of the first two and only part of the third.

Where the NDA still earns its place

I don't want to overstate this. NDAs are useful and nobody should stop using them. They protect trade secrets, pricing, source code, strategy and all the commercial information that has nothing to do with personal data. They also support the security side of a data relationship. Section 8(5) expects reasonable security safeguards, and a contractual duty of confidentiality is a sensible layer within that.

The point is narrower. An NDA is a supporting document in a DPDP compliance structure. It should never be the load-bearing wall.

What I'd do this quarter

If you run a business or manage compliance for an organisation that handles personal data, here is a practical starting list:

- Inventory your data flows. List every party that sends you personal data and every party you send it to: clients, payment providers, cloud hosts, analytics tools, marketing agencies, HR and payroll vendors, consultants.
- Work out your role for each flow. Are you the Data Fiduciary deciding why and how the data is used, or a Data Processor acting on someone else's instructions? Your obligations change with the answer.
- Check the basis for each flow. Is it consent, a Section 7 legitimate use, or nothing you can point to? Be honest about that last category.
- Read your notices against your practice. If your notice does not describe a sharing arrangement, your consent does not cover it.
- Replace NDA-only arrangements with data processing agreements wherever personal data is involved. Keep the NDA for commercial secrets.
- Build a withdrawal path. If an individual withdraws consent, can you tell your processors to stop and delete? If that takes a week of emails, fix it before the Board asks.

- Train the people who sign. Procurement and business teams are usually the ones signing NDAs and assuming the job is done. They need to know when a data protection agreement is required instead.

Why this matters commercially

The penalty schedule under the Act is steep. Failure to maintain reasonable security safeguards can attract a penalty of up to ₹250 crore, and there are separate heads for failing to notify a breach and for breaching obligations relating to children's data. Nobody should design a compliance programme around the maximum figure. But investors, enterprise customers and procurement teams increasingly read data protection posture as a signal of how seriously a company is run. "Our clients have signed an NDA" will not survive a serious diligence question.

The short version

An NDA protects the relationship between two companies. Consent protects the person whose data moves between them. One cannot stand in for the other, because they have different signatories, different purposes and different consequences when they fail. So when a founder asks why an NDA isn't enough, the honest answer is that it was never built to do this job. It protects the business. The Act protects the individual. A compliance programme has to account for both.



Adv. Ashutosh Jain

Legal Team - International
Navodaya Chamber of
Commerce