Non-Disclosure Agreements (NDAs)

Preamble

NDAs, or non-disclosure agreements, are legally enforceable contracts that create a confidential relationship between a person who has sensitive information and a person who will gain access to that information. A confidential relationship means one or both parties has a duty not to share that information.

Non-disclosure agreements are also known as confidentiality agreements, confidentiality disclosure agreements, and non-disclosure contracts. You may encounter one at the beginning of a business relationship or large financial exchange. For example, an employer or client may ask a new hire or contractor to sign a confidentiality agreement to protect the organization's sensitive data.

An NDA specifically focuses on an individual's or organization's information privacy, which differs from other business contracts like service or sales agreements that focus on the terms and conditions of service or transactions.

The purpose of a non-disclosure agreement is twofold: confidentiality and protection. Information protected by a confidentiality agreement can include everything from product specs to client rosters. Business models, test results and even embargoed press releases or product reviews can all be covered by an NDA.

An NDA creates the legal framework to protect ideas and information from being stolen or shared with competitors or third parties. Breaking an NDA agreement triggers a host of legal ramifications, including lawsuits, financial penalties, and even criminal charges.

NDAs offer a level of protection to your business so that even accidental breaches are covered.

There are three essential functions of an NDA:

Identifying protected information: By drawing a line between what information is confidential and what can be shared, NDAs classify information. This allows parties to work freely within the boundaries created by the confidentiality agreement.

Protecting sensitive information: Signing an NDA creates a legal obligation to keep sensitive information confidential. Any leak of that information is a breach of contract.

Protecting patent rights: Because public disclosure of a pending invention can sometimes void patent rights, an NDA can protect an inventor as they develop their new product or concept.

Generally speaking, non-disclosure agreements fall into two main categories: unilateral and mutual (there's also the multilateral type, but those aren't as common). In a unilateral NDA, one party agrees not to reveal confidential information. In a mutual NDA, both sides agree that they will not share confidential information.

In all other aspects, these two types of confidentiality agreements are identical, especially when it comes to enforcement and the consequences of a breach.

An employment contract is an excellent example of a unilateral NDA. When an employee is hired, they sign a unilateral NDA agreeing not to share information learned on the job. By contrast, if one company is merging or acquiring another company, a mutual NDA ensures none of the parties participating in the process divulge confidential information.

When drafting your confidentiality agreement, here are a few questions that will determine whether you need a unilateral or mutual NDA:

Business Type: Does the activity involve a mutual exchange of information or multiple actors (e.g., mergers and acquisitions, joint ventures, teaming agreements)?
Reciprocity: Are both sides equally protected and obligated so that neither is unfairly “favored” by the agreement?
Number of Parties: Are there more than two parties participating, or is each participating party providing information?

All NDAs should include these specific elements:

Identification of Parties: Also known as “parties to the agreement”, the purpose of this section is to identify the people and/or entities involved in the non-disclosure contract. It explains who the disclosing party and recipient of are, using names and addresses. Relevant parties such as attorneys, accountants, or business partners may also be included.
Definitions: This section of the NDA lays out the different types of information covered by the agreement and establishes rules regarding how it is handled. It answers the question of what information is confidential.
Obligations: What happens if protected information is shared? An NDA not only sets out the specific behavior expected from each signatory, but it also lays out the consequences of breaching the agreement.
Scope: A clearly defined scope ensures an NDA’s enforceability. Using general terms like “proprietary information” isn’t specific enough and won’t hold up in a legal setting. Scope should lay out what specific information the NDA covers
Time frame: Most NDAs don’t last forever, and many confidentiality agreements explicitly state the number of years that sensitive information must be kept secret. Even those with an indefinite time frame will often indicate when information is no longer protected by the agreement.

Return of Information: After the conclusion of business between the parties, an NDA may require that the recipient confirm that sensitive information has been returned or destroyed.

Exclusions: These are the types of information which do not need to be kept confidential. This might include public knowledge, previously disclosed details, or information someone knew before entering a business or financial relationship with a company or firm.

Remedies: If there's a breach of the confidentiality agreement, what happens? There are many possible courses of action, or remedies. These may include a restraining order, payment for damages, and other actions for breach of fiduciary duty and copyright, patent, or trademark infringement.

Limitations of NDAs

Non-disclosure agreements (NDAs) have some limitations, including:

Enforcement challenges: Enforcing an NDA can be challenging, particularly if the information has already been disclosed or if the scope of the NDA is too broad. Even if a breach of the NDA is identified, it can be difficult to prove damages or to obtain an injunction.

Public interest: In some cases, there may be a public interest in disclosing certain information, such as in cases of illegal activity, public health and safety, or government transparency. NDAs cannot be used to prevent the disclosure of information that is in the public interest.

Limited protection: An NDA only provides protection for information that is specifically identified and defined in the agreement. If information is not covered by the NDA, or if it is disclosed in a way that is not prohibited by the agreement, it may not be protected.

Time-limited protection: NDAs are typically time-limited, meaning that they only provide protection for a specific period of time. After the NDA expires, the information may no longer be considered confidential and may be disclosed freely.

Limited jurisdiction: NDAs are typically governed by the laws of a specific jurisdiction, which may limit their effectiveness in other jurisdictions. In cases where the disclosing party is located in a different jurisdiction than the receiving party, it can be difficult to enforce the NDA.

Reputation risks: In some cases, the use of NDAs can lead to negative publicity or damage to a company's reputation. This can occur if the NDA is seen as an attempt to cover up wrongdoing or to silence victims of harassment or discrimination.

Of course, not all information can be protected. Public records, including SEC filings or company addresses, are not covered by these confidentiality agreements. The courts can also interpret the scope of an NDA in ways that one or more participants may not have initially expected. If the information covered in an NDA is revealed in another way—like through a court proceeding or subpoena—then the NDA no longer applies.

Additionally, managing multiple NDAs as an organization quickly becomes untenable without standardized language. When the number of NDAs starts reaching into the hundreds, reviewing, negotiating, and concluding unique contracts manually is extremely demanding and time-consuming. A standard, adaptable confidentiality agreement addresses this issue, but only if the organization takes the time or consults with experts to create a standard NDA that meets all its needs.

Creating an NDA

To create a legally-binding non-disclosure contract, you must use specific language when defining confidential information, parties, and scope. Broad language that can be interpreted many ways may not hold up in a legal dispute. Also, NDA creators have to

be careful not to disclose sensitive information they want covered by the NDA before the contract is signed. Non-disclosure contracts do not cover previously known information.

There is currently no standard system for NDAs, leaving organizations to figure out how to create them on their own. This places heavy demand on legal teams who could be spending time on other priorities. A standard NDA helps with this, and in a perfect world the contract is automated, accepted with the click of a button, and stored and updated electronically in case you need it later.

You do not need a lawyer to create and sign a non-disclosure agreement. However, if the information you are trying to protect is important enough to warrant an NDA, you may want to have the document reviewed by someone with legal expertise. Some contract lifecycle management software helps with this as well as providing a system for managing NDAs on a corporate level.

Contract lifecycle management software brings thoroughness and clarity to the NDA creation process. It ensures that you:

> Stay focused and fair. A non-disclosure contract should only include agreements to keep information private. Provisions like non-solicitation and non-competes will likely result in pushback from the signing party.
> Are brief. Generally, an NDA should fit on one page. Use clear and concise language that focuses only on disclosure.
> Use templates wisely. Organization-wide NDA templates are helpful, but every use case is unique. Read through the confidentiality agreement to ensure that the definitions, access, and safeguards it describes make sense for the situation.
> Know your terms. Provisions on severability, change-in-control, and exclusion of damage are not always necessary. Other times, they require extra clarity.

If writing an NDA on your own seems overwhelming or complicated, consider using contract lifecycle management software backed by legal experts. These programs come with digital contract management systems that store, track, organize, and collect signatures on contracts. With a workflow designers, data repository, and collaboration tools, you'll have everything you need to automate contract tasks like keeping up with renewal dates and obligations. These systems greatly improve efficiency for organizations handling multiple contracts.

How to Enforce an NDA

Enforcing a non-disclosure agreement (NDA) can be challenging, but there are several steps that companies can take to protect their confidential information and enforce the terms of the agreement. Here are a few general steps:

Identify the breach: The first step in enforcing an NDA is to identify the breach. This may involve monitoring employees, reviewing documents or communications, or conducting an investigation.

Send a cease and desist letter: Once a breach has been identified, the company should send a cease and desist letter to the party who has breached the NDA. The letter should outline the breach, demand that the party cease all further disclosures, and provide a deadline for compliance.

Seek injunctive relief: If the breach continues after the cease and desist letter has been sent, the company may need to seek injunctive relief from a court. This may involve filing a lawsuit and requesting a temporary restraining order or preliminary injunction to prevent further disclosures.

Pursue damages: If the breach has resulted in damages to the company, such as lost profits or damage to reputation, the company may also seek monetary damages through a lawsuit.

Consider alternative dispute resolution: In some cases, it may be more efficient or cost-effective to pursue alternative dispute resolution, such as arbitration or mediation, rather than litigation.

It's important to note that the specific steps for enforcing an NDA may vary depending on the terms of the agreement and the jurisdiction in which it is being enforced. If you aren't a lawyer yourself, consult with legal counsel to ensure you're following the appropriate procedures and maximizing your chances of success.

What Are the Consequences of Breaking an NDA?

The consequences for breaching a non-disclosure agreement (NDA) can vary depending on the terms of the agreement, the nature of the information that was disclosed, and the jurisdiction in which the agreement is being enforced. Here are some examples:

Legal action: The party that was harmed by the breach of the NDA can take legal action to enforce the agreement and seek damages for any losses that were incurred. This may involve filing a lawsuit, seeking injunctive relief, or pursuing alternative dispute resolution.

Financial penalties: NDAs often include provisions for financial penalties in the event of a breach. These penalties may be outlined in the agreement itself or may be determined by a court as part of a legal action.

Reputation damage: Breaching an NDA can damage a person's or company's reputation, particularly if the breach involves sensitive or confidential information. This can lead to loss of trust and future business opportunities.

Termination of employment or contract: Breaching an NDA can result in termination of employment or contract, particularly if the agreement was a condition of the employment or contract.

Criminal charges: In some cases, breaching an NDA can result in criminal charges, particularly if the information that was disclosed was related to national security, government secrets, or other sensitive information.

Overall, the consequences for breaching an NDA can be significant, both in terms of legal and financial penalties and damage to reputation. Companies and individuals should take NDAs seriously and ensure that they are complying with the terms of the agreement to avoid these consequences.

The Checklist

1. Identify the Parties

Identifying the parties to the agreement is the first step in examining an NDA. Ensure that everyone is identified accurately and that their names are spelt appropriately. Who is providing the secret information and who is receiving it should be made absolutely clear in the agreement.

2. Define the Confidential Information

What information is considered confidential should be expressly defined in the NDA. Trade secrets, client lists, financial data, and any other confidential information that the disclosing party wishes to keep private could fall under this category. Ensure that all the information that has to be protected is included in the definition of confidential information.

3. Specify the Purpose of the NDA

The NDA's aim should be made crystal clear. This might involve talking about possible business prospects, assessing potential investments, or serving other similar objectives. Ensure that the NDA's objective is specified clearly and corresponds to the rationale for the disclosure of the sensitive information.

4. Specify the Duration of the Agreement

The lifespan of the agreement should be plainly stated in the NDA. This could be until a particular day, until a certain period, or even until a certain event. Make that the NDA's duration is reasonable and that the confidential information is adequately protected.

5.Identify Permitted Disclosures

Any permitted disclosures of the secret material should be expressly stated in the NDA. For instance, the receiving party could need to provide the information to its staff members, subcontractors, or legal counsel. Ensure that the considered acceptable disclosures are specified explicitly and that they are only made available to those who truly require the information.

6. Specify Obligations of the Receiving Party

The terms of the receiving party's duties should be explicitly stated in the NDA. These might entail commitments to uphold confidentiality, use the private information solely for authorised purposes, return the private information upon termination of the NDA, or destroy the private information. Confirm that the receiving party's requirements are specified clearly and are sufficient to safeguard the confidential information.

7. Identify Remedies for Breach

The remedies that the disclosing party may pursue in the event of a breach of the agreement should be stated outright in the NDA. This could come in the form of monetary compensation, an injunction, or other relief. Validate that the repercussions for a breach are fair and that the confidential information is sufficiently protected.

8. Specify Governing Law and Jurisdiction

The governing laws and jurisdiction that will apply in the event of a dispute should be plainly stated in the NDA. This may include the country or state in which the parties are situated. Validate that the controlling law and jurisdiction are fair and provide a precise framework for addressing any conflicts that may arise.

9. Review Any Additional Terms and Conditions

At last, check the NDA for any additional terms and conditions that may be there. These might cover clauses that deal with liability limitations, assignment, or indemnification. Inspect that any extra terms and conditions are acceptable and consistent with the NDA's objective.

In conclusion, NDAs are vital contracts that facilitate the legal cover of organisations' sensitive information. It's crucial to properly analyse NDAs before signing them in order to guarantee that your private information is well safeguarded.

Some important Clauses in the NDA

Definition of Confidential information
Every kind of information to be shared and kept secret by the receiving party has to come under this heading so that the dispute in future can be avoided. Confidential information should be defined accurately and specifically to avoid misinterpretation or confusion. This clause clearly spells out what information is not to be disclosed.

Exceptions
• The information which is in or has come into the public domain otherwise than through a breach of this Agreement or fault of the other Party.
• The information which has been approved for its use or release by prior written permission of the other Party.
• The Confidential Information is required to be disclosed by any Statutory Requirement or Application of the Law or by the Court’s Order.
• The disclosed information doesn’t come under the definition of Confidential Information.
• The information was independently developed by other parties without making use of the Confidential Information.

Duties and obligations
• Undertaking not to disclose the Confidential Information directly or indirectly to any third party without the prior written permission from the other Party.
• To disclose the Confidential Information only to the concerned consultant and employee on the need to know basis and by executing an appropriate written NDA with them.
• To protect each other’s Confidential Information in the same manner and degree as they protect their own Confidential Information.
• To take due diligence to protect and safeguard the integrity of the Confidential Information and to protect it from unauthorized disclosures
• To promptly inform the other Party of accidental disclosure of any Confidential Information and together take steps to retrieve and protect such Confidential Information.

- To use the Confidential Information only for the purpose of the proposed transaction.