5 Tips to get value & compliance when requesting or signing an NDA?

A Non-Disclosure Agreement (NDA) is one of the most widely used and abused legal documents in business today. The purpose of an NDA is to secure and protect confidential information when there is a compelling need to share confidential information between two or more parties. This paper is not a detailed legal review (and we always recommend that your lawyer prepares/reviews NDA's where they are new to your business).

Tip 1

Choose the correct type of NDA, Unilateral or Bilateral(Mutual-reciprocal).

If the confidential information flow is one way from the providing party to the receiving party, then a unilateral NDA is most appropriate, in this instance the providing party gains legal agreement from the receiving party to the providing parties terms and clauses outlined in the unilateral NDA. It is assumed that the receiving party do not submit any of their confidential information to the providing party and therefore they have no protection if they do provide it. In certain situations the providing party may be big or have power , and they try and insist you sign their unilateral NDA. In these cases, if you as the receiving party will, or may share some of your confidential information that you should decline to sign the unilateral NDA, and request this more powerful provider to provide their mutual/reciprocal NDA (Most enterprises have both types of NDA's). A Bilateral (Mutual/reciprocal) NDA normally has equal terms and clauses that apply to each party, so both parties have the same rights and protections from the NDA. In my experience 90% of NDA's are, or should be Bilateral. On occasion the weight of the requirements on one party may differ with the other party and in these circumstances legal advice should be sought prior to signing.

Tip 2

Be definitive on the purpose of the NDA and relevant confidential information

An NDA regardless of type above is normally put in place between two parties for a purpose. Having a clear definition of that purpose linked to confidential information provides clear criteria and a basis for requesting and for providing the relevant confidential information. Detail and a record should be noted in a request for confidential information, and in the provision of confidential information which always provides the link between the purpose and the exchange. This approach can also a basis for dialog should there be any misunderstanding in advance of an exchange, it is also a record following the exchange. This approach creates the framework boundaries for only appropriate confidential information to be shared.

Tip 3

Mark the level/label on all confidential information digitally or physically

There is a natural tendency to mark all or most of an organisations information as confidential and/or include a © Symbol. This in my opinion creates a situation where the parties "can't see the wood for the trees". The reality is that most information is either not actually confidential in nature, or by provenance/history has already been compromised in some way through previous action. Therefore it is important to have a confidentiality labelling system within an organisation that guides

its members to appropriately manage and handle confidential information. Of course there are many different types of confidential information such as inventions, technology, financial, personnel related, commercially related. A simple defined category labelling and rule system that is consistently applied only to relevant confidential information should be in place. Here is a simple example:-

- ***Secret:-*** Absolutely strategically or tactically sensitive information that is only available and should only be visible to a small number of named company stakeholders.
- ***Legally Confidential:-*** Highly sensitive confidential information that is only available to persons or organisations who have a legal confidentially agreement with the organisation for the specific purpose that this information is relevant to. Access to such Information is controlled and recorded, it may be more widely shared than "Secret" but anyone entitled to and / or in receipt can be identified.
- ***Company Confidential:-*** Important and sensitive information that by its nature may get more widely shared within an organisation , however cannot be shared to anyone or any organisation who does not have an appropriate contract with the organisation.
- ***Commercially Confidential:-*** Day to day business often requires the sharing of information that if found in the wrong hands could have commercially damaging consequences for the organisation, yet there needs to be flexibility in the exchange of information to carry out day to day processes. Examples might include submitting a proposal in response to a tender that requires pricing or a unique design to be disclosed. The sharing of some operational advantage with a supplier or partner to enable them to provide their product and/or service effectively. In these types of scenarios it is important that there is a related legal and binding confidentiality clause traceable in the process of these day to day transactions and the commercially sensitive information being disclosed is marked confidential/commercially sensitive and covered / linked to the legal agreement, document and clause .

Tip 4

Know when there is a sound business case for involving legal professionals

At one end of the spectrum I have seen organisations that require every potential legally related activity or artefact to be passed through legal for approval, and of course the other end of the spectrum where there is no, or very limited involvement of the legal profession, often where the primary source of legal documents and information is from the Internet. At the conservative end with high legal involvement, there is a potentially significant cost and efficiency/effectiveness issue within the business, and at the other end there is likely to be a large invisible legal exposure/risk. . Some sub tips are as follows:-

- *A standard set of approved and issued NDA templates*
- *An NDA format that is un-editable as regards, core legal clauses , but allows for the core editable variables/schedules that subject matter experts can complete.*
- *A simple traceable registers and check out of a template and tracking to check back in of fully signed NDA (Or abandonment with reason)*
- *Identify those roles who frequently are requested to handle NDA's train and empower them to issue and sign own NDA's and standard 3rd party NDA's (This usually starts with one or two*

non-legal operational personnel who regularly handle NDA's and have become familiar with the terminology and requirements). Individuals need to be named on an approved list.

- *All 3rd party NDA's get a 2nd set of recorded eyes applied if not already identified as requiring formal legal review.*

Tip 5

Create a process where the evidential nature of information in the organisation is secure

This is not just about NDA's and related confidential information, but also the information environment that could have direct or indirect compliance risk, both for your organisation as a receiver and provider of confidential information and also for the ownership, provenance and future use of innovative information for future value creation. It is important that all information but particularly confidential information you create, update, receive or modify has a record that can prove its ownership, Provenance, authenticity and integrity, this is just good practice. You must be able to demonstrate that you look after confidential information whether it be your own or received from a 3rd party and, that you comply with NDA obligations.

So whether it be physical , verbal or digital confidential information you must have a process that demonstrates how it is managed , stored, shared and processed within your organisation.

Another important perspective relates to the NDA exception/exclusion Clauses. The terms, conditions and obligations defined in the NDA are nullified in certain defined circumstances, some examples are:-

- You can prove the information marked as confidential was, previous to receipt and notification, available in the public domain.
- You independently received the information from an alternative legitimate source without restrictions
- You had already freely and independently developed or acquired the related information and/or idea.
- Statutory obligation to provide the information.

So to give comfort to all stakeholders you need to have the recorded non refutable evidence of your information management. As most data and information is now created and processed digitally a simple IT solution is required.

Creating digital evidence and an audit trail, to assure your confidential information and that of 3rd parties, are managed and do not restrict your business or value creation.

The simplest and most cost efficient manner is to use a solution such as Digiprove (www.digiprove.com) there are 3 different tools from Digiprove that can be used depending on your business context. Each of these solutions will assure the ownership, provenance, authenticity and integrity of information you create , process and/or manage. You are not required to send any confidential information files to Digiprove so your confidential information is retained in your own environment.

1. Digiprove self-protect allows on-line manual certification of any digital content at any point in time suitable for low volume scenarios
2. Digiprove Autoprotect runs in the background automatically and at intervals chosen by you automatically certifies all files and folders you select. Just download and install on your server and/or desktop.
3. Digiprove API & SDK allows simple and rapid integration of the Digiprove technology into your information management systems, giving you the flexibility at any point in your process or in time to have automatic certification of your digital information.