How To Utilize NDAs and DPAs to Your Full Advantage

Some thoughts on protecting your confidential information and the difference between NDAs and DPAs.

When it comes to the world of business, there are few things that can cause issues like data breaches. These problems can take multiple forms, from confidential data accidentally being exposed, to an industry partner or employee exposing things you wanted to keep under wraps. The legal and financial ramifications of issues are widespread. There are, however, safeguards you can put in place to be able to take action against those behind data breaches. In general, these agreements are called NDAs and DPAs, but to use them to their full potential, you need to keep a few things in mind.

What Are NDAs/DPAs?

Note that NDAs and DPAs are not interchangeable. Here are a few details on each.

NDAs: Also known as non-disclosure agreements, these create a legal obligation for one party to keep certain information of the other party private. For example, software companies may want to keep the details of their next product secret, a restaurant may do this for their recipes, or a film set may have extras sign these so they don't take pictures of production.

DPAs: Also known as data processing agreements, these documents were recently instituted under the U.K's Data Protection Act and the EU's general data protection regulation (GDPR). The goal of DPAs is to try and establish a baseline for protecting sensitive data business have on their customers (financial records, medical records, etc.). Basically, when a vendor, client, or partner signs one of these, you are afforded certain legal rights and a guarantee they will hold to this baseline of protection, generally relating to consumer data.

Enforcing and Empowering Your NDAs/DPAs

So, we understand the basic purpose of these documents, but how do you leverage them to ensure you are legally protected? One of the first things you want to do is have a clear definition of what is confidential information (for NDAs) or the different types of data you will be covering (for DPAs). This is important because if you give a broader definition, it may be difficult for your legal team to properly enforce the agreements down the line.

When it comes to DPAs specifically, you also need to be careful of the shifting landscape of evolving technology and privacy policies constantly changing. Where information is stored in the cloud, appropriate security measures or regulations may be changing often, and you want a DPA that brings these into account. One way to make this happen is by bringing your chief privacy officer to the table when drafting a DPA. Their insight may prove essential for keeping you covered. In addition, with NDAs, you want to balance achieving protection and limiting the amount of overly burdensome controls over an industry partner.

Depending on the sensitivity of your project/IP, one missed clause or vague statement in your NDAs or DPAs can keep them from properly fulfilling their purpose. The last thing you want to do is put your business at risk due to such a simple mistake. The best way to avoid this problem is to trust an experienced attorney to guide you through the initial drafts of these key documents. This way, you know you and your business have the proper legal protection in all possible scenarios.