EUGENE F COLLINS

Non-Disclosure Agreements – *Return and Destroy Obligations in the era of Cloud Storage*

Non-Disclosure Agreements – Return and Destroy Obligations in the era of Cloud Storage

7 May 2019

In light of technological developments, can a recipient of confidential information governed by an NDA be sure they are in compliance with the return and destroy obligations in most standard NDAs?

Introduction to NDAs

Non-Disclosure Agreements ("NDAs") govern the exchange of confidential information between two or more parties. They are often entered into by those considering the purchase of a business or asset, an investment or joint venture arrangement. The sharing of sensitive or proprietary information is therefore required between parties to enable commercial assessment of the merit of the proposed action.

Return and Destroy Obligations

To-date, NDAs typically contain simple absolute obligations on the recipient of confidential information not to copy or save it and to return or destroy the information at any time at the request of the party who has disclosed it. Although such obligations are burdensome from a practical perspective, they have, until now, at least been possible to meet. Returning or destroying hardcopy documents, CDs or USB sticks is straightforward and returning or deleting files from an internal computer system usually requires minimum technical expertise.

How to satisfy such Obligations in the era of Cloud Storage

Many businesses and private individuals now use advanced online storage platforms (a.k.a. the "Cloud") as part of their standard IT operating procedures. Information received by email, opened on a computer or downloaded, is often automatically taken onto the recipient's internal IT system and then saved into the Cloud, often without an individual's knowledge or the requirement for a specific command from an individual to do so.

Considering these technological advances, how then can a recipient of confidential material governed by an NDA ensure they are in compliance with the return and destroy obligations in most standard NDAs? How can the disclosing party best protect its valued information and ensure that is does not remain in the possession of the other parties' information indefinitely (in the Cloud) and which may possibly become accessible to other parties in future?

It is our experience that a significant number of the NDAs circulating in practice still do not address these new changed circumstances.

If you intend to receive confidential information under an NDA…

- Review the NDA keeping in mind your own work practices and the operation of your business' software system.
- Qualify or limit any absolute obligations on you to return or destroy confidential information so that such obligations are expressed to be ones to which you will adhere "*in so far as is reasonably practicable and technically possible*".
- To the extent possible, ensure that softcopy confidential information is kept separate to your own business information – speak to your IT department and, depending on the scale of the transaction, consider obtaining separate Cloud storage for the confidential information which can be secured and user limited in future, if not destroyed. The NDA could reflect such a step.
- Be prepared to provide an internal systems report at the end of a commercial engagement showing the various searches done for the confidential information and the commands to delete it.

If you intend to disclose confidential information under an NDA…

- Include in the NDA a clear obligation on the recipient that the information must remain confidential in future notwithstanding any difficulties associated with the return or destruction of confidential information stored in the Cloud.

- Query the information storage practices of the recipient.

- Consider whether including an obligation to use specific Cloud storage for your confidential information is appropriate. Whether or not separate Cloud storage is used, include a requirement that the recipient appropriately secures confidential information maintained in the Cloud indefinitely, especially if its full destruction cannot be assured.

Possible Future Trends

It is likely that future NDA templates will more precisely reflect the new widespread use of online information management systems. Obligations to return and destroy are likely to be supplemented or replaced by more precise requirements relating to the *securing* of information.

Some virtual data room providers now offer in-built document protections such as auto-destruct features whereby, regardless of the actions of the recipient of the information and its eventual location on their system, the information will self-destruct at a designated point in future or on command of the discloser.

Use of such protective software programs may become commonplace, an acknowledged feature of NDAs and indeed a pre-requisite to the disclosure of any confidential information by a discerning party.

For further information, please contact Deborah Kelly, Partner and Head of Corporate, Doreen Mescal, Corporate Solicitor or another member of the Corporate Team at Eugene F. Collins

Deborah Kelly
Partner, Head of Corporate
T +353 1 202 6460
E dkelly@efc.ie

Doreen Mescal
Solicitor, Corporate
T +353 1 202 6563
E dmescal@efc.ie