The 'dark' side of the data room: disclosure dangers in M&A and finance transactions

03 October 2018 | Contributed by Patrikios Pavlou & Associates LLC

AUTHOR

Elena Georgiou

Given the corporate environment's ever-changing nature and business needs and the importance of data protection at the EU level, the topic of due diligence in M&A and financial transactions warrants examination. The disclosure, transfer and processing of data raises concerns at several stages of the due diligence process during a transaction and undoubtedly makes things more complicated.

Legal due diligence

Legal due diligence is the exercise pursuant to which legal professionals examine a target company's affairs by investigating its structure, constitutional documents, agreements and other corporate records. Assessing the potential legal risks of acquiring a target company, as well as its equity and assets, is vital in the context of M&A transactions. The ultimate aim of a due diligence exercise is to green-light a corporate, financing, restructuring or M&A transaction and reduce the likelihood of any unpleasant surprises following its completion.

Legal due diligence usually culminates in the preparation of a report that:

- represents the findings of the corporate review and examination;
- sets out the key issues that should be brought to the attention of the parties to the upcoming transaction; and
- provides potential recommendations regarding any problematic issues that might endanger the successful execution and conclusion of a deal.

During a legal due diligence examination, a variety of documents are disclosed, including:

- the target company's memorandum and articles of association;
- shareholders' agreements in the company's articles of association;
- corporate registers;
- corporate certificates issued by the Registrar of Companies;
- corporate approvals passed by the company's board of directors or shareholders;
- minutes from the board of director or general or extraordinary shareholder meetings; and
- agreements and contracts relating to IP rights, financing, restructuring or obtaining security (eg, pledge agreements, guarantees, or agreements governing the relationship of the company with its employees).

These documents encompass only one part of the due diligence exercise, as financial and tax advisers must also carry out financial due diligence.

To facilitate the flow of information used for due diligence in the digital era, and in the spirit of the 'think green – keep it on the screen' approach, a virtual data room is usually established. This allows legal and financial professionals and potential purchasers or investors to avoid the need to meet face to face, exchange pleasantries and instead provides access to a virtual data room where all relevant

information and documents are uploaded. Each party is offered the opportunity to conduct their own risk assessment of the transaction in question.

Data protection in M&A transactions

The above exercise gives rise to a dilemma: a target company must abide by data protection rules, as well as confidentiality obligations, while allowing the transacting parties to access a large amount of information in order to complete their due diligence successfully.

The General Data Protection Regulation (GDPR) is the European Union's main data protection legislation and has introduced increased harmonisation of data protection laws across EU member states. The GDPR defines 'personal data' as:

> *Any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.*

The GDPR applies to businesses that process personal data as data controllers or data processors, regardless of whether the processing takes place in the European Union. Companies that disclose contracts, agreements or other documents that contain personal data during a due diligence must be aware of the dangers of violating data protection provisions and implement the appropriate safeguards for the dissemination of such information, especially when a data room is used.

Under the GDPR, personal data must be:

- processed lawfully, fairly and in a transparent manner;
- collected only for a specified, clear and legitimate purpose;
- adequate, relevant and limited to what is necessary in relation to the purpose for which it is processed;
- accurate and up to date where necessary;
- not kept in a form which permits identification of the data subjects for longer than is necessary for the purpose for which the data is processed;
- processed in a manner that ensures its security, using the appropriate technical and organisational measures to protect against unauthorised or unlawful processing and against the data's accidental loss, destruction or damage;
- not transferred to another country without appropriate safeguards being in place; and
- made available to data subjects who are allowed to exercise certain rights in relation to the data.

Companies are responsible for and must be able to demonstrate compliance with the data protection principles listed above.

Personal data must always be processed lawfully, fairly and in a transparent manner in relation to the data subject and certain conditions must be fulfilled, including:

- the data subject must give their consent;
- the data processing must be necessary for the performance of a contract with the data subject;
- legal compliance obligations must be met;
- the data subject's vital interests must be protected; and
- the data must be processed to pursue legitimate interests and must not prejudice the data subject's interests or fundamental rights and freedoms.

In light of the above, data disclosed during M&A and financial transactions must be disclosed lawfully, fairly and in a transparent manner. Companies are advised to disclose only information that is necessary for a deal to go through. The setting up of a data room raises further concerns relating to the security of that information and digital protection issues of data disclosure and processing.

Issues of consent can complicate matters in cases where the data being processed and disclosed is:

- sensitive personal data (ie, the subject's religious, ideological, political or union-related views or data relating to the subject's health, racial origin, social security measures and administrative or criminal proceedings); or
- a 'personality profile' (defined as a collection of data permitting an assessment of a natural person's personality).

Justification based on legal compliance obligations or overriding public interest cannot be easily evoked in the context of a due diligence exercise and would require the data subject's consent or the pursuit of a private interest. In the case of sensitive personal data, it could make sense for companies to cease processing such data, unless there is a specific purpose for which it is deemed necessary.

Consent must be based on appropriate information and be given voluntarily. Considering the magnitude of documents in a transaction, a company could be lost in a labyrinth of consents if it tries to obtain the consent of each party involved. This also raises issues of timing and confidentiality, as finance or M&A transactions are usually strictly confidential.

This potentially leaves only the justification of an overriding private interest, whereby a company can claim that the relevant personal data will need to be disclosed and processed for the performance of a contract that is connected to the data subject. However, this justification is not as straightforward as it might seem, as the company will have to weigh the disclosure interest versus the data subject's privacy.

The nature of data contained in such documents and their virtual nature in the digital era may complicate matters further, as a virtual data room requires careful handling and supervision, including setting up access restrictions and limiting the its contents to the perusal and review of the documents contained therein.

Comment

Unless companies can navigate their way around the rules set out by the GDPR, it is highly likely that they will encounter significant difficulties and potential data protection breaches in the context of due diligence work undertaken for M&A transactions. It is advisable to involve a GDPR specialist before and during the setting up of an information system through which information for due diligence will be disclosed and disseminated, particularly with regard to a virtual data room, in order to shed some light in those 'dark' corners.

For further information on this topic please contact Elena Georgiou at Patrikios Pavlou & Associates LLC by telephone (+357 25 87 15 99) or email (egeorgiou@pavlaw.com). The Patrikios Pavlou & Associates LLC website can be accessed at www.pavlaw.com.