Avoiding conflicts between due diligence and privacy

May, 25 2011

By Manuela Cavallo and Giuseppe Battaglia

Introduction

The impact of data protection law on due diligence is an increasingly important aspect of M&A transactions. Italian law has no specific provisions on data protection in due diligence; nor has the Data Protection Authority issued administrative provisions on the subject. Nevertheless, parties to mergers and acquisitions must think carefully about the data protection aspects of their deal.

Due diligence often involves data relating to entities and individuals other than the target. It extends to financial statements and accounts, correspondence and any contracts or other documentation about the target that a potential acquirer might consider relevant. M&A professionals are likely to become aware of data about natural or legal persons which are third parties in respect of the deal process (eg, the target's customers, suppliers and employees). Such information may be essential to a decision on the deal and its structure.

Investigations during due diligence may qualify as 'data processing' under the Privacy Code (Legislative Decree 196/2003),(1) and professionals who undertake due diligence must comply with certain information and communication obligations in order to protect the privacy of the data subjects in question. Therefore, before beginning due diligence on a target, such professionals must determine:

- whether and how disclosure of information may trigger the application of the code; and
- whether solutions can be found to make due diligence activity consistent with the code.

Key provisions of Privacy Code

Due diligence may involve information that constitutes 'personal data', 'identification data' or 'sensitive data' within the meaning of the code.(2) Private entities may not process personal data unless the data subject:

- has been informed of the processing - which fulfils the so-called 'duty of information'; and
- has expressly opted into such processing.

However, consent is not required in certain circumstances - for example, if such processing is necessary "for the performance of obligations of a contract to which the data subject is a party, or to comply with specific requests made by the data subject prior to entering into a contract".(3)

Most Italian commentators believe that the opt-in rule does not apply if processing during due diligence relates to data belonging to the target, the vendor or the potential acquirer. However, the rule applies to the processing of data that relates to the target's customers, suppliers and employees.

Exemption from consent requirements

Seeking consent from customers, suppliers and employees is feasible only in theory, as confidentiality is generally essential in the preliminary phase of an acquisition. Moreover, such an obligation would represent a significant obstacle to the deal. However, the code does not require consent in all circumstances; an exception applies to "data relating to economic activities that are processed in compliance with the legislation in force as applying to business and industrial secrecy".(4)

Some commentators consider that this provision exempts business data processing during due diligence, but the applicability of the exemption is unclear.

Work-arounds for consent

Regardless of the applicability of ad hoc consent exemptions under the code, M&A professionals should seek an alternative to obtaining the consent of data subjects. There are two options to consider.

One option is to anonymise the information as far as possible. This approach will not always be acceptable to the potential acquirer, especially if it has a particular interest in identifying a key client or employee.

Alternatively, professionals who perform due diligence may qualify as 'persons in charge of data processing' pursuant to the code. As such, disclosure of personal data without consent to such professionals will not be considered communication to third parties and will not breach the code. In order to make this solution viable, it is essential to ensure that:

- the individuals in charge of data processing accept the role in writing; and
- the target acts as 'data controller' within the meaning of the code, managing data processing within the scope of due diligence activity.

However, instructions given by the target in its data-controlling capacity should not preclude the performance of due diligence by specialised professionals; otherwise, the target may be liable to the potential acquirer for the breach of clauses concerning the performance of due diligence. It is advisable for the vendor to include instructions on due diligence activities in the data room rules that it agrees with the potential acquirer.

Work-arounds for duty of information

Regardless of the approach to the issue of consent, a duty of information will still apply. As far as employee data is concerned, a possible approach is for employment contracts to include general information and consent clauses, whereby the employee expressly consents to:

- the company's employment records being disclosed to specialists in a due diligence process; and
- the company's data on employment being disclosed to a third party that proposes a merger or an acquisition.

A similar approach can be adopted in agreements with customers and suppliers.

Impact on cross-border due diligence

In deals involving companies from outside the European Union, information and consent duties affect not only data processing itself, but also the transfer of data abroad, to which consent and information duties also apply.

Such transfer may be allowed under a data transfer agreement, provided that the latter is correctly executed. The target and the would-be acquirer may choose to enter into such an agreement on the basis of the standard clauses approved by the European Commission, either in the letter of intent or by means of a separate contractual deed. However, from a practical perspective, the execution of a data transfer agreement is likely to prolong negotiations. Furthermore, such an agreement will not necessarily be acceptable to an acquirer, which would thereby assume specific contractual obligations with an associated risk of liability.

Alternatively, data transfer to non-EU countries may be approved by the Data Protection Authority on a case-by-case basis.

Consent exemptions relating to data processing for economic activities do not apply to crossborder due diligence, as they fall outside the scope of Article 43 of the code (which specifically mentions the circumstances in which data may be transferred to non-EU countries without the data subject's consent).

If the processing concerns data which relates purely to legal persons or associations, such data can be transferred freely from Italy to non-EU countries, regardless of form or means.(5)

Comment

The impact of data protection rules on due diligence is all too rarely discussed. Vendors must ensure that they approach the issue cautiously during due diligence, regardless of whether the potential deal is domestic or international. Similarly, potential acquirers should adopt ad hoc measures to ensure that the processing of data relating to the target's employees, clients and suppliers does not break the law.

Endnotes

(1) Article 4(1)(a) of the code extensively defines 'data processing' as any activity concerning "collection, recording, organisation, keeping, interrogation, elaboration, modification, selection, retrieval, comparison, utilisation, interconnection, blocking, communication, dissemination, erasure or destruction of data, whether or not such information is part of a database".

(2) 'Personal data' is any information relating to individuals or persons that are or can be identified, even indirectly, by reference to other information, including a personal identification number.

'Identification data' is personal data that allows the data subject to be directly identified. 'Sensitive data' is personal data that may disclose racial or ethnic origin, religious or philosophical beliefs, political opinions, membership of political parties or trade unions, health and sexual attitudes. In the context of an M&A deal, concerns over sensitive data may arise in connection with the target's employment contracts.

(3) Article 24(1)(b) of the code.

(4) Id, Article 24(1)(d).

(5) Id, Article 43(1)(h).