Data protection

Wim Nauwelaerts looks at how EU data privacy law affects the preparatory stage of mergers and acquisitions

Business acquisitions typically involve the up-front review of target-related information, sometimes by several potential buyers. The information reviewed during such a 'due diligence' exercise may include customer data and employee files, which are likely to constitute 'personal data' under EU data privacy rules. In Europe, personal data is protected by stringent rules and can be processed only under certain conditions. However, effective compliance with EU data privacy rules in the context of business transfers is often neglected, exposing both sellers and potential buyers to possible private claims and / or public sanctions.

Caveat emptor

When companies or business units are put up for sale, common sense suggests that potential buyers review all relevant company information before acquiring the target(s). The information under review frequently includes detailed data concerning the company's customers and employees (eg, customer contact lists, employment agreements, stock incentive plans). Although potential buyers usually sign a confidentiality agreement, European data privacy rules are not always observed.

Under EU Directive 95 / 46 / EC (Directive), processing of personal data – ie, any handling of information relating to an identified or identifiable natural person – is subject to stringent requirements and limitations, designed to protect the rights and freedoms of individuals in Europe. Processing of personal data is considered lawful only if it meets certain criteria imposed by law. In practical terms, anyone who wishes to process an individual's personal data within Europe will first need to identify a legitimate basis for such data processing.

In the particular context of M&A, sellers have two main options to legitimise the disclosure of personal employee data. First, the disclosure could be based on the employee's consent. Although this option may work for certain key personnel, it is not very practical for multinationals with a vast work force, or when the proposed transaction is still confidential. Moreover, most national data privacy authorities take the view that consent should be confined to cases where the employee has a genuine free choice. Faced with a potential M&A scenario, not all employees may be in a position to consent freely.

Alternatively, the seller could invoke that processing of personal data is necessary for the purpose of pursuing legitimate interests with potential buyers (to whom the seller discloses the data). Selling a business could be regarded as a legitimate interest and hence a lawful basis for disclosure of personal data to third parties, provided that the interests of the selling and buying parties are not overridden by the rights and freedoms of the individuals whose personal data is at stake. This criterion requires that a careful balance be struck between the interests of the sellers / buyers on the one hand, and the interests of the employees on the other. Although there is no uniform interpretation of this concept, most human resources data – including identity data and salary information – can usually be processed in accordance with this 'weighing-of-interest' rule. The recipients of the data must, however, comply with certain confidentiality and security requirements, which include the implementation of appropriate technical and organisation measures.

As far as customer information is concerned, obtaining consent may not be practically possible in all cases, in particular when the transaction is still confidential. If only basic customer data is disclosed (eg, name, address and contact telephone / facsimile number), it may suffice to rely on the seller's business interest in disclosing that data. In addition, the seller may consider informing its customers of the anticipated disclosure, to avoid complaints from indignant customers who discover that their personal data was disclosed to third parties without their knowledge.

Following review of the documents made available by the seller, potential buyers will generally prepare a report on their due diligence findings. If personal data on customers and / or employees were lawfully disclosed to a potential buyer, the latter would be allowed to integrate such data in its due diligence report and make use of it in its negotiations with the seller. Nonetheless, personal data contained in due diligence reports should not be used for other purposes, such as marketing or the re-sale of the business to third parties.

General rules

In addition, the Directive contains particularly sweeping rules that apply when personal customer and / or employee data is transferred outside Europe, for example, to a potential buyer's headquarters in the US. As a rule, what constitutes an outbound transfer of personal data is broadly interpreted and includes transmitting (hard copy or electronic) documents in various ways.

Pursuant to Art 25 of the Directive, transfer of personal data to a country outside Europe is prohibited in principle, unless that country ensures an adequate level of protection for the privacy rights of the individuals concerned. There is a great deal of uncertainty about whether a particular privacy regime would be deemed 'adequate'. So far, the European Commission has acknowledged the adequacy of the level of protection offered in a limited number of countries only (ie, Argentina, Switzerland, Guernsey and the Isle of Man). Although there is a substantial flow of personal data from Europe to the US and Japan, these countries are currently not considered to offer adequate data privacy protection.

Wim Nauwelaerts is counsel at Hogan & Hartson Email: Wnauwelaerts@hhlaw.com

Ad hoc contracts

Sellers and potential buyers could also consider using *ad hoc* contracts that are individually negotiated to comply with legal requirements regarding transfer of data outside Europe. In most European countries, such contracts will need to be approved by the local data privacy authorities prior to the anticipated data transfer. These approvals can take several months to obtain and may therefore not be suitable for M&A scenarios that involve the transfer of personal data outside Europe.

As a user-friendly alternative to *ad hoc* contracts, EU data privacy law provides model clauses for transfers of data to recipients located outside Europe. These model clauses do not require prior approval by local data privacy authorities. If a potential buyer outside Europe elects to abide by the principles set forth in the model clauses, it will have to adhere to higher standards than normally expected under EU data privacy law. As a result, the model clauses are probably less suitable for transferring M&A-related personal data outside Europe.

As data privacy laws in Europe are relatively new and only recently enforced, it may not always be possible to abide by the strict letter of the law. However, at a minimum, (potential) parties to a merger or acquisition need to show they have considered these issues, seek to minimise circulation of personal data to cases where it is strictly necessary, and provide reasonable protection for the data that are disclosed. This may include reviewing personal data in Europe only, where possible. As companies and their officers run the risk of criminal and civil liability (possibly resulting in monetary penalties and sometimes even imprisonment), they cannot afford a nonchalant attitude when it comes to disclosing and transferring personal data.

Nonetheless, EU privacy rules do include several exceptions that allow for international transfers of personal data where there is no 'adequacy' determination in place for the relevant jurisdiction. Relevant to M&A are situations where:

(i) the customer or employee has given its unambiguous consent to the transfer of its personal data;

(ii) the transfer is necessary for the conclusion or performance of an agreement concluded or to be concluded between the seller and potential buyers, which is in the interest of the individual whose personal data is transferred; or

(iii) the selling and potentially buying parties have entered into individually negotiated or 'model contracts' to legitimise the transfer.

Cross-border data

Still, there are some serious drawbacks to these exceptions. Where employee consent is required to legitimise cross-border data transfers from Europe to third countries, opt-in or affirmative consent will be required almost always. As part of the unambiguous consent requirement in Art 26(1) of the Directive, several European countries (eg, Austria, Belgium and Spain) also oblige the seller to inform its employees that personal data will be transferred to a country that may not ensure 'adequate' privacy. Furthermore, sellers wishing to rely on consent should always examine whether the country from which the data is to be exported accepts employee consent as a valid basis for legitimising such transfers.

The seller may choose to transfer employee information on the basis that a transfer is necessary to enter into an agreement with a third party (outside Europe) which ultimately will benefit the employee. The data privacy authorities in most EU countries take a narrow view of what is 'necessary' to enter into such an agreement. Consequently, they might question whether it is essential for potential buyers to 'export' personal data to a country outside Europe. In other words, they might argue that the review of such personal data may just as well take place in Europe, or that the exchange of anonymised data instead would be equally effective.