How EU data privacy affects due diligence

Data privacy is often forgotten during mergers and acquisitions, exposing buyers and sellers to private claims as well as public penalties. Wim Nauwelaerts explains

When companies, business units or company assets are put up for sale, the information under review frequently includes detailed data concerning the company's customers and employees. Customer contact lists and contract summaries, employment agreements, stock incentive plans and stock option contracts are some of the documents that are typically analyzed and/or photocopied by potential buyers. Although the seller usually ensures that potential buyers agree to some form of confidentiality obligation before access to these documents is granted, European data privacy rules are not always adequately complied with in the preparatory process of a merger or acquisition.

Consent

Specific legislation governing the collection, use, processing, or disclosure of personal data and the free movement of data in Europe was introduced in 1995, through the adoption of Directive 95/46/EC. Emanating from the European Parliament and the Council, Directive 95/46/EC was subsequently transposed into the national laws of the current 25 EU member countries and three European Fair Trade Association-countries (Iceland, Liechtenstein and Norway), jointly referred to as the European Economic Area (EEA). Under EU data privacy rules, processing of personal data (that is, 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 personal data is considered lawful only if it meets certain criteria. In practical terms, anyone who wishes to process an individual's personal data within Europe will first need to identify a legitimate basis for that data processing.

In the particular context of M&A, sellers have two main options to legitimize the disclosure of personal employee data to potential buyers. First of all, the disclosure of personal data could be based on the employee's consent. Although the seller may be able to obtain the consent of some key employees, this may not be a practical solution if the seller has a large work force, or if the proposed transaction is (still) in a confidential stage.

Moreover, most national data privacy authorities in Europe take the view that consent should be confined to cases where the employee has a genuine free choice and is subsequently able to withdraw their consent without detriment. Faced with a potential acquisition, not all employees may be in a position to consent freely. Nevertheless, if some of the personal data is sensitive in nature (for example, pertaining to an individual's racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, health or sex life) the seller will have no other choice than to rely on consent.

Selling a business could be regarded as a legitimate interest and hence a lawful basis for disclosure of personal data to third parties

Another option would be to invoke the necessity of processing for the purpose of pursuing legitimate interests with potential buyers (to whom the seller discloses personal 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 are at stake.

This criterion requires that a careful balance be struck between the interests of the sellers and buyers on the one hand, and the interests of the employees on the other. Although there is no uniform interpretation of this criterion by the different data privacy authorities, non-sensitive employee data (including identity data, salary information or educational background) can usually be processed in accordance with this weighing-of-interest rule. However, if this criterion is relied upon, employees are entitled to object to the processing of their personal data at any time. Furthermore, the recipients of the data must comply with certain confidentiality and security requirements, which include the implementation of appropriate technical and organization measures to prevent accidental or unlawful disclosure, loss, alteration or access of personal data.

Obtaining consent may not always be practically possible. In most cases where only basic customer data are disclosed (such as, name, addresses and contact telephone or fax numbers), it may be enough to rely on the seller's business interest in disclosing that data as a legal basis for processing. In addition, the seller may consider telling its customers that its customer base will be disclosed to potential buyers, and that each customer has the opportunity to have its personal data deleted before that disclosure. This practice (if possible from a confidentiality viewpoint) is likely to avoid complaints from indignant customers who discover that their personal data were disclosed to third parties without their knowledge.

After the review of 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, that buyer is allowed to integrate the data in its due diligence report and make use of it in its negotiations with the seller. Nonetheless, potential buyers should make sure that the personal data in due diligence reports are not used for other purposes, such as marketing or the re-sale of the business to third parties.

In addition to these general principles on personal data processing, sweeping rules apply when personal customer and/or employee data (gathered in Europe) are transferred outside the EEA, for example, to a potential buyer's head-

quarters in Japan. As a rule, what constitutes an outbound transfer of personal data is broadly interpreted and includes transmitting documents to third parties electronically or in hard copy.

Transfer of personal data to a country outside the EEA is prohibited in principle, unless that country ensures an adequate level of protection for the rights and freedoms of the individuals whose personal data are transferred. But European data privacy laws do not define adequacy, leaving uncertainty about whether a particular privacy regime would be deemed *adequate* or not. So far, the European Commission has acknowledged the adequacy of the level of protection offered in a limited number of countries only (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 jurisdictions are not considered to offer adequate data privacy protection.

Sweeping rules apply when personal customer or employee data gathered in Europe are transferred outside the EEA

However, EU privacy rules 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 are transferred; or (iii) the selling and potentially buying parties have entered into individually negotiated or ad hoc contracts. Alternatively, certain standard contractual clauses that have been approved by the European Commission (model contracts) may be used to legitimise the transfer. Still, there are some drawbacks to these exceptions when putting them to use.

Employee consent for the transfer of personal data outside the EEA is distinct from, for example, the consent required to disclose data to third parties within the EEA. Where consent is required to legitimize cross-border data transfers from Europe to third countries, opt-in or affirmative consent will almost always be required. Several European countries also call for the seller to tell its employees that their personal data will be transferred to a country that may not ensure adequate privacy. Since most data privacy authorities endorse the view that consent from employees is either suspect or invalid, it is a risky proposition for a seller to rely on even opt-in employee consent for transfers to potential buyers outside the EEA. In any event, sellers that prefer to rely on consent should always first examine whether the country from which the data are to be exported accepts employee consent as a valid basis for legitimizing such transfers.

The seller may choose to transfer employee information on the assumption that the transfer is necessary to enter into an agreement with a third party (outside the EEA) that ultimately will benefit the employee. So far, there has been no in-depth discussion in the EEA of what would be considered necessary in this context. The data privacy authorities in most EU countries appear to take a narrow view of what is necessary to enter into such an agreement. Consequently, they might question whether it is really necessary for potential buyers to export personal data to a country outside the EEA. In other words, they might argue that the review of such personal data may just as well take place in the EEA, or that the exchange of anonymized data instead would be equally effective.

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 the EEA. Ad hoc contracts generally provide that the transferred data must be processed consistently with EU data privacy rules and, in many instances, with the laws of the country from which the data are exported. In addition, most local data privacy authorities require that such contracts are approved by them before the anticipated data transfer. These approvals often take at least one or two months to obtain and might therefore be unsuitable in mergers and acquisitions deals that involve the transfer of personal data outside the EEA.

Since ad hoc contracts can be quite cumbersome to use, the European Commission adopted model contractual clauses for transfers of data to recipients outside the EEA. These model clauses do not require prior approval by local data privacy authorities. However, if a potential buyer in, for instance, the US elects to abide by the principles set out in the model clauses, it will have to adhere to higher standards than are normally expected under EU data privacy law. Moreover, the individuals whose data are transferred will become third party beneficiaries of the agreement and both the data exporter and data importer will be jointly and severally liable for damages. These and other onerous requirements make the model clauses perhaps 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 sometimes be difficult to abide by the strict letter of the law and still do business. However, at a minimum, (potential) parties to a merger or acquisition need to show that they have considered these issues, sought to minimize circulation of personal data and provided 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. ■

Wim Nauwelaerts is counsel at Hogan & Hartson in Brussels