Data privacy and cyber risk in M&As — are you prepared?

Davinia Brennan, Associate at A&L Goodbody, examines the data protection compliance issues that arise on Mergers & Acquisitions

The significant increase in merger and acquisition ('M&A') activity in 2014 is expected to continue this year. As M&As involve the disclosure of target-related information during evaluation of assets and liabilities, prior to the final merger or acquisition, it is vital that companies involved in these transactions comply with their data protection obligations. Information disclosed concerning a target company's employees or customers may constitute 'personal data' under the Data Protection Acts 1988 and 2003 ('DPAs').

In addition, target companies should be aware of the heightened cyber risk arising when conducting such transactions, due to the volume and nature of information that is shared between the parties — and that you are only as strong as your weakest link. Such information is particularly attractive to cyber criminals or competitors.

It is not scaremongering to point out that cyber risk needs to be treated as a high priority by company boards, as the consequences of this risk materialising are well-established, including, reputational damage; financial loss and loss of customers. The recent data security breaches at Target and Sony in the US show the potential for Board members to be held accountable for data security breaches, where they fail to provide effective oversight.

This article discusses the data privacy issues arising in relation to the disclosure of employee and customer data during the due diligence process, and the practical steps which organisations involved in M&As can take to ensure compliance with the DPAs, and to protect themselves from cyber risks.

Data privacy issues

M&As generally require, as part of the due diligence process, the disclosure by the target company, and the review by the prospective purchaser, and its advisers, of employee data. The difficulty with disclosing such information, via a data room or otherwise, is that the DPAs impose obligations in regard to the processing (e.g. disclosure) of personal data. 'Personal data' includes information such as the employees' names, addresses, dates of birth, and PPS numbers.

How can employee data be lawfully disclosed?

The Data Protection Commissioner, ('the DPC') has published guidance entitled: 'Transfer of Ownership of a Business' (copy available at www.pdp.ie/docs/10073). It recommends that, wherever practicable, employees should be informed if their records are to be disclosed to a prospective purchaser and, if the merger or acquisition proceeds, informed of the extent to which their records are to be transferred to the new employer. However, due to the secrecy surrounding negotiations in M&As, it would evidently not be desirable to inform employees of the disclosure of their personal data mid-deal.

Sellers have two key methods of lawfully disclosing personal data of employees to the prospective purchaser.

Consent through Data Privacy Policy: Pursuant to section 2A(1)(a), the seller may disclose the data where it has obtained its employees' consent to do so. In an ideal world, the seller's Data Protection Policy will provide that certain specifiable personal data may be disclosed to third parties during any potential sale process. If so, this will mean that employees should be aware of the possibility that their personal data may be disclosed to any prospective purchasers of the company. In his guidance note, the DPC approves of this approach. Organisations might further consider including a provision in their employee contracts providing for the transfer of employee data in the event of a merger or acquisition (although simply including this would not represent 'effective' consent, legitimising the processing).

Due to the difficulty in establishing that consent has been obtained in this way, organisations tend to rely on the alternative ground to justify the disclosure of personal data during the due diligence process (see below). One further practical problem is that clients often want to keep potential sales secret until the last moment, and so asking for employee consent is not appropriate.

Legitimate interests: Section 2A(1)(d) permits the disclosure of personal data where it is necessary for the purposes

(Continued on page 8)

(Continued from page 7)

of the legitimate business interests pursued by the data controller or by the third party to whom the data are disclosed, and it does not cause unwarranted prejudice to the fundamental rights and freedoms or interests of the employees. The transfer of personal data would, no doubt, be in the legitimate interests of both the seller and the prospective buyer in the context of a merger or acquisition. The DPC, in his guidance note, has also endorsed this ground to justify the disclosure of data.

What type of employee data may be disclosed?

The DPC recommends that, as far as practicable, all employee information to be put into a data room, or otherwise disclosed for review by a prospective purchaser, should first be anonymised. This would involve the redaction of personal information, such as employees' addresses, dates of birth, PPS numbers, and any other information such as might enable the relevant individual to be identified from the data provided.

Disclosure of 'sensitive personal data', such as employees' health data, racial or ethnic information, details of trade union membership is only permissible if further legitimate processing conditions set out in section 2B of the DPAs are satisfied. For example, medical or trade union information may be lawfully disclosed if an employee has explicitly agreed to such disclosure. However, the employer would need to show that such consent was freely given, which would be difficult in the context of the employer/employee relationship.

In his guidance note, the DPC has warned that disclosure of 'sensitive personal data' should not be necessary during the due diligence process and should be avoided. The DPC recommends that only anonymised aggregate data relating to absence levels (as opposed to sickness records of identifiable employees) should be disclosed to the prospective purchaser.

"The transfer of personal data would, no doubt, be in the legitimate interests of both the seller and the prospective buyer in the context of a merger or acquisition. The DPC, in his guidance note, has also endorsed this ground to justify the disclosure of data."

The Data Protection Principles

The Eight Data Protection Principles, contained in section 2(1) of the DPAs, reflect the key responsibilities of data controllers under the DPAs. To ensure compliance with these principles, the target company should seek formal assurances from the potential purchaser that any employee data disclosed during the acquisition process will be used solely for the evaluation of assets and liabilities; will be treated in confidence and will not be disclosed to other parties; will be kept safe and secure, and will be destroyed or returned after use. This might be achieved by requiring the prospective purchaser to execute a formal confidentiality or non-disclosure agreement, prior to granting access to the information via a data room or otherwise.

Transfer out of the EEA

When a merger or acquisition involves the transfer of employee data to a country outside the EEA, the target company should ensure that there is a proper basis for making the transfer. The DPC has published guidance on Transfers Abroad (copy available at: www.pdp.ie/docs/10074), which sets out when such transfers are legitimate. In the context of a merger or acquisition, the key means of lawfully transferring employee data outside of the EEA are by: obtaining employees' consent; ensuring the prospective purchaser, if located in the US, is a member of Safe Harbor regime, or through the use of the EU Commission's approved Model Clauses.

Retention of personal data after the sale

The seller may wish to retain some employee data after the sale, in order to deal with any liabilities that might arise. The DPAs allow the retention of such data, as long the seller has a justifiable need to keep the data, and only keeps it for as long as necessary. The seller should keep the information safe and secure from any unauthorised access, disclosure or losses, and should delete or destroy the data securely when it is no longer needed.

Disclosure of personal data after completion of the sale

Following the merger or acquisition, the unredacted personal information relating to the employees may be lawfully disclosed to the new employer or owner. Such further disclosure is permissible under the DPAs without obtaining the employees' consent, insofar as it is necessary for the purpose of the transfer and the legitimate business interests of the former and/or the new employer, as permitted by section 2A(1)(d) of the DPAs.

In addition, in the case of the transfer of a business (as opposed to a sale of shares) such disclosure is permitted under section 8(e) of the DPAs because it is required by law. The relevant law is section 21 of the Employees (Provision of Information and Consultation) Act 2006, which transposes into Irish law Article 3(2) of EU Council Directive 2001/23/EC on the safeguarding of employees in the event of transfers of businesses. It requires the transferor (original

employer) to provide to the transferee (new employer) information relating to the terms and conditions of employment of the staff being transferred. It applies to any information about which the original employer knows or ought to have known at the time of transfer. Failure by the original employer to fully and accurately disclose the relevant information may result in a cause of action for the new employer against the original employer for any loss which consequently arises.

The UK Transfer of Undertakings (Protection of Employment) Regulations 2006, as amended by the Collective Redundancies and Transfer of Undertakings (Protection of Employment) (Amendment) Regulations 2014 (TUPE), contains a similar disclosure obligation when a business is transferred to a new employer. However, it sets out the specific individual employee information which must be provided to the new employer, before the business transfer is completed. The Information Commissioner's Office in the UK has published guidance (www.pdp.ie/docs/10075) to help organisations comply with their data protection obligations when providing employee information.

The new employer should review the information in the personnel files they have acquired, and delete or destroy any unnecessary information.

Transferring customer personal data

It is likely that customer data may also need to be disclosed as part of a potential merger or acquisition. In his guidance note, the DPC warns that all customer data, insofar as they constitute 'personal data', should be anonymised prior to disclosure to a prospective buyer, as there is no basis in the DPAs for the release of such information as part of the consideration of a merger or acquisition process.

Following the completion of the sale, unredacted customer personal data may be disclosed to the new owner. However, the customer should be informed of their new service provider, and of the proposed transfer of their data before it occurs.

The DPC's investigation into the sale of Dublin City Council's waste management business to Greyhound Recycling and Recovery highlights the importance of notifying customers in advance of any transfer of their data, in order to meet the 'fair processing' requirements of the DPAs. Ideally, the seller's terms and conditions of service will contain a clause informing customers of the possibility of their personal data being transferred to any legal successors of the company in question.

Avoiding cyber risks

Whilst cyber security was once relegated to IT departments and security professionals, it is now recognised as a business risk which needs to be managed by company boards.

In January 2014, the Corporate Finance Faculty of the ICAEW and the UK government published guidance entitled 'Cyber-Security in Corporate Finance' (www.pdp.ie/docs/10076). The guidance looks at the six key phases of a corporate finance transaction: (1) preparation; (2) engaging, selecting and appointing external advisers; (3) initial approaches; (4) preparing information about the business; (5) financing terms of the transaction; and (6) completion. It provides useful questions, and practical steps that those involved can ask, and take, to protect themselves from cyber risks, during each phase of the transaction.

It also highlights that, whilst good cyber-security measures will go a long way to protecting sensitive and valuable information, they will not completely eradicate cyber-threats. For that reason, it is vital that companies have in place a data security breach incident management plan to reduce the impact of a breach and the time it takes to recover from it.

Top compliance tips

- Execute a formal confidentiality or non-disclosure agreement with prospective purchasers prior to giving them access to information via a data room or otherwise;
- Anonymise employee and customer data due to be put into a data room or otherwise disclosed for review by prospective purchasers;
- Do not disclose excessive information;
- Do not disclose sensitive personal employee data; and
- Ensure there is a proper legitimate basis for transferring personal data outside of the EEA.

Conclusion

It is vital that companies involved in M&As are aware of their data protection obligations when handling personal information, take all appropriate steps during the due diligence process to anonymise employee and customer data, and ensure that prospective purchasers are subject to appropriate contractual terms regarding confidentiality and security of the data disclosed.

Davinia Brennan
A&L Goodbody
dbrennan@algoodbody.com