Data protection

How to seal the deal

Ann Bevitt of **Morrison & Foerster (UK) LLP** examines the data protection issues facing both sellers and buyers during the course of a business or share sale.

Illustration: Getty Images

The recent introduction of fines of up to £500,000 for serious breaches of the Data Protection Act 1998 (DPA) means that organisations can no longer afford to overlook data protection considerations when acquiring or selling businesses (*see News brief "Data protection fines: how to avoid them", www.practicallaw.com/5-501-5230*). Data protection issues arise at all stages of a business or share sale, regardless of sector or size. This article considers these issues throughout a transaction's lifecycle, from both the seller's and buyer's perspectives, including:

- Advice to sellers on how to put a business into good data protection shape before embarking on the sale process, and to buyers on the data protection issues they should be considering before the sale process.
- The data protection issues that arise in due diligence for both sellers and buyers.
- The data protection issues which arise in connection with the sale agreement itself.
- Post-completion issues for both the seller and buyer (including handling the integration of the newly acquired data).

The article also considers recent enforcement activity by the Information Commissioner (the Commissioner), and the situations in which parties to M&A transactions are most vulnerable to potential fines for non-compliance.

PRE-DEAL PREPARATION

Almost all transactions will involve the transfer of personal data from seller to buyer (that is, data which relate to a living individual who can be identified from those data (or from those data and other information which is in the possession of, or is likely to come into the possession of, the data controller), including any expression of opinion about the individual and any indication of the intentions of the data controller or any other person in respect of the individual (*section 1(1), DPA*)) (*for background on data protection regulation, see feature article "Data protection: complying with the new regime", www.practicallaw.com/7-100-8493*).

This article first appeared in the November 2010 issue of PLC Magazine.

The types of personal data most commonly transferred are the seller's staff and customer data. At a very early stage, the seller should check that the business is in good enough shape in terms of data protection to ensure that the transaction can proceed smoothly. Reviewing data protection compliance at this stage should also allow sufficient time for any necessary remedial steps to be taken.

Notification compliance

Data controllers are required to notify the Commissioner that they are processing personal data other than for the purposes of: staff administration (including payroll); advertising, marketing and public relations (in connection with their own business activity); and accounts and records (*section 17, DPA; paragraphs 2-4 of the Schedule to the Data Protection (Notification and Notification Fees) Regulations 2000 (SI 2000/188)*). Notifications need to be renewed annually and the appropriate notification fee paid (*section 18(5), DPA*).

If the seller has notified the Commissioner, it should check that its notification is up to date; if it has not notified, it should check that it is only processing personal data for the purposes set out above, or that an exemption to notification applies (for example, where no processing is carried out on a computer, or where the sole purpose of the processing is the maintenance of a public register (*sections 17(2) and (4), DPA*)).

While data processors are not required to notify, it should be noted that an organisation can act as both a data controller and data processor in respect of different data. A data controller (either alone or jointly or in common with other persons) determines the purposes for which and the manner in which any personal data are processed. A data processor is a person (other than an employee of the data controller) who processes the data on behalf of the data controller (*section 1(1), DPA*).

Data protection principles compliance

The first, seventh and eighth principles are the key principles on which organisations will need to focus to ensure that their level of compliance is adequate in the context of a business or share sale. However, organisations should also be aware of the requirements of, and their obligations under, the other data protection principles (*see box "Data protection principles"*).

Fair and lawful processing. Under the first principle, personal data must be processed fairly and lawfully. In particular, an organisation must meet at least one of the conditions in Schedule 2 to the DPA (most likely that the individual has given his consent, or that the processing is necessary for the performance of a contract to which the individual is a party, or for the taking of steps at the request of the individual with a view to entering into a contract (*see box "Fair and lawful processing conditions"*).

In the case of sensitive personal data (*section 2, DPA*), the organisation must meet at least one of the conditions in Schedule 3 to the DPA (*see box "Fair and lawful processing conditions"*).

Most sellers will process both sensitive and non-sensitive data and should therefore ensure that they meet at least one of the conditions in the relevant schedule for each piece of data processed.

Organisations must comply with the fair processing code set out in Part II

Data protection principles

1. Personal data shall be processed fairly and lawfully and, in particular, shall not be processed unless:

- At least one of the conditions in Schedule 2 to the Data Protection Act 1998 (DPA) is met; and
- In the case of sensitive personal data, at least one of the conditions in Schedule 3 to the DPA is also met.

2. Personal data shall be obtained for one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes.
3. Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed.
4. Personal data shall be accurate and, where necessary, kept up to date.
5. Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes.
6. Personal data shall be processed in accordance with the rights of data subjects under the DPA.
7. Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, and damage to, personal data.
8. Personal data shall not be transferred to a country or territory outside the EEA unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.

(*Schedule 1, DPA*)

This article first appeared in the November 2010 issue of PLC Magazine.

Fair and lawful processing conditions

Schedule 2 conditions: personal data	Schedule 3 conditions: sensitive personal data
The data subject has consented to the processing of personal data.	The data subject has explicitly consented to the processing of the personal data.
The processing is necessary for the performance of a contract to which the data subject is a party.	The processing is necessary to exercise or perform any right or obligation conferred or imposed by law in connection with employment.
The processing is necessary for compliance with any legal obligation to which the controller is subject, other than an obligation imposed by contract.	The processing is necessary to protect the vital interests of the data subject (where their consent cannot reasonably be obtained) or of another person (where consent by the data subject has been unreasonably withheld).
The processing is necessary in order to protect the vital interests of the data subject.	The processing is carried out in the course of the legitimate activities of a not-for-profit organisation that exists for political, philosophical, religious or trade union purposes where the processing relates to a member or person in regular contact with the organisation.
The processing is necessary for the administration of justice or the exercise of functions of a public nature.	The data subject has deliberately made the personal data public.
The processing is necessary for the purposes of legitimate interests pursued by the data controller or the third party or parties to whom the data are disclosed, except where the processing is unwarranted in any particular case by reason of prejudice to the rights and freedoms or legitimate interests of the data subjects.	The processing is necessary in connection with legal proceedings, to obtain legal advice or to exercise legal rights.
The processing is carried out in circumstances specified in an order made by the Secretary of State.	The processing is necessary for the administration of justice or the exercise of functions of a public nature.
	The processing is necessary for medical purposes and is carried out by a health professional or someone owing an equivalent duty of confidentiality.
	Where the information relates to racial or ethnic origin, the processing is necessary to review equality of opportunity and is carried out with appropriate safeguards.
	The processing is carried out in circumstances specified in an order made by the Secretary of State.

of Schedule 1 to the DPA. Broadly, this code sets out the requirements for the fair obtaining of personal data and, in particular, the information that should be provided to individuals in relation to the intended processing.

Appropriate technical and organisational measures. To comply with the seventh principle, organisations must have in place appropriate technical and organisational measures to prevent the unauthorised or unlawful processing of data and to ensure against accidental loss or destruction of, or damage to, personal data.

Taking into account current technological developments and the cost of implementing security measures, organisations must ensure a level of security appropriate to the harm that might result from the unauthorised or unlawful processing of, and the accidental loss or destruction of, or damage to, data. Organisations must also take reasonable steps to ensure the reliability of employees who have access to the personal data.

The seller should therefore review the adequacy and appropriateness of its own technical and organisational security measures, taking into account the sensitivity and confidentiality of the data being processed, and the steps it has taken to ensure the reliability of its employees who handle personal data. The seller should also check that the business has written contracts in place with any data processors engaged by the business which address the requirements of the seventh principle regarding this relationship.

Transfer outside the EEA. The eighth principle states that personal data may not be transferred outside the EEA to countries that do not have an adequate level of protection for individuals in relation to

This article first appeared in the November 2010 issue of PLC Magazine.

the processing of personal data. The European Commission (the Commission) considers that few countries outside the EEA offer adequate protections with respect to the use of personal data.

A decision as to whether there is an adequate level of protection may be based on a finding of adequacy by the Commission, or after an assessment made by the organisation itself. The use of Commission-authorised standard model contracts will be sufficient to provide the adequate safeguards required by the DPA (*www.practicallaw.com/9-501-7717*).

There are a number of exemptions to the eighth principle, the most relevant of which, in the context of a business sale, are that the individual has given his or her consent to the transfer, or that the transfer is necessary for the conclusion or performance of a contract.

The seller will need to review what transfers of what personal data to which countries outside the EEA the business has made and to ensure that there is adequate protection for such transfers of data, or that an exemption applies (*see box "Transfer outside the EEA: exemptions"*).

Other general compliance

Individuals have certain rights in relation to their personal data, including the right to access their personal data (subject access requests) (*section 7, DPA*) and to require organisations to cease, or not to begin, processing their personal data, if such processing is likely to cause substantial and unwarranted damage or distress (*section 10, DPA*). Individuals can also obtain court orders for the rectification, blocking, erasure or destruction of data which are inaccurate (*section 14, DPA*). The seller should ensure that it has a process whereby individuals can access, check and correct their personal data and, if appropriate, have those data erased or destroyed, to allow individuals to exercise these rights.

Ability to sell the personal data

In order to be able to sell the personal data as part of the business or share sale, the seller will need to have given notice to individuals that their data may be sold to a third party at some point in the future, so that the sale complies with the fair processing code (*see "Data protection principles compliance" above*). Organisations can achieve this by, for example, including in the privacy policies on their customer-facing website, or in their fair processing notices to employees, a provision permitting, respectively, the transfer of their customer and employee data to a buyer.

Notifying individuals

To avoid having to notify individuals that their data are to be disclosed to potential buyers, organisations should anonymise data.

If sellers do disclose personal data, the first data protection principle requires them to notify individuals of the disclosure of their personal data. This may not be legally and/or commercially possible to do (for example, if insider trading restrictions apply).

Disclosures required by law are exempt from the first data protection principle (except the requirement to satisfy a Schedule 2 and/or 3 condition) (*section 35(1), DPA*). However, the exemption only applies to the extent to which giving notice would be inconsistent with the processing. Accordingly, unless giving notice would in some way prejudice or jeopardise the transaction, the seller should notify individuals of the disclosure of their personal data to potential buyers, unless it is not legally and/or commercially possible to do so.

Failing to notify individuals is a breach of the first data protection principle and technically punishable by a fine, although the circumstances in which such a breach will be likely to cause substantial damage or distress are limited (*see "Recent enforcement activity" below*).

TUPE. The issue of notification becomes a particular issue on a business sale, when there is a transfer of employees to the buyer. In such circumstances, the seller is required to provide the buyer with various detailed information on individuals and their employment terms (employee liability information) no later than 14 days before the transfer (*regulation 11, Transfer of Undertakings (Protection of Employment) Regulations 2006 (SI 2006/246)*) (TUPE 2006). As this is a legal requirement, it appears that the seller is not required to notify employees of the disclosure of their employee liability information, to the extent that this might prejudice or jeopardise the transaction.

On a share sale, as TUPE 2006 does not apply, there is no equivalent provision, so sellers should either anonymise data so as to avoid the need to notify individuals, or notify individuals of the disclosure of their personal data where it is both legally and commercially possible to do so.

Identifying data to be retained

If the seller is not selling all parts of a business, it may need to retain some data after the transaction is completed. It may also need to retain data to comply with its statutory record keeping obligations (for example, in respect of PAYE and statutory sick pay). As well as identifying which data need to be retained, the seller will also need to ensure that it can satisfy at least one of the conditions in Schedules 2 and/or 3 to the DPA in respect of such retention (*see box "Fair and lawful processing conditions"*).

Pre-deal preparation for the buyer

Early on, the buyer should try to identify potential data protection issues or areas of concern that may arise during the transaction. The main considerations for the buyer at this stage are likely to be:

- Identifying what data are required to carry on the business post-acquisition.
- How the buyer's proposed use of the data post-acquisition may differ from the seller's current use.
- Whether the business being acquired is "data heavy" and, more generally, what the significance of the data is to the transaction.

By addressing these issues at an early stage, the buyer will be in a better posi-

tion to deal with the due diligence process in a data protection-compliant way and also to negotiate the sale and purchase agreement. The buyer will also be able to identify what steps it may need to take post-completion to achieve an appropriate level of compliance.

DUE DILIGENCE

The due diligence process presents data protection challenges for both the seller and the buyer.

Due diligence issues for the seller

Wherever possible, data should be anonymised before disclosure in the due diligence process, or, at the very least, obvious identifiers such as names should be removed.

As some personal data are likely to be disclosed by the seller to the potential buyer(s) and their advisers and representatives during the due diligence process, the seller will need to consider how it will make the business's personal data available while complying with the data protection principles. As a minimum, the seller should:

- Make sure that those working on the deal are aware of their data protection responsibilities.
- Require all parties to whom data are to be disclosed to enter into confidentiality agreements and not use data for any purpose other than the transaction.
- Put in place appropriate practical safeguards to ensure the security of the data disclosed (for example, by using a data room).

If the seller uses a data room, it will need to control access to it and supervise its use. It should ensure that each user signs up to rules of use and that printing capabilities are limited or controlled.

To comply with the seventh principle, if the seller has used a third party data processor to set up its data room, it should ensure that the business has a written contract with that third party which requires the third party only to act on the seller's instructions and to put in place appropriate technical and organisational measures to prevent the unauthorised or unlawful processing of data and to ensure against accidental loss or destruction of, or damage to, personal data (*see "Data protection principles compliance" above*).

If personal data are being transferred outside the EEA then the seller will need to ensure that the host country has an adequate level of protection or that an exemption to the eighth principle applies (*see box "Transfer outside EEA: exemptions"*).

Due diligence issues for the buyer

Potential buyers should focus their requests for data on those data that they really need at this stage of the transaction. From a practical perspective, buyers should ensure that they treat data received from sellers in a way that allows them to return it easily if, for example, the acquisition does not go ahead, as they will no longer be able to satisfy a Schedule 2 and/or Schedule 3 condition

Transfer outside EEA: exemptions

The eighth data protection principle does not apply in certain limited circumstances. These include where:

- The data subject has consented to the transfer.
- The transfer is necessary:
  - for the performance of a contract between the data subject and the data controller or for the taking of steps, at the request of the data subject, with a view to entering into such a contract;
  - for the conclusion or performance of a contract between the data controller and a person other than the data subject which is entered into at the request of the data subject or is in the data subject's interests;
  - for reasons of substantial public interest;
  - for the purposes of, or in connection with, any legal proceedings, the obtaining of legal advice or establishing, exercising or defending legal rights; or
  - to protect the vital interests of the data subject.
- The transfer is part of the personal data on a public register and conditions applicable to the register are complied with.
- The transfer is made on terms of a kind approved by the Information Commissioner (the Commissioner).

(*Schedule 4, Data Protection Act 1998*)

Data controllers must consider whether the third country and the circumstances surrounding the transfer will ensure that an adequate level of protection will be given to personal data, and also whether the parties can put into place adequate safeguards to protect that data, before considering whether any of the derogations to the eighth principle apply (*"Data Protection Act 1998: The eighth data protection principle and international data transfers", Section A3 (www.ico.gov.uk)*).The Commissioner does not consider it good practice to rely on an exemption in order to avoid the requirements of the eighth data protection principle.

This article first appeared in the November 2010 issue of PLC Magazine.

in respect of their processing (that is, retention) of the data if the acquisition is not proceeding (*see "Data protection principles compliance" above*).

Due diligence questionnaire. To highlight any issues with the seller's level of data protection compliance, the buyer should request details of the following in the due diligence questionnaire:

- The notification (if any) to the Commissioner, or the reasons for not notifying.
- All inquiries, notices, complaints, proceedings and claims brought by individuals or the Commissioner within a limited period (for example, the last three years).
- Any outstanding subject access requests.
- Any data protection or associated policies (for example, document retention policy and website privacy policy).
- Fair processing notices issued to staff.
- The sources of personal data, and how personal data are obtained and used, both internally (for example, whether staff data are transferred to a head office outside the EEA for centralised HR services) and externally (for example, whether customer databases are created or held centrally).
- Copies of all material data processing or controller/processor agreements.
- The seller's approach to compliance (that is, which conditions it relies on in Schedules 2 and 3 to the DPA and on what adequacy mechanism or exemption it relies to process data and transfer them outside the EEA).

Receipt of personal data. If the seller discloses personal data to the buyer during the due diligence process, the buyer will be receiving and therefore itself processing the personal data disclosed by the seller. To avoid the buyer having to notify the seller's employees and customers of its processing of their personal data, the buyer should ensure that the data it receives from the seller is anonymised. If the buyer receives personal data disclosed by the seller, it is arguably required to give notice to those individuals whose personal data it is processing, unless it is not possible to do so (for example, if legal restrictions apply) (*see "Notifying individuals" above*).

SALE AND PURCHASE AGREEMENT

There are standard data protection warranties which buyers commonly seek from sellers, including that:

- The seller has complied with the data protection legislation (in all material respects).
- The seller has notified the Commissioner (if necessary) and paid any notification fee applicable up to completion.
- The notification is up to date and correct.
- There are no outstanding subject access requests.
- There are no outstanding inquiries, notices, complaints, proceedings or claims brought by individuals or the Commissioner; there have been no such inquiries, notices, complaints, proceedings or claims within a limited period (for example, the last three years); and the seller has no reasonable grounds for believing that an individual may bring a claim or that the Commissioner will take enforcement action.

Buyers should consider whether all of these warranties are appropriate for a particular sale.

If a seller is unable to give a particular warranty (for example, because there is an outstanding investigation by the Commissioner), it will have to make a specific disclosure against that warranty.

POST-COMPLETION

There are a number of issues to be considered post-completion, for both parties.

Issues for seller

After completion, the seller should focus on ensuring that its data processing continues to be compliant. The sale of part or all of a business may affect an organisation's notification(s) to the Commissioner, so these should be checked to ensure that they are up to date (for example, by deleting categories of data, purposes of processing and recipients of data which are no longer applicable). The seller should also check that it is not retaining legacy data which it no longer requires, as to do so would breach the fifth data protection principle (*see box "Data protection principles"*).

Where there are unsuccessful buyers (for example, in auction sales), the seller should also follow up with those potential buyers who were unsuccessful to ensure the return or secure disposal of personal data disclosed to them in the due diligence process.

Issues for buyer

The buyer will also need to check its notification(s) with the Commissioner as these may need updating post-completion to reflect the acquisition of the new business. If the buyer is planning further integration of the data obtained with the new business within its own organisation (for example, the merger of databases), its notifications may also require updating in light of these changes.

Any unnecessary data received from the seller should be deleted. The buyer should, for example, review the personnel files of the newly acquired staff and destroy any unnecessary information.

Data processing agreements between the seller and data processors which are relevant to the buyer's processing of data post-completion should be no-

vated to the buyer. If these agreements duplicate those which the buyer already has in place, the buyer may need to consolidate its arrangements with suppliers. This process may offer the buyer a chance to review the level of its compliance when contracting with data processors generally.

Finally, buyers may wish to take advantage of the opportunity the post-completion period presents to undertake an audit of data processing compliance generally within the newly acquired business.

Five ways to avoid a fine

Organisations contemplating an M&A transaction should:

- Have policies and procedures in place which deal with both the appropriate handling of personal data in a transactional setting and what to do when a problem arises.
- Conduct a risk assessment to identify the risks associated with the processing of personal data in the context of each transaction.
- Focus on those risks involving sensitive personal data and/or the personal data of large numbers of individuals, where the risk of substantial damage or distress is greater.
- Not turn a blind eye to problems: if they become aware of an issue, they should act quickly to put it right.
- Learn from past mistakes and past transactions to improve their data protection practices.

RECENT ENFORCEMENT ACTIVITY

Since 6 April 2010, the Commissioner has had the ability to impose monetary penalties of up to £500,000 where he is satisfied that there has been a breach of any of the DPA's principles which is: serious; of a kind likely to cause substantial damage or distress, either deliberate or reckless; and no reasonable steps are taken to prevent the contravention.

The Commissioner has issued guidance about the issue of monetary penalties (the guidance) (*Information Commissioner's guidance about the issue of monetary penalties prepared and issued under section 55C (1) of the Data Protection Act 1998; www.ico.gov.uk/upload/documents/library/data_protection/detailed_specialist_guides/ico_guidance_monetary_penalties.pdf*).

The guidance is helpful in giving organisations an idea about how the Commissioner will exercise his power. It deals, among other things, with the circumstances in which a breach should be regarded as serious; how bad damage or distress has to be to be characterised as substantial; and in what circumstances breaches should be regarded as deliberate or reckless.

The Commissioner's approach

The guidance lists a number of factors, the presence of one or more of which will make the imposition of a monetary penalty more likely.

Where an organisation has expressly, and without reasonable cause, refused to submit to an audit which could reasonably have been expected to reveal a risk of the contravention, a fine is more likely. Accordingly, the Commissioner is using the threat of a fine to persuade organisations in the private sector to submit to voluntary audits of their data protection compliance, in lieu of a power to audit such organisations compulsorily.

The guidance also lists a number of factors, the presence of one or more of which will make the imposition of a monetary penalty less likely. There is also an amnesty if the Commissioner discovers a breach through a voluntary audit; in this case, he will not impose a monetary penalty.

If an organisation is reckless because it knew or ought to have known about the contravention, it can still escape a fine if it took reasonable steps to prevent the contravention. The guidance provides examples of where the Commissioner is more likely to find that a data controller has taken reasonable steps (for example, risk assessments, good governance/audit arrangements). However, although an organisation may in this way avoid a fine, there may still be reputational damage to the business as a result of data breaches which result in public censure and negative publicity and these could themselves have a direct impact on the value of a business.

How much?

Once it has been decided that a monetary penalty should be imposed, a number of issues are likely to be relevant to the Commissioner's decision as to what would be an appropriate monetary penalty in a particular case, including the nature of the contravention, its effect, the organisation's behavioural issues, the impact of the monetary penalty on the organisation, and the Commissioner's aim to eliminate any financial gain or benefit obtained by the organisation from non-compliance. Again, no indication is given of the weight that will be attached to a particular factor in any given case.

Areas of risk in M&A transactions

The new power to fine is a significant change in the UK's data protection regime, giving "teeth" to something that was seen as relatively "toothless". Organisations will be very keen to see how the Commissioner flexes his new muscles in the coming months. Until the Commissioner actually imposes such a fine, it is very difficult to assess the adequacy of the power.

This article first appeared in the November 2010 issue of PLC Magazine.

Related information

Links from www.practicallaw.com
This article is at www.practicallaw.com/4-503-6370

Topics

Data protection	www.practicallaw.com/8-103-1271
Acquisitions: private (assets)	www.practicallaw.com/5-103-1079
Acquisitions: private (shares)	www.practicallaw.com/1-103-1081

Practice notes

Overview of UK data protection regime	www.practicallaw.com/7-107-4765
Data protection issues on commercial transactions	www.practicallaw.com/5-200-2146
Selling a database	www.practicallaw.com/2-107-4763
Cross-border transfers of personal data	www.practicallaw.com/0-201-5764
Employer obligations under the Data Protection Act 1998	www.practicallaw.com/3-200-2213

Previous articles

Data protection fines: how to avoid them (2010)	www.practicallaw.com/5-501-5230
Data protection: impact on commercial transactions (2003)	www.practicallaw.com/9-102-3685
Data protection: complying with the new regime (1998)	www.practicallaw.com/7-100-8493

Web links

Information Commissioner's Office	www.ico.gov.uk

For subscription enquiries to PLC web materials please call +44 207 202 1200

In the meantime, given the Commissioner's collaborative approach, it seems unlikely that inadvertent or even careless breaches will result in fines. Rather, there will need to be a deliberate and wilful wrongdoing for a fine to be imposed. This suggests that the "reckless" element of the "knowingly or recklessly" pre-condition for a fine will not be the focus of the Commissioner's enforcement activity. It is also likely that organisations with a poor record of compliance are likely to be the first to receive fines under the new power.

In the context of M&A transactions, this means that organisations with a poor record of compliance in other areas may be at greater risk of being fined if there are errors in their handling of data during a transaction. To reduce this risk, organisations should ensure that they pay due attention to data protection issues throughout a transaction's lifecycle, but particularly when data are disclosed during the due diligence process and on completion, as these stages of a transaction pose the greatest risk of data loss and potential fine (*see box "Five ways to avoid a fine"*).

Ann Bevitt is a partner at Morrison & Foerster (UK) LLP.

This article first appeared in the November 2010 issue of PLC Magazine.