Bloomberg BNA

WORLD DATA PROTECTION REPORT >>>

News and analysis of data protection developments around the world.
For the latest updates, visit www.bna.com

International Information for International Business

VOLUME 16, NUMBER 12 >>> DECEMBER 2016

Things That Go Bump in the Night: Confronting Data Protection Monsters in the M&A Closet

By Emma Flett and Jennifer Wilson

The revelations of the data security breach affecting at least 500 million Yahoo! Inc. user accounts at an advanced stage of a proposed billion-dollar acquisition of the company by Verizon Communications Inc. is the stuff of every dealmaker's nightmares. The breach, which has been brandished by tabloids across the world as a "mega-breach" and the "biggest hack in history," is reportedly expected to result in substantial delays to deal closing, painstaking investigations and a reduced purchase price. The situation has recently been compounded with Yahoo's Dec. 14 disclosure of another record-breaking breach of more than one billion user accounts that occurred in Aug. 2013.

Emma Flett is an intellectual property partner in Kirkland & Ellis International LLP in London. She can be reached at emma.flett@kirkland.com.

Jennifer Wilson is an associate at Kirkland & Ellis in London. She can be reached at jennifer.f.wilson@kirkland.com.

The Verizon/ Yahoo deal is not the first merger and acquisition (M&A) transaction to hit the headlines from a data protection perspective, however. In the lead up to the acquisition of WhatsApp Inc. by Facebook Inc. in 2014, the proposed use and transfer of WhatsApp's user data to Facebook for targeted advertising and other purposes was publicly scrutinised by the U.S. Federal Trade Commission. Two years later, Facebook's processing of user data obtained from its WhatsApp messaging service has found itself back in the spotlight.

Nought may endure but mutability!

While the Verizon/ Yahoo and Facebook/ WhatsApp acquisitions have perhaps thrust data protection into the public spotlight of M&A activity, privacy concerns are not (and should not be) limited to high profile deals involving the world's digital and telecommunication giants. In a world awash with more personal information than ever before, data has become "the new oil" and a

key business asset for almost all companies, even in respect of those viewed as traditional "brick & mortar" businesses. New technologies and business models have led to data collection and analysis becoming an almost ubiquitous business practice, viewed as essential to the heartbeat of a business in maintaining its competitive edge. Coupled with this brave new information age in which we live, the elevation of data protection compliance as a board level issue (particularly in light of moves by European governments to introduce personal liability for directors in respect of cybersecurity breaches); growing customer awareness and expectations regarding the ways in which businesses treat (and mistreat) their personal data; and the advent of anti-trust type fines for data protection compliance under the new General Data Protection Regulations (GDPR) in the EU from May 25, 2018, are all factors contributing towards data protection becoming an increasingly important item in the long list of items to be considered as part of any business sale or acquisition.

Despite this shift in focus, data protection issues are often neglected by sellers, buyers and their advisors during the M&A process, and key compliance issues may not be identified until well into the transaction (or in some cases, not at all). Consider for example, the announcement by tour-booking and review site Viator Inc. in 2014 that it had been the victim of a data breach affecting an estimated 1.4 million customers, only two weeks after online travel site TripAdvisor Inc. had acquired the company for over $200 million. At best, failure adequately to address these issues at an early stage in the process can result in a last minute dash to find a compliance solution at a critical moment in the transaction. However, where a target's data forms one of its key assets, a critical or systematic failure to comply with applicable data protection laws may mean that the entire business model on which a transaction is premised is not viable. Targeted due diligence may therefore reveal issues that go directly to deal value and in some cases, deal feasibility.

In short, data protection issues can no longer be afterthoughts in the process of selling or acquiring a business and pre-transaction planning is critical. How then can parties to an M&A transaction ward off data protection monsters and uncover compliance skeletons in the closet?

A gripping tale of . . . preparation, preparation, preparation.

Like a terrifying character in any hair-raising horror film, data protection considerations can creep up on unsuspecting parties at any stage of a transaction. However, parties to a deal should prepare in advance for these issues to be addressed at three key touch points so as not to be caught unawares:

- during the initial engagement, evaluation and pre-deal planning process;
- during the due diligence process and negotiation of transaction documents; and
- on completion of the transaction, during any information technology (IT) integration or transfer of personal information to the buyer.

In addition to identifying potential data protection risks and liabilities during due diligence into a target's trading activities and operations, data protection compliance issues exist as a result of the mere performance of due diligence itself. As almost all M&A deals will involve the exchange of personal data between parties (often with a cross-border aspect), these issues should be considered in the early planning stages of any transaction. This article will address both compliance during the M&A process itself, and the key considerations for sellers and buyers in tackling potential data protection nasties in respect of the target's activities prior to and following the transaction.

Privacy concerns are not (and should not be) limited to high profile deals involving the world's digital and telecommunication giants.

Lurking in the shadows: the initial engagement, evaluation and pre-deal planning process.

In light of the lessons learnt from others' M&A data protection horror stories, savvy sellers should invest ahead of any transaction to make sure their house is in order from a compliance perspective. In terms of compliance with the U.K. Data Protection Act 1998 (DPA), this will involve ensuring that the seller is compliant with the eight core data protection principles enshrined in the DPA. In particular, sellers should ensure any personal data held by the company is adequate, relevant to the purposes for which it has been collected and not excessive for those purposes, and that it is not being kept for longer than necessary for those purposes. Prior to completion, a seller should audit the personal data it holds and assess compliance with the principles of the DPA. In particular, at a basic level, consideration should be given to the following:

- When was consent obtained to the processing of the personal data involved and how was consent provided?
- Was the fair processing information provided to the individual data subjects clear and intelligible? How was it provided?
- Which entity or entities within the seller's group control the personal data vis-à-vis those group entities or third parties that simply process the personal data? Under the DPA, the data controller is the person or entity who determines the purposes for which, and the manner in which, any personal data are processed. A data processor, on the other hand, is any person or entity who processes personal data on behalf of and under the instructions of the data controller. In this context, it's worth noting that personal

data may at any one time be processed by a wide number of different data controllers or data processors.

- To the extent that the seller acts as a data controller, have appropriate notifications been made to the Information Commissioner's Office (ICO) in the U.K., and/or other data protection authorities in the relevant Member States in which the data controller operates?

- Is the personal data held by the seller, adequate, relevant and not excessive in relation to the purposes for which it is processed by the seller? Is the relevant data accurate, and where necessary, kept up to date? Consideration should be given as to the purposes for which personal data is retained by the seller. If retaining this information is unnecessary for the purpose for which it was originally collected (e.g. to fulfil a one off order by a customer), then the seller should consider deleting this data prior to completion of the transaction.

- Does the seller have up-to-date privacy policies in place that accurately reflect the nature of its data processing activities? Are the commitments made to data subjects in these policies complied with in practice?

Before engaging with a target, potential buyers should factor data protection and data security considerations into their overall deal strategy given that these can impact on a target's business objectives, regulatory profile and overall valuation. Some key strategic issues to consider include:

- Will there be any changes in the way the target collects, uses, stores, discloses and protects both customer and employee personal data, in accordance with the buyer's strategic plans for the business?

- As a result of the target's public-facing privacy and data-sharing commitments, will customer consents need to be sought post-completion to amend the privacy policies? Will personal data acquired through the target under existing privacy policies and fair processing notices need to be kept separate to avoid any uses of the data post-completion in contradiction with these commitments?

- Does the target's current product and service offering mirror the buyer's plans for the future of the business, or does the buyer envisage offering new products and services, or adopting new technologies or platforms (e.g., payment processing platforms) which could impact on the target's privacy profile and compliance requirements? Will privacy impact assessments and amendments to the target's privacy policies, procedures or privacy-by-design efforts be necessary to support these new products, services and/or technologies?

- Does the acquirer intend to expand the business into any new markets of relevance from a data protection perspective? In particular, does the acquirer intend to enter into any highly regulated sectors (e.g., health care or financial services)? Post-completion of the deal, does the acquirer anticipate expanding the business into any new countries, and if so, what impact could this have on the target's regulatory profile?

- If the buyer intends to expand the business in terms of its current product and service offering, customer demographic or geographical reach etc., will any customer profiling, market research or direct marketing campaigns be required to support and measure the success of this expansion? If so, what are the implications in terms of compliance with the relevant data protection and direct marketing requirements?

Other basic preparatory considerations that should be made by acquirers early on in an M&A process, even before formal due diligence begins, include:

- identifying the volume and nature of personal data (belonging to customers, suppliers or vendors, employees and others) held by the target;

- evaluating what information is required to carry on the business of the target post-acquisition;

- considering if and how the buyer's proposed use of the personal data differs from the seller's current use; and

- determining whether the target is reliant on or stores any sensitive personal data, regulated data or other notable categories of personal data (e.g., data relating to children). Under the DPA, sensitive personal data consists of information about a data subject's racial or ethnic origin, political opinions, religious or similar beliefs, trade union membership, physical or mental health or condition, sexual life, or commission of or proceedings for any offence committed or alleged to have been committed by the data subject. It is also worth considering the extent to which the target processes any of the new "special categories of personal data" due to be introduced under the GDPR (namely, genetic data and biometric data, where processed to uniquely identify a person). To the extent the target holds large volumes of sensitive personal data; the buyer will want to quickly establish which of the conditions for processing sensitive personal data the target is relying on.

If personal data contained in disclosures cannot be anonymised, parties may need to adopt a risk-based approach.

Given the strategic importance of many of these issues, parties on both the sell and buy side should review the target's privacy policies and applicable laws to determine what personal data can be shared by the target during the due diligence process and any notable restrictions on transfers of personal data that could impact on the transaction (discussed further below) at an early stage in the evaluation of a potential merger or acquisition.

In the spotlight: investigating and addressing potential data protection issues.

As discussed above, transfers of personal data between potential acquirers and sellers are almost inevitable during the disclosure and due diligence stages of an M&A transaction. Under the DPA, a seller acting as a data controller in respect of any personal data is required to notify the relevant data subjects of the disclosure of their personal data to any third party, including a prospective acquirer of the business. In some circumstances the consent given by the data subject at the time of data collection (e.g. in an employment contract or privacy policy) may contemplate and cover onward transfer of personal data in a sale context. In most circumstances, however, notifying the relevant data subjects is likely to be commercially undesirable given that the parties will be taking significant efforts to keep knowledge of the proposed deal to a limited group of individuals.

Anonymisation

One way of avoiding having to provide fair processing notifications at this stage would be to fully anonymise any personal data included in the information to be disclosed to the prospective buyer and its advisors so that it falls outside the scope of the DPA. In reality, effective anonymisation of all personal data contained in due diligence disclosures may be impracticable. Alternatively, sellers should consider holding back all personal data during due diligence until a later stage in the transaction (for example, once exclusivity with one potential acquirer has been granted, thereby limiting the number of potential recipients of the personal information).

A risk-based approach

If personal data contained in disclosures cannot be anonymised, parties may need to adopt a risk-based approach, which weighs up the need for disclosure against the commercial and legal risks (based on the volume and sensitivity of personal data involved). In any case, where disclosures of personal data (as opposed to sensitive personal data—see further below) are unavoidable, sellers should seek to minimise the volume of personal data provided to prospective acquirers as far as possible and limit disclosures to those that are absolutely necessary to the due diligence exercise or transaction as a whole. In addition, the risk of onward disclosure of personal data should be reduced by requiring prospective buyers to enter into non-disclosure agreements including confidentiality undertakings that ensure the personal data will only be used to evaluate the assets and liabilities of the business and will be returned to the sellers and/ or adequately deleted should the merger or acquisition not go ahead.

It may also be necessary to include restrictions in such non-disclosure agreements on the potential buyer and its advisers from transferring personal data outside the EEA, or if such cross-border transfers are necessary (for example, where a buyer based outside the EU is considering an EU target), only allow such transfers if certain conditions are met (such as entry into standard contractual clauses). In most M&A deals, non-disclosure agreements will be entered into prior to the due diligence exercise. However, parties should be alert to any likely disclosures of personal data that may be made prior to the formal due diligence process, and back-date the effective date of non-disclosure agreements as appropriate to protect such information. From a practical standpoint: access to personal data should be in a secure environment; electronic transmissions of data should be encrypted; third-party hosts of data should be carefully vetted; and those given access should accept the confidentiality and purpose-limitation undertakings mentioned above as a strict condition of access.

Categories of data

In terms of particular categories of data which may be relevant to a disclosure exercise:

- It is recommended that all customer and supplier data, where it constitutes personal data (e.g., personal contact details) or sensitive personal data, is anonymised prior to disclosure to a prospective purchaser as there is no basis in the DPA for the release of such information as part of the consideration of a merger or acquisition process (absent individuals' express consent). Again, a risk-based approach can be taken dependent on the volume and sensitivity of personal data. For more information, see below under "Facing the nightmare: assessing the risk of non-compliance."

- Disclosure of sensitive personal data (e.g. medical conditions of identifiable customers, sickness and attendance records relating to employees, race and ethnicity of individuals—see defined terms below) will invariably require a data subject's explicit consent and should be avoided. Generally, such disclosures should not be necessary in the context of due diligence exercises. As an alternative, the seller may disclose aggregated data from which the individuals cannot be identified (e.g. the number of customers with a particular condition, or employee absence levels).

- As regards employee personal data, the Transfer of Undertakings (Protection of Employment) Regulations 2006 will require a seller to provide the buyer with certain information about transferring employees, including their identity prior to completion of the transaction. Any such information will be provided under a legal obligation and does not therefore need to be anonymised to comply with the DPA. However, any additional information on employees will not need to be provided by the seller under a legal obligation and should therefore be anonymised as far as possible prior to disclosure.

Tailored due diligence

In terms of the assessment of a target's data protection compliance and information security profile, due diligence should be tailored as far as possible to the company's trading activities and operations. In the digital age and particularly in light of the overreaching principle of "accountability" underpinning many of the provisions of the GDPR, simply reviewing privacy policies and data protection provisions in employee contracts etc. in a vacuum is no longer adequate.

Transactional lawyers advising a target's risk profile from a data protection perspective should adopt a holistic approach which not only assesses how that company gathers, uses, stores, protects and destroys personal data according to the black letter of its general information governance policies and contracts, but also whether these procedures are followed in practice. To do so, as well as requesting the target's privacy policies and internal guidelines for use of personal data, it is also worth asking management of the target (or, even better, the target's data protection officer if it has one) to provide:

- A "map" of the target's data flows, outlining where and how it collects and stores personal data and any related security controls in place in respect of the platforms and systems used to collect and store data. This information will be key to building a solid understanding of where the target's personal data is stored, how it is governed, who has access to it and actual or potential issues around security of the personal data. Digging into the target's security framework for how data is collected and stored may quickly unearth red flags in the early stages of the deal (e.g., if no or scarce security controls exist).

- Copies of the target's employment agreements, employee handbooks and contracts with customers (in so far as these contain information on data protection and fair processing notices, and consents to processing of personal data). Data protection provisions in agreements with data processors appointed by the target should also be reviewed.

- Copies of documentation and policies relating to how the target handles data subject access requests, data breach management, information governance and the retention, encryption and destruction of personal data.

- Documentation on security audits and privacy impact assessments carried out by the target. Unsurprisingly, audit and privacy impact assessments are due diligence gold and could provide the ultimate key to discovering a target's compliance skeletons in the closet.

- Documentation on physical security guidelines and access guidelines to offices, data centres, computer rooms and servers.

- Security checks and controls related to hiring employees, including whether background checks are carried out. A company's data security is only as strong as its weakest link. Heed the horror stories of corporate espionage, in which a business hires an "ex" employee of a competitor who, weeks after joining, mysteriously walks out of the building with the business' crown jewels in terms of its commercially sensitive information and trade secrets. From a data protection perspective, it is important to understand what controls (if any) are in place when it comes to access by employees to critical data systems and repositories. A company that allows employees of all levels to access freely its stores of personal data, without any data separation or ring-fencing of particular categories of personal data, suggests lax information governance and data security practices.

- A "team sheet" of the individuals responsible for data protection compliance and information security within the target, and confirmation as to how well these individuals are resourced for the task at hand. In this respect, it is worth noting that the GDPR will require that dedicated data protection officers are appointed by all public authorities, as well as by organisations (regardless of whether they are data controllers or processors) where the core activities involve "regular and systematic monitoring of data subjects on a large scale" or where the entity conducts large-scale processing of "special categories of personal data" (such as that revealing racial or ethnic origin, political opinions, religious or philosophical beliefs). While the GDPR does not establish the precise credentials data protection officers must have, it does require that they have "expert knowledge of data protection law and practices." As such, the resourcing and level of expertise of an organisation's data protection officer is likely to become a useful indicator of a target's compliance profile under the GDPR.

- As an obvious point, information relating to the target's risk profile, including regarding any historic data breaches (actual or attempted), as well as data subject complaints or investigations by the ICO (in respect of companies based in the U.K.) or any other data protection authorities should be requested.

- An increasingly important road map for buyers will be the target's IT business continuity plan, and information as to testing or implementation of this plan in practice. This information should point to the key risks and details of the target's IT system, and may even serve as a useful signpost for potential issues to be confronted post-acquisition in terms of the integration of the buyer and seller's IT systems.

- Beyond a thorough review of the target's privacy policies, inquisitive buyers may also consider (anonymously) signing up online to newsletters or other communications from the seller to test the extent to which its privacy commitments to customers are honoured in practice. An influx of spam from unrelated third parties as a result of doing so, may suggest a target is sharing personal data with third parties (which may or may not be detailed in its privacy policy).

The overreaching objective in requesting the above information and documentation should be to paint a detailed picture of the overall data protection health and well-being of the target. Of course, there is no magic wand to this type of due diligence and the questions asked and documentation requested should be tailored to the nature of the target's business and industry sector, as well as the buyer's strategic plans for the business (as discussed above). In addition, the level of diligence carried out may be dictated by a number of factors (including the risk tolerance of the buyer and time constraints around the speed at which the deal is to occur). Arguably, limitations in the depth of due diligence resulting in spooky data protection "unknowns" should

translate into more fulsome representations and warranties in the deal documents. On the other hand, unearthing compliance issues though detailed data protection due diligence is also likely to lead to stringent and robust data protection provisions and pre or post-completion undertakings from the seller in the transaction agreements.

Either way, the findings of the seller's data protection due diligence will significantly inform the representations, warranties and indemnities sought from the seller in the deal documentation. By way of example, sellers should be asked to warrant that the target has: (i) provided adequate notice and obtained any necessary consents from data subjects required for the processing of personal data; (ii) abided by any privacy choices (including opt-out preferences) of data subjects relating to personal data; (iii) adopted appropriate technical, physical and organisational measures and security systems and protocols designed to protect personal data against accidental disclosure or unlawful access; (iv) put in place written agreements with all data processors which comply with data protection laws and the target's own privacy policies; and (v) not experienced any breach, security incident, or violation of data protection laws, or of its own privacy policies in relation to personal data.

Data protection considerations in merger and acquisition deals do not end with the signing of transaction documents.

The buyer may also want to seek indemnities in respect of any breaches of data protection laws, on a general basis or in relation to specific concerns identified through its due diligence. In negotiating the survival period of these provisions, a buyer should consider the length of time required to fully integrate the IT systems of the target and secure the target's network following completion, as well as any limitation periods for data protection related claims and investigations.

Address red flags without delay

Notwithstanding the need for carefully crafted representations and warranties in the deal documentation, at a practical level, significant data protection red-flags uncovered by due diligence should be addressed without delay. If the risks or vulnerabilities in the target's IT security framework are significant, or key personal data is tarnished in a material way or cannot be transferred to the buyer, the value of the target may be affected and a renegotiated purchase price may be appropriate. Alternatively, if data protection or security issues can't feasibly be resolved prior to completion, buyers may need to consider how best to apportion financial risk with the seller, for example, by requiring an escrow account to hold back part of the purchase price to address potential post-closing liabilities. As the sellers are unlikely to be in a position to assess these liabilities post-completion, this is likely to entail detailed provisions being negotiated as to the mechanisms around this hold-back. At a more prescriptive level, buyers may ask that the target takes specific remedial steps prior to completion, such as amendments to its privacy policies and fair processing notices, the implementation of certain security measures (such as encryption or more regular back-ups of data), or the tightening-up of data protection provisions in the target's agreements with data processors.

The aftermath: avoiding post-completion data protection fallout.

Data protection considerations in M&A deals do not end with the signing of transaction documents. While (or, most likely, before) celebratory champagne corks are popped, data protection practitioners must ensure that any transfers of personal data as a result of the transaction are compliant with data protection law. The position will differ depending on whether the transaction is an asset or share sale. On a share acquisition, as there will be no actual asset transfer other than relating to the shares in the target company, the identity of the data controller will not change on completion. As a result, fair processing information does not need to be given to the relevant data subjects, unless the acquirer proposes to use their personal data for a new purpose. From a reputational and customer service perspective, however, acquirers may wish to notify data subjects that their data has "changed hands." This is likely to be the case where, for example, the identity of the target as a member of a particular group was an important basis on which the data subjects originally entrusted the target with their personal data.

In an asset sale, the transfer of personal data on completion of a business sale will amount to processing. As both parties are effectively acting as data controller at the point of transfer, both parties will be under a duty to inform the data subjects that their personal data is transferring to a new data controller. In practice, it is seen as adequate for one of the parties to provide this notification. For practical reasons and as the seller will no longer be the data controller of that data post-transfer, it is more common for the buyer to notify the data subjects on behalf of both parties. As a result, contractual assurances to the effect that the buyer will provide appropriate "fair processing information" to the relevant data subjects are often contained in the deal documentation. Data subjects' express consent will need to be obtained by the buyer (in both an asset and share sale) before it is able to use the personal data acquired as result of the transaction for any new purposes not already detailed in the target's privacy policies and customer agreements.

To the extent that the data being transferred in an asset sale is sensitive personal data then, under the black letter of the DPA, the seller or original data controller must obtain the express consent of the relevant data subjects before the sensitive personal data can be transferred to the buyer, unless one of the alternative (and very narrow) bases for processing sensitive personal data set out in Schedule 3 of the DPA is present.

In respect of employee sensitive personal data, this may include the fact that the transfer is necessary for the per-

formance of the outgoing data controller's obligations under employment law (including in compliance with the Transfer of Undertakings regulations (TUPE)). Beyond employee data, however, it is difficult to think of an asset sale satisfying any of the other conditions set out in Schedule 3 of the DPA. Where obtaining express consent to the transfer of any other categories of sensitive personal data is not feasible, sellers and acquirers may therefore find themselves in a compliance conundrum on the point of transferring such data as part of an asset sale. Given the nature of sensitive personal data, a careful assessment of the likely impact on the relevant data subjects should be carried out. Any transfers of sensitive personal data likely to cause the data subject damage or distress should be avoided at all costs. Where consent to the transfer of sensitive personal data cannot be obtained, to the extent that such transfers are highly unlikely to cause damage or distress to the relevant individuals, parties may be forced to adopt a risk based approach (discussed below).

Facing the nightmare: assessing the risk of non-compliance.

As discussed above, at certain stages during the M&A process, parties may be backed against a wall from a data protection compliance perspective and may need to weigh up the enforcement and reputational risks of non-compliance vis-à-vis the commercial risk of not proceeding with the transaction. Currently, the enforcement risks in the U.K. are as follows:

- While breach of a principle of the DPA is not in itself a criminal offence, the ICO has the power to issue an enforcement notice, which will require the data controller to comply with the relevant principle, or cease the non-compliant processing, within a specified period. Failure to comply with such a notice is a criminal offence.

- A data controller may also face a fine (a monetary penalty notice) as well as civil proceedings if there has been a serious breach of the data protection principles. The ICO has the power to impose financial penalties of up to 500,000 pounds ($620,610) for a serious contravention of the data protection principles, where the contravention was of a kind likely to cause substantial damage or substantial distress. In an asset sale, where sensitive personal data is disclosed or transferred to the buyer, the failure to comply with the requirement to obtain a data subject's explicit consent to the transfer of such data to a new data controller, is likely in itself to be viewed as causing damage or distress to the data subject.

Beyond the criminal and civil sanctions attached to contraventions of data protection laws, sellers and buyers alike should be aware of the adverse reputational impact a breach of data protection law during the M&A process or transfer of customers or employees' personal data may have on the ongoing business. In addition, recent examples of regulatory bodies more closely scrutinising data protection issues in M&A transactions, coupled with the introduction under the GDPR of fines for non-compliance of up to 4 percent of annual worldwide turnover of the preceding financial year or 20 million euros ($20.8 million) (whichever is the greater), are likely to focus attention on data protection requirements during the M&A process, and raise the stakes in terms of carrying out thorough due diligence. We expect to see interesting developments in this area of M&A process in the next few years.

Sweet dreams. . . .

In an era where personal data has become the lifeblood of many businesses, a company's observance of data protection laws can go to the value of the business to a potential buyer. As recent headline grabbing horror stories have demonstrated, buyers cannot afford to be kept in the dark with regards any data protection nasties. There is no longer an excuse for data protection due diligence to be overlooked or inadequately tailored to a target's risk profile. Data protection issues should be carefully considered, planned for and handled at the outset and throughout the M&A process. Strategic issues with data protection at their core can creep up at various stages of a deal, including during the development of an acquisition or approach strategy at the genesis of a deal, through to the integration and transition strategy post-completion. Data protection issues don't vanish on completion, and wary buyers should continue to assess and review progress in meeting data protection compliance requirements and audits following signing of the deal lest they continue to be haunted by compliance ghosts of the past.