ESTABLISHED 1987

UNITED KINGDOM REPORT

PRIVACY LAWS & BUSINESS
DATA PROTECTION & PRIVACY INFORMATION WORLDWIDE

Disclosure of personal data in M&A due diligence phase

Data protection laws play a role in most mergers and acquisitions transactions because all companies process personal data.
By **Lore Leitner** and **Elli Laine** of Wilson Sonsini Goodrich & Rosati.

For a long time, data protection issues have been overlooked in mergers and acquisitions (M&A) transactions due to a general lack of awareness around privacy issues combined with limited enforcement. However, with the introduction of the General Data Protection Regulation (GDPR) in May 2018, the data protection rules are now enhanced by stronger enforcement powers and more significant sanctions.

The GDPR imposes different

Continued on p.3

GDPR EU Representative – the "hidden obligation" and Brexit

Does your company require an EU Representative? **Tim Bell** from DPR Group discusses the issues.

"What's a Representative?", "Ah, you mean the DPO?", "We don't process any data in the EU, so we're fine".

It can be frustrating when attempting to discuss the role of the EU Data Protection Representative obligation under Article 27 of GDPR with companies which may require it, and sometimes even with fellow privacy professionals, but the lack of awareness of this requirement is relatively understandable. Now, as with so many other business activities, "Brexit" is adding an extra level of

Continued on p.5

Issue 102 **March 2019**

M&A ... from p.1

obligations on both sellers and buyers which must be dealt with at different stages of M&A transactions. This article sheds light on typical data disclosure issues in M&A transactions' due diligence phase and gives tips to best approaches in practice. It will cover (1) the concept of personal data during M&A transactions, (2) roles of the parties, (3) pre-merger non-disclosure agreements, (4) limiting the amount of disclosed personal data, (5) relying on a legal ground when disclosing personal data, and (6) international data transfers.

Introduction

During the legal due diligence phase a potential buyer will review documentation pertaining to a target company. The purpose of legal due diligence is to assess the value of the target and to understand the legal risks that the potential transaction may entail. Due diligence projects typically include the processing of personal data where documentation including personal data is disclosed, reviewed and commented on by various advisors. Personal data can often be central to the valuation of the target.

Concept of Personal Data

The concept of "personal data" raised much discussion even before the GDPR came into force. In the 2003 *Durant* case[1], the UK Court of Appeal stated that information should pass a "biographical significance test" to be considered personal data, i.e. personal data should affect a person's privacy. However, the court did not consider the issue of identifiability of a data subject, which is generally considered to be the key aspect of personal data definition.

Subsequent to the *Durant* case, both the UK Information Commissioner's Office (ICO) and other European data protection authorities presented a broader interpretation of the concept of personal data. The ICO stated that the "biographical significance" is only applicable in borderline cases where it is not clear whether information is personal data, and context or common sense do not provide the answer. In addition, the EU Court of Justice (CJEU) ruling in the *Nowak* case established that the regulators' purpose with the definition of "personal data" in the 1995 EU Data Protection Directive was to assign a wide scope to the concept, potentially including all sorts of information where it relates to the data subject.

As such, the GDPR's definition of "personal data" is almost identical to the definition of the 1995 Directive, but GDPR also sets more explicit examples of personal data, including location data, IP addresses and cookie identifiers. The explicit examples leave less room for interpretation or national deviations.

In spite of personal data now being far less debated, and indeed accessed as a significantly broad concept, there is still some variance in the interpretation of its scope. HR and company records obviously include personal data, but the status of signatures in commercial contracts and information related to data subjects in litigation documentation are examples of uncertain areas. In light of the aforementioned *Nowak* case and the GDPR's definition, it is at least recommended to interpret the concept of personal data broadly for the purpose of M&A transactions, even where this may mean erring on the side of caution and being overly inclusive.

Data Processing Roles of the Parties

In most M&A scenarios, both the buyer and the target will process personal data in the context of a transaction and will do so for their own distinct business purposes; the buyer to evaluate the target, and the seller to invite a favourable bid. The buyer typically receives personal data from the target and must comply with all data controller obligations under the GDPR, in addition to potentially entering into a data sharing agreement when processing the personal data it received. In those cases, both the target and the buyer (and potentially the seller) will each independently be responsible for ensuring compliance with the data protection laws. Neither party processes personal data on the other party's behalf.

In reality the roles depend on the actions of the parties as well as how means and purposes of processing are determined. The parties may, in fact, jointly determine the purposes and the means of processing, and would then qualify as joint controllers for data processing with respect to the M&A transaction. To clarify the parties' intentions, it is recommended that the parties' roles as independent controllers are defined in pre-merger documentation.

The vendor providing data room services acts as a data processor when the target or the seller uploads documentation including personal data to the data room, as the vendor processes personal data on their behalf. Due to this factor, the seller should make sure they enter into a data processing agreement under Article 28 of the GDPR with such vendors.

Pre-merger NDAs

Parties usually also enter into a non-disclosure agreement (NDA), designed to govern the disclosure and use of confidential information during the diligence process. It is now market practice for the NDA to include data processing provisions to allocate data protection obligations and risks. Even though the target and the buyer both act as data controllers, it is still recommended that the parties add data processing terms to limit the potential buyer's data handling practices.

In such an NDA, the parties would ideally agree on who is responsible for replying to data subjects' requests and for providing adequate information to data subjects. It should also include specifications of legal grounds that the parties rely on for the anticipated processing and transfers of personal data. In addition, the NDA should underline that the transaction does not create a joint controller relationship, but that the two parties act as independent controllers.

Also, the NDA should include conditions for data disclosures during the due diligence. The potential seller and target disclose information including personal data to the potential buyer. For such disclosure to be lawful, the buyer may only use the data for the agreed purposes. Additionally, it is essential to make sure that adequate data security is applied when the data is disclosed.

Limiting the amount of disclosed personal data

In accordance with the GDPR's data minimisation principle, the processing of personal data during the due diligence process should be restricted to personal data that is adequate, relevant and limited to what is necessary in relation to the purposes for which it is processed. This means that the seller should limit the disclosure of data to what is absolutely necessary for the buyer to make a purchase decision and to assess the target's value. The buyer should not request more personal data than what is necessary for the buyer's purposes at each phase of the due diligence process. Before any disclosure, the target should also ensure that the data subjects are adequately informed of all processing of their data, including disclosure of personal data to potential buyers in relation to M&A transactions.

In practice, the necessity of disclosure should be evaluated in different stages of the due diligence:

- At an early stage the target should not provide the names or contact details of its employees or customers. Personal data should be removed or masked using anonymization or pseudonymization techniques.
- At the due diligence stage, the target can gradually disclose more personal data, such as names, contact details and reimbursement information of management and/or key employees. At a further stage, the target can disclose personal data of mid-level employees.
- Closer to the final bid the target may disclose personal data of all key employees as well as unmasked data about key customers, if such disclosure is possible under applicable law and not hindered by, for example, purpose limitation.

The target should not disclose sensitive data, such as health data, unless it is strictly necessary for example in relation to HR. In any event and as further defined below, the target must ensure that it can rely on a legal ground to disclose sensitive data to the buyer and that the buyer can rely on a legal ground to process such data.

If the transaction does not go through, the buyer must delete all personal data it received in connection with the due diligence. The buyer should not retain the data for longer than is necessary for the purposes for which the data was disclosed to it, i.e. to evaluate the purchase of the target. The timing of deletion or return of personal data would also depend on the data processing terms agreed in the NDA.

Disclosure must rely on a legal ground

The processing of personal data under the GDPR must always be based on a legal ground. In M&A transactions, personal data is often disclosed and used on the basis of the "legitimate interest" of the buyer and the seller. To rely on a legitimate interest, the interests of the buyer or the seller must be balanced against the data subjects' interests using a balance test. The legitimate interest may only be relied on where the data subjects' interests and rights do not override the buyer's and the seller's interests. If the M&A transaction has negative impacts on the data subjects, for example if the transaction could lead to redundancies or reducing employee benefits, the applicability of a legitimate interest should be reassessed. In such an event, other legal grounds such as consent should be considered.

It should be noted that when the parties are processing personal data on the basis of a legitimate interest, data subjects have the right to object to the processing of their personal data and should be informed of this right, unless the controller demonstrates compelling legitimate grounds for the processing to override the particular data subject's interests, rights and freedoms. Again, if a data subject exercises their right to object, the controller should balance the data subject's interests, rights and freedoms with the controller's own legitimate grounds, taking into account the particular arguments submitted by the data subject.

Prior to the GDPR, companies often relied on consent when the potential seller disclosed personal data to the potential buyer to complete the M&A transaction. Apart from the above-mentioned exceptions (disclosure of sensitive data or data subject's overriding interests), this approach is no longer recommended, in particular due to the GDPR's stringent consent requirements. Consent must be freely given, specific, informed and unambiguous, and data subjects may withdraw their consent anytime. Obtaining a GDPR-compliant consent is challenging, in particular in an HR context, due to the imbalance of power between employer and employee. Additionally, if a data subject withdraws their consent, the parties have to cease all processing activities based on consent.

International data transfers

Under the GDPR, personal data may only be transferred outside of the European Economic Area (EEA) to countries that have been recognized by the European Commission as providing an adequate level of data protection, or to non-adequate countries where an applicable transfer mechanism recognised under the GDPR is applied.

If the buyer is not located in a country providing an adequate level of data protection and is not a US company that is certified under the Privacy Shield principles, model clauses are usually the most feasible transfer mechanism. The parties can incorporate or attach controller-to-controller standard contractual clauses to the NDA.

To avoid having to deal with cross-border transfers of data and to ensure data subjects' rights remain protected, it is best practice to conduct all due diligence involving personal data in the EEA.

Conclusions

Finally, the increased potential of sanctions encourages companies to plan disclosures of personal data in detail at different stages of a due diligence process. The concept of personal data should be interpreted broadly and it is essential to ensure that only necessary data is disclosed at each stage of the due diligence process. The parties should enter into an NDA, or a similar contract, to agree on each party's obligations related to the data processing. The disclosure of personal data should be limited to what is absolutely necessary at different stages of the transaction.

The parties to the transaction should also ensure that the processing

of personal data during the due diligence process is notified to the data subjects and that both parties can rely on legal grounds under the GDPR. Additionally, the parties must make sure that, in case of an aborted transaction, the retention and deletion of personal data is agreed upon.

Data protection breaches are gaining significant media coverage and data subjects are becoming increasingly aware of their rights. Breaching the GDPR could lead to both financial and reputational damages. Although the GDPR harmonizes EU data protection rules across Europe, there are many deviations under national laws, especially in relation to employee personal data. The parties should also take such deviations into consideration when planning the processing of personal data in connection with a transaction.

AUTHORS

Lore Leitner is Of Counsel, Privacy and Data Protection Practice, Wilson Sonsini Goodrich & Rosati (UK), LLP, London
Elli Laine is an Associate, Privacy and Data Protection Practice, Member of the Finnish Bar, Wilson Sonsini Goodrich & Rosati, LLP, Brussels
Emails: lleitner@wsgr.com
elaine@wsgr.com

REFERENCES

1 Reference [2003] EWCA Civ 1746; [2004] FSR 28; Court of Appeal
www.5rb.com/case/durant-v-financial-services-authority/
www.5rb.com/wp-content/uploads/2013/10/Durant-v-Financial-Services-Authority-CA-8-Dec-2003.pdf
amberhawk.typepad.com/amberhawk/2014/02/roll-out-the-bunting-durant-judgment-is-good-as-dead-and-buried.html

EU Representative ... from p.1

confusion to the role.

Essentially, the EU Representative is required by any company which sells to, or monitors, individuals in the EU, but has no establishment (office, factory etc.) in the Union. The company (or, less commonly, individual) appointed to this role acts as the point of establishment in the EU, taking on the administration and liabilities of the data controller or processor based outside. The effect of the extra-territorial nature of the Representative is that it isn't required by companies in the EU – they are already established here – so there's no need for them to know about it, and as a result we're not discussing it in the EU, or including reference to this obligation in the plethora of materials which have come out of the EU in the last couple of years in the run up to, and during the initial operation of, GDPR. That makes sense; GDPR can be complicated and frightening already, without listing additional, unnecessary requirements.

The knock-on effect of this, for those companies outside of the EU which are obliged to appoint an EU Representative, is that their preparations – usually based on materials sourced from the EU (and where else would they seek their information on this EU law?) – never even touch upon this requirement. There are exceptions of course, but the issue is exacerbated by the fact that the larger multinationals headquartered outside of the EU which are able to justify the expense of a decent privacy consultant will usually also have an office of some kind in the EU, meaning this requirement isn't imposed on them either.

The EU Commission hasn't helped in spreading word of this responsibility, presumably taking the view that companies which will need to make the appointment will simply have to read the Regulation to appreciate this requirement (accusations that the Union has no sense of humour are clearly unfounded). Our organisation coined the phrase the "hidden obligation" in December 2017, to highlight this failure to spread awareness of the EU Representative role.

The EU Representative obligation – a summary

For reference, Article 27(1) states:

- Where Article 3(2) applies, the controller or the processor shall designate in writing a representative in the Union. [Article 3(2) gives extra-territorial effect to GDPR].

There are some exclusions and, in summary, an organisation is obliged to appoint an EU Representative if it:

- has no establishment (a location undertaking "effective and real exercise of activity through stable arrangements" [Recital 22]) in the EU, and
- sells goods or services in the EU, or monitors individuals there, and
- is not a public authority, and
- does not satisfy the *occasional* exemption (see the "Exclusions" section below).

Some of the vagaries of the requirement have, fortunately, been clarified by the European Data Protection Board "Guidelines 3/2018 on the territorial scope of the GDPR" (the "Guidelines") issued in November 2018, but this clarification was to be found at the back of the Guidelines following a thorough assessment of the extra-territorial effect of GDPR and, as a result, they may also have been missed by many.

The Guidelines confirmed:

- The EU Representative should be established in the EU Member State where the non-EU data controller or processor has the largest number of data subjects;
- Notwithstanding their location in such Member State, the EU Representative should be easily accessible to data subjects in other Member States where the data controller or processor provides their goods/services or monitors individuals;
- That the Representative can be held liable for their clients' failures to meet the requirements of GDPR.

The last part was a sobering revelation to many, but simply clarified the position set out in Recital 80 of the Regulation – "The designated representative should be subject to enforcement proceedings in the event of non-compliance by the controller or processor".

While the liability position may be uncomfortable for those considering – or already providing – these services, it makes sense in the context of how GDPR views the Representative role.

Join the Privacy Laws & Business community

The *PL&B United Kingdom Report*, published six times a year, covers the Data Protection Act 1998, the Freedom of Information Act 2000, Environmental Information Regulations 2004 and Privacy and Electronic Communications Regulations 2003.

PL&B's United Kingdom Report will help you to:

Stay informed of data protection legislative developments.

Learn from others' experience through case studies and analysis.

Incorporate compliance solutions into your business strategy.

Learn about future government/ICO plans.

Understand laws, regulations, court and tribunal decisions and what they will mean to you.

Be alert to future privacy and data protection law issues that will affect your organisation's compliance.

Included in your subscription:

1. Online search functionality
Search for the most relevant content from all *PL&B* publications and events. You can then click straight through from the search results into the PDF documents.

2. Electronic Access
We will email you the PDF edition which you can also access via the *PL&B* website. You may also choose to receive one printed copy.

3. E-Mail Updates
E-mail updates keep you regularly informed of the latest developments in Data Protection, Freedom of Information and related laws.

4. Back Issues
Access all the *PL&B UK Report* back issues since the year 2000.

5. Events Documentation
Access UK events documentation such as Roundtables with the UK Information Commissioner and *PL&B Annual International Conferences*, in July, Cambridge.

6. Helpline Enquiry Service
Contact the *PL&B* team with questions such as the current status of legislation, and sources for specific texts. This service does not offer legal advice or provide consultancy.

To Subscribe: www.privacylaws.com/subscribe

"I particularly like the short and concise nature of the *Privacy Laws & Business* Reports. I never leave home without a copy, and value the printed copies, as I like to read them whilst on my daily train journey into work."

Steve Wright, formerly Data Privacy & InfoSec Officer, John Lewis Partnership

Subscription Fees

Single User Access

UK Edition **£450 + VAT***
International Edition **£560 + VAT***
UK & International Combined Edition **£900 + VAT***
* VAT only applies to UK based subscribers

Multi User Access

Discounts for Multiple User licence (up to 10) and Enterprise licence (unlimited users).

Subscription Discounts

Introductory discount (first year): 30% off for DPAs, public sector, charities, academic institutions, use code SUB30; 20% off for other organisations, use code SUB20.

Discounts for 2 and 3 year subscriptions

International Postage (outside UK):

Individual International or UK Edition
Rest of Europe = £25, Outside Europe = £35

Combined International and UK Editions
Rest of Europe = £50, Outside Europe = £70

Satisfaction Guarantee

If you are dissatisfied with the *Report* in any way, the unexpired portion of your subscription will be repaid.

Privacy Laws & Business also publishes the International Report.
www.privacylaws.com/int