January 25, 2018

Impact of GDPR on M&A Transaction Process

By Barry Fishley

As many will by now be aware, a major new data privacy law – the General Data Protection Regulation ("**GDPR**") will come into force on 25 May 2018, introducing substantial changes to current European privacy laws. This update will focus on the practical ways the GDPR will impact the M&A transaction process, and in particular the approach potential sellers should be taking.

1. Increased Jurisdictional Scope

One of the most significant changes under the GDPR is its enhanced territorial scope. The new law will apply to organisations holding or using data about individuals located in the EU, even in the absence of any physical EU presence, where organisations:

- offer goods or services within the EEA (e.g. by having EU language versions of a website); or
- monitor the on-line behaviour of individuals in the EU (e.g. by using cookie technology).

If these extra-jurisdictional provisions apply, non-EU organisations will have to comply with the entirety of the GDPR or suffer the enhanced penalties regime (see below). Full compliance with the GDPR's 99 Articles will require, among other things, rapid reporting of data breaches to EU privacy regulators, compliance with various rights granted to individuals including the individual's right to have their data deleted and the maintenance of detailed internal records of data processing operations.

2. Enhanced Penalties

One of the most well-publicised changes under the GDPR is its enhanced penalties. Organisations that commit a serious breach of its provisions face potential fines up to the greater of EUR 20m or 4 % of the worldwide annual revenue.

3. But Otherwise, Business As Usual?

Despite the rather ominous headlines above, the GDPR is unlikely to necessitate any significant practical changes to the M&A transaction process under the current regime. The same considerations will continue to apply, and the various safeguards being used will likely remain adequate.

3.1 What types of personal data could be disclosed prior to sale?

The personal data that most typically will be disclosed as part of the due diligence process will include employee data and/or customer data particularly where the business being sold is a B2C business. The

GDPR confirms but also expands the current definition of personal data to include location data and possibly browsing history.

3.2 Satisfying the legitimate interests condition

Personal data can only be disclosed if a fair processing condition can be satisfied. As before, the key processing condition in an M&A context is likely to be the legitimate interest condition – i.e. that it is **necessary** for the purposes of a legitimate interest of the seller and/or the third party potential bidder to receive the personal data as part of the sale process and that these interests outweigh any potential prejudice to the individual of having his/her information disclosed.

Accordingly, the seller has to make an assessment of what types of personal data it is necessary to disclose prior to sale. For example, bidders will not necessarily need to see personal data relating to every employee in the business; rather it is more likely to be necessary for the seller to disclose certain personal data relating to senior management or the board of directors so that bidders can properly assess the leadership team. Outside of this select group of individuals, it will be generally more difficult to use the legitimate interest condition to lawfully disclose personal data relating to employees.

For sellers, this means that information should be redacted or anonymised as far as possible so that it does not identify any individual as data that is no longer personally identifiable falls outside the scope of the GDPR. For example, uploading blank model contracts would remain a best practice in the case of non-key employees having no special clauses in their employment agreements. Similarly, disclosing personal data relating to individual customers may be avoided by providing anonymised data and/or data which provides general information or aggregated data (e.g. age profile, geographic characteristics, types of product/service purchased etc.).

Where it is necessary to disclose personal information, appropriate safeguards should be put in place so as to materially reduce or eliminate any adverse consequences for the individual. This means practices that are already commonplace (e.g. restricting which individuals have access to data, ensuring non-disclosure agreements are put in place prior to disclosure and ensuring that all information is kept in a secure virtual data room) should continue.

3.3 More stringent consent requirements

As before, sellers should avoid relying on consent as the fair processing condition as far as possible. This is particularly so under the GDPR, which will bring stricter consent requirements into force. However, where sensitive personal data, termed 'special category data' under the GDPR (which includes information relating to health, sexual orientation and political opinions) is to be disclosed, sellers will often only be able to rely on explicit consent in order to satisfy a fair processing condition. The GDPR additionally requires consent to be unambiguous and involve a clear affirmative action. Regulators have already stated that consent in an employment context cannot always be relied on as it may not be deemed to be "freely given". Given these difficulties, it is highly recommended that any sensitive information is redacted or anonymised such that it no longer can identify any individuals.

3.4 Notification obligations

One of the main principles of EU data privacy laws is that the personal data should be processed fairly and lawfully. In this context, "fairly" requires the seller to inform the individual that his/her personal data may be disclosed to potential bidders. This thread continues under the GDPR. However, clearly, notification will be commercially undesirable where the parties want any knowledge of the proposed deal to be restricted to as few people as possible.

This obligation may not be an issue where the personal data to be disclosed relates to senior management (i.e. pursuant to the legitimate interest condition), who are closely involved with the sale process as they still may well have been notified of the disclosure.

References to potential disclosure within the context of M&A in privacy policies may be sufficient notification to customers.

3.5 Security considerations

Security will remain a key tenant of the privacy regime, and particularly so in light of the enhanced breach notification obligations under the GDPR (notification of breach to the data privacy regulator and individuals will be mandatory, unless the breach is unlikely to result in harm such as where the data is unintelligible, e.g. encrypted, and such breaches must be notified to the regulator within 72 hours, if feasible). As a result, if sellers employ the services of an organisation to host a virtual data room ("**VDR**"), among other things, the agreement with the provider should contain commitments relating to data security and co-operating with the seller so that it can properly respond to requests made by data subjects to exercise their rights. Erasure or return of any personal data when no longer needed should also be included.

3.6 Exporting personal data

The GDPR continues to provide that personal data may not be transferred, stored or accessed outside the EEA unless an adequate level of protection for the rights and freedoms of the relevant individuals can be ensured. Such transfers may be necessary in the course of an M&A transaction if, for example, servers holding data room information are located outside the EEA, or where potential bidders are established outside the EEA. Currently, most sellers will rely on the following ways of demonstrating that there is "adequate protection" and this will remain the case under the GDPR:

(i) the transfer is carried out in accordance with **model contracts** adopted by the European Commission which provide standard wording for the transfer of data to an entity established outside the EEA; or

(ii) where data is stored in the USA, the entity in the US holding the data is registered under the **EU/US privacy shield**.

Barry Fishley

Expertise

Barry Fishley is a partner in the London office and has had wide ranging experience in data protection, technology, intellectual property, e-commerce and general commercial matters.

He advises financial institutions, major international companies and private equity funds on a range of transactions and issues including data protection, technology and intellectual property aspects of M&A and banking transactions, complex international licensing arrangements, outsourcing, strategic alliances, manufacturing supply and other international commercial transactions.

In the areas of data protection and privacy, Barry has extensive experience of advising on the consequences of a security breach, international transfers of data, privacy audits and general compliance.

Barry regularly speaks and writes on various topics. His most recent work was a series of presentations on cyber security including cyber security implications for M&A.

Barry is recommended in *Legal 500 UK* for his media & entertainment expertise.

Contact Details

Barry Fishley
Partner
barry.fishley@weil.com
110 Fetter Lane
London, EC4A 1AY
Tel. +44 20 7903 1410

If you would like more information about the topics raised in this briefing, please speak to your regular contact at Weil or to any member of the Technology & IP Transactions Group.