M&A AND THE NEW EUROPEAN DATA PROTECTION RULES: *ADDITIONAL RISKS FOR TRANSACTIONS AND HOW TO AVOID THEM*

By Hanno Timner & Alex van der Wolk

Hanno Timner is the co-managing partner of the Berlin office of Morrison & Foerster LLP, and the head of the Employment and Labor practice group in Germany. He advises and represents national and international employers in all labor law issues and disputes. Alex van der Wolk is a partner in the Berlin office who specializes in data protection information/communications technology law. He advises global companies on data protection strategy and compliance governing all aspects of information management.
Contact: htimner@mofo.com or avanderwolk@mofo.com.

After almost five years of intense debate, European Union (EU) institutions have finally agreed on a new European data protection framework: The General Data Privacy Regulation (GDPR). The GDPR is expected to come into effect in 2018. The next two years will give companies a transitionary period in which to prepare for the changes effected by the GDPR.

In the M&A context, purchasers should consider how the new framework may affect the risks and liabilities involved in a transaction, taking into account increased powers of data protection authorities (DPAs) and the potential for significant fines. The following aspects of the GDPR are of particular importance regarding M&A transactions:

- **Does the target company fall within the scope of the GDPR?** A very notable change is that the GDPR applies not only to companies established in the EU, but to all companies targeting EU markets or consumers. Therefore, companies in non-EU countries may soon find themselves with a significant investment backlog in privacy/compliance and may be exposed to previously unknown compliance risks.

- **Does the target company meet the GDPR's compliance burdens?** The new framework provides comprehensive recordkeeping obligations and mandatory data protection impact assessments(DPIAs).

- **Does the target company have a data-protection officer (DPO) in place?**

- **What is at stake?** Penalties for non-compliance will reach unprecedented heights with new maximum fines of £20 million or 4% of group annual worldwide revenue (whichever is higher).

Scope of Applicability

The GDPR will apply to the processing of personal data by controllers and processors that are established in the EU, but also to companies outside of the EU that (*i*) offer goods or services to individuals located in the EU (regardless of whether payment is sought); or (*ii*) monitor the behavior of individuals in the EU (insofar as that behavior takes place in the EU).

- The "offering of goods or services" criterion requires some form of targeting of individuals in the EU. The mere accessibility of a website from the EU, or the use of a language that is also used in Europe (where such language is also the language of the controller's country) does not necessarily lead to applicability. A combination of factors, such as the ability to order goods and services in an EU language, payment options in EU currencies, and providing local content, may lead to the determination that the company is targeting EU individuals.

- The "monitoring behavior of individuals" criterion—which will potentially include the tracking and the profiling of EU individuals through

websites, cookies and other remote activities—requires that such behavior take place in the EU.

Consequently, even if the target company is located outside of the EU, it may still be subject to the GDPR.

Compliance: Documentation Duties & Mandatory DPIAs

Purchasers should closely evaluate the type of processing activities that the target company is engaged in and make an inventory of its current state of compliance. The purchaser will then be in a better position to assess which measures and potentially substantial investments are necessary within the next two years to meet the new level of compliance required under the GDPR. In particular, the new regulation introduces comprehensive recordkeeping duties, mandatory processes to safeguard data subjects' rights, and DPIAs for high-risk processing activities.

- The GDPR requires data controllers and processors to maintain extensive records of processing activities (Art. 30), which must be available to DPAs. These records must provide, among other things, the name and contact details of the controller or processor and data protection officer, if any; the purposes of the processing (controllers); the categories of processing (processors); the transfers (including the list of the third-party countries to which data will be sent); the retention and erasure periods (controllers); and a description of the company's technical and organizational security measures.

- Furthermore, companies should have processes in place to meet the requirements on individuals' rights. This includes procedures on how to grant access to data, as well as how to trace and remove individuals from databases (the so-called "right to be forgotten"). The procedures should allocate these responsibilities within the company and provide target response times.

- Purchasers should screen target companies for high-risk processing activities that require a DPIA, such as profiling or the large-scale use of sensitive data. DPAs will maintain lists of the processing activities for which DPIAs will be required. The DPIA is a written review process that companies should implement; it includes a systematic description of the company's processing operations and an assessment of the necessity and proportionality of the processing, as well as its risks and safeguards. Importantly, if the DPIA indicates that the processing would result in a high risk that cannot be mitigated, the company must consult with the DPA. If the DPA is of the opinion that the processing would violate the GDPR, it will provide written advice to the controller (Art. 36(2)) and may (ultimately) use its enforcement powers (Art. 58) and prohibit the processing.

Does the Company Need a DPO?

The GDPR introduces an obligation to appoint a DPO (Art. 37) for controllers and processors, which is currently not mandatory under the EU Data Protection Directive 95/46/EC, but is required under some national laws (*e.g.* in Germany). The appointment of a DPO is obligatory where the "core activities" of an entity involve the large-scale processing of sensitive data or "regular and systematic monitoring of data subjects on a large scale" (*e.g.* online behavior tracking or profiling, or the monitoring of employees by an employer). This may affect many multinationals (if, for instance, they engage in such activities as Data Loss Prevention or have centrally managed employee expenses). The GDPR furthermore sets requirements for the qualifications of a DPO, so companies are advised to review whether their organizations are subject to the DPO requirement.

Increase in Fines and Enforcement Powers for DPAs (Art. 55 and 83)

The past years have seen an increased level of enforcement initiated by the DPAs in the EU (*e.g.* in

Spain, France and Belgium). In the M&A context, the Bavarian DPA announced in July 2015 that it had imposed substantial administrative fines on both the seller and the purchaser of a company who had transferred personal customer data as part of the transaction.

The stakes are raised under the GDPR. The new framework grants broad powers to the DPAs, encompassing the power to launch investigations, suspend data flows, terminate processing activities and impose fines of increasing levels of severity. Certain infringements (such as those pertaining to consent requirements, individual rights, transfer restrictions and compliance with certain DPA orders) may be sanctioned with fines of up to £20 million or 4% of a group's global annual turnover (whichever is higher being the maximum).

The GDPR also grants broad rights for individuals to lodge complaints with DPAs and obtain judicial remedies and compensation from companies.

CONFERENCE ROUND-UP: REGULATORY UNCERTAINTY, EMAIL SCAMS & CYBERSECURITY TOP LIST OF LEGAL CONCERNS

By Sameena Kluck & Joe Raczynski

Sameena Kluck is a Strategic Account Executive for Thomson Reuters and Westlaw. Prior to that, she managed client relationships with Am Law 150 law firms in the Washington, D.C., area. Joseph Raczynski is with Thomson Reuters Legal managing a team of Technical Client Managers for both the Large Law and Government divisions. He serves the top law firms in the world consulting on legal trends and customizing Thomson Reuters legal technology solutions.
Contact: sameena.kluck@thomsonreuters.com or joseph.raczynski@thomsonreuters.com.

Recently, two separate conferences were held addressing cybersecurity, internal and client data security and the increasingly contentious regulatory environment that surrounds those issues. These dispatches detail the highlights of each conference:

Regulatory Uncertainty & Cybersecurity Makes Lawyers and their Clients Nervous

WASHINGTON, DC—Uncertainty reigned at the inaugural Regulation of Financial Services 2016 conference.[1] Throughout numerous panels addressing different issues affecting the financial services industry, attorneys from law firms and financial services companies repeatedly expressed uncertainty about conflicting regulations and statutes, both domestically and internationally.

The conference, held June 8 and presented by Thomson Reuters' *Legal Executive Institute*, was designed to give lawyers, banking and compliance professionals some insight into the current state of global regulatory policies and financial technology.

The initial panel, titled "Proceed with Caution: Assessing Global Sanctions in the Changing Regulatory Landscape," focused on the recent developments in global sanctions in the financial services sector. Several panelists—mostly general counsels and compliance officers—discussed the difficulty companies now have in navigating the varied compliance and sanctions policies set by the US, EU, and other countries, and the increased uncertainty that has resulted.

Indeed, the number one thing compliance professionals look for is certainty, so when there is uncertainty, most companies will take as little risk as possible and end up engaging in less business to reduce their exposure, said Chaim Levin, Chief Legal Officer and General Counsel for the Americas at Tradition Group. Alma Angotti, Managing Director in Global Investigations & Compliance of Navigant Consulting agreed, noting that a huge shift in complexity has arisen as sanctions have moved from party-based to transaction-based. "It's more difficult to operational-