New burdens in due diligence

HOW REVAMPED EU PRIVACY REGULATIONS IMPACT GLOBAL M&A
Summary

It is difficult to overstate the scale and reach of the European Union’s General Data Protection Regulation, set to apply on May 25, 2018. The GDPR is widely considered to be the most comprehensive reform developed in the last 30 years for the protection of personal data, and is expected to become a global standard for online privacy.

As stated by the European Commission, the law is designed “to give citizens back control over their personal data, and to simplify the regulatory environment for businesses.” The EC has sought to standardise the data privacy laws across the European Union and to provide residents with “a high standard of protection” for their personal data throughout the bloc of nations.

EU regulators have raised the bar substantially in terms of what is required to comply with the law and instituted harsh penalties for non-compliance and data breaches. The regulation will apply to all companies based in the EU. It also exercises extraterritorial jurisdiction to include any non-EU companies that offer goods and services to EU residents and in so doing control or process personal data. This means businesses all over the world will need to comply or face potentially drastic consequences.

The broad sweep of the Regulation and the repercussions for running afoul of it mean that companies pursuing mergers and acquisitions will be wise to place a stronger emphasis on the due diligence process, verifying more thoroughly a target’s compliance with the GDPR’s strict mandates to safeguard personal data.
GDPR: High Standards and Accountability

The GDPR will supersede the existing Data Protection Directive 95/46/EC in a move to bolster and standardise the oversight and enforcement of personal information protections, as laws in EU member states have diverged since the directive was first adopted in 1995.

Under the new regulation, companies will be held to a substantially higher standard of accountability on how they gather, manage and use personal data. EU citizens will enjoy:

- **ENHANCED RIGHTS**
- **A MORE FORMIDABLE LEGAL STANDING**
- **STRONGER SAY IN THE HANDLING OF THEIR PERSONAL INFORMATION**

This includes the “right to be forgotten,” meaning they can request businesses delete their data if it is incorrect or no longer necessary. Portability of data when requested by individuals, and rights to actively consent for each use of personal data are also augmented.

Another important guideline includes the need for certain companies to appoint a **data protection officer**. The International Association of Privacy Professionals estimates that 28,000 DPOs will be needed just in Europe to achieve complete compliance by the May 2018 deadline.

A key element, to assist in enforcement, will be that non-EU data processors and controllers, who regularly collect data on a large scale, are required to appoint a local representative to act as a point of contact for regulators within EU member states where they do business.
Breaches, Non-Compliance Will Be Expensive

One of the most critical changes looming with GDPR is the requirement that businesses notify authorities in member states within 72 hours of becoming aware of a data breach. That is a significant acceleration in the notification process, considering companies are often still attempting to understand the scope of a breach within that time frame. They are also required to report the breach to the data subjects “without undue delay.”

There is an exception, however, to the 72-hour disclosure stipulation when the breach “is unlikely to result in a risk to the rights and freedoms” of the data subjects.

In addition to the extraterritorial scope of the GDPR, perhaps the most important aspect of the regulation is the stiff penalties that can be levied for non-compliance or data breaches. Violators risk being slapped with fines of up to 4 percent of annual revenue, or €20 million, whichever is higher. For large companies, that presents a danger of fines amounting to hundreds of millions, or even billions of dollars. This makes the incentive to comply with the law unambiguous.

Despite the spectre of massive fines, Gartner has said organisations are not prepared for the new regulatory regime and predicted that by the end of 2018, more than 50 percent of companies affected by the GDPR will fall short of full compliance.

That does not mean the road to May 2018 is not paved with good intentions. A PwC survey found:

+ More than half of US multinationals said GDPR was their top data-protection priority this year
+ Seventy-seven percent of those polled planned to spend $1 million or more to mitigate the risk of infringement

Some, however, indicated they are not willing to accept the risk of hefty penalties for non-compliance. Nearly one-third of respondents plan to reduce their presence in Europe, PwC said, and 26 percent intend to leave the EU market altogether.

As European regulators further clarify how they interpret GDPR, “more American companies are likely to re-evaluate the return-on-investment of their European initiatives,” the firm added. That could inhibit potential deal activity.
Impact on Global M&A

At the very least, companies pursuing mergers or acquisitions can expect to engage in a much more comprehensive due diligence process to fully assess a target’s ability to comply with GDPR.

“Additional diligence at all stages of the M&A process will be paramount,” wrote Gail Crawford, a partner at Latham & Watkins and chair of the firm’s Internet & Digital Media Industry Group. Crawford added that there should be a greater emphasis on verifying important compliance features, including:

- The existence of data protection officers
- Records of data processing activities
- Whether the entity generates privacy impact assessments for new projects

“Understanding how a target collects, stores, uses and transfers personal data will be vital in understanding the valuation and risk associated with a transaction,” she stated.

It will be incumbent upon buyers to comprehensively evaluate the target’s privacy policies for both online and mobile media, vendors and other third-party affiliations to confirm they all adhere with GDPR, or the buyer risks the possibility of steep post-merger fines for non-compliance.

Due diligence is also an opportunity to take measure of how a target stores, uses and protects its data, with an eye toward any potential post-merger integration challenges. Future business goals need to be aligned between target and buyer, which means current consents from data subjects need to be evaluated to verify they will allow for different uses of the data after a deal closes.

If the target is not in compliance, the issues may require changes to the purchase agreement, including the following, according to the law firm Nixon Peabody:

- Exclusion of certain non-compliance liabilities from the deal
- Add specific indemnities related to non-compliance issues
- Include covenant enabling ongoing safeguards of sensitive information by the target company
- Addition of a new closing condition requiring target company to take steps to address non-compliance issues or the implementation of missing IT safeguards
A High-Profile Lesson

Yahoo! Inc.’s sale to Verizon Communications Inc. is instructive as a lesson for deep due diligence ahead of GDPR’s start date. The transaction closed at a price discounted by $350 million when past data breaches came to light after the deal was announced. It was a costly hit for Yahoo, though fortunate for Verizon that the breaches were disclosed before the deal was completed. The companies also agreed to share some of the legal liabilities related to the breaches.

Understanding whether a seller previously experienced a breach, and how it may have responded is imperative for evaluating its readiness to comply with the new EU regulations.

Privacy attorney Kate Lucente told technology news site GeekWire late last year that she had seen a deal significantly discounted because the target could not document that it had the proper privacy practices in place, and the buyer considered a significant portion of the company’s customer data unusable after the close.

For targets, the smart approach is to be proactive. “The best protection for a seller in an M&A transaction is to demonstrate that all steps needed to achieve compliance have been put in place and do not negatively impact the business,” wrote middle-market M&A adviser Livingstone Partners.

Enforcement: Still Some Unknowns

Though the prospect of onerous penalties has companies treading very carefully, uncertainty on just how EU enforcement actions will play out may temper some anxiety over GDPR.

The regulation stipulates the member state in which a company has its main office or establishment will have supervisory responsibility and can coordinate with other EU authorities.

“It remains to be seen how this will work in practice and whether companies will have the ability to influence which lead supervisory authority is allocated to it, along with the political and tactical manoeuvring this may entail to ensure the most preferable outcome for the company,” attorneys Jonathan Millard and Tyler Newby of Fenwick & West, wrote for an American Bar Association publication.

That suggests companies could have some leeway with authorities if they are found to be non-compliant, indicating there may be some avenues to avoid the most punitive sanctions.
Conclusion / Outcomes

While the EU’s GDPR will likely bring additional costs and raise the regulatory load on businesses, it shouldn’t dramatically alter the rationales companies have for pursuing deals -- namely their desire to boost sales and profit growth, fend off competition, or as a means to attain greater innovation. So long as the benefits of a transaction outweigh the potential costs incurred by complying with the GDPR, it is unlikely the regulation will act as a substantial drag on future deal making.

To the extent that the regulations create a stronger defense against data breaches and tighter oversight of the uses and protection of personal data, it should be viewed as a support to best corporate practices and a natural enhancement to value.

As Deloitte’s Peter Gooch, cyber risk services partner, observed: “Organisations should not see this as just a regulatory compliance program. Having the right privacy requirements embedded into an overall customer engagement strategy can also be a competitive advantage.”

When GDPR goes into effect in May 2018, companies interested in making deals will need to embrace a more rigorous due diligence process if they wish to avoid breaking the EU’s more stringent data privacy laws.

The regulation may initially impose the burden of a longer due diligence period, potentially higher deal costs and more resources devoted to compliance. However, the benefits should be stronger vigilance and more trust in data privacy; a positive outcome for the long-term strength of businesses and consumers around the globe.
About Merrill Corporation

Merrill Corporation provides technology-enabled platforms for content sharing, regulated communications and compliance services. Merrill clients trust our innovative cloud-based applications and deep subject expertise to successfully navigate the secure sharing of their most sensitive content, perfect and distribute critical financial and regulatory disclosures, and create customised communications across stakeholders. Merrill clients turn to us when their need to manage complex content intersects with the need to collaborate securely around the globe.

Merrill Corporation secures solutions at every phase, so you can secure ongoing impact and growth.

To discuss how Merrill Corporation can help you manage and share content securely online, please contact us.

EMEA Contact Information  
+44 (0)20 3031 6300

APAC Contact Information  
+852 2536 2288

US Contact Information  
888.688.4400

Email  
info@merrillcorp.com

Website  
merrillcorp.com

© MERRILL COMMUNICATIONS LLC. ALL RIGHTS RESERVED.