ARTICLE

Data Risks and Challenges in M&A Transactions

At the recent PrivSec Global event, Sonia Cheng, Senior Managing Director and EMEA Head of Information Governance & Privacy at FTI Consulting, led a panel with Ahmed Baladi, Privacy & Cybersecurity partner at Gibson, Dunn & Crutcher and Linda NiChualladh, Head of Privacy (Legal) at Citi. The session covered the underlying risks and considerations associated with data in M&A transactions and the skills needed to brave a complex M&A data landscape.

For the last 10 years, while global M&A activity has been booming, the volume of data used by businesses has also exploded. With the advent of new technologies and advancements in digital transformation, the data universe will reach 163ZB (zeta bytes) by 2025. This increase in data combined with intensifying global data protection regulations is introducing new responsibilities and elevated risks around M&A activity. During the session, the panellists set the stage by discussing these increased risks and the implications of established and emerging data privacy laws including the GDPR, California Consumer Privacy Act, California Privacy Rights Act, Brazil's General Data Protection Law and others.

Further complicating the issue is that operationalising privacy compliance at scale is a significant challenge for global multinational corporations. Organisations may be tempted to 'just standardise' on GDPR, but data protection legislation and broader legal context and cultural value systems must be considered to achieve an effective privacy programme. Understanding the kind of data being used, and critically why it is being processed, will be key to achieving alignment.

How Privacy Law and M&A Intersect

Competition law is about helping to make sure there is a level playing field that allows people to innovate, offering consumers choice and good pricing. In recent years, many companies have amassed significant volumes of data, and the competition question raised is whether a smaller entrant was to have access to that information, would they be able to compete? Because much of the data is considered personal data, there is a clash around data privacy—the user who gave that data did not consent to have that data be shared with other parties or used for other purposes beyond the original intent. This has resulted in competition authorities looking at whether a company's acquired access to personal data distorts the ability for others to compete in the market. Cases have arisen in Germany and other countries with competition authorities scrutinising failures to comply with data protection laws as

a way to examine competition abuses—especially in the big tech and ad tech arenas. An example would be an industry leader leveraging its customer data in ways not compliant with GDPR to influence its market power and competitive advantage. In other sectors, there have been instances where the GDPR has been used to block data sharing even when access has been authorised by the competition authorities. With these types of developments, competition regulators are complementing the work of data protection authorities, and in some instances, may impose an even bigger impact on privacy compliance.

Privacy and Data Risks Throughout the Deal Lifecycle

There are several issues acquiring companies must consider in terms of privacy and security risk across each of the phases of an M&A transaction. The most critical takeaway is the importance of defining business objectives and understanding how data is to be used to accomplish the deal's purpose, considering the range of potential exposures, remedies authorities may require to approve the deal and the business benefits expected—from the very beginning. Many companies assume that when they acquire a company, they also acquire all the rights and uses owned by the target company, but cases throughout Europe have demonstrated that user consent does not automatically transfer in a merger or acquisition. This is one stark example of potential downstream risks that can arise when the objectives and limitations associated with data are not understood before investing in a deal.

— **Phase One: Due Diligence.** In this stage, acquiring companies must identify opportunities and red flags, and conduct a privacy and security risk assessment on the business. The findings will help inform how risks impact valuation. This must go beyond the framework of a standard risk assessment. Target companies should be looking not only for problems or lack of compliance but also the business purposes for the acquisition—which will help identify whether the target already obtained consent from its consumers to share data with third parties or affiliate companies. A liability assessment also needs to be considered, to account for what will happen in the event of a data breach or privacy violation—who will bear responsibility for mitigation and resolving these types of issues post-acquisition? Finally, parties must determine how the new company will fit into the global organisation in terms of current and future needs, including where data will be located, which third-parties will touch the data and what mechanisms will be used to conduct data transfers.

— **Phase Two: Regulatory Approval.** As a transaction faces scrutiny by competition authorities, a range of remedies may be requested. Competition authorities will look at whether sharing of data between the merging entities will lessen competition. If they determine a problem, they may request the sale of certain data assets. But sometimes these concessions conflict with privacy law—if a transaction reaches that point, the parties may have a serious uphill battle in taking the deal across the finish line. In other cases, the remedies may be so extreme that they dilute the value of the target. This potentiality reinforces the critical nature of a comprehensive due diligence before a deal is submitted to the authorities for approval.

— **Phase Three: Post-Closing and Integration.** The panellists had some practical advice on how to prioritise activities following closing. The first was to determine the cost and timing for remediating any non-compliance identified during the deal lifecycle and prioritising the highest-risk aspects first. By extension, companies need to revisit new liabilities. For example, some companies—such as a U.S.-based business that acquired an EU-based organisation subject to GDPR—may need to manage the risk of data contamination via ring-fencing or other mitigation steps. Obtaining new consents or introducing new privacy notices are additional activities that will help manage risk as the two companies are integrated.

Innovative Approaches to Tackle M&A Data Risks

Throughout the discussion, the panellists reiterated the importance of understanding the target company's data position and the ultimate objectives for that data at the outset. Best practices for doing so include:

— **Know your data.** Whether target or acquirer, it's critical for companies to have a clear picture of its information landscape to reduce downstream risks. Data mapping is an important step. Policies and procedures to ensure alignment around privacy, security, information governance, handling of confidential or trade secret information and IT operations must be revisited and updated.

— **Be prepared for handling emerging data sources.** Business-critical and privacy-sensitive data is now generated in a myriad of communication sources, collaboration tools and streaming tools. Handling data from these "emerging" sources may require bespoke solution development to support collection, search or other data management needs.

— **Accelerate data review.** Merger clearance investigations are becoming increasingly intense in terms of the volume and variety of internal documents and data that must be produced to regulators. Likewise, organisations need efficient ways to analyse data during due diligence. Technology-assisted review tools used in e-discovery matters (such as predictive coding) can be utilised to accelerate review.

— **Leverage technology to automate ongoing compliance.** Data identification, classification, data loss prevention and digital rights management solutions can help streamline and support ongoing ring-fencing measures to protect sensitive data or critical IP.

The regulatory landscape is fast evolving, very complex and when intersected with data issues, the risks for M&A are significantly multiplied. Data can bring tremendous value, but it can also be a long-term privacy risk. This is why it's crucial to recognise the sensitive nature of data today, how it can impact M&A and invest adequate time and resources into making the right decisions from the very beginning.

The views expressed in this article are those of the author(s) and not necessarily the views of FTI Consulting, its management, its subsidiaries, its affiliates, or its other professionals.

SONIA CHENG
Senior Managing Director
+44 (0)79 7750 0709
sonia.cheng@fticonsulting.com

FTI Consulting is an independent global business advisory firm dedicated to helping organisations manage change, mitigate risk and resolve disputes: financial, legal, operational, political & regulatory, reputational and transactional. FTI Consulting professionals, located in all major business centres throughout the world, work closely with clients to anticipate, illuminate and overcome complex business challenges and opportunities.©2020 FTI Consulting, Inc. All rights reserved. **www.fticonsulting.com**.

1299 - 01/21