Data Protection Risks in M&A and Investment Transactions

By:Ryan J. Perry
January 31, 2023

When companies think about data protection risks, they usually think about mitigating risk associated with enforcement actions brought by a regulator in response to compliance gaps with applicable data protection laws. Or they consider risks arising from a data breach. In addition to those risks, however, data protection has become one of the most prominent issues in many corporate transactions, including most mergers and acquisitions as well as investment transactions. Accordingly, transaction associated risks (such as special escrows, special indemnities, purchase price adjustments, increased transaction cost, potential deal killer, etc.) should also be considered as businesses think about data protection. Buyers and investors expect their targets to be prepared to confront privacy and data security challenges wherever they may appear.

Privacy Issues in Corporate Transactions Generally

Data protection issues typically arise in corporate transactions in three components of the deal: (1) due diligence; (2) representations and warranties; and (3) disclosure schedules. When conducting due diligence, the buyer/investor asks questions about the company's data protection practices and inspects relevant documents, such as privacy policies, security programs, and customer/vendor contracts (including data processing addenda).

In the representation and warranty provisions in the purchase agreement, the company represents and warrants to the buyer/investor that various facts about the company are true. This may include contractually representing that the company is in compliance with applicable data protection laws, that the company is in compliance with its own policies, that it has implemented and maintains security measures over the company's systems, as well as representations concerning the company's vendor management practices as they relate to data protection. And, if any of the representations or warranties in the purchase agreement are not true with respect to the company, the company would disclose the facts that make the relevant representation or warranty untrue in a disclosure schedule to the purchase agreement. Failure to comply with applicable data protection laws or material contracts may have different impacts on a transaction depending on the type of transaction (i.e. an investment or an M&A transaction) as well as the nature and scope of the compliance gap.

Data Protection Considerations in Investment Transactions

Investors' data protection expectations typically vary depending on how early stage the company is. In Series Seed or Series A rounds, frequently the company has not had the resources to dedicate to data protection compliance. As a result, often there are compliance gaps that come up in due diligence and need to be disclosed in the disclosure schedule. By Series B and on, however, it is likely that investors will expect a more sophisticated approach to data protection. Occasionally, when the compliance gaps are significant enough or where the investor is particularly sophisticated (e.g., a strategic investor), the investor may impose covenants on the company in the Investor Rights Agreement (IRA) that puts the company on the clock to assess and achieve compliance targets within specified period of time. This effectively earmarks a portion of the investment proceeds that will have to be spent on data protection compliance, lest the company breach its IRA.

Data Protection Risks in M&A

Frequently the company is more mature by the time an M&A event comes up than in the investment context. Therefore, the buyer will often expect a higher level of sophistication of the target. Because the buyer will be taking control of the company and thereby assuming the company's liabilities following the closing, the buyer will often conduct a more robust due diligence process than in the investment context. Accordingly, the representations and warranties will typically be more fulsome and granular than in the investment context. And, unlike the investment context, the existing management team typically does not retain control of the company following closing of an M&A transaction. Therefore, in the event of material non-compliance, the buyer would typically address the issues through risk allocation strategies rather than covenants. These strategies may include requiring fundamental representations, special indemnities, special escrows, and limiting disclosures "for informational purposes only" (which means that the disclosure would function as a disclaimer of fraud with respect

to the issue disclosed, but not to a breach of the representation itself). From a seller's perspective, these can increase transaction costs, negatively affect the risk allocation, and delay the transaction. If compliance gaps are material enough, buyers may even revisit the purchase price, reducing the seller's upside.

If the company is not sophisticated from a data protection perspective, the buyer may have to invest a significant amount of time and capital post-closing to address the company's compliance gaps. Even if the company has considered data protection and has achieved some measure of compliance, integrations can still be challenging from a data protection perspective. For example, if the buyer is subject to a regulatory regime that the company is not, it may be necessary to keep data siloed between the company and the rest of the buyer's assets while the company becomes compliant with that regulatory regime. This may delay synergies that motivated the transaction in the first place.

Preparing for a Transaction

"*The best time to plant a tree was 20 years ago. The second-best time is now.*" If a company has not taken measures to comply with applicable privacy regimes in all areas of business in the past, now is the time to begin taking steps towards compliance. This could include engaging in a concept called "privacy by design," which means considering data protection from the beginning of the company (especially in each phase of product development). And any company anticipating a transaction should consider engaging data protection counsel and kick off the compliance process as early as possible prior to any corporate transaction. It typically takes several months to achieve material compliance with applicable data protection laws, depending on the regulatory regimes that may apply.

If you have questions about M&A or investment readiness from a data protection perspective, please contact Ryan J. Perry or any other member of Morse's privacy and data security team.

The author would like to acknowledge the contributions to this article by, and give thanks to, Monica Sax, Northeastern University School of Law (NUSL) 2022.