Lathrop GPM

LEGAL UPDATES

Data And Privacy Issues In M&A Transactions

Does your company handle personal data in the course of its business operations? In today's world, the answer is most likely yes. Nevertheless, many companies (particularly small to mid-sized), though aware of their compliance obligations under specific data protection laws, have put off implementing a comprehensive privacy and security program, often due to budgetary concerns or lack of resources.

06/10/2020 | 3 minute read

Does your company handle personal data in the course of its business operations? In today's world, the answer is most likely yes. Nevertheless, many companies (particularly small to mid-sized), though aware of their compliance obligations under specific data protection laws, have put off implementing a **comprehensive** privacy and security program, often due to budgetary concerns or lack of resources. Other companies, primarily in "brick and mortar" sectors, have often bypassed privacy compliance because it has traditionally been considered a "tech company" priority. However, in the context of merger and acquisition transactions – no matter the industry or sector – this can be a deal-breaker in certain circumstances, and target companies must understand that delaying compliance until it is pertinent to an M&A deal can impact their ability to close the transaction under the most favorable terms.

Compliance with applicable data protection laws has become increasingly critical to merger and acquisition transactions because where personal information is one of the main assets to be acquired it may end up being of little value if it cannot be used or leveraged by the buyer. Even where a seller is not subject to one of the more stringent privacy laws, such as the General Data Protection Regulation (GDPR), the California Consumer Privacy Act (CCPA) or any one of the sectoral laws (e.g., HIPAA), it likely must contend with a patchwork of federal and state laws that require companies collecting personal information to provide disclosures and secure the information at the very least. Conversely, buyers will want assurances that the personal information that they are acquiring is "clean", for lack of a better word. As such, having a privacy program in place will increase the chances of a successful transaction.

What does this mean in practice? A buyer will need to clearly understand what personal information the seller obtains, collects and discloses in the course of its business operations. More critically, the seller should be prepared to demonstrate **how** it has complied with applicable data protection laws, including, for instance, with respect to external-facing consumer disclosures. In addition, whether compliance by the target company has been ongoing or rather an eleventh-hour effort made only in the context of an exit strategy is a key question. Why is "longevity" important? Because if personal information has been collected and retained over the course of several years – and constitutes one of the main assets of the seller – but was **not** collected in a manner compliant with applicable data protection laws, there is a high degree of probability that it cannot be transferred to the buyer. While this is less of a concern for businesses that do not traditionally deal with personal data, it is helpful in optimizing a seller's value and mitigating risks to be cognizant of the laws that require compliance well before an exit. Of course, the buyer must also evaluate how it intends to use the personal information – as this may not be entirely consistent with past disclosures made by the seller – which may require additional opt-in requests from consumers to make such new uses. In other words, there are a number of moving pieces that must be properly addressed by privacy counsel on both sides of the transaction.

Buyers should include in both their representations and warranties, and due diligence questions, requests for information designed to assess a seller's privacy practices and policies and whether they comply with applicable laws. This should include:

- Identifying personal data flows, with respect to both online and offline data collection.
- Determining whether privacy policies (as updated periodically) that comply with applicable laws have been in place over time *and* reviewing the specific language for any potential impediments to a transfer.
- Ensuring that the target company has periodically assessed which privacy rules apply.
- Identifying the use of data through cloud or third party applications, as well as assessing all vendors or third parties that may have access to the personal data.
- Identifying the representations made to individuals and third parties regarding privacy and data security.
- Understanding the history of data breaches, if any, and the target company's current security policies and processes.
- Where applicable, ensuring that the target company has provided proper opt-ins or opt-outs for individuals.
- Understanding data retention policies.

Although this additional diligence around privacy may take more time and extend the timeframe for closing, it is becoming industry standard in M&A transactions and even financings. Depending on the outcome of the review and the value of the personal information, adjusting the purchase price may be a negotiation point.

M&A aside, the same issues can also affect a sale in bankruptcy, as we explained here, or disclosures that are made in the context of an IPO. In fact, risk factors set forth in S-1 statements increasingly focus on privacy risks. So what does this mean? Companies that collect and rely on personal information in the course of business can no longer gloss over privacy concerns in the context of M&A transactions, as this can affect the purchase price, the timeframe for closing the transaction, and the overall viability of a transaction.