



## Data Privacy Considerations in M&A Transactions

By: John Bradley and David Rosenfield, Troutman Sanders LLP

Data privacy regulations, high-profile data security breaches, and fines and other regulatory enforcement have significantly affected mergers and acquisitions (M&A) transactions in recent years. M&A participants are well-advised to focus on data privacy early and throughout an M&A transaction, given the potential adverse consequences of a security breach, which include reputational damage, fines and other regulatory enforcement, loss of business, class action lawsuits, and resulting damages.

### Legal Environment

Data privacy is implicated under numerous regulations. The Federal Trade Commission, for example, uses its general regulatory and enforcement authority to pursue actions in data security breaches. Some data privacy regulations, such as the EU General Data Protection Regulation (GDPR) and the most recently enacted significant data privacy regulation, the California Consumer Privacy Act (CCPA), which will take effect January 1, 2020, are specifically directed at data privacy, and impose, or will impose, extensive obligations on virtually all businesses within their geographic scope, most particularly in the context of consumer personal information. Industry-specific data privacy regulations such as the Gramm-Leach-Bliley Act (GLBA), which applies to financial institutions, and the Health Insurance Portability and Accountability Act (HIPAA), which applies to the healthcare industry, also impose extensive obligations on businesses that fall within the industries covered.

The overall trend in the data privacy legal environment is decidedly toward more onerous and complex compliance obligations, higher compliance costs, more frequent enforcement, and greater consequences for noncompliance.

### Commercial Environment

In addition to complying with data privacy regulations, businesses must comply with the terms of their commercial contracts pertaining to data privacy, which dictate how data that flows between contracting parties may be used, handled and stored. These commercial terms increasingly extend beyond customary nondisclosure obligations, and often include a litany of data privacy-related obligations, such as requiring specific data security processes, reporting and audit obligations, data security breach procedures and notification requirements, and special indemnities.

### Due Diligence

Buyers, sellers and M&A practitioners should approach data privacy diligence in the same way they approach similar critical M&A issues. This approach should include identifying the seller's key risks that flow from its industry, its geography, the types of data collected or obtained, and how that data is used, handled and stored. M&A participants also should ensure that the seller has the right to make available to the buyer and its representatives information of a sensitive nature, the disclosure of which may trigger violations of data privacy regulations or a breach of contract.

Due diligence should include examination of the seller's privacy policies, data security programs and processes, both qualitatively and from an information technology (IT) perspective, to ensure that appropriate processes and sufficiently robust IT assets are in place to protect data. A buyer should also evaluate the seller's breach history and response times. Buyers should engage a dedicated team of data privacy and IT experts to assist with this diligence.

Overall, the buyer's due diligence review should enable the buyer to assess data privacy risks associated with the seller's business and identify any outstanding or potential liabilities that may impact valuation or require special indemnities.

### Representations and Warranties, and Indemnities

M&A transactions involving businesses that handle sensitive data should employ carefully drafted data privacy representations and warranties. In addition to legal and commercial compliance, savvy buyers will use data privacy representations and warranties as a risk allocation tool to fix liability for failures of IT system design, poor information handling processes and even certain post-closing data privacy security breaches. Well-drafted, comprehensive data privacy representations and warranties should address at least the following areas, where applicable:

- ▶ General legal compliance (e.g., GDPR and, after January 1, 2020, CCPA compliance);
- ▶ Industry-specific data privacy regulatory compliance (e.g., GLBA or HIPAA compliance);

- ▶ Disclosure of arrangements under which data is shared with third parties;
- ▶ Data privacy security breach history;
- ▶ Regulatory notices, and both external and internal data privacy investigations;
- ▶ Suitability of data privacy processes and related IT infrastructure;
- ▶ Employee data privacy training;
- ▶ Description of the types of personal information collected and maintained; and
- ▶ Security assessment reports and related remediation of data security gaps.

In private-target M&A transactions, buyers may seek special line-item indemnities and longer survival periods for data privacy security breaches, whether known or unknown at the time of signing or closing. Data privacy issues in many M&A transactions are best handled on a customized basis depending on a variety of factors, including those discussed above.

### Post-Closing Integration

Post-closing integration may involve the mass transfer of data from the seller to the buyer, implicating numerous data privacy considerations. Even if personal information is not formally transferred, a buyer will have access to and may seek to obtain, handle and use the personal information held by the target company post-closing. A buyer should be mindful of the need to maintain strict controls on its access to, and handling and use of, personal information held by the target company. A post-closing integration plan developed concurrently with the due diligence phase of the M&A transaction is essential in situations in which data privacy is of particular concern. A buyer should charge its team of data privacy and IT experts engaged in the diligence process to work with the buyer's integration team to ensure regulatory compliance, appropriate regulatory and consumer notices, and other proper steps are taken to limit post-closing integration risks.

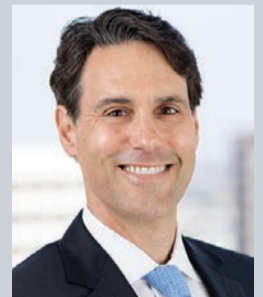
### Conclusion

The data privacy legal environment is developing rapidly, and the attendant risks and potential adverse consequences will impact M&A transactions for years to come. Data privacy should be among the critical M&A issues addressed early in and throughout an M&A transaction's life cycle, from structuring the deal to due diligence and documentation, and to post-closing integration. Buyers should engage a dedicated team of data privacy and IT experts to assist from the commencement of an acquisition transaction, and should keep them involved throughout the transaction and through post-closing integration.

**For more information about the legal developments affecting U.S. mergers & acquisitions, you may access a complimentary copy of Troutman Sanders' *M&A Perspectives* online at <https://online.flippingbook.com/view/701714/>**

#### John Bradley

John Bradley's two decades of experience and in-depth knowledge enable him to effectively represent public and private companies in a wide variety of corporate and securities matters. His practice includes representation in mergers and acquisitions on behalf of buyers and sellers; corporate governance and advising senior executives, directors, and public company boards and committees; periodic and other reporting under the Securities Exchange Act of 1934; debt and equity securities offerings, including registered public offerings under the Securities Act of 1933; venture capital financings; software licensing transactions; and drafting and negotiating a wide variety of business agreements. He also counsels clients on a broad range of other business-related matters.



#### David Rosenfield

David Rosenfield focuses his practice on the representation of public and private companies in connection with corporate governance, mergers and acquisitions, securities offerings, securities regulation, and general corporate law.

