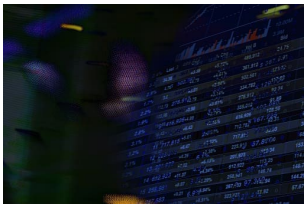

Data Privacy Concerns in Private Equity

Mar 01, 2020

Categories:

Blogs
Private Equity Industry Blog

Authors:

Craig J. Cox
Daniel A. Murray

Privacy, data security and data ownership issues are increasingly relevant for buyers in M&A transactions. This may result from the industry involved, the importance of data as a company asset, the use of data in the company's marketing and sales, or because the company's operations involve regulated data. Applicable laws include GDPR in Europe, CCPA for California, HIPAA for the United States, and PIPEDA for Canada.

Data issues should be a primary concern for buyers, both when conducting due diligence into a target company and when documenting the sale with appropriate representations and warranties and indemnity provisions. Failure to properly address these issues in an acquisition could subject the buyer to private causes of action from customers and other individuals and to action from regulators.

Due Diligence Concerns

Disclosure requests should address several key areas. Buyers need to understand a target's treatment of regulated data such as health data, financial data, customer personal data, and data related to minors. Buyers should learn how companies interact with both customers and vendors.

Contracts with Data Subjects

Buyers need to understand a company's privacy policies and contractual obligations related to customers. What kind of consent has been obtained from customers? Does the consent cover the types of activities that the buyer will engage in? The results of these analyses may impact the valuation of any deal. Remember, even if customer data isn't at issue, data privacy laws may apply to employee data.

Post-acquisition, buyers may need to provide notification to, or obtain additional consents from, data subjects. Note what laws

FBT Gibbons

apply and what further consent is needed. If the acquisition is confidential, consent from customers will have to wait until the deal is completed.

Contracts with Vendors

Also relevant are contracts with suppliers that may collect or store data on behalf of the company, as well as any contracts the company may have to collect, process or store customer data for. Buyers should investigate a target's security procedures and history of breaches. Does the company use third parties to perform security or vulnerability assessments or data audits? How does the company manage its network and data? Remember that one vendor is the data room provider. The parties will want to ensure that the data room provider complies with applicable law. Certain data may need to be protected from disclosure during the acquisition process. Pseudonymization or anonymization of personal data may be necessary.

Reps & Warranties

Representations and warranties can determine the target's compliance and track record under applicable laws. This includes having the target confirm that they have established policies to comply with applicable data privacy and security laws and best practices. Also, confirm any security breaches, audits, or governmental investigations relating to data privacy and security that involve the target. Buyers should require the target to identify every jurisdiction for which the target possesses protected data.

Indemnification

Do your best to apportion risk of data privacy non-compliance. However, some laws, such as GDPR, may limit the extent to which apportionment can remove risk to either party. Seek appropriate insurance coverage when possible.

Learn more about Frost Brown Todd's Privacy & Data Security team.

FBT Gibbons

FBT Gibbons