Hashed & Salted | A Privacy and Data Security Update
February 2022

Data Privacy and Security Considerations in M&A Transactions

Over the past decade, attention to privacy and cybersecurity due diligence in merger and acquisition (M&A) transactions has drastically increased. Gone are the days of assuming that privacy and cybersecurity regulations impact only companies operating within the technology and innovation sectors. Today, any company that collects personal information—even minimal information like name, username, age and password, or even just device identifiers—about its customers, clients, employees, business representatives and users may be subject to data privacy and security regulations in the U.S. and around the world. A seller's compliance with applicable data privacy and security regulations can be pivotal and at times a deal breaker for certain M&A transactions, especially when the personal information collected by the seller is one of the main assets being acquired by a potential buyer.

Even in circumstances where the personal information collected by the seller is not the main asset being acquired by the buyer, as more and more states as well as countries around the world are working to adopt and implement data privacy and security regulations, privacy and cybersecurity due diligence may be an essential part of the diligence process in M&A transactions. Although a seller may not be subject to some of the more comprehensive privacy laws, like the European Union General Data Protection Regulation (GDPR), the California Consumer Privacy Act (CCPA), the California Privacy Rights Act (CPRA), or the Health Insurance Portability and Accountability Act of 1996 (HIPAA), companies still may be subject to a variety of international, federal, and state privacy and data security regulations that affect their day-to-day operations.

Both the buyer and the seller should be aware of data privacy and security considerations that they may encounter during an M&A transaction.

The Virtual Data Room

Often during the due diligence process and in the early stages of M&A transactions (i.e., negotiation of a letter of intent or a term sheet), the parties may share certain information relating to clients, suppliers, vendors and key employees. First and foremost, to the extent such information includes personal information or other sensitive data, the seller should ensure it has the necessary consents and approvals to disclose such information to the buyer. In addition, the sharing of this information should be subject to appropriate nondisclosure agreements and disclosed via a secure method—for example, an encrypted virtual data room (VDR)—that allows limited and controlled access. To the extent that the seller can limit the sharing of personal information, it should do so, by limiting disclosures to the buyer to what is actually necessary and needed by the buyer to evaluate its business operations. For example,

Attorney Advertising

instead of sharing with the buyer all employment agreements, which may include employee personal information, the seller should consider sharing its generally used template employment agreement with the buyer.

As data privacy and security laws and regulations are changing, to the extent that these laws extend protections to residents of a particular state or country in their capacities as employees and business representatives (such as the CPRA will do, once effective as of January 1, 2023), the seller should also contemplate in its nondisclosure agreements with the buyer, and in its agreements with the company, hosting the VDR provisions providing assistance with responding to requests from customers, employees, and business representatives regarding the use and disclosure of their personal information.

Data Privacy and Security Due Diligence

During the due diligence phase of the M&A transaction, the buyer is seeking to obtain information regarding the seller's business operations, which may include information about the seller's IT systems, employee and consumer information; vendor management processes; and financial information. With respect to data privacy and security due diligence, the buyer needs to understand and evaluate what and how personal information is collected, stored, used and disclosed by the seller. Most importantly, the buyer needs to understand and the seller should be able to demonstrate how it has complied with applicable data privacy and security laws (e.g., updating its privacy policy from time to time to comply with changes to or the adoption of new data privacy and security regulations). The potential buyer should ask due diligence questions and seek information from the seller that is designed to:

- **Identify what personal information is collected by the seller.** The buyer should understand the extent to which the seller collects, stores, uses, discloses or otherwise processes personal information, including from whom the personal information is collected (including website and mobile app visitors, customers, employees and business representatives); the nature of the personal information being collected; and the countries where the collection, storage, disclosure or other processing of personal information occurs.
- **Identify the flow of personal information with respect to both online and offline data collection**. The buyer should understand, whether via data flow charts or other materials, how the personal information flows within and outside the seller's organization, both online and offline.
- **Evaluate the seller's privacy policies and other disclosures across all media platforms**. The buyer should evaluate whether the seller's privacy policies and related disclosures appear to comply with applicable laws and best industry practices and adequately disclose how the seller collects, uses, stores and discloses personal information. Note that depending on the seller's industry and the states/countries in which its business operates, there may be industry-specific and/or location-specific privacy and data security laws and regulations applicable to the seller's business. In addition, where applicable, the buyer should seek to determine how the seller has provided privacy choices to individuals from whom it collects personal information and/or obtained any necessary consent in order to process such information and/or share such information with third parties.
- **Evaluate the existence of information security policies and procedures**. In addition to reviewing privacy policies and disclosures, the buyer should review the seller's information security policies and procedures to determine whether the seller has appropriate procedures in place to address its handling and use of the personal information collected. This may include review of policies and procedures that address (i) data encryption, (ii) employee remote-working arrangements, (iii) access to and control of personal information, (iv) business recovery and continuity, (v) data breach and security incident response, and (vi) data retention. The buyer may also want to review the results of any audits conducted of the seller's information security safeguards and procedures.
- **Assess the steps that the seller has taken to comply with applicable privacy laws**. The buyer should review and ask the seller to provide information that allows the buyer to evaluate the steps that the seller has taken to comply with the privacy laws applicable to its business. This includes requesting and reviewing the seller's data maps, records of processing

activities and any other data assessments prepared by or for the seller. Understanding the steps that the seller has taken to comply with the privacy laws applicable to its business, including the steps the seller has taken to operationalize applicable privacy requirements, will help the buyer assess any material data privacy and security risks posed by the seller's business operations. In addition, the buyer can better identify any steps that it will need to take post-closing to either (i) close any gaps in the seller's compliance with the privacy laws applicable to its business or (ii) help determine how to integrate the seller's business operations into the buyer's business processes.

- **Identify the representations made to individuals and third parties regarding the privacy and security of their personal information**. The buyer should seek to determine whether the disclosures made to individuals and third parties regarding the collection, use and disclosure of personal information in the seller's privacy policy and other privacy-related disclosures and agreements accurately reflect the way such information is collected, used and disclosed by the seller. This evaluation should include determination of whether the seller can share such personal information with the buyer. The buyer should take steps to avoid assuming liabilities once the transaction is consummated in connection with any personal information shared with it during the due diligence process.
- **Assess all vendors or third parties that may have access to personal information collected by the seller**. The buyer should evaluate the seller's vendor management and risk procedures, as well as any third-party agreements, to determine whether appropriate safeguards and agreements are in place to the extent the seller shares with its vendors and other third parties any personal information it receives.
- **Understand the history of data breaches and security incidents**. The buyer should be informed of any data breaches or security incidents, even if they did not rise to the level of a notifiable breach. To the extent the seller has had any data breaches and/or security incidents, the buyer should ask for information relating to how such data breach was handled, including any and all remedial actions taken after the breach and/or incident has been resolved. In addition, it is important for the buyer to ask the seller to identify any past, threatened or pending litigation, complaints, regulatory inquiries, administrative fines or penalties relating to any data breaches, security incidents or seller's privacy practices, and to explain how these matters were addressed and/or resolved.

Note that depending on the outcome of the review and the value of any personal data being transferred to the buyer, adjusting the purchase price may be the subject of further negotiations between the buyer and the seller.

Negotiating the Purchasing/ Acquisition Agreement

In addition to conducting data privacy and security due diligence, the buyer should include certain representations and warranties in the actual purchasing/ acquiring agreement (e.g., the stock purchase agreement) related to the seller's data security and privacy practices. Such representations and warranties may relate to (1) the seller's compliance with applicable data privacy and security laws and/or (2) pending or threatened data privacy claims and/or litigation against it. The buyer may also seek indemnification for third-party claims that arise due to the seller's failure to comply with applicable data privacy and security regulations and/or its own privacy policies, notices and related disclosures. The seller should seek to ensure that it has not made any representation and warranties that are not true, and it should limit in an appropriate manner indemnification rights granted to the buyer.

Post-Signing/Closing

By properly assessing and managing data privacy and cybersecurity concerns during the due diligence phase of the M&A process, the buyer can better ascertain what should be done post-closing or post-signing to allow for the legal transfer of personal data. Whether it requires the buyer and the seller to enter into transition service agreements or the buyer to update and revise its own privacy policies due to statements made in the privacy policies and disclosures of the seller, taking the time necessary to adequately perform data privacy and security due diligence helps prevent avoidable losses and the imposition of penalties and fines on the buyer. The buyer should allocate time and create realistic times frames for due diligence to assess the risks posed by the seller's privacy and data security infrastructure, even in instances where the personal information collected by the seller is not the main asset being acquired by the buyer.

Related Professionals

Tanya Forsheit . . . . . tforsheit@loeb.com
Jessica B. Lee . . . . . jblee@loeb.com
Bianca Lewis . . . . . blewis@loeb.com

This is a publication of Loeb & Loeb and is intended to provide information on recent legal developments. This publication does not create or continue an attorney client relationship nor should it be construed as legal advice or an opinion on specific situations.

© 2022 Loeb & Loeb LLP. All rights reserved.

6867 REV1 02-15-2022