KEYNOTE INTERVIEW

Rethinking data privacy

The private equity industry is aware that regulatory risks can affect the approval, success and profitability of an investment. EisnerAmper's Louis Bruno and data risk expert Matthew Bernstein discuss data privacy and how to manage the risks

Investors are aware of cybersecurity concerns and the need to protect data, but the risks associated with data have expanded as regulators are focused on data privacy and how companies collect, use and share personally identifiable information (PII).

Compliance is challenging in today's environment, where massive amounts of data, commoditised technology infrastructure and presumed value to be extracted create incentives to keep, store and process everything. Firms that identify data privacy risks as part of the due diligence process and take the necessary steps to comply with the regulations will protect their investment and help ensure attractive exit opportunities.

New data privacy laws passed in the EU and California require that GPs not only safeguard data but know what data they possess, which requires a kind of due diligence that many firms might not be doing. Private equity firms not only have to make certain that they, as a firm, comply, but that their portfolio companies do as well.

SPONSOR
EISNERAMPER

To understand these new obligations and how to meet them, we sat down with Louis Bruno, principal at EisnerAmper, and Matthew Bernstein, who has over 20 years of experience working with major organisations on information management standards and solutions.

Q What are the key new regulations surrounding data privacy for private equity?

LB: Protecting an individual's rights to privacy continues to be a focus of lawmakers across the globe as evidenced by the European General Data Protection Regulation, the state of California's Consumer Privacy Act, draft US federal legislation and the increasing public attention to the use of data. In addition, in the US, the SEC's Office of Compliance Inspections and Examinations issued a recent alert regarding compliance with Regulation S-P, the primary SEC rule regarding data privacy notices and safeguarding policies of investment advisors and broker-dealers.

MB: In addition, and of particular concern to PE firms, the US Treasury's Committee on Foreign Investment in the United States reviews sales to foreign entities, and now requires the consideration of personal data. If a transaction contemplates a sale to a foreign buyer, CFIUS can potentially prohibit transactions where the target firm possesses "personally identifiable information".

PE firms must assess the extent of retained PII, a counterparty's geopolitical relationship with the US, and the potential remedies when determining a buyer's qualifications. CFIUS raises the stakes for PE firms to reduce the type and scope of PII.

Q Given those new obligations, where are the risks?

LB: Compliance is certainly challenging. Although many organisations have established certain information-risk policies and mitigated some of these risks, typically with a cybersecurity programme, other risks remain unaddressed. Firms must be able to determine their obligations, identify their data, update policies and implement new procedures to accurately mitigate the risks.

MB: There are massive amounts of available data out there, but the risks associated with not governing these data are growing. Companies are more and more reliant on finding value in their data, while at the same time the public, regulators, and politicians are increasing their scrutiny of how companies use consumers' data.

Given the global focus on an individual's right to privacy, PE managers need to realise that the reputational impact associated with non-compliance can cripple a business and outweigh any regulatory fine. That reputational impact may even interfere with the successful exit of a portfolio company.

LB: Private equity firms should also be aware that data privacy risks are not limited to companies in the technology sector or those which process large volumes of sensitive PII, such as in healthcare. Businesses outside data-heavy industries may harbour hidden risks as they will have PII that has been collected over time, which may not be easily identifiable, and for which the necessary marketing and use consents are missing. In many cases, firms are not fully aware of all their business processes that capture PII and where it is stored internally.

Q Most firms employ third parties to manage data, so could those service providers pose risks as well?

MB: This is my biggest concern. The increasing trend of 'externalisation' and outsourcing of data management poses a challenge to PE firms, given the diversity of systems and applications used by portfolio companies. Identifying third-party risks is challenging because almost every widely used communication, processing and storage platform operates outside the four walls of the company.

Portfolio companies are likely to use tools like Box, Slack, LinkedIn and Twitter to communicate both internally and externally. Enterprise management solutions like Salesforce and Workday, and cloud providers like AWS, Microsoft Azure and Google Cloud are the platforms of choice for fast developing companies.

The PE firm also will bear responsibility for the management of these data, regardless of the fact that the data are external. Awareness of, and responsibility for, these data privacy risks cannot be outsourced.

LB: There's an obligation to ensure vendors are aware of and comply with relevant regulations. Service providers, especially those serving commerce generally rather than financial services firms in particular, are typically unaware of the regulations and not acting on their own to develop and implement these policies.

Solutions and services may provide safeguards and make functionality available, but it is up to the user firm to determine the rules it is subject to, identify its data subject to those rules, instruct the system or service provider to act on those rules, and ensure adherence. Safeguarding personal data is a core tenet of all data privacy laws and regulations, and the potential for a breach may be greater where the portfolio company does not directly manage its data. ■

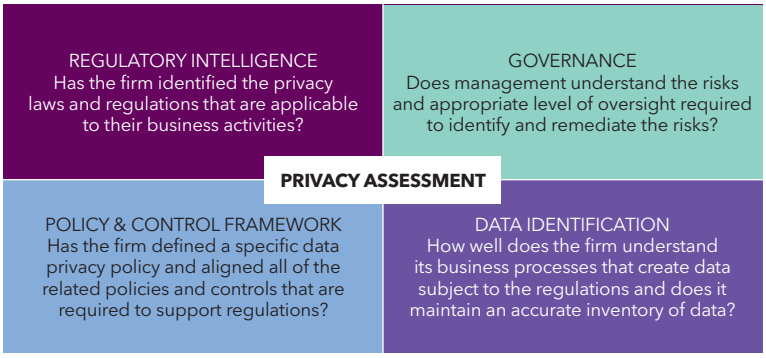
Q So how should GPs look at identifying and managing those risks?

LB: Addressing these risks involves a broader effort than just assessing a firm's cybersecurity risks; the due diligence process must identify specific data privacy risks. In addition to obvious customer-related privacy policies, an acquisition target will need to have appropriate policies covering the personal data of its employees, and much more detailed contracts with third-party processors than in the past.

In addition, firms must be able to demonstrate compliance to regulators, which requires adequate management oversight and expanded internal procedures. Increased documentation of how and why data is captured, defined processing activities, and procedures for responding to data subject access requests will be necessary. The potential vulnerabilities to data breaches will need to be identified and appropriate procedures for data breach notification and internal training implemented.

MB: To assess and quantify these risks in an acquisition target, expanded due diligence will be required. Are the appropriate technical and organisational measures in place to comply with the regulations, particularly with respect to the security and management of personal data? Are there historical compliance gaps, including data breaches?

These should be identified as part of the due diligence process, and post-acquisition remedial plans and allocation of liability for their associated costs should be defined early in the deal process. Warranties and indemnities are likely to be much more keenly negotiated, given the potential liabilities, and understanding the technical and business fundamentals will be a critical part of this process.



Louis Bruno is a principal in EisnerAmper's global compliance and regulatory practice. He assists investment advisors, wealth managers and banks with strategic data and regulatory compliance-driven initiatives.

Matthew Bernstein led information practices in various financial services businesses at Deutsche Bank for more than 20 years. He works with firms to define, develop and operationalise information risk management standards and technology solutions.