Vendor Management: A Critical Component of Privacy Compliance

Jacqueline Klosek and Kendrick Nguyen

Engaging external vendors to perform business functions can benefit organizations in a wide range of ways, including by improving efficiency and reducing costs. At the same time, however, contracting with external vendors for projects that will involve access to personally identifiable data of employees, customers, clients and other individuals (collectively, personal data) can involve substantial risks that can leave the enterprise exposed to potential liability.

Companies of all sizes, industries and geographic locations increasingly are subject to a host of complex requirements regarding personal data privacy and security. In addition to such legal obligations, data subjects, including consumers and employees, are progressively more concerned about the privacy and security of their personal data. Such obligations must be taken into account in connection with internal business operations and, even more significantly, when contracting with third-party vendors.

In light of the foregoing, this article will explore some of the most significant privacy and security risks that may be implicated by providing external vendors with access to personal data. It will also examine key strategies to minimize the risks that may be associated with such arrangements.

Risk Management Strategies:

Counteracting the risks posed by engaging vendors to provide services will involve a concerted plan of due diligence, coupled with effective contract management.

Due Diligence Strategies for Effective Vendor Management

There are a number of steps that should be taken to reduce risks of providing a third-party vendor with access to personal data. In particular, the following suggestions are recommended:

- Conduct an internal privacy audit to obtain a thorough understanding of the scope and depth of processing activities that will fall within the responsibilities of the vendor.

- Identify reasonable foreseeable internal and external risks to the security, confidentiality and integrity of customer information against unauthorized disclosure, misuse, alteration, destruction or other compromise of such information, and assess any safeguards in place to control such risks.

- Conduct thorough due diligence into the vendor's experience, and the experience of any subcontractor, with privacy and data security, including by investigating (i) Any privacy complaints and investigations that may have arisen with the context of servicing other clients; (ii) The means and methods use by the service provider to protect its clients data; and (iii) The service provider's privacy and security policies.

- Obtain a thorough understanding of the data protection laws in force in the host country and, (i) If adequate, require the vendor to warrant to comply with those laws; and (ii) If inadequate, require the service provider to warrant that it will comply with more stringent privacy and security requirements.

- Conduct an internal data audit in effort to obtain complete knowledge of the data that will be transferred to the vendor.

- Where overseas transfers will be required, ensure that all necessary prerequisites for the transfer have been undertaken.

- Review all vendor and subcontractor contracts to ensure sufficient compliance with the company's internal information security and privacy programs.

Jacqueline Klosek

Kendrick Nguyen

Negotiating a Vendor Contract

Negotiating a contract with proper security and privacy provisions is an essential part of vendor management. A vendor contract should contain certain privacy, security and transferability provisions to safeguard sensitive data over which vendors would have control. A company also may want to include provisions prohibiting or limiting a vendor from providing a subcontractor access to the company's personal data.

There are key clauses that should be considered for inclusion in a contract with a vendor that will have access to personal data. The clauses are general provisions that should be considered for inclusion in contracts that involve service

provider access to a company's confidential, proprietary or otherwise sensitive data. Of course, certain legislation, including, notably, the Health Insurance Portability and Accountability Act of 1996, together with its regulations, and the Gramm-Leach-Bliley Act, and its rules, impose specific requirements that must be included in vendor contracts. Where specific regulatory issues are involved, these clauses must be revised to address the specific requirements of the applicable regulations. These key clauses are:

- Control of Company Data
  As between vendor and company, all company data is, and shall remain, the company's exclusive property. If the company requests, the vendor shall promptly retrieve and deliver to the company a copy of all company data, or such portions as may be specified by the company, under the vendor's control or in its possession, in an industry standard format and on the media as agreed by the parties, at any time, upon the company's request. At any time, the company may request, in writing, that the vendor destroy or erase all copies of the company data under the vendor's control or in its possession, and the vendor shall comply with all such requests. Under no circumstances shall the vendor withhold any company data. Notwithstanding any other provision in this agreement, the vendor shall not possess or assert any lien against or to company data.

- Privacy Requirements
  The vendor agrees that (i) It shall not use any company data except to the extent necessary to carry out its obligations under the agreement; (ii) It shall not disclose company data to any third party, including, without limitation, its third-party service providers without the company's prior written consent and an agreement in writing from the third party to use or disclose company data; (iii) It shall maintain, and shall require all third parties approved under subsection (ii) To maintain, effective information security measures to protect company data from unauthorized disclosure or use, and (iv) It shall provide the company with information regarding such security measures upon the company's reasonable request and promptly provide the company with information regarding any failure of such security measures or any security breach related to company data.

- Compliance with Privacy Regulations and Policies
  The vendor represents and warrants that its collection, use and disclosure of company data is, and will at all times, be conducted in full compliance with the company's then-applicable privacy policies, and with all applicable data protection and/or privacy laws, rules and/or regulations.

- Safeguarding Company Data
  The vendor shall maintain adequate administrative, technical and procedural access controls and system security requirements and devices necessary to protect all company data from threats or hazards: (i) To the privacy, confidentiality or integrity of the data, (ii) From unauthorized or unauthenticated access to the data, and (iii) Viruses. To the extent that the vendor's affiliates or other agents or contractors have access to the company data, the vendor shall maintain agreements with such entities consistent with the requirements of this agreement and that require such entities to adequately protect the confidentiality of company data and comply with all terms and conditions of this agreement related to the company data. Company data only will be disclosed to third parties as specifically authorized by the terms of this agreement.

- Security and Protection
  The vendor will maintain adequate, commercially available environmental, safety, facility procedures, data security procedures, and other safeguards against the disclosure, destruction, loss or alteration of all company data in the possession or under the control of the vendor. The vendor will immediately notify the company in writing in the event of any actual or attempted unauthorized access to or use of any company data or any facilities associated therewith, the extent of any such intrusion and how the company was affected. The vendor shall cooperate fully with the company's investigation and respond to each actual and attempted security breach. The vendor will not, and will ensure that, its personnel do not, break, bypass, or circumvent, or attempt to break, bypass or circumvent, any security system of the company or obtain, or attempt to obtain, unauthorized access to any company data or other confidential information. The vendor shall provide the company with a complete back-up of all company data on a regular basis, as requested by company, but no less frequently than once per week.

- Indemnification
  The vendor agrees to defend, indemnify and hold the company harmless for any disclosure, or any breach of privacy or security, of any company data under the vendor's control, possession or management. In the event the vendor chooses to disclose company data to any third party or subcontractor, having obtained the prior written consent of the company and an agreement in writing from the third party to use or disclose company data as required under the agreement, the vendor agrees to remain contractually liable for the functions that are subcontracted. Furthermore, the vendor agrees to defend, indemnify and hold the company harmless for any acts and omissions of any third party to whom the vendor discloses company data.

Ensure That You Have an Exit Plan

While the vendor management strategies outlined may help to reduce some of the most significant privacy and security risks, clearly notwithstanding the contents of the underlying agreement, the vendor may, for one reason or another, intentionally or inadvertently, breach

*See **Vendor Management,** page 11*

continued from page 9

the requirements of the agreement in such a way that it becomes incumbent upon the company to terminate the relationship. Of course, other factors may lead to the termination of the business relationship. For all of these reasons, it will be extremely important to have an effective exit strategy before it is actually needed. Such exit strategies should, among other things, provide for an effective mechanism for obtaining control of all personal data provided or made available to the vendor.

Conclusion

Safeguarding personal data is a major concern for most businesses. When a company turns to outside vendors to handle business functions, it is essential that the company take appropriate steps to protect the security and the privacy of the personal data provided or made available to the external vendors. The importance of negotiating proper data protection clauses into the agreement with the vendor cannot be overstated. Together with the vigilant application of internal privacy and security policies, proper vendor management can help companies to maintain the trust of its customers, protect valuable proprietary information and avoid potential civil liability that arises from security and privacy breaches.

Jacqueline Klosek, CIPP, is a Senior Associate with Goodwin | Procter LLP and a CIPP. She is co-chair of the IAPP International Working Group. She is the author of The Legal Guide to e-Business (Praeger, 2003), Data Privacy in the Information Age (Greenwood, 2000) and the forthcoming, War on Privacy. She may be reached at jklosek@goodwinprocter.com.

Kendrick Nguyen is an Associate with Goodwin | Procter LLP. He may be reached for comment at: knguyen@goodwinprocter.com.