The Metropolitan
Corporate Counsel®

www.metrocorpcounsel.com

Volume 15, No. 3 March 2007

The Case For Factoring Data Privacy And Security Considerations Into A Company's Outsourcing Strategy

Jacqueline Klosek and Andrew Lurié

GOODWIN PROCTER LLP

Not too long ago, offshore outsourcing was viewed as being very risky from a reputation and image perspective. Today, however, offshore outsourcing has become standard fare for many companies and its prevalence continues to grow, with work being sent not only to traditional destinations like India and China but also to newer locations like the Philippines, the Czech Republic, Poland and Mexico with increasing frequency. As companies become more comfortable in their reliance upon offshore outsourcing, they must continue to guard against its often overlooked – but substantial – inherent privacy risks.

Companies that collect, store, use and otherwise process personally identifiable data ("PID") are often subject to a wide range of contractual, legislative and regulatory requirements that impact their rights and obligations with respect to such PID. Furthermore, companies in certain industries, such as health care and financial services, are subject to even more stringent requirements. While universally viewed as an onerous task, complying with such requirements becomes even more complicated when one or more business functions are outsourced to an offshore service provider, especially when such outsourcing involves transferring PID overseas.

In light of the foregoing, this article will explore some of the most significant privacy requirements that may be implicated by offshore outsourcing arrangements, as well as several key strategies for minimizing the associated risks.

Privacy And Security Requirements

Companies of all sizes, industries, and geographic locations are increasingly subject to a host of complex requirements regarding PID privacy and security. Such obligations become even more critical when the company is engaged in outsourcing, especially overseas, where there may be less actual control over the service provider and where the legal and regulatory environment impacting the service provider will be different.

Privacy laws can impact the very ability of companies to transfer data across national borders. In the EU, for example, comprehensive data protection laws limit the ability of entities to transfer PID out of the EU unless the country of destination either provides "adequate" protection to PID or has another compliance solution in place.[1]

While the EU data protection legislation has garnered much of the attention for its stringent and comprehensive requirements, one must not overlook the growing number of U.S. privacy laws that must be considered when entering into an outsourcing relationship in which PID will be transferred to an offshore service provider. Although U.S. privacy legislation does not yet comprehensively apply to all types of PID, the existing individual laws, while limited in scope, greatly affect the collection and use of certain types of PID.

The Health Insurance Portability and Accountability Act of 1996 and the regulations issued pursuant thereto (collectively, "HIPAA")[2] governs the privacy and security of certain types of health-related PID,[3] regulating health plans, health care providers, and health care clearinghouses (collectively, "Covered Entities"). Among its many requirements, HIPAA establishes strict controls regarding the use and disclosure of health-related PID and requires Covered Entities to create and distribute privacy policies explaining such use and disclosure.

While HIPAA's requirements apply specifically to Covered Entities, HIPAA can impact other businesses because it requires Covered Entities to execute Business Associate Agreements with all third party service providers that it will provide with access to health-related PID. This requirement is likely to be of particular importance within the context of outsourcing transactions.

For financial institutions,[4] Subtitle A of Title V[5] of the Gramm-Leach-Bliley Act ("GLB Act")[6] is of chief importance, for it generally restricts such institutions' ability to disclose a customer's financial PID to non-affiliated third parties. The GLB Act also obliges financial institutions to inform their customers about their information-collection and information-sharing practices and, in most cases, to provide customers the opportunity to "opt out" of

***Jacqueline Klosek** is Senior Counsel at Goodwin Procter LLP. She is the author of* War on Privacy *(Praeger, 2006);* The Legal Guide to e-Business *(Praeger, 2003); and* Data Privacy in the Information Age *(Greenwood, 2000). **Andrew Lurié** is an Associate with Goodwin Procter LLP.*

Please email the authors at jklosek@goodwinprocter.com or alurie@goodwinprocter.com with questions about this article.

having their information shared with non-affiliated third parties.

Particularly important to the outsourcing equation, the GLB Act requires the FTC and certain other federal agencies to establish standards with which financial institutions must comply in order to protect the security of their customers' PID. Furthermore, the FTC has issued a rule[7] requiring each financial institution to develop, implement, maintain, and continually update a comprehensive information security program involving administrative, technical, and physical safeguards. As part of such program, each financial institution must perform a security audit to identify internal and external risks to the security of customer PID and assess the sufficiency of any current safeguards. Additionally, and most likely to impact offshore outsourcers, financial institutions must assure that all contractors or service providers that they engage are capable of maintaining appropriate safeguards for the customer PID and require them, by contract, to implement and maintain such safeguards.

Apart from the GLB Act, financial institutions engaging in outsourcing must also be mindful of other recommendations and advisory documents. Significant in this regard are the recommendations issued by the Joint Forum of the Basel Committee on Banking Supervision, International Organisation of Securities Commissions (IOSCO), and the International Association of Insurance Supervisors. These guidelines recommend that a firm's senior management should remain responsible for all activities that are outsourced and emphasize establishing a coherent policy for risk management by (i) drawing up comprehensive and clear outsourcing policies; (ii) negotiating appropriate outsourcing contracts; and (iii) analyzing the financial and infrastructure resources of the service provider.

While the federal data privacy laws examined in the previous sections are among the most relevant, a number of other existing data laws can impact a company's outsourcing services to an offshore service provider, including a growing body of state and foreign laws concerning privacy and data protection. Companies engaged in outsourcing or contemplating a prospective outsourcing relationship must continuously monitor this evolving legal and regulatory environment, as such requirements can have an impact not only on the company's own activities but also on the activities that it is outsourcing.

Risk Management Strategies

Get to Know the Players in the Outsourcing Relationship

In order to help to reduce the above-mentioned privacy risks associated with offshore outsourcing, it is recommended that the company controlling the PID and engaging the service provider:

• Conduct an internal privacy and data audit to understand PID processing activities within the organization and to obtain complete knowledge of the PID that will be transferred to the service provider.

• Conduct thorough due diligence into every service provider's experience with privacy and data security, including by investigating (i) any privacy complaints that have arisen through servicing other clients; (ii) how the service provider protects its clients' PID; 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 service provider to warrant compliance with those laws; and (ii) if inadequate, require the service provider to warrant compliance with more stringent privacy and security requirements.

• Ensure that you have complied with all necessary prerequisites for transferring PID to the overseas service provider, including without limitation, obtaining all required data subject consents.

Control The Service Provider's Ability To Subcontract

As part of controlling the risks raised by a service provider in the context of an outsourcing relationship, a company should strive to place limits on the ability of such service provider to subcontract the services. Conducting thorough due diligence on the service provider is not likely to be of much value if the service provider is allowed to subcontract to other, perhaps less security-conscious service providers without restriction. Because properly drafted contractual measures can reduce these risks, the outsourcing agreement should do one or more of the following:

• Prohibit the service provider from subcontracting without the outsourcing company's prior written consent in each instance. When considering consenting to a subcontractor, the outsourcing company should conduct adequate due diligence of each subcontractor.

• Require the service provider to remain contractually liable for the functions that are subcontracted and require the service provider to defend, indemnify, and hold the outsourcing company harmless from the acts and omissions of the subcontractor.

• Retain the outsourcing company's right to review the terms of all subcontracting agreements and/or require the service provider to include certain mandatory provisions in all subcontracting agreements, including, for instance, provisions regarding data privacy and security, confidentiality, and intellectual property ownership.

Ensure That A Viable Exit Strategy Is In Place

Irrespective of how advantageous the outsourcing relationship is, it is likely that, at some point, the relationship will come to an end. The proper time for contemplating the end of the relationship is when negotiating the underlying services agreement that will govern the relationship. It is incumbent upon the company to have a viable exit strategy in place so that the company will be able to quickly take control of its PID and/or transfer the same to a successor provider.

Conclusion

As long as offshore outsourcing continues to offer business advantages, companies of all sizes and from a variety of industries are likely to continue to incorporate it into their overall business strategy. While outsourcing can be accompanied by significant risks, particularly in the areas of privacy and data protection, the above risk management techniques can help to decrease the likelihood of privacy violations, thereby increasing the likelihood that the outsourcing relationship will be a positive and productive one.

---

[1] *At present, only a very limited number of countries have been deemed to provide "adequate" data protection for the purposes of EU data protection laws.*

[2] *Public Law 104-109*

[3] *[I]nformation that is a subset of health information, including demographic information collected from an individual, and (1) is created or received by a health care provider, health plan, employer, or health care clearinghouse; and (2) relates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual; and (i) that identifies the individual; or (ii) with respect to which there is a reasonable basis to believe the information can be used to identify the individual. 45 C.F.R. 164.501 (Definitions).*

[4] *Any institution the business of which is engaging in financial activities as described in section 4(k) of the Bank Holding Company Act (12 U.S.C. § 1843(k)).*

[5] *15 U.S.C. § 6801-6810.*

[6] *Statute* (Public Law 106-102, 15 U.S.C. § 6801, et seq.).

[7] *FTC, Standards for Safeguarding Customer Information, Final Rule, 16 C.F.R. 314 (2002).*