BNA International

World Data Protection Report

International Information for International Businesses

Monthly news and analysis of data protection and privacy issues from around the world

Managing your data processors: legal requirements and practical solutions

Peggy Eisenhauer
Privacy & Information Management Services

This article has been published in the August 2007 issue of BNAI's World Data Protection Report

www.bnai.com

BNA International Inc., a subsidiary of The Bureau of National Affairs, Inc., Washington, D.C., U.S.A.

UNITED STATES

Managing your data processors: legal requirements and practical solutions

Margaret P. Eisenhauer[1] is the founder of Privacy & Information Management Services – Margaret P. Eisenhauer, P.C., a full-service privacy, security and information management law firm. If you have any questions or comments about this article or third party data processing standards generally, please do not hesitate to contact Peggy Eisenhauer at 404-914-1163 or via email to peggy@privacystudio.com

Companies are increasingly subject to fiduciary-like duties with regard to sensitive personal information. These duties include protecting the information with reasonable security measures, preventing misuse of the information (such as uses outside of a privacy notice), and notifying individuals of security breaches. The duties mandate both internal controls and oversight of data processors.

While information security is often perceived as a "U.S. issue" due to the publicity over security breaches in this country, the obligation to secure personal information appropriately and to manage third party data processors is truly global.

This article explores some of the regulations and regulatory actions that have created security obligations and offers some practical advice for managing the risks associated with third party data processors. It does not attempt to provide a comprehensive statement of any set of security requirements or solutions.[2]

U.S. security requirements

An array of U.S. laws imposes requirements on companies to protect personal information. At the Federal level, privacy and security regulations historically tied to uses of personal information (such as credit reporting). More recently, laws have been passed to regulate the information handling practices of all companies within certain industries. For example, companies in the following industries are subject to comprehensive requirements regarding their handling of personal information:

- All companies "significantly engaged in activities that are financial in nature" are subject to the Gramm-Leach-Bliley Act (GLBA) and the GLBA Privacy and Safeguards Rules,
- All healthcare providers, health insurance companies and healthcare information clearinghouses are subject to the Health Insurance Portability and Accountability Act of 1996 (HIPAA) Privacy and Security Rules, and
- All schools and institutions that receive funds from the Department of Education are subject to the Family Educational Rights and Privacy Act (FERPA).

In each case, the laws require that the subject entity pass the legal obligations on to any entity that accesses or receives regulated personal information from it.

For example, the GLBA Safeguards Rule requires financial institutions to develop and implement a comprehensive information security program that is appropriate to the size, complexity, nature and scope of the activities of the institution and that contains "administrative, technical and physical safeguards" to protect the security, confidentiality and integrity of customer information.[3] The safeguards must be reasonably designed to (i) insure the security and confidentiality of customer information, (ii) protect against any anticipated threats or hazards to the security or integrity of the information, and (iii) protect against unauthorised access to or use of the information that could result in substantial harm or inconvenience to any customer.[4]

A GLBA-compliant information security program is required to have certain elements, including a designated employee to coordinate it, audit systems to determine risks, and certain procedures to take with service providers to assure the security of the information is maintained. With regard to service providers, the Safeguards Rule specifically requires financial institutions to "oversee service providers, by: (1) taking reasonable steps to select and retain service providers that are capable of maintaining appropriate safeguards for the customer information at issue; and (2) requiring your service providers by contract to implement and maintain such safeguards."[5]

Similarly, the HIPAA Security Rule set forth strict requirements for all data processors, which are classified under HIPAA as "business associates." The Security Rule allows covered entities to permit a third party vendor (called a "business associate" or "BA") to create, receive, maintain, or transmit electronic protected health information on the covered entity's behalf only if the covered entity obtains satisfactory assurances that the BA will appropriately safeguard the information.[6] The Security Rule then establishes the minimum requirements for all BA contracts. Each BA must agree to (1) implement administrative, physical, and technical safeguards to protect the confidentiality, integrity, and availability of the information; (2) ensure that its agents implement appropriate safeguards; (3) report security incidents; and (4) authorise termination if the BA violates a material term of the contract.[7]

But even companies that are not subject to a Federal privacy law may well be subject to state privacy or security laws that require it to manage its data processors. State legislators have been passing privacy and security laws to "fill the gap" by imposing regulations on entities not covered by the Federal laws listed above. Federal and state regulators have also developed general theories of liability for failure to have reasonable security as well.

In 2004, California became the first state to impose a general security standard on businesses that maintain personal information. CA Civil Code 1798.81.5 targets entities that are *not* covered by GLBA, HIPAA or other Federal laws.

This law requires businesses that handle sensitive personal information (such as Social Security numbers, state-issued ID

numbers, financial information or medical records) about Californians to maintain reasonable security procedures and protect the information from unauthorised access, destruction, use, modification or disclosure. This law also compels businesses to impose security requirements on entities that process data for them.

Over 35 states have enacted security laws. While many of these laws focus on security breach notification, several parallel the California law and require companies to protect personal information.

Additionally, many states also specifically regulate the processing of Social Security numbers, due to the association of Social Security numbers and identify theft. Following California's lead again,[8] many state laws also prohibit any person or entity from: (i) publicly posting or displaying Social Security numbers, (ii) printing Social Security numbers on cards used to access products or services, such as insurance cards, (iii) requiring individuals to transmit Social Security numbers over the Internet unless the connection is secure or the SSN encrypted, (iv) requiring individuals to use Social Security numbers to access a website, unless a password or other authentication device is also required to access the website, or (v) printing an individual's Social Security number on any document mailed to the individual, unless the number is required to be on the document by law.

Even absent a specific law, companies are required by the U.S. regulators, such as the Federal Trade Commission (FTC) and state attorneys general, to have reasonable safeguards in place to protect sensitive personal information, including credit card numbers, medical information and Social Security numbers. The FTC and state attorneys general actively bring enforcement actions against companies that fail to employ reasonable security for personal information. These actions are brought under their general jurisdiction to restrict unfair and deceptive trade practices, and they have created a *de facto* national requirement that companies implement appropriate privacy and security programs, including vendor and employee oversight.[9]

To avoid FTC action, companies must also prohibit data processors from using personal information in any manner that is inconsistent with the companies' published privacy notices. In other words, when a company collects personal information subject to a published privacy notice, it cannot permit any third parties to use the personal information for any purpose that contravenes the notice. As the FTC has opined in the CartManager case,[10] companies and data recipients must be "in sync" – data recipients cannot do things that exceed the scope of the companies' privacy notices, and companies must know and manage the actions of their data recipients.

International security requirements

Approximately 60 countries have enacted data protection laws, which generally obligate companies to protect the privacy and security of personal information. Comprehensive data protection laws exist throughout Europe as well as in many Asian countries (Japan, Korea, Hong Kong and Taiwan), Australia, New Zealand, Canada, Israel, Tunisia, Chile and Argentina.

While all personal information (including just name and address) is protected by these international laws, the sensitivity of the data does affect the required level of security. For example, laws based on the E.U. Data Protection Directive 95/46/EC require data controllers to "implement appropriate technical and organisational measures to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing." Taking into account the nature and cost of available security technology, "such measures shall ensure a level of security appropriate to the risks represented by the processing and the nature of the data to be protected."[11]

Similarly, Canada's Personal Information Protection and Electronic Documents Act (PIPEDA) includes security in Principle 7, which mandates that "personal information shall be protected by security safeguards appropriate to the sensitivity of the information."[12]

Many data protection authorities have published guidance for companies on information security and vendor oversight. In some cases, the authorities mandate particular controls for sensitive data processing.[13] In other cases, the authorities publish "best practice" recommendations that companies are advised (but not required) to follow.[14]

International data protection laws also require companies to manage third party processors. For example, Article 17 of the E.U. Directive requires data owners (controllers) to choose processors that can provide "sufficient guarantees in respect of the technical security measures and organisational measures governing the processing to be carried out" and to ensure compliance with those measures. The Article goes on to require that processing performed by a third party processor must be governed by a written contract or legal act binding the processor to the controller and stipulating that (i) the processor shall act only on instructions from the controller, and (2) the security measures described above shall be met.

Data protection authorities have also published regulations as guidance on the management of third party processors.[15] These instructions focus generally on vendor qualification, contracting, oversight, and security.

Practical solutions for managing the risks associated with third party data processors

In order to meet the U.S. and international requirements for information security, companies must manage their own internal processes as well as those of their agents. This means that companies must select only those vendors that have the capability and controls to respect limits on data processing (so that personal information is only used to perform the designated services for the company) and provide reasonable security for the personal information.

Due diligence

Conducting formal due diligence on prospective data processors is the first step. It is critical that companies ask prospective vendors the following types of questions about their privacy and security programs as part of their pre-contract due diligence. If the vendor cannot answer the questions satisfactorily, additional effort must be made to

ensure that necessary controls will exist during the processing relationship.

1. Do you have a written policy regarding the confidentiality and security of information you process for customers? If so, please provide a copy. Is this policy implemented with specific, written security procedures? Please provide contact information for your chief security officer and chief privacy officer.
2. Have you implemented a formal security program containing administrative, physical and technological controls to protect your computer systems, operating systems, networks, applications and databases?
3. Will the information we provide you be segregated? Do you have procedures to limit access to only those workers who need access to perform services for us?
4. Would our information be encrypted or otherwise protected during transmission to/from us and among your workers and processors? What secure transmission technology do you employ?
5. Do you have procedures to limit the ability of workers to download information from your systems and network onto desktops, laptops, PDAs or other portable devices? Are all laptops and portable devices encrypted?
6. Have you established physical and logical security domains with highly-restricted access? Would our information be maintained in the highest level domain? Would paper copies of our information be kept in locked file cabinets?
7. Do you have procedures to redact or limit the display of sensitive data elements (such as Social Security numbers) in your computer systems?
8. Do you conduct background checks on all workers? Do workers sign confidentiality agreements? Are workers trained on privacy, security and confidentiality? Are workers monitored for compliance with your policies and procedures?
9. Has your security program been audited or assessed by a third party? If so, when was it conducted and by whom? Please provide a copy of the report.
10. Do you have established procedures to detect and respond to a security incident?
11. Would your professional liability insurance be sufficient to cover all costs associated with an incident involving our information? Please provide coverages.

Due diligence on the prospective vendor is not the only due diligence to be done, however. Companies also need to ask appropriate questions about the proposed processing arrangement. For example, what personal information will the vendor need to perform the services? Does any of the information constitute "sensitive personal information" under the company's data classification scheme? Will the personal information be physically transferred to the vendor (and, if so, how)? Or will the vendor access the data remotely? If so, from where? What types of access controls will be used? Only when these answers are known can the risks of the processing arrangement be understood and managed.

Vendor contracts

Assuming due diligence has been satisfactorily completed, the company then needs to enter into an appropriate contract with its processor. The contract should define the specific processing instructions and establish minimum necessary security controls. It should also address incident response and provide for any additional safeguards that may be needed, given the nature of the data being handled. Consider the following standard contract provisions:

1. Definitions. In addition to standard definitions of "personal information" and "sensitive personal information" (which tie to the company's data classification policy), the vendor contract should clearly define the scope of the processing services to be provided. Ideally, the processing services are described with particularity in a services contract or on a statement of work.
2. General Limitations. The company should expressly limit the vendor's processing so that: "vendor will process personal information only as authorised and as necessary to perform the services." The company may want to consider other limits on the processing, such as use of unauthorised subcontractors. The company may wish to prohibit any unauthorised cross-border transfers of the personal information.
3. Reporting. The vendor should be obligated to notify the company of any issues related to its processing as well as of any third party requests for access to the data or third party complaints or inquiries regarding the processing. Unless a response is legally required, the company should prohibit the vendor from responding to access requests or inquiries without the company's consent. Vendor should be obligated to assist the company in its response to any requests, complaints or inquiries.
4. The contract should clearly classify "personal information" as company information subject to the company's standard confidentiality provisions. Consistent with the company's confidentiality provisions, vendor should be limited in its ability to disclose personal information. For example, the company may limit disclosures to those vendor employees who require access to perform the services, who have been subject to appropriate background checks, who have executed non-disclosure contracts, and who have been trained on privacy and security obligations.
5. The contract should describe the specific security measures that should be used to protect the personal information. At minimum, the contract must require the vendor to have implemented and documented appropriate operational, technical and organisational measures to protect personal information against accidental or unlawful destruction, alteration, unauthorised disclosure or access. The contract should also require the vendor to regularly test and monitor the effectiveness of its safeguards, controls, systems and procedures and to periodically assess internal and external risks to the security, confidentiality and integrity of the personal information. The vendor should be required to monitor its workers and subcontractors for compliance with the security program requirements.
6. Ideally, a company "security requirements document" should be provided to the vendor to ensure that the company's specific expectations are met. For example, this document would describe expected safeguards for transmission of sensitive information over a network,

Social Security number processing, encryption, remote access, business continuity controls and the like. If the vendor is handling any payment card data, the contract should specifically require compliance with the Payment Card Industry Data Security Standard.

7. The company should have the right to audit the vendor's facilities and to terminate the contract if material gaps are identified and not promptly remediated.
8. The vendor should be required to promptly and thoroughly investigate all allegations of unauthorised access to, use or disclosure of the Personal Information, and to notify the company immediately upon discovery of any such unauthorised access to, use or disclosure. The company may wish to allocate some or all of the costs associated with responding to a security breach to the vendor. If so, this should be covered in the indemnification provision, and the company should require the vendor to maintain sufficient insurance coverage.
9. Upon termination of the contract, the vendor should be obligated to either (i) return the personal information (and all media containing copies of the personal information), or (ii) purge, delete and destroy the personal information. The contract should specificy that electronic media containing personal information will be disposed of in a manner that renders the personal information unrecoverable.
10. The contract should require the vendor to stay informed of and to comply with the legal and regulatory requirements for its processing of personal information. The vendor should also be given a copy of any applicable company privacy notices and required to comply with these as well.

Once the contract is finalised, company personnel should consider what types of ongoing oversight are needed. At minimum, the company will want to monitor the vendor's financial condition and obtain periodic assurances regarding compliance and security. For critical vendors (such as vendors that process significant volumes of sensitive personal information), periodic assessments should be conducted. These can be conducted by company audit resources or by third parties. Vendors may also be able to provide independent assurance, such as SAS-70 Type II reports.

Managing the inevitable oops

No matter how effective your security controls (or those of your vendors), some type of security incident is generally inevitable. Having a formal incident response plan allows you to react quickly and professionally when an incident does occur. Considering incident response in advance also allows you to maintain an appropriate perspective if the breach is caused by a vendor.

Most companies expect their vendors to manage the risks of incidents as well as (or better than) they do, but companies generally are not willing to pay for vendors to insure against incidents. Companies should assume that their vendors' workers are just as likely to make mistakes as their own employees are. The best strategy is to partner with your vendors in your collective effort to minimise mistakes and manage outcomes.

In any incident, companies generally remain accountable for the mistakes of their vendors. While a company can allocate responsibility for responding to (and paying for) incidents, the affected individuals are the *company's* customers or employees, and the company needs to make sure they are treated accordingly. Consequently, companies should generally take ownership of public aspects of the breach response, working closely with the vendor to understand the incident and craft the best response.

If a security breach occurs, the company and the vendor need to quickly assemble a trained incident response team. The team should consist of appropriate company and vendor decision-makers in the security/IT, legal, privacy, HR, and communications functions. Other leaders may be called upon as needed, such as account executives and customer support. External advisors may also be needed, such as forensic specialists, media consultants and outside counsel. The incident response team should then tackle the following tasks in order: (i) mitigation of any ongoing harm, (ii) investigation of the incident, (iii) analysis of any legal compliance obligations, (iv) development of a communications plan, (v) provision of restitution and/or customer support, (vi) response to any complaints/inquiries, and (vii) analysis of organisational learning.

Additionally, companies must realise that responding to a security breach involves more than legal analysis. While consumer notification may be motivated by legal compliance obligations, the messages delivered should reflect the personal nature of the company's relationship with the individual. This dictates that if a company notifies any individual regarding a breach, it must notify all affected individuals, even if they live in states that do not have notification laws. It also requires the company to consider offering remediation services (such as credit monitoring) and to tailor the messages to the affected population. Companies should be prepared to answer follow-up questions from the individuals, via phone or email.

Finally, companies must also be willing to apologise for the mistakes that they and their vendors make. Key messages for every breach communication should be: (i) this is what happened, (ii) this is what we are going to do to make it better, (iii) these are the steps we're taking to help prevent it from happening again, and (iv) we are really sorry. These are messages that help diffuse consumer emotion and enable the company to move past the incident. These messages, along with evidence of the formal nature of your vendor management program will also help diffuse regulatory concerns about your security controls.

Conclusion

Companies today have fiduciary-like duties towards the individuals who entrust their information to them. Companies must, as a matter of law, provide reasonable security for the information and ensure that the information is used appropriately, in accordance with its privacy notices. This means that they must develop and implement robust information security programs that include management of third party processors.

Effective oversight of vendors requires undertakings before, during and after the relationship. Before you send a vendor personal information, the prospective service provider should

be examined, qualified and bound by appropriate and detailed contract provisions. During the term, the vendor should be monitored – vendors who process sensitive data should likely be assessed by you or an independent third party. At the end of the term, steps should be taken to ensure that all the personal information has been returned or destroyed. Additionally, companies and vendors should anticipate and plan for incidents.

1 Peggy Eisenhauer is founder of Privacy & Information Management Services – Margaret P. Eisenhauer, P.C., a full-service privacy, security and information management law firm. She helps companies develop, implement, and assess privacy and fair information practices, including policies governing the collection, use and disclosure of consumer, professional and employee information. She has extensive experience with U.S. and international privacy and security laws. In addition to a J.D. degree with honors from the University of Georgia School of law, Ms. Eisenhauer has a Masters of Science in Information and Computer Science from the Georgia Institute of Technology. She is a Fellow of the Ponemon Institute, a Certified Information Privacy Professional (CIPP) and a member of the International Association of Privacy Professionals CIPP Advisory Board. *Ms. Eisenhauer is admitted to practice law in Georgia and Florida, U.S.A.* She can be reached via email to peggy@privacystudio.com or via telephone at 404-914-1163.

2 This article and its attachments have been prepared for informational purposes only and are not legal advice. If you have any questions about any particular legal requirement or your specific processor relationships, please engage a lawyer who can provide legal advice.

3 16 C.F.R. § 314.1(a)

4 16 C.F.R. § 314.3

5 16 C.F.R. § 314.4(d)

6 45 C.F.R. § 164.308(b)(1)

7 45 C.F.R. § 164.314(a)

8 See CA Civil Code 1798.85

9 See, *e.g.,* FTC actions against DSW Shoe Warehouse, BJ's Wholesale Club, linked from *www.ftc.gov/privacy/*

10 See, *e.g.,* the FTC's action against Vision I Properties, LLC, doing business as CartManager International, linked from *www.ftc.gov/opa/2005/03/cartmanager.htm.*

11 Article 17, Directive 95/46/EC of the European Parliament and of the Council of October 24, 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, OJ L281 31 (1995)

12 Personal Information Protection and Electronic Documents Act (2000, c. 5). The Model Code for the Protection of Personal Information, CAN/CSA-Q830-96 is contained in Schedule 1

13 See, *e.g.,* Polish security regulations (THE REGULATION OF APRIL 29, 2004 BY THE MINISTER OF INTERNAL AFFAIRS AND ADMINISTRATION as regards personal data processing documentation and technical and organisational conditions which should be fulfilled by devices and computer systems used for the personal data processing, Journal of Laws of 2004, No. 100, item 1024, and the Appendix), Spanish security regulations (ROYAL DECREE 994/1999, of June 11, which approves the Regulation on Mandatory Security Measures for the Computer Files which contain Personal Data), and Italy's security regulations (*Official Journal n.216,* 1999*)*

14 See, e.g., Canada's voluntary guidelines for security breaches ("KEY STEPS FOR ORGANISATIONS IN RESPONDING TO PRIVACY BREACHES" 2007), OR AUSTRALIA'SA2 A2Information Sheet 6 - 2001 Security and Personal Information

15 See, *e.g.,* the U.K. Information Commissioner's Data Protection Good Practice Note: "Outsourcing– a guide for small and medium sized businesses", and Hong Kong's "Must Take Security Measures to Protect Personal Data when Engaging Outsourced Contractor" (Report Number: R06-2599; Date issued: October 26, 2006)