

Data Privacy and PCI Compliance – Minimize Data and Effort

Chris Zoladz, Navigate LLC

Hotels, restaurants, country clubs, spas and many other organizations routinely collect, process and store personally identifiable information¹ (“PII”) pertaining to their customers and employees as a necessary part of daily business. This information is subject to a myriad of U.S. State security breach laws and the upcoming “Standards for the Protection of Personal Information of Residents of the Commonwealth”² which pertains to Massachusetts residents and becomes effective March 1, 2010.

In addition, if you are doing business in international markets such as the European Union, Canada or Australia, there are data protection laws that have been in effect for years.

There is also the Payment Card Industry Data Security Standard³ (“PCI DSS”) that the credit card companies require to be implemented to protect credit and debit card information (referred to hereafter as credit cards). PCI DSS compliance is not a law, but is a contractual obligation in merchant agreements that companies sign to be able to accept credit cards. While the data breach laws deal only with legal requirements after PII has been breached and does not address the proactive protection of PII, the new Massachusetts law and PCI DSS require specific security measures for the protection of PII and credit card data. However, the security requirements are not identical. To add to the complexity, the international data protection laws are much more general and do not mandate specific security measures that must be in place but instead use terms such as “appropriate technical and organizational measures to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access.”

In the U.S., the legal stakes may be getting higher in the future. Specifically, Senator Leahy introduced a bill, S. 1490 “*Personal Data Privacy and Security Act of 2009* to prevent and mitigate identity theft, to ensure privacy, to provide notice of security breaches, and to enhance criminal penalties, law enforcement assistance, and other protections against security breaches, fraudulent access, and misuse of personally identifiable information.” This bill, if passed in its current form would nationalize the current state security breach laws and would require organizations that have PII to implement certain security measures similar to the Massachusetts law. Keeping abreast of the evolving legal and PCI DSS requirements can and will continue to be a challenging task for many hospitality companies, especially smaller companies. For this reason, actions that minimize and simplify your compliance effort, and reduce the cost of compliance and risk should be a high priority.

¹ Personally identifiable information (“PII”) is defined as an individual’s first and last name, or first initial and last name, in combination with other information elements specific to the individual, including, but not limited to address, telephone number, e-mail address, credit card information, medical information, compensation information, government issued ID such as social security number, or other similar specific factual information, regardless of the media on which such information is stored (i.e., on paper or electronically). Note: This definition represents the most common elements in the statutory definitions of PII.

² See <http://www.mass.gov/Eoca/docs/idtheft/201CMR1700reg.pdf> for text of the law.

³ See <http://www.pcisecuritystandards.com> for a copy of the standard.

PII Minimization

Protecting all PII in every location that it exists can be a very expensive approach. The most impactful action you can take is also the most obvious – limit the amount of PII that needs to be protected. A core business practice should be to only collect the minimum amount of PII required to execute the business transaction, manage your workforce or meet any legal requirement. The less PII that is collected and stored, the less that has to be protected and is at risk of breach. This can require simple or significant changes to current business processes and information systems but is worth the effort.

Eliminating Duplicate Data

Duplicate PII is a common occurrence and can be identified by conducting a PII inventory. As an example, some hotels still follow the practice of imprinting a guest's credit card on a registration card even though it was successfully swiped and authorized in the property management system. This practice is not only unnecessary, it creates a paper record of the credit card that now must be protected and is subject to loss or theft.

Numerous instances of the same PII can also be found in computer systems, files on desktops or laptops, network servers, back-up tapes, portable media such as flash drives, CDs or back-up tapes and also in paper records. Each of these instances of PII must be protected and represents a data repository that can be lost or stolen.

The cost to protect duplicate PII can be substantial, not to mention the storage costs. Every reasonable effort should be made to minimize PII and the locations where it is stored to the minimum number of places practical to meet your business and legal needs.

Social Security Numbers

Social security numbers deserve special attention because over time many organizations have used the social security number as a static unique identifier. The result is that this seemingly ideal identifier likely resides in numerous information systems and on paper forms. This information may pertain to job applicants, current employees, former employees, club members or customers. While the social security number is needed for certain tax purposes, any use beyond that purpose should be discontinued and another means to assign a static unique identifier, not related in any way to the social security number, should be implemented.

Third Party Service Providers

Your compliance obligations generally extend to the PII that you provide to third party service providers. Therefore, if you use third party service providers that have PII pertaining to your employees or customers to provide services such as payroll processing, benefits administration, website reservation system, etc., the PII they handle should be included in the inventory and data minimization effort. Managing compliance for the PII you maintain can be challenging but the PII entrusted to third party service providers needs to be as carefully managed.

Data Disposal

After identifying duplicate data, it is important that the duplicate data that can be eliminated is securely deleted. For paper based records it is fairly straightforward as a cross cut shredder or third party shredding service can be used to securely destroy this data. For data stored on electronic media such as desktops, laptops, servers, flash drives, etc. it should be deleted. Technically, the data on these electronic devices could be restored with specialized software until the disk space is overwritten; however, simple deletion is better than maintaining the unnecessary file. If the duplicate data that is to be deleted resides on electronic devices that are no longer needed such as old laptops, all data should be permanently deleted prior to disposal. If you do not have internal IT resources that have access to the specialized software to permanently delete all the data you should use a third party service provider that specializes in secure deletion of data from electronic devices. One such service provider is Intechra⁴. These service providers can also ensure the devices are disposed of in accordance with Environmental Protection Agency requirements.

Complying with data privacy and PCI DSS requirements can be difficult. The first step in your compliance strategy should be to reduce the amount of data to be protected to the minimum amount practical and still meet your business and legal needs. When it comes to data privacy and PCI DSS compliance, less PII is more.

Chris Zoladz is the Founder of Navigate LLC. He may be reached at chris@navigatellc.net. This information provided is general and educational and not legal advice. For more information, please visit www.hospitalitylawyer.com.

⁴ <http://www.intechra.com>