MORRISON | FOERSTER

Legal Updates & News

Bulletins

Massachusetts Delays Effective Date of New Data Security Regulation

November 2008

Related Practices:

- Privacy and Data Security

Privacy and Data Security Update, November 14, 2008

In an announcement released late on Friday, November 14, 2008, the Massachusetts Office of Consumer Affairs and Business Regulation ("OCABR") extended the general deadline for compliance with that state's new data security regulation to May 1, 2009. The original compliance deadline was January 1, 2009.

In addition to establishing the new May 1, 2009 general compliance deadline, the Friday announcement extended until January 1, 2010 the deadlines for encrypting non-laptop portable devices and obtaining compliance certifications from vendors that have access to personal information of Massachusetts residents.

As described at greater length in an earlier Morrison & Foerster Legal Update ("New Massachusetts Regulation Requires Encryption of Portable Devices and Comprehensive Data Security Programs" (Sept. 12, 2008)), the Massachusetts regulation requires all persons that own, license, store or maintain personal information concerning Massachusetts residents to take comprehensive measures to protect that information from unauthorized access, disclosure or misuse. Besides the general requirement that affected companies must assess the risks to such information and develop written, comprehensive security programs to address those risks, the regulation mandates a number of measures that are not specified in the data protection laws to which most businesses already are subject. Notably, the Massachusetts regulation requires:

Encryption

Under the new regulation, "to the extent technically feasible, [affected entities must implement] encryption of all transmitted records and files containing personal information that will travel across public networks, and encryption of all data to be transmitted wirelessly" as well as "all personal information stored on laptops or other portable devices."

This part of the regulation has forced many businesses with Massachusetts customers to review their encryption capabilities and accelerate the purchase and deployment of hardware and software to extend those capabilities. Although laptop encryption programs already are underway or completed at many companies, securing the bewildering variety of smaller, cheaper portable devices available to employees is an issue that many companies had not begun to address when the regulation was adopted. The scale and uncertainty of this problem made the January 1, 2009 deadline unrealistic, especially for smaller businesses.

In its Friday announcement, OCABR acknowledged that laptops "are more easily encrypted than other portable devices such as memory sticks, DVDs and PDAs," and accordingly extended the deadline for encryption of those non-laptop devices to January 1, 2010. The compliance date for encryption of laptops and data sent over public networks and wireless systems, however, is the new general compliance date of May 1, 2009.

Vendor Oversight

Companies that share personal information of Massachusetts residents with vendors, for whatever purpose, are responsible under the new regulation for the careful selection and oversight of those vendors. Specifically, companies subject to the Massachusetts regulation must take "reasonable steps to verify that third-party service providers with access to personal information have the capacity to protect such personal information,

including (i) selecting and retaining service providers that are capable of maintaining safeguards for personal information; and (ii) contractually requiring service providers to maintain such safeguards." Also, before granting a third-party contractor access to personal information of Massachusetts residents, a company must "obtain from the third-party service provider a written certification that such service provider has a written, comprehensive information security program that is in compliance with the provisions of these regulations."

Recognizing that these requirements may "overburden[] small businesses during harsh economic times," the Friday announcement extends the deadline for obtaining written vendor certifications until January 1, 2010. All of the other service provider obligations, however, are subject to the May 1, 2009 extended compliance date.

Minimization

Another important feature of the Massachusetts regulation is the requirement that organizations maintaining personal information of Massachusetts residents must "limit[] the amount of personal information collected to that reasonably necessary to accomplish the legitimate purpose for which it is collected; limit[] the time such information is retained to that reasonably necessary to accomplish such purpose; and limit [] access to those persons who are reasonably required to know such information in order to accomplish such purpose or to comply with state or federal record retention requirements."

This "minimization" standard, which resembles the privacy requirements in effect in the European Union, is profoundly different from the usual American approach to data use and collection. Except for certain types of business, such as financial and health care organizations, U.S. businesses are generally free to collect personal information for any lawful purpose and to use and disclose that information as they see fit, subject to any restrictions in their own privacy policies. The new regulation will require businesses that maintain personal information of Massachusetts residents to limit their collection, disclosure and use of that information according to the purpose for which it was collected.

These minimization requirements are subject to the new, general compliance deadline of May 1, 2009.

Identifying Personal Information

The new regulation also includes language that requires an organization to "identify paper, electronic and other records, computing systems, storage media, including laptops and portable devices used to store personal information, to determine which records contain personal information, except where the comprehensive information security program provides for the handling of all records as if they all contained personal information." If Massachusetts interprets this provision literally, it will impose a monumental obligation on organizations to identify every piece of paper and every electronic device or system that contains Personal Information. While the delay in the effective date may be aimed at assisting small businesses, the obligation to identify the Personal Information will be virtually impossible for any organization to achieve.

The identification obligations are subject to the new, general compliance deadline of May 1, 2009.

Conclusion

The extension of the Massachusetts compliance dates is a welcome development, especially in the uncertain economic environment facing U.S. businesses. The new deadlines still are not overly generous, however, and compliance efforts should remain a high priority at companies that maintain personal information of Massachusetts residents.