

# ADVERTISING, MARKETING & PROMOTIONS

>> ALERT

## COMPLIANCE DATE FOR MASSACHUSETTS' DATA SECURITY REGULATIONS MAY NOT EXTEND PAST MARCH 1, 2010

Massachusetts has been the focal point of the privacy and data security industry ever since the Office of Consumer Affairs and Business Regulation (OCBAR) issued the "Standards for the Protection of Personal Information of Residents of the Commonwealth" pursuant to the state's comprehensive data security law which was enacted in 2007.

These regulations require businesses, wherever located, that own or license personal information about Massachusetts residents to implement a written comprehensive security program, encrypt certain data and comply with other security requirements. The regulations have been modified several times by OCBAR and the effective date of the regulations has been pushed back numerous times. However, the current compliance date is March 1, 2010 and may not be extended.

While there are many intricacies to the regulations, the three key aspects are: (1) implementation of a comprehensive written information security program (WISP), (2) encryption of certain personal information and (3) requiring businesses to bind their third party service providers by contract to implement and maintain appropriate security.

**1. WISP** - Under the regulations, entities that own or license personal information concerning Massachusetts residents must develop, implement and maintain a comprehensive written information security program. Personal information is defined as first name (or

initial) and last name, combined with social security number, driver's license number or state-issued identification card number or financial account number or credit or debit card number.

The regulations adopt a "risk-based" approach towards security so that administrative, technical, and physical safeguards are appropriate to (a) the size, scope and type of business; (b) the amount of resources available to such business; (c) the amount of stored data; and (d) the need for security and confidentiality of both consumer and employee information. However, every WISP must include, at a minimum, the following:

- >> Designate one or more employees to maintain the program.
- >> Identify and assess reasonably foreseeable internal and external risks to the security of personal information.
- >> Develop security policies for employees relating to the storage, access and transportation of records containing personal information outside of the business premises.

### THE BOTTOM LINE

Now is the time for businesses to ensure that they will be in compliance with Massachusetts data security regulations come March 2010.

- >> Impose disciplinary measures for violations of the WISP.
  - >> Prevent terminated employees from accessing records containing personal information.
  - >> Oversee service providers (discussed further on page 2).
  - >> Reasonable restrictions upon physical access to records containing personal information.
  - >> Regular monitoring to ensure that the program is operating in a manner reasonably calculated to prevent unauthorized access to or unauthorized use of personal information.
- >> *continues on next page*

# ADVERTISING, MARKETING & PROMOTIONS

## >> ALERT

- >> Review the scope of the security measures at least annually or whenever there is a material change in business practices that may reasonably implicate security.
- >> Document responsive actions taken in connection with any incident involving a breach of security.

**2. Security and Encryption** - Every WISP must include the establishment and maintenance of a security system covering its computers. Since there is no one-size-fits-all security model, the elements of this requirement are to be implemented "to the extent technically feasible."

Among the many requirements of this provision are requirements to encrypt the transmission of certain personal information. Specifically, a business must:

- >> Encrypt all records and files containing personal information transmitted across public networks.
- >> Encrypt all data containing personal information transmitted wirelessly.
- >> Encrypt all personal information stored on laptops or other portable devices.

**3. Service Providers** - The regulations will change the way many businesses deal with their vendors. If a service provider has access to personal information, then the business must

require the service provider, **by contract**, to implement and maintain appropriate security measures for this personal information. Many vendor forms specifically disclaim any liability for security, so this statutory requirement is a major change for some companies.

Since this requirement could necessitate amending existing service provider agreements, there is a two year grace period to implement this requirement. Therefore, if a service provider contract was entered into prior to March 1, 2010 and does not contain appropriate security language, then the contract does not need to comply with this requirement until March 1, 2012. Essentially, businesses have two years to amend their old contracts.

### WHAT BUSINESSES SHOULD DO NOW:

- 1. Take Stock** - Review operations to analyze how personal information is collected, stored, handled and disclosed. This process should include people from all departments, including information technology, human resources, marketing, administration and legal.
- 2. Review Security** - Analyze existing security systems and procedures, and upgrade any deficiencies or gaps.
- 3. Encryption** - Implement encryption for personal information where necessary.

**4. Vendor Contracts** - Review existing service provider contracts and amend those that are not in compliance with the regulations. Ensure that all new service provider contracts have appropriate security language.

**5. WISP** - Develop a written information security program that, at a minimum, complies with these Massachusetts regulations.

**6. Training** - Implement training programs for all applicable employees on the proper use of your computer systems, the importance of security and the terms of your written policy.

### FOR MORE INFORMATION

Gary Kibel, Partner  
212.468.4918  
gkibel@dgllaw.com

Alison Winter, Associate  
212.468.4976  
awinter@dgllaw.com

or the D&G attorney with whom you have regular contact.

### DAVIS & GILBERT LLP

T: 212.468.4800  
1740 Broadway, New York, NY 10019  
[www.dgllaw.com](http://www.dgllaw.com)

© 2009 Davis & Gilbert LLP