Massachusetts Data Protection Law: Third-Party Provision Effective March 1

February 17, 2012 By Bruce E. H. Johnson

Effective March 1, 2012, any company, wherever located, that is holding the "personal information" of Massachusetts residents must amend its existing vendor contracts to require compliance with Massachusetts data security regulations. 201 CMR 17.03 (f)(2).

http://www.mass.gov/ocabr/docs/idtheft/201cmr1700reg.pdf

http://www.computerworld.com/s/article/9223709/Final_phase_of_Mass._data_protection_law_kicks_in_March_1

http://www.computerworld.com/s/article/9155978/Deadline_looms_for_Mass._data_protection_law

This requirement for contracts with third-party vendors applies to the personal information of all Massachusetts residents, including customers, employees and others. The data security rules require businesses to encrypt sensitive personal information on Massachusetts residents that is stored on portable devices such as PDAs and laptops or on storage media such as memory sticks and DVDs. Any personal information that is transmitted over a public or wireless network must also be encrypted.

If any of your clients owns or licenses personal information about Massachusetts residents, it may be time to review compliance with the Massachusetts law. Please feel free to consult with a member of the PrivSec practice group regarding this issue.

To read more about the Massachusetts law, please visit our Nov. 17, 2008 advisory here.

Tags: Data Breach & Security