

Update: Renegotiating IT Vendor Agreements in Light of Massachusetts Data Privacy Regulations — A Temporary Reprieve and a “Clarification”

Winter 2010

John J. Smith, VistaLaw International, LLC

In the June 2009 issue of *VistaLaw Views*, we discussed the new Massachusetts data privacy regulations and cautioned readers to take a close look at their vendor contracts and contracting policies in light of expanding regulatory data privacy and information security mandates. On the leading edge in this arena sit the comprehensive Massachusetts information security “Standards,” thrice postponed. **The regulations are now scheduled to go into effect in March 2010.**


Even with recently announced and welcome relaxations, the Standards are the most rigorous set of mandates for data security policies and practices in the country. This update continues our focus on just one aspect of the “Standards” — the duty to oversee third party IT service providers with access to personal information about Massachusetts residents. The latest relaxations bring both relief and confusion — relief with an extended compliance deadline, confusion as to just how parties are expected to come into eventual compliance.

IT Vendor Contracts — Some third party vendor agreements are grandfathered for a time.

The “Standards” require companies to “select and retain” third party IT service providers “capable of maintaining appropriate security measures ... consistent with these regulations.” Even as now twice modified from previous versions, this seemingly simple requirement to “select” and “retain” entails substantial administrative and operational burdens that parties should begin to shoulder well before the grace period expires.

Indispensible steps.

- ▶ First, **catalogue all contracts** involving transfer of sensitive personal data to a vendor, for whatever purpose.
- ▶ Second, **evaluate the relative vulnerabilities** within each identified contractual arrangement, identifying both severity of security risks and effectiveness of safeguards.
- ▶ Third, **do (and document) real-time due diligence** to determine whether a vendor or prospective vendor actually provides effective safeguards, what kind, and at what level. This must be on-going.
- ▶ Fourth and finally, **procure written representations and commitments** from the vendor that its data security measures meet all specified mandates, administrative, operational, and technical.



The latest relaxations bring both relief and confusion – relief with an extended compliance deadline, confusion as to just how parties are expected to come into eventual compliance.

Tackle the most problematic or risk-laden contracts first, those involving data of the highest sensitivity or risk of loss or misuse.

And while you are doing those, consider these:

1. **Break the problem down into manageable pieces.** Tackle the most problematic or risk-laden contracts first, those involving data of the highest sensitivity or risk of loss or misuse. Address the new contract or contract renewals where leverage might be greatest. But triage is only the first step.
2. **“Flow Down” the obligations.** Incorporate and expand standard legal compliance commitments to encompass later regulatory developments, such as the “Standards.” Make sure you neutralize other “boilerplate” disclaimers that might operate to nullify an expansion. While you cannot delegate away your own responsibility, you can share the pain.
3. **Remember: your vendor’s negligence doesn’t excuse your own regulatory jeopardy.** Proving vendor negligence depends on the applicable standard “duty of care,” an elusive concept in cyberworld. And even when vendors follow industry standards or use all reasonable efforts, data gets lost, stolen or corrupted.
4. **Get a solid indemnification.** If you can. A vendor of course will (not unreasonably) seek to avoid or to minimize the scope of its indemnification, offering instead assurances like agreeing to “commercially reasonable” steps to protect the data, or limiting the obligation to gross negligence or intentional acts. Have the indemnification cover not only third party claims (like claims of personal injury from the data subjects themselves), but also administrative actions, and the costs of providing remedial measures (notification, free credit reporting services, etc.) in the event of a security breach.
5. **Document everything.** In almost all cases a company’s compliance efforts will be judged in light of a company’s size, resources, and the sensitivity level of the personal data in its custody. Given the high likelihood that compliance will fall short in one way or another with some regulatory prescription somewhere, create a convincing contemporaneous record of its efforts.

New Effective Transition Dates

The Office of Consumer Affairs and Business Regulation has issued a “clarification” of when affected parties must revisit existing or negotiate planned new or renewed contracts with third party IT vendors. Here’s the clarification:

[A person — that’s you — must require] such third-party service providers by contract to implement and maintain such appropriate security measures for personal information; provided, however, that until March 1, 2012, a contract a person has entered into with a third party service provider to perform services for said person or functions on said person’s behalf satisfies the provisions of 17.03(2)(f)(2) even if the contract does not include a requirement that the third party service provider maintain such appropriate safeguards, as long as said person entered into the contract no later than March 1, 2010.

OK with that?

A grace period, yes; but tempus fugit.

Well, here’s what some people are saying what this means:

- ▶ If you have a relatively short-term contract in place today, do not worry about revising it just because of the new regulations.
- ▶ If, prior to March 1, 2010, you enter into a wholly new contract or a renewal of a contract with a third party vendor for a term of less than 2 years, you don’t have to add special new language — although it would certainly be prudent to do so if you can.
- ▶ If you enter into a new or renewed contract after March 1, 2010, you must assure by express contract provision that your vendors “implement and maintain such appropriate security measures for personal information.”
- ▶ Any contract with an expiration date on or after March 1, 2012 should contain such a requirement.
- ▶ For any **grandfathered** contract expiring after March 1, 2012, you and your vendor must comply with the new regulation for the remainder of the term (that is, from March 1, 2012 until the end of the agreement).



About the Author

John J. Smith is a principle in the DC office of Vistalaw International LLC, with over thirty years of experience as both in-house and outside counsel to companies engaged in the information technology sector. He is a member of the bars of the Commonwealths of Massachusetts and Virginia, the State of New York, and the District of Columbia.

About VistaLaw International

With offices in DC, London, Paris, and Madrid, VistaLaw is an innovative firm of experienced former senior in-house legal counsel, whose service offerings include negotiation of complex commercial contracts and corporate governance and regulatory compliance reviews. For more information, visit www.vistalaw.com.

In effect, you have a temporary grace period to avoid renegotiating shorter-term contracts in the near term, but you should begin now to bring your longer-term contracts in order. Of course, you are still on the hook regardless of what your vendor contracts state.

Tempus fugit. Start now to avoid the scramble.

VistaLaw International LLC

International Square
1875 I Street N.W. Fifth Floor
Washington, DC 20006, USA
Tel: +1 202-429-5526

This VistaLaw Views article is for informational purposes only and is not intended as legal advice serving as a basis for decisions in specific situations. This information is not intended to create, and receipt of it does not constitute, a lawyer-client relationship.