



## FEATURES

● PRINT ● EMAIL ● DIGG ● DELICIOUS

# When Privacy Laws and Hosted CRM Collide

Your company may run afoul of the law if it transfers data across the border.  
By **Pam Baker** on **March 27, 2008**

Every corporation needs to keep information on its customers close at hand. How else could a company expect to adequately service thousands of virtual strangers or appropriately dote on big spenders? But to do so can put your business at odds with pesky **privacy laws** that can do more than just dampen its good intentions — they can seriously cut into profits.

“Unfortunately, some enterprises are not addressing this issue at all because they are not aware of the danger,” said Jennifer Albornoz Mulligan, an analyst at Forrester.

The issue is particularly blindsiding if your company uses a **hosted CRM** solution and hasn't safeguarded itself from liabilities outside of its premises and its control.

“Common pitfalls are **not asking or thinking about where your information is stored**,” warned Mulligan. “Laws in the **EU**, Canada and other privacy-sensitive countries forbid the transfer of personally identifiable information outside of the country to countries with nonadequate privacy protection. This includes both customer and employee information.”

“Using an outsourcer or hosted CRM makes it very easy to accidentally or blindly transfer data outside of the country without the necessary legal protections,” she said.

## Where It Is Viewed Is Where It Is

But just ensuring that your hosted CRM vendor is storing your data in the U.S. is not adequate protection against prevailing privacy laws.

“Information that is even viewed on a screen in a different country is considered to have been transferred, even if the database isn't stored in that country,” said Mulligan.

Even in the U.S., the law is tightening its grip on who knows what, when and how.

“There is a very wide range of local legislation in place and emerging in the various states,” warned Michael Weathersby, an attorney and partner of Evert Weathersby Houff. “There is little doubt that these restrictions will become more prevalent as irresponsible dissemination of personal data results in or becomes an attributed source of identity theft.”

In short, privacy laws are growing in reach and number in the U.S. and elsewhere.

To combat these problems, many companies are battening down the hatches.

“I worked at a large health care company and implemented a national CRM application based on a hosted CRM

system. Although they were OK with contact information, they would not approve any health-protected information [HPI] from being stored on outside servers,” said Lonny Nathanson, partner at Levitate IT. “Regardless that the information was **encrypted**, stored apart from other companies’ data, could not be ‘seen’ by the vendor and had strong passwords for users, they were not about to let any HPI data outside their own firewalls.”

## **Avoiding Missteps**

There are a number of steps your company can take to build its own shield.

“The best practices are to thoroughly investigate what your outsourcers and hosted companies are doing with your information. Their promises of compliance to laws should be included in your contracts, and penalties [should be] listed for noncompliance,” said Mulligan.

Ultimately, the burden of responsibility lies with your company.

“You cannot transfer the risk to the outsourcer. If you are the data owner, and that data violates data privacy laws, it is your responsibility, no matter who you hired,” said Mulligan. “Therefore, you need to have serious conversations with your vendors so that you understand what they intend to do with your data and if it meets your needs.”