COMPLIANCE WEEK
THE LEADING INFORMATION SERVICE ON CORPORATE GOVERNANCE, RISK, AND COMPLIANCE

# CCOs Play a Stronger Role in Data Privacy Practices

By Aarti Maharaj

As data privacy laws proliferate around the world, they are creating a web that traps how corporations use personal data in their operations. The challenge for compliance officers: how to play a more strategic role in the organization, ensuring your business doesn't get stuck.

So far that effort hasn't been easy. In the Compliance Trends 2015 report published by Compliance Week and Deloitte, 59 percent of compliance officers are either "somewhat confident" or "not confident at all" that their IT systems can fulfill the data collection and reporting requirements they have. That can cause problems in how your business gathers data, how it uses data, and even how the business recovers from regulatory and reputation risks when it *loses* data, through hackers or otherwise.

"The issue for chief compliance officers is that they are increasingly struggling to connect regulatory requirements to IT issues," says Todd Cipperman, founding principal of Cipperman Compliance Services. "Technology is its own discipline and I don't see compliance officers becoming technologists overnight."

The forward march of technology—specifically, data storage in the cloud—does chief compliance officers few favors. According to research firm Gartner, by 2017 50 percent of an organization's business data will reside outside the physical walls of your corporate data center, up from less than 10 percent today. According to Eurostat, the statistical office of the European Union, about 20 percent of enterprises will rely on cloud computing across the Organization for Economic Co-operation and Development. (Finland is currently leading the race at 50 percent, Poland in the rear at 6 percent.)

The problem is that few compliance officers are involved in high-level discussions around cloud computing and data privacy controls, which can be disastrous for companies as they expand into new locations.

"Employee data is becoming something on the forefront of compliance," says Marie Blake, executive vice president and chief compliance officer at BankUnited N.A. "To avoid an in-house privacy breach, you have to think about what is included in privacy data, like information governance, and you have to move with the direction of the industry."

Currently the industry is moving to play catch up with the risk. One example is the massive breach of financial institutions at JPMorgan and several other large banks last year, where prosecutors and IT security reportedly are still sizing up exactly how the attacks happened and how widespread the damage was (tens of millions of customer records, at least).

IT security tools will help that threat, but often tools address one specific risk. If the process for governing information is weak overall, that leaves the company exposed to any number of other risks your IT security tools don't address. And the moves in Europe and elsewhere around the world to strengthen data privacy laws makes that need for information governance all the more acute.

"From a compliance perspective you want to put policies in place to defend a claim," Cipperman says. "This is sometimes hard for compliance officers to do because it's not easy to understand what are the data security operations in place."

Pressure on CCOs

"The CCO mandate is to be aware of and ensure their organization adheres to the laws and regulations relevant to their business. Therefore they should absolutely be at the table for discussions around technology," says Janet de Guzman, director of compliance at OpenText, an enterprise information management firm. "Data and privacy protection is becoming a critical part of the compliance function because it's not only their own data at stake but the data of their customers and other stakeholders."

Blake says that not many CCOs are involved in their companies' data privacy committees, and she expects that to change over time as companies realize that CCOs bring critical knowledge about regulatory requirements to their cyber-security discussions.

"The inclusion of the CCO function in defining controls related to things like cloud computing has yet to hit maturity," Blake said. She compared it to vendor management, where initially compliance officers were not involved but are now vital voices at the table. (Think of all the

## EU ON DATA PROTECTION REFORM

The following is an excerpt from the European Council on data protection reform.

In the last few decades, the European Union has adopted several pieces of legislation to protect personal data, the main one being the 1995 data protection directive. However, since the Lisbon Treaty, protection of personal data has been a fundamental right under EU law, recognized by the Treaty on the Functioning of the European Union and the EU Charter of Fundamental Rights. This means the Union now has a specific legal basis to adopt legislation to protect this fundamental right.

Rapid technological developments in the last 2 decades have brought new challenges for the protection of personal data. The scale of data sharing and collecting has grown exponentially, sometimes taking place on a global level, and individuals are increasingly making personal information publicly available. The economic and social integration resulting from the functioning of the internal market has also led to a substantial increase in cross-border flows of data. To take all these developments into account and promote the digital economy, there is a need to ensure a high level of protection of personal data, while at the same time allowing for the free movement of such data within the EU.

In the case of personal data used for law enforcement purposes, there is a growing need for authorities in the member states to process and exchange data as part of the fight against transnational crime and terrorism. In this context, clear and consistent rules on data protection at EU level are fundamental to improving cooperation between those authorities.

Source: European Council.

trouble third parties can bring to your business.)

"I see that evolution in the information security and data protection space as well," Blake says. "It's simply a matter of time for banks to further include the CCO into that realm of information governance."

Ground Zero for privacy regulations complicating business operations is, of course, France. French data protection laws date back to the 1970s, and the tough stance of the Commission Nationale de l'Informatique et des Libertés, its data protection authority, has flummoxed many U.S. businesses. Last year CNIL fined Google €150,000 ($164,000) for changes the company made to its privacy policies.

The enforcement was triggered by an announcement that Google planned to replace product-specific privacy policies with single, overarching terms without notifying users ahead of time. An investigation by the Article 29 Working Party, an advisory body comprised of DPAs from 28 European member states, ruled that Google's privacy policy violated the European Data Privacy Directive because users were not informed of what data would be collected, or why, and data retention timelines were not public.

Regulatory skirmishes like that will force companies to consider data privacy compliance more seriously as they plot business moves. Europe is simply the biggest example, not the only one.

"The data security laws in the EU are complex, with non-EU countries beginning to follow suit," says Meena Elliot, chief legal officer at Aviat Networks, a $350 million maker of wireless transmission systems. "Google is facing challenges concerning the EU's views on the right to be forgotten from the Web. At the moment, there is no such requirement in the United States."

> "The inclusion of the CCO function in defining controls related to things like cloud computing has yet to hit maturity."
>
> Marie Blake, Chief Compliance Officer, BankUnited, N.A

But Google has been facing intense heat, especially from France. Recently the company received a formal notice from CNIL calling for Google to delist links from all European versions of Google Search and all global versions as well.

In response, Google argues that while European law enforces the right to be forgotten, its scope is limited and can't be applied globally. In fact, content (read: data) that is illegal in one country may be legal in another—one more challenge that companies face as they grapple with data privacy compliance.

"Google's stance in this case means a lot for compliance officers, and it serves as a warning for companies as they expand into new regions," de Guzman says. "It shows that the chief compliance officer constantly needs to be aware of new legal developments and have strong policies in place as governments around the world roll out new or more stringent data privacy laws."

"The compliance function has dramatically evolved over the years," Blake says. "Now we are engaging more in IT solutions that help to protect customer information. Although the functions between compliance, IT, and information security are still somewhat separated, we work very closely with these areas to have a sense of the overall controls in place to protect consumer and employee data." ■