CORPORATE COMPLIANCE INSIGHTS
THE PREMIER GLOBAL NEWS SOURCE FOR COMPLIANCE, ETHICS, AUDIT & RISK

JULY 2, 2019
KON LEONG

Uncovering the Data and Compliance Issues Banks Face Today

Advancements in technology have transformed the horizon of financial services, but these innovations are also raising challenges of their own in areas like cybersecurity, social media, data privacy and third-party risks. ZL Technologies' CEO, Kon Leong, discusses the latest data trends and their impact on banks.

The Interaction of Separate Privacy Regulations (GDPR and CCPA)

As more and more privacy regulations come into play, the landscape begins to resemble a checkerboard of various requirements, making operating across borders increasingly difficult. For example, for multinational institutions managing data from many regions, it can be a difficult technological challenge to identify who personal data belongs to and then apply the appropriate action. This challenge grows as new privacy regulations with their own requirements appear. Moreover, privacy measures have to seamlessly communicate with other management functions, such as SEC compliance — which, counter to privacy regulations that require deletion, mandates retaining documents — records management, e-discovery, analytics and more. Consider the following example: An organization receives a request to delete a subject's data. Can they delete it? No, they have to check if it's needed for records, legal and compliance. Each of these functions need to be managed holistically, and therefore using point solutions to satisfy them individually creates its own logistical nightmares.

An Increased Need for Information and What's Next

Prior to GDPR, we had already started to see a convergence of the critical data management functions toward holistic data governance. We were on path for a complete convergence within the next decade. Privacy regulations have moved up the timeline of this convergence. Enterprises are slowly recognizing that privacy must be included within

the equation of information management. Or, to state it even more directly, information management and privacy are one and the same. The controls needed to truly manage data are the same ones needed meet privacy requirements. This is an overlooked aspect of privacy that is often lost in privacy conversations.

The Pros and Cons of Cloud Deployments

The cloud's benefit to financial institutions revolves around the versatility it offers as a component of hybrid data management. Cloud, on-premise, hybrid, multicloud and in-place management are all management modes that should be deployed in synergy as part of an organization's greater data management strategy. The ability to manage across all modes provides a type of flexibility that is key to navigating today's governance landscape.

Employee Data Under GDPR

While customer data, often stored in structured database systems, is most commonly discussed in the context of privacy, internal data such as employee-created documents are just as relevant. This is data created *by* humans *for* humans, found in repositories such as file shares, SharePoint sites and email. Managing this data is necessary to GDPR compliance; however, what is missed is the fact that once it is managed, it also provides unlimited potential for business use cases such as analytics. For example, with control over employee communications, it becomes far simpler for managers to identify subject matter experts and "STPs"—the same 10 people in every department that get everything done. On simple review of company communications and the go-to people light up like a Christmas tree. Of course, internal analytics must be treated with care, but we've seen that the need to protect employee data can actually be an extra push to take analytics to the next level. It's counterintuitive since analytics and privacy seemingly serve opposing purposes, but once you see past that, you realize it all comes down to data management.