COMPLIANCE

Why Proactive Data Management is Key to Conquering Compliance

FEI Daily | 12/12/2018

by Michael Powell

Compliance with GDPR requires absolute control over enterprise data, something fractured compliance measures cannot adequately handle.

©Olivier Le Moal/ISTOCK/THINKSTOCK

At the heart of all business operations is one goal: make money. As such, organizations structure around revenue generating channels, often to the detriment of the bigger picture, and a fissure occurs. On one side, revenue generating activities; on the other, the unpleasant necessities of running a business. Too often, compliance is swept into the latter until a crisis brings it into glaring focus.

The latest such event is the enactment of the EU's General Data Protection Regulation (GDPR) which fundamentally changes how organizations approach personal data. Compliance with GDPR requires absolute control over enterprise data, something fractured compliance measures cannot adequately handle. To cohesively comply with GDPR and the bevy of other regulations to which financial services firms are subject, a comprehensive, proactive, and unified data management strategy is key.

Identify All Data Sources

The first step to building a proactive data management strategy is understanding your current environment: what you have and where it is. Most likely, data is scattered across dozens of environments, if not more, ranging from file shares to email servers to communication resources like Slack or Dropbox. While these sources all provide value to end-users, they complicate compliance measures, especially as new sources—and instances of each source—are added. Remember: regulators won't care that no one communicated a new source to you; they'll only care you didn't know about it.

Many of the biggest challenges compliance officers face in complying with GDPR and numerous other regulations can be traced back to these data silos. In the past, collecting and reviewing regulated communications was the industry's largest data management challenges. While no easy task, it pales in comparison to GDPR's scope: all EU resident data held *anywhere* in an organization's environment.

The transition to a compliant data management strategy begins with locating these disparate data sources and bringing them all under the purview of the compliance team. There are three possible approaches to this task. The first, to merely disallow use of anything behind a few easily manageable systems, is unworkable in practice. Organizational efficiency relies on storing and acting upon data in more than one location. The second is to apply the full array of compliance processes to each silo individually, a typically labor intensive and error-prone endeavor. For large enterprises, this is simply not sustainable. The final option is to govern everything through a single archive or repository and add new data sources as they emerge. This level of unity and automation removes redundant steps, simplifying compliance processes while making the fewest changes at the business-process level.

Know What's Coming Down the Pipeline

Financial services' regulatory landscape is constantly shifting as new regulations are added and existing ones get changed or reinterpreted. To keep up, compliance officers need require the ability to holistically view and act upon all organizational data. A system which allows this sort of universal access simplifies the handling of myriad requirements while providing valuable continuity in an otherwise shifting field.

If there's one thing the financial services industry knows well, it's that regulation is inevitable. While it's important to understand current regulations (including GDPR), it's also important to be prepared for what's next. The last thing you want is to restructure your organization's entire governance and compliance procedure just to repeat the whole process when the next regulation hits. That's why a proactive approach to compliance is so important.

Make Compliance a Priority

Proactive compliance requires organizations approach corporate data globally. This data cannot be kept in silos across technologies or business units if it is to be effectively utilized for compliance purposes. But doing so requires buy-in across the enterprise which means making compliance a priority.

Organizations' fractured treatment of enterprise data is a serious problem. When a department or team adopts a new tool, compliance is typically an afterthought (if it's ever considered at all). While it's important that compliance officers identify new data sources and potential sources early, they're seldom involved in the process in any real capacity.

As it stands now, the compliance team is generally a separate entity from other business units. This means, for instance, that the records management department could make the final deletion/disposition decision on a set of documents without an up-to-date view into compliance needs. Or the marketing team could add a new tool without understanding how the captured data must be handled under GDPR. This same issue carries throughout the enterprise in different forms. When compliance isn't an organizational priority, enacting proactive compliance procedures is an uphill battle.

Fortunately, the same governance initiatives that enable proactive compliance can, done properly, benefit core, revenue-generating business processes as well. Business analytics can be applied to the newly collected data. Legal can enter meet-and-confers better prepared and significantly reduce review fees. Records can work more efficiently. The entire organization benefits when compliance becomes a priority.

Michael Powell is a Solutions Consultant at ZL Technologies.