GDPR: The answer to the question "should we bother?"

Jan 29, 2019

OPINION by Kon Leong

Complying with privacy regulations is largely about data management. Therefore, effective privacy initiatives will also facilitate and strengthen an overall foundation for holistic data management.

Even as organisations grapple with privacy regulations such as the General Data Protection Regulation (GDPR) and the ensuing California Consumer Privacy Act (CCPA), there's uncertainty about the true nature of the financial risks they pose.

GDPR in theory could carry fines of up to four percent of global sales, but whether sanctions of this severity will truly be levied is a common question among large organisations. Some would even contend it makes sense to wait and see what regulators do before spending money on privacy initiatives.

Such lines of reasoning miss a few crucial points. Given the potential magnitude of the sanctions, regardless of their likelihood, top management such as the board of directors are now on notice as fiduciaries. They should have a very clear answer as to what the organisation is doing to mitigate risk.

Moreover, as new privacy regulations continue to be developed, what steps are they taking to prepare their organisation for this new landscape? They have a fiduciary responsible to ensure proper measures are taken to prevent severe fines and avoid reputational damage.

No one wants to be made the poster boy on a privacy breach and consequent fines. It should also be noted that the usual risk-deflection method of insuring away the risk is not available. In that sense, regulatory compliance is no longer business as usual, and neither is privacy.

The good news is that complying with privacy regulations is largely about data management. Therefore, effective privacy initiatives will also facilitate and strengthen an overall foundation for holistic data management.

To demonstrate, GDPR calls for the "right to be forgotten"— in other words an organisation must delete an individual's personal data upon request. Implementing the technology and processes to comply with such requests is not an easy ask. Consider how many different formats, locations, and patterns in which personal data can lie.

At the moment, executing a search across the enterprise to find a subject's personal data would challenge the current framework in many large organisations. Other difficulties lie in the ability to demonstrate how that data is being processed, per Article 30, and determining whether that data can in fact be deleted (legitimate business interests may prohibit that).

These technologies align with other necessary governance functions. For instance, the ability to perform an enterprise-wise search using complex queries dramatically improves the eDiscovery process. Few organisations have an adequate solution for finding and preserving documents across thousands of mailboxes and file shares for eDiscovery, but there is significant overlap between these capabilities and the capability to pinpoint personal data for GDPR.

GDPR is decidedly more difficult, but when fully implemented these technologies also serve as a highly competent eDiscovery tool. Additionally, defensibly deleting personal data that isn't necessary to the company also serves to mitigate risks associated with data breaches. Organisations are now grappling with understanding where various types of data—including personal data—lie throughout the enterprise, and how they can defensibly delete unneeded data. A successful GDPR compliance initiative will provide insight into this issue and enable much-needed data cleanup.

Finally, categorising data based on its various functions, such as records management, eDiscovery, analytics, and compliance, not only help to satisfy Article 30 of GDPR, but also strengthens each of these functions. Calibrating and synchronising the various management policies based on a hierarchy of functions ensures proper lifecycle management.

GDPR might seem like a headache at the moment, but complying with it puts organisations in an excellent position to manage enterprise data holistically moving forward. The truth is, the IT architecture of large companies has been overwhelmingly silo-based for the past several decades. Documents have lain across the enterprise in repositories, each managed in isolation and each serving a different function.

However, as the different components of information management converge, a siloed approach has become less and less feasible. GDPR simply hastens the timeline of when organisations must bridge across silos and manage data holistically because GDPR in fact respects no silos. It would be wise to see GDPR and other new privacy regulations as a sign of this continued convergence and to adapt accordingly. This is just the beginning.

Contributed by Kon Leong, CEO of ZL Technologies.

**Note: The views expressed in this blog are those of the author and do not necessarily reflect the views of SC Media UK or Haymarket Media.*