Compliance requires an evolved availability approach

By Claude Schuck

16 Apr 2018

Let's face it, data compliance is hardly a new thing. But given the extent at which the reliance of organisations on data has grown in recent years, its level of importance has increased exponentially. Simply put, fall foul of the regulatory environment and the financial and reputational impact could potentially force your business to close its doors.

In South Africa, companies are at an interesting crossroads when it comes to regulatory affairs. With the deadline for the local Protection of Personal Information Act (PoPI) looming and the European implementation of the General Data Protection Regulation (GDPR) set for the end of May, organisations are rushing to ensure their compliance.

PoPI requires effective data management structures

Claude Schuck 31 Oct 2017

But in the urgency to get ready, are organisations risking the effectiveness of their data storage strategies? Perhaps more pointedly, are South African companies using the pressure to become compliant as an excuse to put existing backup and business continuity plans on the backburner?

Lessons learnt

Whether it is PoPI, GDPR, or something else entirely, there are several guidelines to keep in mind when it comes to data compliance. These can be classified into five principles – knowing your data, managing your data, protecting the data, documentation and compliance, and continuous improvement.

Firstly, data knowledge is gained by identifying the personally identifiable information (PII) your organisation collects and who has access to it. Managing data is geared towards establishing the rules and processes to access and use PII.

> *Data protection revolves around implementing and ensuring security controls are in place to protect the information and respond to data breaches.*

Five steps to managing GDPR compliance

Obed Lesejane 1 Mar 2018

As the fourth principle indicates; documenting company processes, executing on data requests, and reporting any issues are critical to the success of getting to the 'compliant' stage.

Finally, an organisation must constantly evaluate procedures for data privacy and protection, and test and refine their protocols as the digital business evolves.

The road ahead

These principles must feed directly into the backup and business continuity plans of organisations. But while they seem obvious, the challenge has been to remain focused on applying them considering the evolving regulatory environment.

> *Decision-makers need to embrace a newway of maintaining an always-on environment. This means they must integrate all elements of compliance into their backup plans and vice versa. The one does not operate in isolation of the other.*

Perhaps the most important thing to remember is that even when the business becomes compliant, the journey does not stop. It is not some form of ‘fire-and-forget’ way of managing data.

Compliance, just like a business continuity and data strategy, is an ongoing process that requires a focus that integrates with the entire strategic approach of the business.

ABOUT CLAUDE SCHUCK

Claude Schuck is the regional manager for Africa at Veeam.

- Compliance requires an evolved availability approach - 16 Apr 2018
- Prioritise keeping your Bitcoin safe, secure, and available - 16 Mar 2018
- #BizTrends2018: Welcoming a new era of availability - 22 Jan 2018
- PoPI requires effective data management structures - 31 Oct 2017
- Addressing the risks of data loss - 11 Sep 2017

View my profile and articles...

For more, visit: https://www.bizcommunity.com