BIZCOMMUNITY

Understanding data sovereignty and its importance to your business

By Bryan Balfe

22 Sep 2015

With the recent passing of the Protection of Personal Information (PoPI) Act into law, the issue of data sovereignty has come into focus in South Africa. While not a new topic, PoPI has highlighted its importance and the potential effect on local businesses. Essentially, data sovereignty is the concept that information converted to digital form is still subject to the laws and legislation of the country in which the data is located.

jackmac34 via pixabay

With regard to PoPI, data sovereignty is specifically referenced in Section 72, which dictates regulations for which data may or may not cross the constitutional borders of South Africa electronically. While PoPI is not yet enforceable, the penalties for non-compliance when it is are hefty, and businesses would do well to gear themselves now to ensure they can meet requirements when the time comes. Understanding data sovereignty laws and the implications of this on business is essential.

The implications of Section 72

Since the enactment of PoPI, there has been much discussion around the implications of Section 72, which deals with trans-border information flows and under what conditions this is permitted, if at all. PoPI does not prohibit the transfer or storage of data overseas, yet there are exceptions that allow for this. This is particularly relevant given the growing prevalence of cloud-based data storage, which often results in data being stored across borders.

Ultimately, PoPI simply requires that organisations be careful when utilising online or cloud-based storage, applications or data transport mechanisms, that their data is still protected. If the destination or country of storage has similar or better data protection laws in effect, then there are no prohibitions on the transmission or storage of data within those countries.

While Section 72 does not prohibit cross-border data transfer, it does highlight a number of data issues, including the need to understand what data your business is keeping, where this data resides, and where it is being sent to. Lax practices with regard to third party activities and applications, including business-critical data stored on notebooks and smart devices, access to unsecured public cloud storage and other unfortunately common business practices could potentially land businesses in hot water.

Typically in many organisations there is a significant amount of data residing outside of corporate-owned data centres or firewalls - including laptops and other personal devices, in peer-to-peer sharing applications, and in online repositories of questionable locations. This needs to be addressed to prevent non-compliance problems.

Burdens of proof

Data sovereignty is not prescriptive, but rather requires that organisations make informed decisions based on their own security and compliance requirements. Organisations need to be aware that there are now certain burdens of proof that they need to satisfy with regard to demonstrating their ability to safeguard data. This does not apply to all data, but specifically to personal, private and sensitive corporate information.

For compliance and data security purposes, it is necessary to police where your data resides, in order to ensure that it does not fall into the wrong hands. Compliance is less about where data is allowed or not allowed to go, and more about ensuring due diligence is conducted on the destination. If cloud-based services are hosted in countries with strong data protection legislation, there is no issue of non-compliance. However, organisations need to know this, and understand where their data is, in order to ensure that they do not run into problems. To do this, organisations need to understand how data flows through their organisation as well as where it ultimately resides.

Where and what

The first step in PoPI compliance around data sovereignty, is to understand where, and what types are data are being stored. This must be done before it is possible to control data effectively, which is essential not only from a compliance perspective, but also for data security purposes. Once organisations can understand and assess where their data resides, they can then assess the risks involved and ascertain whether or not data is well managed from a compliance and risk perspective.

From there, a plan can be put into place to shore up any issues. However, simply blocking access to commonly used third party services like Dropbox will not solve the problem, as this will typically result in other unsafe data practices. Organisations need to support collaboration, file sharing, the sending of large documents, and other processes that typically drive employees to utilise third-party solutions, with a viable alternative that is secure and does not compromise data security and compliance.

At the end of the day, PoPI is here to stay, and compliance is not an optional process. However, ensuring data is secure is not just an exercise in compliance, but is also essential for protecting intellectual property, optimising storage and ensuring business continuity. The enactment of PoPI has simply formalised these requirements, and made best practices around data security legally enforceable. The benefits of compliance go beyond avoiding penalties, and enable organisations to address loopholes in policies and practices and ensure improvements can be made.

ABOUT BRYAN BALFE

Channel Manager at CommVault in South Africa

- Understanding data sovereignty and its importance to your business - 22 Sep 2015
- Controlling data risk in the BYOD onslaught - 19 Aug 2015
- What enterprises can learn from the MSP revolution? - 13 Aug 2015
- Warning signs your archiving strategy is not geared for the future - 24 Jul 2015
- Driving forces behind cloud computing - 22 Jun 2015

View my profile and articles...