BIZCOMMUNITY

PoPIA and Covid-19: Data strategies must adapt to change

By Chris du Bruyn

30 Jun 2021

The way companies view and approach disaster recovery (DR) and business continuity (BC) strategies have changed drastically in the past year, largely due to the Protection of Personal Information Act (PoPIA). DR and BC are normally considered critical in the event of natural disasters, hardware failure. However, the pandemic has amplified the need for backup and recovery.

Chris du Bruyn, operations director at Gabsten Technologies | image supplied

This is because data management requirements will need to be aligned with PoPIA with most employees now working from home (WFH) and the increase in endpoint devices used outside of the traditional office environment.

Compliance in the face of all this change is much easier to achieve with the right IT partner who can assist with understanding what data the organisation has, and where it’s stored. Only by effectively understanding their data can companies achieve compliance with PoPIA.

2020 vs 2021: what’s changed?

Before the Covid-19 lockdown that started in March 2020, companies had data pipelines that were running on-premises. Their footprint was small and even with the cloud in play, everyone had a clear understanding of who was responsible for information and data as it passed through the organisation. Then suddenly social distancing became the norm and everyone was forced to work from home and things got complicated.

With thousands of people now working from home, mostly on public networks, on-premises strategies have had to change to ensure that business and confidential information is secured and handled in a compliant manner. Now, everything is mostly cloud-based and companies have had to make sure that the data they are protecting from home or remote locations is secure up to the point where it moves into the cloud.

Compliance starts with understanding

Now, more than ever, it is critical for companies to grasp that they will not be able to achieve compliance without understanding what data they have, particularly if it’s personal information.

Additionally, companies must ensure the data that they have, whether it’s backup or production, is secure. While this is one of the biggest challenges currently with WFH, some things haven’t changed and the 3-2-1 backup rule is still relevant here. Companies need to keep at least three (3) copies of their data and store two (2) backup copies on different storage media, with one (1) located offsite.

With PoPIA, the offsite requirement becomes critical, particularly in light of PoPI’s requirement that this offsite data be stored locally. With so many companies moving to the cloud, it’s imperative that they determine exactly where the data is hosted.

Heightened compliance requirements

It’s important to remember that organisations are accountable for their data, especially if their employees are working from home. WFH does not absolve the company of responsibility for data protection, the company must find a way to ensure that their data is secure, irrespective of where it is stored and moved.

Companies will also have to re-assess their entire data management strategy and processes to ensure that personal information is properly handled and that it is destroyed in line with the time requirement of PoPIA, which limits the amount of time for which personal information can be kept. Destruction of information is important and companies need to have a clear plan as to how they're going to do it, especially when it comes to backups.

To ensure that they do not fall foul of PoPIA and avert the legislative penalties, companies must ensure that their data is secure.

6 critical PoPIA compliance steps to take before 1 July

Rian Schoeman 14 Jun 2021

Staff training with regards to PoPIA is vital to ensure that employees are adequately informed on the legislative requirements and that they understand what processing limitations apply to the data that they handle every day.

Additionally, businesses need to consider their data quality to allow them to eliminate information that is no longer relevant to the company. They will need to obtain data subject opt-in which includes informing the data subjects what information is held on them, for what purpose and when the data will be destroyed.

Further complicating the situation is the fact that PoPIA enables data subjects to request that their data be destroyed. This means that any company holding data pertaining to that individual needs to be able to immediately find, identify and destroy that information, even at a backup level.

PoPIA shouldn’t come as a surprise

Organisations have had more than enough time to prepare for PoPIA’s arrival, as it’s been on the cards for a number of years already. Given that the effective date is just around the corner, those organisations that have not yet got their compliance ducks in a row would do well to choose a data services partner that can help them meet all the necessary DR and BC requirements while facilitating and securing the new norm of working from home.

ABOUT THE AUTHOR

Chris du Bruyn is operations director at Gabsten Technologies.