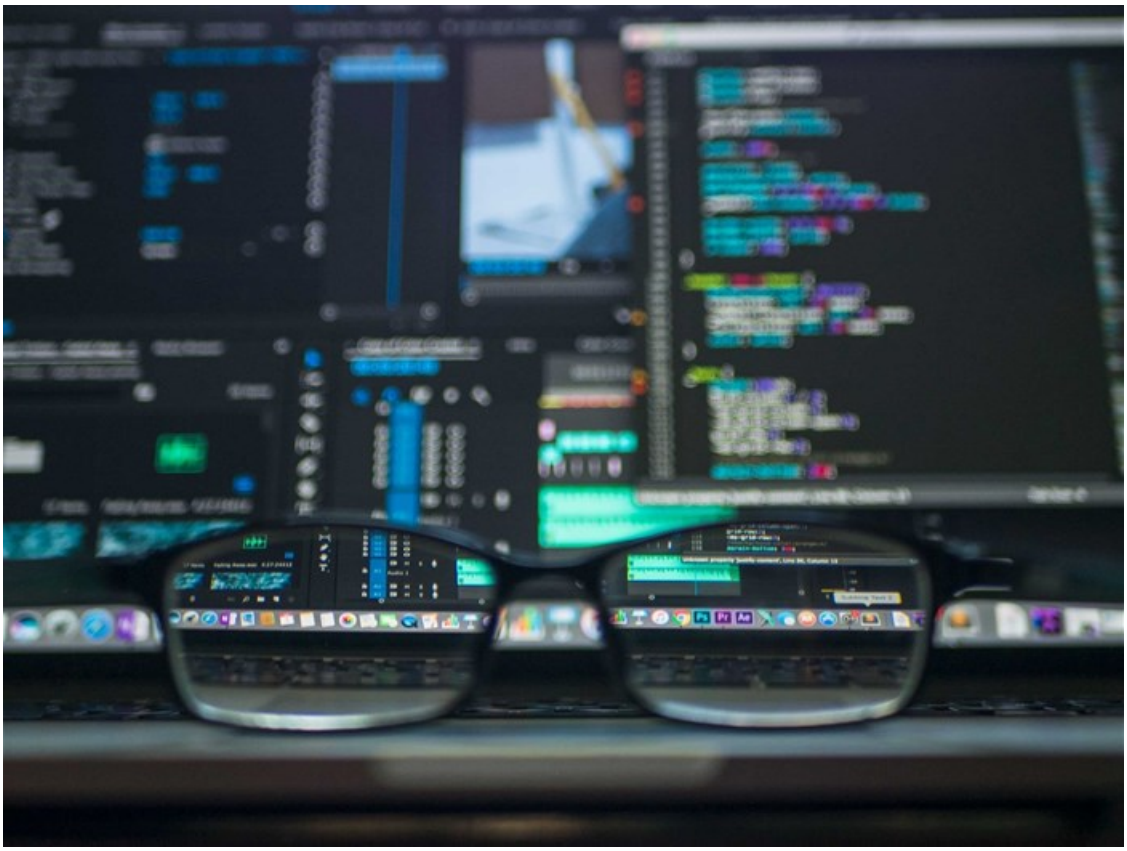
BIZCOMMUNITY

# Can data privacy concerns be managed when moving to the cloud?

By Gary Allemann

7 Sep 2022

The cloud, while offering many benefits, raises concerns around compliance, and some organisations have taken the approach of staying out of the cloud for this reason. However, while legislation such as the Protection of Personal Information Act (PoPIA) does add a layer of complexity to a cloud migration, the reality is that these laws apply regardless of where data is stored, and we need one policy to govern data across the entire environment.



Source: Unsplash

## More than just personal

When it comes to PoPIA compliance, it is important to understand that the law has several classifications of data that need to be protected, including data that deals with children, sensitive information such as religious affiliation and medical history, and personally-identifying information such as ID numbers.

It all needs to be protected under the law, but how that is done may differ according to the classification it falls under.

For businesses, data protection isn't just about the law either. All sorts of data are generated and contained within a business that could be detrimental if it falls into the wrong hands, including intellectual property such as new products and business innovation, as well as financial information.

## The danger lies on the inside

Every business is different, and every business' data is unique, so there is no one size fits all approach that will work, either for compliance or business reasons, whether data is stored on-prem or in the cloud. However, one common factor

seen with the majority of recent breaches and security incidents is that they have arisen through the abuse of authorised privileges.

What does this mean? It simply means that malicious actors have gained access to a data profile, through whatever means, including phishing or another cyberthreat, that has permission to access data that it should not be able to access.

Data permissions are frequently too broad, granting far too much access. This means that should someone with malicious intentions gain access to an authorised user profile, they will be able to see more than they should and do things like delete, copy, or share data, which also should not be permitted.

Data security and data privacy both come down to the need for more granular access control and permissioning.

## So how do we manage data privacy?

We need to define policies that limit data access only to that which people need to do their job, based on the individual and their context within the organisation. Data access can be filtered by role, by geography, by specific region, and even by data subject, and once segmented can be further limited at an aggregate level. Then, if someone with malicious intent gains access, the damage they are able to do is extremely limited.

Requirements for data security and privacy have evolved and it has become imperative to deliver fine-grained access control down to the individual level, irrespective of whether data is housed in the cloud or not.

Security policies must be consistently applied, measured to ensure they are being followed, and processes need to be put into place to alert to unusual behaviours that may signal a breach or malicious activity, respond to a breach, and identify what has been compromised.


Pick n Pay migrates IT infrastructure to Amazon Web Services

25 Aug 2022

The bulk of data breaches is caused by too much access to data and these privileges being abused. This needs to be addressed, and while the cloud obviously adds a layer of technical complexity to this exercise, the principles remain the same.

It all comes back to data management and data governance – if you haven't defined what data you have and classified it, it is impossible to apply data access control.

At a media briefing in late June, advocate Lebogang Stroom-Nzama, a full-time member of the Information Regulator

announced that their patience with transgressors was wearing thin. Whilst the stance to date has been to educate, in the future, potential fines of up to R10m, as legislated by PoPIA, will be a more likely outcome of breaches.

An integrated solution that provides a consistent, reusable, repeatable and auditable process across multiple platforms, is the answer to addressing this technical complexity and managing data privacy and PoPIA compliance, both on-prem and when moving into the cloud.

## ABOUT GARY ALLEMANN

MD of Master Data Management He is passionate about Information Communication Technology (ICT) and more specifically data quality, data management and data governance.
- Major trends impacting 2023 information and development planning - 27 Jan 2023
- Why data management is key to unlocking the digital transition of African banks - 12 Sep 2022
- Can data privacy concerns be managed when moving to the cloud? - 7 Sep 2022
- Effective WFH streamlined through data management as the next frontier - 8 Mar 2021
- Data governance is key to differentiating your customer experience - 20 Mar 2020

View my profile and articles...