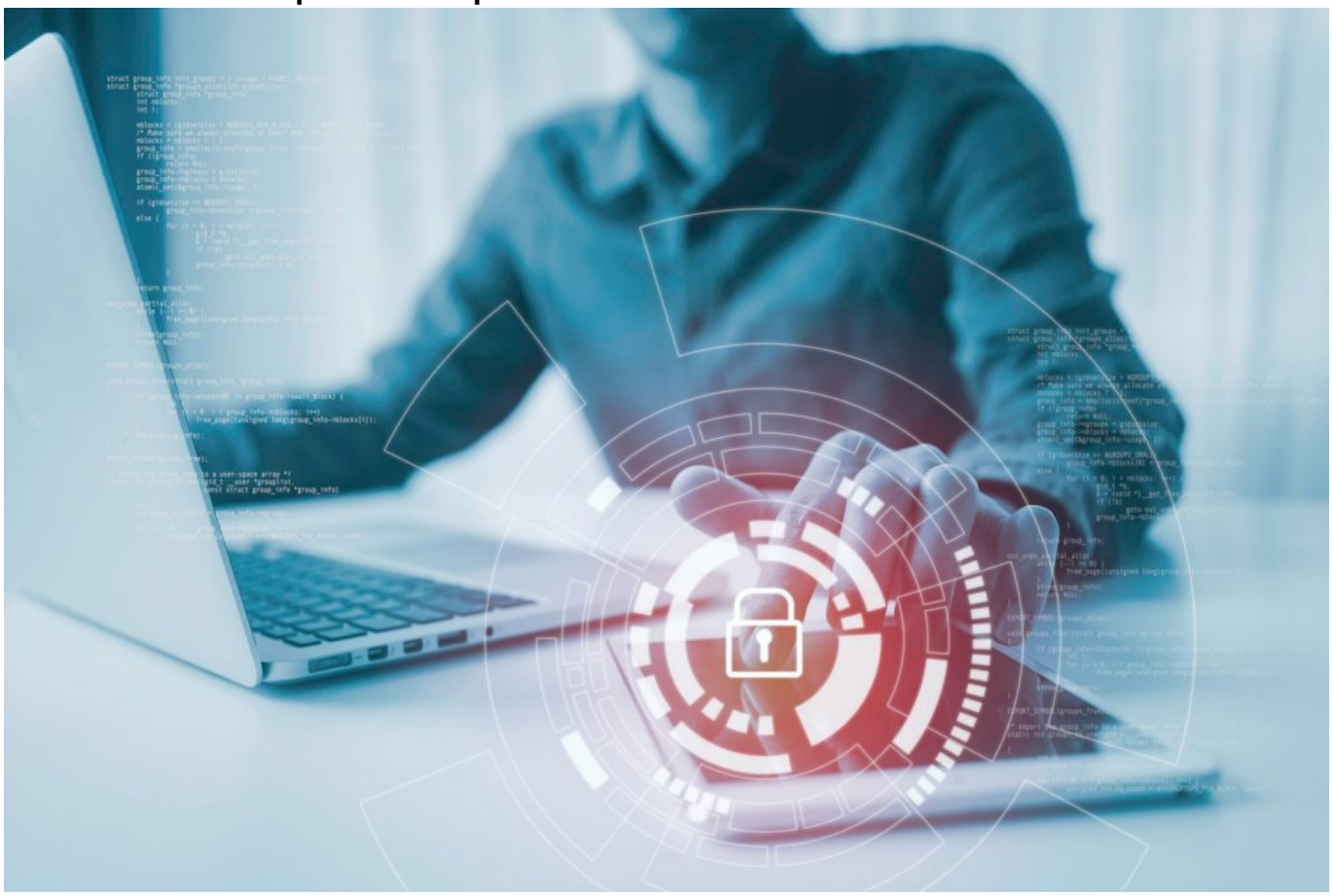
How will POPIA impact cloud providers?



While Covid-19 has seen organisations shift to cloud platforms overnight to help them remain operational while their workforces are operating remotely, too many are not up to speed with what this means in terms of their data.

This is particularly true now that the Protection of Personal Information (POPI) Act is coming into play, says Stuart Oberholzer, Information Security Compliance Manager at PaySpace, a leader in online payroll and HR software.

Discussing the role and responsibility of cloud providers in regard to complying with the POPI Act, Oberholzer noted that although cloud providers and third parties such as managed service providers are obligated to protect any personal data they handle, process or store, when it comes to ensuring the safety of their information, the onus is on the organisation that contracted them.

“Primarily, cloud providers need to ensure that data is stored within South Africa’s borders. In fact, should any data be stored outside the country, they should seek legal advice, and also get full consent from the data owners to make sure that any affected customers are aware of this,” he explains.

In addition, he says anyone who is storing data outside South Africa should make sure it is being stored in a territory that has either similar or stronger regulation in place than POPIA. “In terms of data responsibility, it ultimately lies with the customer to make sure their data is safe and secure. They need to understand where their data is being stored and if they haven’t been contacted by their cloud provider yet, they should take the initiative and contact them.”

Speaking of what cloud providers themselves need to do to prepare for POPIA, he says as with any other business, they need to understand their processes, such as how they are storing data, and ensure they are not processing any data that they shouldn't. "They can prepare themselves and their customers by fully understanding the requirements of the Act, in terms of what is required from them, as well as what their customers need to do."

In addition, he says any cloud providers that are hosting data need to ensure that the data is being stored securely, and that it can't easily be breached by an attacker.

Oberholzer refers to sections 21(1) and (2) of the Act, which specifies: "A responsible party must, in terms of a written contract between the responsible party and the operator, ensure the operator, which processes personal information for the responsible party, establishes and maintains the security measures referred to in Section 19. The operator must notify the responsible party immediately where there are reasonable grounds to believe the personal information of a data subject has been accessed or acquired by any unauthorised person."

He says to remember that cloud providers need to ensure there is clarity in terms of what is expected from each party. "By being prepared, they can help customers prepare. Ultimately, data protection in the cloud is a two-way street. The cloud provider is responsible for making sure data is stored correctly, that only the authorised people have access to it, that data is fully backed up, and that service is uninterruptible."

The customer, Oberholzer says, must ensure that their networks are secure, and that all devices that are used to access their information are secure too. "Ultimately, it is a shared responsibility model. Cloud providers must inform their customers that POPIA is happening, but at the end of the day, it is up to the customer to ensure that their own processes are POPI compliant."

Offering one more piece of advice, Oberholzer says cloud providers need to stay up to date with what the Information Regulator has to say and keep a close eye out for any updates. "As the POPIA process is refined, there are bound to be announcements and amendments that will ultimately affect every organisation. Check the Regulator's website daily, follow any directives that are issued, and make the changes at once."

This will not only help cloud providers protect their customers; it will also help to shield the provider from any reputational damage that might result from a possible leakage of data. "It is a common misconception among South African organisations when outsourcing to a third-party provider that any risk relating to a data breach transfers to that service provider, but this isn't the case. The POPI Act stipulates that the main responsibility of data protection lies with the company itself."