BIZCOMMUNITY

How to ensure PoPIA compliance among BYOD remote workforces

By Sián Fields

4 May 2021

Our personal devices, such as mobile phones, laptops and tablets are increasingly used to access movies, download Apps, store music or stream content from platforms like Netflix or Showmax. And they are often shared among family members, such as children who regularly use their parents' devices to enjoy online content. But, with PoPIA (Protection of Personal Information Act) finally coming into effect on 30 June this year, which aims to enforce protection of personal information by creating the lawful conditions for how this information must be managed, are employees - and the businesses that hire them - violating its rules? Potentially yes...

The increase in remote work, due to the national Covid-19 response, has also heightened this situation, as 79% of South African professionals now work from home, according to recruitment agency Michael Page, and their devices often contain sensitive or personal company information.

How then can a company ensure that its employees protect any personal data that they may have access to, when they are not located on the grounds of the organisation?

When the PoPI Bill first came into being in 2009, it certainly had not forecasted the current pandemic, but with the world of work changing and remote work becoming a more permanent thing, compliance to the Act needs to now account for this new phenomenon and companies need to adapt their corporate privacy compliance.

Shared responsibility

Companies are not solely responsible for compliance; employees also have to be accountable for maintaining corporate privacy when working remotely, which could be at home or a coffee shop. The latter could also have unsecure Wi-Fi networks, which immediately compromises a company's information security.

Residential developments not PoPI Act compliant could be fined up to R10m

Marina Constas 3 May 2021

Employees often use their own personal devices for work purposes. This could be such as having a company email on their personal phone, or accessing the shared Dropbox or other cloud-based servers via their personal laptops or tablets. And, even if the devices are possessions of the company which then should be better secured, they could still be used by other people in the home if sufficient protection of information has not been put in place.

Putting secure measures in place

As a start, companies should ensure that all laptops, computers and wireless technology are password controlled, while any personal information needs to be encrypted when in transit or at rest. Anti-virus software and personal firewalls should also be installed.

If laptops are left open on desks, or at the kitchen table, at home, there is a risk that others can gain access to company information. For this reason, employees need to ensure that it is logged off or shut down when they are not using it. They also need to remove any information that they are no longer using from their devices.

Issues can also arise when an employee's device is stolen or lost. If they fall into the wrong hands, there is a potential treasure trove of information waiting for hackers to mine. As such, all devices should have a PIN and password in place. Making a record of the phone's IMEI number, as well as the make and model number is also key. Companies should also investigate partitioning laptop hard drives for additional protection.

Digital ID verification on the rise

With the increase in remote work, more companies are turning to digital ID verification systems. This as the traditional security model within firms is no longer applicable as the IT perimeter cannot be defined in terms of location and asset ownership. Functions could include, among others, biometrics, facial or eye scanners, and even voice recognition.

PoPI Act readiness: 6 things to do

Anna Collard 12 Apr 2021

While this is a necessary and practical move forward as companies cannot request employees' physical ID in an office, it does unfortunately open them up to hacking, as there are so many more identification options to hack. This just creates a bigger vault of personal information that they can access. These hackers will throw resources at it using very clever people as there is value in obtaining and using this information illegitimately.

How to prevent a breach

Just like paper records should always be locked away from anyone else's sight, and not opened when using public transport such as while on an aeroplane or bus, so too must digital devices not be used when travelling. Employees must also avoid using USBs, unless they have been cleared by a company's IT team, create passwords, avoid sending or opening secure data when using a public Wi-Fi network and switch on "Find My Device" to help locate a device if it goes missing.

With just weeks until PoPIA is enacted, it is essential that companies – big and small – identify their risks of how personal information can be accessed. If there is a breach, it needs to be reported immediately to the employee's manager, IT department and Information Officer. The company may also be required to notify anyone whose personal information has been lost.

Covid-19 has put a spin on its compliance, but remote work is unlikely to disappear soon and action must be taken to ensure that personal devices are secure, at all times, and breaches are significantly reduced. Should companies not comply, they will be liable for potentially high fines and possible criminal sanctions.

ABOUT THE AUTHOR

Sián Fields, Intellectual Property and Technology Law Consultant from Reynolds Attorneys