BIZCOMMUNITY

# 3 priorities we should focus on

By Lecio De Paula

1 Apr 2020

The Protection of Personal Information Act (POPIA) in South Africa was meant to come into effect 1 April 2020, but the date has been pushed out. Similar to other legislations that have come into effect recently, the law will have an implementation of about one year, and many organisations have already begun taking steps to comply with POPIA.

Lecio De Paula, Director of Data Privacy, KnowBe4

However, for as many organisations that are ahead of the curve, there are at least twice the amount that are underwater and struggling to comply.

Regardless of your organisation's position, below are three priorities to focus on right now in order to comply with POPIA.

1. **Conduct a business privacy impact assessment**

By this point, you already know that POPIA is applicable to your organisation, so now you need to figure out what exactly you need to do to comply.

This means you need to figure out where you stand in comparison to POPIA's requirements by conducting a business privacy impact assessment. This is where you'll identify privacy risks in your organisation (aka noncompliance) and come up with a plan to either remediate or accept them.

The assessment should consist of a broad series of questions about your organisation as a whole, and also have questions that are more granular to specific processes and departments.

Business privacy impact assessments are the lifeblood of a privacy program and are essentially an audit you conduct against controls that your organisation has in place to comply. These should be conducted on a periodic basis.

2. **Ensure services are compliant**

   Once the privacy impact assessment has been conducted, it's time to focus on the more pressing issues you have chosen to remediate.

   Depending on the type of organisation you're in, different processes may have different priorities. If you're a SaaS tech company, you may begin by first focusing on what you need to do to ensure your services are in compliance with the law (compliant data retention, privacy policies, consent mechanisms, etc.).

   The key is to tailor your approach and tackle each issue with a risk-based approach. High-risk processes should always come first.

   A good approach to take is to start with client/customer personal data processes and work your way towards employee personal data. This will involve collaboration with many departments, so executive buy-in is a must; and privacy compliance should be pitched as business enablement.

   Privacy is there to provide trust to your employees and customers.

## 3. Monitor your systems

Now that you've established policies, procedures or implemented other controls required for compliance, it's time to create a system to effectively monitor the controls you put into place.

What's difficult about privacy is that everything is constantly evolving, and it will always keep you on your toes. Most organisations do not have a robust team of privacy professionals and it's usually limited to a few individuals if any at all.

Automation becomes paramount to ensure you have a robust privacy program with limited resources. Leveraging a governance, risk and compliance (GRC) tool to help you conduct assessments, map controls and data flows will be extremely beneficial in the long run.

If your organisation does not have to budget for one, using a cloud drive folder (albeit a little more tedious) will still work in this regard. You can use this to set up your templates and upload your compliance documentation for ease of access.

In more simplified terms, organisations should audit every location they store personal data on, see what controls are in place to protect this data (technical controls, establishing the legal basis for processing, CIA triad), and document those controls or the controls that are being put in place.

There are various other obligations of course, but initially, it’s all about understanding how, where and why your organisation stores personal data.

Without answering these few questions, you will not be able to comply with other aspects of POPIA, because as the name suggests, it’s all about protecting personal data. And if you don’t know where it’s stored, how you process it and why you store it, it will be impossible to protect.

## ABOUT THE AUTHOR

Lecio De Paula, director of data privacy at KnowBe4