BIZCOMMUNITY

PoPI Act readiness: 6 things to do

By Anna Collard

12 Apr 2021

The KnowBe4 and *ITWeb* online data protection survey in October 2020 discovered that when it comes to the preparedness of their organisation for PoPIA compliance, just under one-third (30%) indicated they were well prepared, while 39% said they were 'somewhat ready'.

Here six things that can be done to improve PoPIA readiness:

1. **Education and awareness:** This should be a top priority for organisations as we approach the PoPIA deadline. This is critical at every level of the business, from top management down to every person who works at the organisation.

   Everyone has to be aware of their responsibilities with regards to handling personal information and their roles when it comes to the safeguarding of personal information. People unfortunately are also the ones who react to phishing with emotion and make mistakes that can cost the business money and reputation and that can put critical data systems at risk.

People play a massive role in ensuring that the organisation remains PoPIA compliant, and the organisation remains secure and safeguarded.

They need consistent training and education so that their understanding of the threats can translate to the ongoing protection of information within the organisation, and to their own security hygiene practices as well.

2. **Information officer:** Secondly, organisations can really benefit from implementing the role of a dedicated information officer – a role that should be created specifically for the task of ensuring compliance and understanding.

Countdown for compliance with PoPIA
25 Mar 2021

The duties of the information officer include, amongst others, attending to the development and implementation of a compliance framework, ensuring that internal PoPIA awareness sessions are conducted and conducting assessments to identify any risks and necessary safeguards to the personal information that's processed.

3. **Mapping exercise:** Thirdly, conduct a data mapping exercise that identifies what type of personal information the organisation collects, who this information is shared with and where it is stored. This is immensely valuable, as it not only highlights areas of vulnerability that may not have previously been identified, but it also identifies potential risks that can be alleviated prior to PoPIA coming into effect.

This exercise can also be used to raise awareness and form part of an overall education drive, as it typically involves interviews with all major department heads. Once this is done, it should be followed with a privacy impact assessment (PIA), that identifies the risks and what could possibly go wrong in an environment.

It is a practical step that plays a pivotal role in embedding a more robust security foundation into the organisation. Part of the PIA would require a review of the security controls.

This will help refine the controls that are in place and identify what has to be improved on. For organisations that do not have these skills or systems in place, they can collaborate with a third party that can help conduct these types of risk assessments and reviews.

4. **Who you share info with**: Speaking of third parties, make sure you unpack who you share the personal information with, how compliant they are and what controls they have in place.

Why POPI compliance is not just an IT issue
Johan Scheepers 7 Dec 2020

They are as much a target as the business, so if they have any vulnerabilities, they can put your organisation at risk. Just make sure that the boxes are ticked with every service provider, platform and system so you are secured and compliant.

5. **Getting a consultant:** Consider hiring a consultant who can go through contracts and online privacy notices, and every other space where information is collected, to ensure that the right notices have been put in place.

These notices must be written in plain English and specify why the information is collected and how it is used so that consumers are informed and aware.

6. **Defining the processes:** The last thing that you should consider is to define the processes that make up your compliance programme and data breach processes.

   If there is a breach, who will notify the regulator, who will notify the customers and the media and what will employees be allowed to say – these are just some of the considerations that should be unpacked in advance to ensure the organisation is absolutely ready for whatever may be ahead.

ABOUT ANNA COLLARD

Anna Collard is the senior vice president of content strategy and tech evangelist at KnowBe4 Africa

- #BizTrends2022: Discriminatory AI and disinformation powered by deep fakes - 10 Jan 2022
- 5 important lessons to learn from the REvil ransomware attack - 13 Jul 2021
- Here's how hackers break into the business environment and how it can be avoided - 11 Jun 2021
- PoPI Act readiness: 6 things to do - 12 Apr 2021
- Top IT security threats in 2021 - 20 Jan 2021

View my profile and articles...