BIZCOMMUNITY

PoPIA: 5 concrete steps to start your journey today

By Gary Allemann

31 May 2021

With a month to go before the Protection of Personal Information Act (PoPIA) comes into effect on 1 July, companies that have left their compliance programme to the last minute may well miss the deadline for compliance.

Source: pixabay.com

One clear lesson to take from the GDPR experience is that a clear plan and roadmap for compliance is essential.

5 steps to PoPIA compliance

If you have just started, then here are five concrete steps to take in the next month:

1. Familiarise yourself with PoPIA

The Act is written in relatively plain language and you should be able to understand the basics from reading through it. As you read, remember that the intention of the Act is to protect the rights of your customers, staff and suppliers, not to destroy your business.

In most cases, what the Act is proposing is common sense - ensuring that sensitive data is not abused and that you use it for the purpose for which it is intended. Increasingly, consumers are preferring to deal with companies that take their rights and needs seriously, so PoPIA compliance can even be a competitive advantage. Of course, if you are unsure of a detail, it would make sense to reach out to your legal advisors for advice.

You may also want to familiarise yourself more broadly with the principles of data privacy, for example by taking our online Data Privacy and Protection Fundamentals Course.

PoPIA: Time is running out to become compliant

Wale Arewa 17 May 2021

2. Register your Information Officer with the regulator

The Act requires that your company formally register your Information Officer with the Regulator's office. In most smaller companies, this will be the CEO or MD, although the role can be delegated. For larger organisations, a Deputy Information Officer can also be registered. Luckily, the Regulator has developed a web portal to allow you to register online. The site also provides an overview of your responsibilities. So beat the rush and do this now.

Visit https://www.justice.gov.za/inforeg/portal.html and complete the online registration form.

3. Switch on the PoPIA compliance features on your website

The European Union's Global Data Protection Regulations have required websites to inform consumers about tracking cookies that may be in use, and give them the option to opt-out or accept cookies. Most modern web development environments (like Wordpress) have standard features that ensure compliance.

If you have not already done this, ask your web developer to enable GDPR compliance, as this is another simple box to tick for PoPIA.

4. Make sure you offer an unsubscribe function

If you use email newsletters, etc. make sure that you offer an opt-out capability and that you take these seriously. Similarly, call centres should take "do not call" requests seriously. Ignoring consumer's requests not to market to them is already illegal, but PoPIA does bring some additional consequences. It also leaves a bad taste in the mouth of many consumers to get unsolicited and irrelevant calls and emails, especially if they have made it clear that they are not interested. Are you marketing to people that actually want to hear from you?

5. Think about your breach processes

In the worst-case scenario, your business may experience a data breach - an unauthorised person accessing and potentially exposing the sensitive data of your customers, suppliers or employees. The Act requires that you inform affected parties that their data may have been compromised within a reasonable time. This is potentially the most visible area of the Act. So, ask yourself, if you (or one of your technical team) becomes aware of a potential breach of customer or other personal data at 3am in the morning, who will you call? You need to understand what your response will be in order to make sure that you manage the situation and minimise the impact.

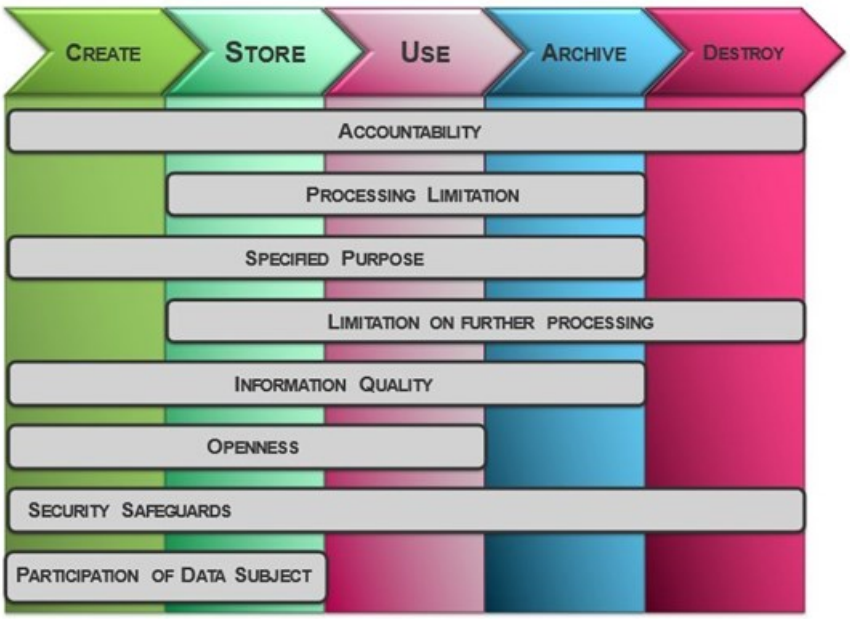
PoPIA: 5 tips to secure electronic signatures in your business

Zeldeen Muller 10 May 2021

PoPIA compliance is a journey

PoPIA requires that you embed sound data management principles through the data lifecycle, in order to ensure that personal data is both identified and that access is limited to users performing a legitimate purpose. For everyone but the smallest businesses, this can involve quite a bit of time and effort and may not be achievable by the July 1st deadline.

But you can make a start.



PoPIA compliance in the data lifecycle.

Image supplied

I recommend a top-down, risk-based approach to achieving compliance. This means identifying high-risk systems and processes and ensuring compliance for each of these, in order. We can help with a risk assessment, gap analysis and plan.

Our PoPIA accelerator leverages technology to provide a prebuilt operating model supporting compliance with PoPIA, GDPR and similar regulations. For bigger businesses, this may be worth exploring, along with other technologies that we offer for identifying, classifying and securing personal data fields.

This is not the time to become overwhelmed. The experiences of GDPR have taught us that companies that have a sensible, top-down plan, and can show that they are acting on it, are meeting the needs of the regulators.

**Disclaimer: This post does not constitute legal advice.*

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.

- PoPIA: 5 concrete steps to start your journey today - 31 May 2021
- Creating the elusive single customer view - 21 Jul 2014
- Big data driving convergence of the CIO and the CMO - 3 Jul 2014

View my profile and articles...