6 critical PoPIA compliance steps to take before 1 July

By Rian Schoeman   14 Jun 2021

The eleventh hour is upon businesses who are not Protection of Personal Information Act (PoPIA) compliant. The effective date of 1 July is upon us.

Photo by Scott Graham on Unsplash

Securing your data will help your business be in good standing with local and international partners. This will also enhance the reputation of your business and exempt you from fines and non-compliance.

Here are six steps your business can take before 1 July to be PoPIA compliant:

1. Encrypt everything

One of the major requirements under PoPIA is to ensure that you apply Generally Accepted Information Security Protocols. While these requirements are not the same for all organisations, some may apply to most businesses. One of these is that you need to secure all places where you store personal information: lock away any paper or file that contains customer information and limit access to the keys.

When it comes to computers, cell phones and servers, they need to be encrypted. Many versions of Windows have built-in encryption, but if you do not use one of those versions, it is time you start looking into encryption for your computers. At least all modern cell phones can be encrypted, and all mobile devices that process personal information need to be encrypted.

2. Train your staff

Now is the time to give your staff proper PoPIA compliance training, if you have not done so. With the PoPIA effective date coming closer, more people are claiming to provide compliance training. If you, like me, receive several emails a day offering PoPIA training, but they do not even state who the trainers will be, you have a cause for concern. This is why it is

crucial to verify trainers' credentials.

3. Enter into data processing agreements with operators

PoPIA requires a Responsible Party - the party that determines what to do with the personal information - to enter into written agreements with any other parties that will be doing further processing on their behalf. These agreements need to state how these operators will be required to process the personal information. Please note, this is not a contract with your customer; but these concern organisations handling personal information on behalf of your business.

4. Get consent now

If your business is planning on engaging in direct marketing, PoPIA is very strict about requesting and getting consent from people outside your contact or customer list. The website of the Information Regulator contains sample documents of such a request, which may be sent via email as an alternative.

Also, keep a record of all such requests and responses, as you are not allowed to advertise directly to people that have not expressly opted in on these requests. Failure to reply to the request does not equate to consent.

5. Get some sort of database in place to record requests from data subjects

PoPIA guarantees data subjects or the people whose information will be processed the rights of access to, correction, or deletion of their personal information. All such requests must be recorded and stored, as well as the action taken. Please note that not all deletion requests have to be adhered to, such as when you are required to process the personal information in terms of a contract.

6.Update your PAIA manual

The Promotion of Access to Information Act (PAIA) requires all companies to have a PAIA manual, but PoPIA added several requirements.

It is, therefore, very important to ensure that you update your PAIA manual to become compliant with PoPIA. This exercise is not as easy as it may seem at first. If you have the funds, hire reputable experts to draft one for your company. If not, refer to the publicly available PAIA manuals of large South African corporations for guidance.

ABOUT THE AUTHOR

Rian Schoeman is the head of legal and chief privacy officer at LAWtrust.

For more, visit: https://www.bizcommunity.com