POPIA : THE VERY FIRST STEPS

While there are many providers selling quick-fix POPIA packs and policies, our view is that POPIA compliance requires:

1. A process of **investigation and classification** of information handled, and then **developing/adjusting systems to effect and demonstrate compliance;**
2. A focus on **information technology systems and safeguards in place**, with an emphasis on **cybersecurity**; and
3. **Training and building awareness in staff** so that systems and safeguards are properly understood and maintained.

At ngoLAW we are in the process of developing an approach which will enable organisations to deal with the requirements of POPIA in a meaningful and effective way.

Developing, testing and then implementing this detailed approach will take some time, and our suggestion is that your organisation begins the POPIA journey with the following immediate steps:

FIRST STEPS	WHAT	HOW
Information Officer	Appoint the required 'Information Officer' and register them with the Information Regulator (note that this Information Officer will also be responsible for PAIA compliance matters)	Via the online portal: https://justice.gov.za/inforeg/ and the application form may be downloaded here: https://justice.gov.za/inforeg/docs/InfoRegSA-eForm-InformationOfficersRegistration-2021.pdf or via email: registration.IR@justice.gov.za
Security of information	Appoint a group/subcommittee or other body to conduct an assessment of the security of storage of information.	IT expertise will be essential for this investigation which should include: • What anti-virus and anti-malware systems do we have? Are they up to date and consistently installed across all devices used by staff and board; • Are all software installations up to date and all latest upgrades and patches installed and accepted? • Are staff and board aware of the dangers of phishing and equipped to recognise, report and not respond to phishing attempts? (Note: training and then testing on this aspect is crucial.)

		• What measures are we taking to ensure that personal devices used for work purposes are secure and protected? • If we use cloud storage, where are our cloud servers located, and are they in jurisdictions which are subject to GDPR/POPIA or similar? • Password protocols: Are staff and board using complex passwords and changing them at required intervals?
Direct Marketing	Calls for funding or promotion of services via email or any other electronic or digital communication (such as instant messaging) may now only be sent to 'an existing or previous donor/beneficiary/customer.	To approach a new donor/customer via electronic communication, you now require their consent in advance. Check that your fundraising/marketing team is aware of this change, and that they have made the necessary adjustments to accommodate it.

For a broad introduction to the principles and basics of POPIA, please see Nicole's presentation on this link: https://www.youtube.com/watch?v=MloJlyYXp7g.

A very useful navigable version of the POPI Act my be found at https://popia.co.za/

We will make available to our clients other useful information, checklists and documents as they are created.

Please contact us with your comments, suggestions and to share your own experiences.

Please feel free to share this document with anyone who may find it useful.

Kind regards and just keep breathing!

Nicole, Janice, Bandile, Lize, Lisa and Dorothy
ngoLAW (Pty) Ltd
Specialist legal consulting to the not-for-profit sector
https://ngolawsa.co.za/