POPI PAINT BY NUMBERS.

a practical guide to compliance

As society moves towards an information rich world, the way that we interact with each other, and do business, has fundamentally changed.

The way that we interact with businesses has also changed. Big Data has become a key ingredient to success, but with this new source of information comes a sense of vulnerability if the information is not stored and used in a safe manner.

Increased protection

The implementation of the Protection of Personal Information (POPI) Act is at the top of financial services providers' management agendas this year.

This will be a landmark piece of legislation as it will put South Africa on par with the rest of the world in terms of protection offered to the public.

POPI promises to be complex, but it needs to be in order to properly regulate the flow of information. This will be particularly strict in the insurance industry.

Start with what you have

Financial services providers need to kick off the compliance process by conducting a proper gap analysis to determine any potential data security shortcomings they may have. Particular attention needs to be given to the lawful processing, storing and safeguarding of clients' and employees' personal information.

Identify the type and purpose of the personal information that is held and where exactly within the organisation it is being processed and stored.

Do what you can today

The various phases of compliance take time. As such, it is imperative to always act without delay.

Come up with immediate yet practical and realistic action plans and deadlines for the various stages to successfully address any of the shortcomings identified above. Include operational staff in the process from the start.

Do not wait to update and align existing agreements, policies and procedures as well as appointment letters with future POPI requirements.

Do not reinvent the wheel

Save time by making use of the various POPI implementation tool kits and checklists that are available online. Use it as a base to work from.

Cut costs

The cost of compliance is real. Keep it as low as possible by engaging with your existing technology information service providers.

They will help you determine what system security and personal information safeguarding controls you have in place, and where it needs to be improved.

Further, brokers need to engage with underwriters or insurers for input, support and guidance where possible.

Appoint an Information Officer

The Information Officer (IO) of a business is by default the sole (or duly authorised) proprietor, owner or CEO of the business.

This is a huge responsibility as it means that IO's can be held accountable for the non-compliance of a business, not just in their professional, but personal capacity.

While both the business and the IO as representative of the business must be registered at the Information Regulator (IR), it is the responsibility of the IO to ultimately report to the IR on the relevant compliance matters.

It is the responsibility of the IO to ensure that the organisation complies with both the Promotion of Access to Information Act (PAIA) and the POPI Act. As such, the IO should ensure that all relevant procedures in the business are regularly updated and that personal information is lawfully processed, safeguarded and if necessary, destroyed.

The bottom-line

Organisations need to include all relevant third parties and business partners in their POPI compliance strategy from the start.

By including them in your compliance readiness assessments from beginning to end, you can unify and align your approach.

This will not only provide you with the peace of mind that you all comply at a practical level, but save you a lot of money, time and effort. POPI will have a major influence on every business sector in South Africa in the future.

Cornea Matthee
Group Compliance and Risk Officer
Centriq Insurance