**11 POPIA QUESTIONS TO ASK YOURSELF BEFORE 30 JUNE 2021**

**Note:** This is a complex topic and there is no substitute for tailored professional advice. What is set out below is of necessity no more than a simplified summary of some practical highlights.

You and your business are at substantial risk if you aren’t fully compliant with POPIA (the Protection of Personal Information Act) on 1 July 2021.

The clock is ticking! Have a look at the Information Regulator’s Countdown Clock here to see exactly how many days (and hours, minutes, and seconds!) you have left.

Be ready! Be compliant! Ask yourself these eleven questions -

1. **Does POPIA really apply to us?**

As soon as you in any way “process” (collect, use, manage, store, share, destroy and the like) any personal information relating to a “data subject” (suppliers, customers, members, employees and so on – whether individuals or “juristic persons” such as corporates and the like), you are a “responsible party”.

The formal definition of a responsible party is “a public or private body or any other person which, alone or in conjunction with others, determines the purpose of and means for processing personal information” - very few businesses and organisations will fall outside that net. Equally you are unlikely to fall under exemptions such as that applying to information processed “in the course of a purely personal or household activity”.

But don’t panic –. compliance is easily attainable for most businesses, particularly if you are a smaller operation with little in the way of sensitive personal information. Answer the questions below to get a feel for areas you need to concentrate on now.

1. **What risks do we run if we don’t comply with POPIA?**

If a data subject suffers any loss as a result of your breach of POPIA, the subject (or the Regulator at the request of the subject) can sue you for damages and you will be liable even if your breach was unintentional and not negligent. You also face criminal prosecution, penalties and administrative fines for some breaches.

1. **Have we registered our Information Officer/s?**

You must register your Information Officer (“IO”) with the Information Regulator – go to the Regulator’s Online Portal for the online and PDF versions of the registration form, plus the email address for support enquiries and a link to the Search page. The IO is responsible (and liable) for all compliance duties, working with the Regulator, establishing procedures, and the like. You are automatically your business’ IO if you are its “Head” i.e., a sole trader, any partner in a partnership, or (in respect of a “juristic person” such as a company) the CEO, MD or “equivalent officer”. You can “duly authorise” another person in the business (management level or above) to act as IO and you can designate one or more employees (again management level or above) as “Deputy Information Officers”.

1. **Do we have a list of all personal information we hold, and how and why we hold it?**

Make a full list of all the personal information you hold/process, whether physically or in electronic form. Then evaluate it against the test that, to collect and “process” personal information lawfully, you need to be able to show that you are acting safely, lawfully, and reasonably in a manner that doesn’t infringe the data subject’s privacy.

You must show that “given the purpose for which it is processed, it is adequate, relevant and not excessive”. Data can only be collected for a specific purpose related to your business activities and can only be retained so long as you legitimately need to (or are allowed to) keep it for that purpose.

1. **What security measures do we have in place?**

You must “secure the integrity and confidentiality of personal information in [your] possession or under [your] control by taking appropriate, reasonable technical and organisational measures to prevent … loss of, damage to or unauthorised destruction of personal information … and unlawful access to or processing of personal information.”

You are at great risk of liability and penalties if you suffer any form of data breach from a risk that is “reasonably foreseeable” unless you can prove that you took steps to “establish and maintain appropriate safeguards” against those risks. If you haven’t already done so, brainstorm with your team all possible internal and external vulnerabilities (physical as well as electronic) and address them.

1. **Do third parties hold/process personal information for us?**

If third parties (“operators”), hold or process any personal information for you, they must act with your authority, treat the information as confidential, and have in place all the above security measures. Further restrictions apply if the third party is outside South Africa.

1. **Do we know what to do if we suffer a breach?**

Any actual or suspected breaches (called “security compromises” in POPIA) must be reported “as soon as reasonably possible” to both the Information Regulator and the data subject/s involved.

1. **Do we do any “direct marketing” and if so do we comply with all requirements?**

Most businesses don’t think of themselves as doing any “direct marketing”, but the definition is wide and includes “any approach” to a data subject “for the direct or indirect purpose of … promoting or offering to supply, in the ordinary course of business, any goods or services to the data subject…”. So for example, emailing or WhatsApping your customers about a new product or a special offer will put you into that net.

If your approach is by means of “any form of electronic communication, including automatic calling machines, facsimile machines, SMSs or e-mail”, you must observe strict limits. Whilst you can as a general proposition market existing customers/clients in respect of “similar products or services” (there are limits and recipients must be able to “opt-out” at any stage), potential new customers can only be marketed with their consent, i.e., on an “opt-in” basis. They can be approached only once for that consent so keep a record of everyone you have asked.

1. **Does our website use cookies and if so do we have a cookie notice and policy in place?**

As countries around the world ramp up their privacy laws, we will all see many more examples of “cookie notices” on websites we visit. You may wonder how your own website should be configured, and the short answer is that if it uses cookies (almost all do), POPIA very likely applies despite the fact that there is no specific mention of cookies in the current legislation. Bottom line – to be on the safe side, have a cookie notice and policy in place. Keep yours simple and user-friendly.

1. **Do we have a privacy policy and a POPIA manual in place?**

POPIA - unlike PAIA (the Promotion of Access to Information Act) - doesn’t require you to have a POPIA manual in place but in larger businesses it is certainly a good idea to prepare one.

However you should certainly have a privacy policy in place. Make sure that everyone in your organisation is aware of it and of how critical it is to comply with it at all times.

1. **Is our staff team ready?**

Check that everyone in your business understands your compliance plan and their own individual roles and responsibilities in it. Make sure that nothing falls through the cracks – assign specific tasks to specific staff members.

***Bodies Corporate and Homeowners Associations – how POPIA affects you***

Bodies Corporate and Homeowners Associations (HOAs) fall into the POPIA compliance net and should be asking themselves the questions above.

In assessing what personal information you hold, how and why you hold it, and who you are sharing it with, remember to include not only scheme owners and HOA members but also your auditors, attorneys, managing agents, the CSOS (Community Schemes Ombud Service), security service providers and the like.

If you have gate security in the form of visitor registers, scanning of licence plates and driver’s licences and so on, be ready to address questions around having lawful reason for collection and retention of all the personal information you are gathering in this manner.