**How to avoid a R10 million fine and/or 10 years in jail**

**The Protection of Personal Information** Act 4 of 2013, (POPIA) comes into effect 1 July 2021. As a business owner, you are responsible, and you may face criminal charges if your business is found to be non-compliant.

Watch this space in our magazines for ongoing information and tips on how to be POPIA compliant.

**POPI Act Compliance Checklist**

|  |  |  |
| --- | --- | --- |
| **Step** | **Y/N** | **Action required** |
| 1. Appoint and register an **Information Officer (IO)–** this may be you, or a responsible member of your team. <https://www.justice.gov.za/inforeg/portal.html>. Define the role of the IO. |  |  |
| 2. Audit: Where and how does your business process, store, and share personal data? **Are there reasonable steps in place to properly protect and secure the data from possible breaches?** (This is harder to identify than you think… databases, phone numbers, addresses, biometrics, emails, messages, signed receipts etc.) |  |  |
| 3. **Analyse what information is required** at each touchpoint and whether it is strictly necessary. Obtain permission to use the information and restrict access to that information. It goes way beyond “Unsubscribe” messages. |  |  |
| 4. Develop a **POPI policy and procedures** for the consent, processing, storing, sharing and destruction of personal information. Insist on suppliers signing SLAs for POPI compliance. Develop a “right to be forgotten” procedure. |  |  |
| 5. Develop a **complaints procedure** and ensure that the relevant people are professionally trained to handle a query or a complaint. |  |  |
| 6. Consider privacy rights and the **potential for harm should hard copy files, laptops, phones, flash drives** etc fall into the wrong hands. This includes all disused technology devices. Take remedial action. |  |  |
| 7. Review **business websites and all social media platforms** in terms of privacy, security, cookie notices etc. and take remedial action. |  |  |
| 8. **Train all staff members** in POPI and make sure the policies are enforced, especially concerning direct marketing. |  |  |
| 9. Develop **ongoing self-audits and compliance checks** and stay abreast of industry best practice or codes of conduct. |  |  |
| 10. **Destroy** all physical and digital personal information that is no longer required for the purpose for which it was originally gathered. Be aware of tax and other statutory limitations. |  |  |