LIVINGSTON LEANDY

Privacy Compliance and Cyber Incident Response Policy

We are living in the Information Age, and technology continues to shape the way we work and interact with each other. Whether in an office, or working remotely, almost every profession imaginable uses some form of data daily. Most people and businesses also store data, and many of us use websites and other forms of communication to generate leads and publish ideas and information.

The legislative environment governing privacy compliance and cyber security is relatively new, and it is evolving rapidly. You've probably heard of POPI[1] (or POPIA), and perhaps the GDPR. You may have also heard that South Africa has a comprehensive new set of cybercrime laws that create new offences and impose additional obligations on some businesses.[2] How does it affect you? Why should you be concerned?

According to Interpol, South Africa suffers from one of the highest instances of cyber-attacks in the world. This ranges from online scams to extortion to business e-mail compromises and other forms of fraud and targeted attacks. It is inevitable that at some point a business or individual will face a cyber attack or some form of data loss and/or theft. What can be done? From a legal perspective, ensure that reasonable security measures are in place, train staff, have appropriate policies and procedures, consider insurance, but above-all, have a plan and a strategy in place: when the inevitable occurs, it will likely mean the attack is unsuccessful, or that at the very least having acted reasonably and in compliance with legislation, legal liability is limited.

In simple terms, and cyber-attacks notwithstanding, if you or your business uses data – and invariably almost every person and business does – then you should be thinking about on-going **privacy compliance**. This could be as straight-forward as a privacy policy and internal procedures and training. The nature of the data and business will determine what needs to be done; for example, a medical lab storing DNA will be very different from a hardware business. If you store data, particularly if it is

[1] The *Protection of Personal Information Act*. If you deal with personal information – and almost every business and person does – then you should have a privacy policy. Do you have a website? Is the privacy policy up to date? How do you deal with cookies (not biscuits!)?

[2] The *Cybercrimes Act*. Did you know? If you are a financial institution or an electronic communications service provider the Cybercrimes Act imposes additional obligations on your business.

personal information, you should have a **cyber incident response policy** that compliments your privacy framework. Usually, this document sets out your company's plan, and the steps that will be taken in the event of a data breach. Critically, if a breach occurs, and there are investigations by law enforcement and the Information Regulator, have you done enough?

If you are feeling a little unsure, or would like further detail, contact us to discuss any aspect of privacy and POPI compliance, as well as for cyber incident management and related issues.

Name:	Dr Lee Swales
Position:	Director
Department:	Commercial & Corporate
Telephone number:	(031) 536 7538
Email address:	lswales@livingston.co.za