LevorLegal

POPI Act Data Privacy Compliance **Health Check**

THESE QUESTIONS ARE BASED ON THE 8 CONDITIONS FOR LAWFUL PROCESSING OF PERSONAL INFORMATION

SET OUT IN CHAPTER 2 SECTION 4 OF POPIA

Accountability

- Have we appointed an Information Officer?
- Have we established a formal POPI compliance project with scope, budget, resources, time frame and etc?
- Can we demonstrate that our staff has been and will continue to be educated and trained on what the POPI means for the business and the way they handle information, and are they putting them into practice?

Minimality

- Can we show the Personal Information which we collect from people is not excessive?

Specific Purpose

- Do we have a clear purpose for gathering, storing or sharing Personal Information?

Consent

- Can we show that the people whose Personal Information we retain are aware of the fact that we have it and for what purpose?
- Do we have a POPI compliant privacy statement which our customers or end users can access and question us on?

Section 22

- Do we have procedures in place to deal with the notification of security breaches?

Special Personal Information

- Can we show that we are adhering to the rules regarding the processing of Special Personal Information?

Quality

- Can we prove the Personal Information is accurate and up to date?

Further Processing

- Do we understand the situations in which POPI allows for the sharing of Personal Information with third parties?

Security Safeguards

- Can we demonstrate that we have implemented measures to ensure that the Personal Information that we collect, and store is secure - whether it is on paper or on computer or any other format?
- Can we show that access to Personal Information is limited only to those with a strict need to know?

Openness

- Do we have a current PAIA manual on our website?

Effective Destruction & Retention Periods

- Do we delete/destroy Personal Information as soon as we have no more need to use it?

Information Officer

- Do we have a process to handle Data Subject requests and complaints?

Chapter 8

- Can we show that we are complying with the rules about Automated and unsolicited Direct Marketing?

Chapter 9

- Can we prove we are complying with the rules about transborder flows of Personal Information?

All Aspects

- Do we have a compliance framework and a clear strategy to ensure sustained and consistent compliance?

INFORMATION SECURITY ASSESSMENTS

As part of a privacy assessment, businesses are advised to undertake an independent information security assessment of the environment against the following 6 data protection orientated information security domains, as required by the relevant privacy regulations:

POLICY MANAGEMENT

THESE SHOULD INCLUDE:

Information Security Policy

(review and update current) including;

- Data Classification
- Access Control
- Password Policy
- Data Security
- Endpoint Security
- Encryption
- Vulnerability Management

Acceptable Use Policy

to be signed as part of the on-boarding process (review and update)

Risk Management Methodology

(strip risk section out of Information Security Policy) including:

- Third Party Risk Management
- Change Management Procedure
- Software Development Lifecycle Policy with consideration to Information Security assurance. ·
- Disaster Recovery and Backup Policy
- Identity and Access Management
- Data Security including Data Loss Prevention
- Encryption & Pseudonymization
- Incident Response Capability
- Third-Party Risk Management

The assessment should aim to provide an understanding of information security strategy and controls implemented by the business in order to establish current maturity and prioritise future efforts.

levorlegal.co.za • alexis@levorlegal.co.za