Personal Information Management Services

We will help you understand and successfully address the organisational impact of the Protections of Personal Information (POPI) Act.

bonutrim consulting

POPI Assessments and Implementations

Our scope of Personal Information Management Services aims to identify organisations Protection of Personal Information Act no. 4 of 2013 (POPI), and Data Protection readiness gaps and build their collective competence in addressing these risks efficiently and effectively.

The Bonutrim Cyber Security team has Experts who can assist clients to with cyber security and exposure to both ransomware, data breaches and other related cyber risks.

- Analysis of processing activities
- Data map assessments
- Records Management Strategy
- Data Breach Management
- IT security

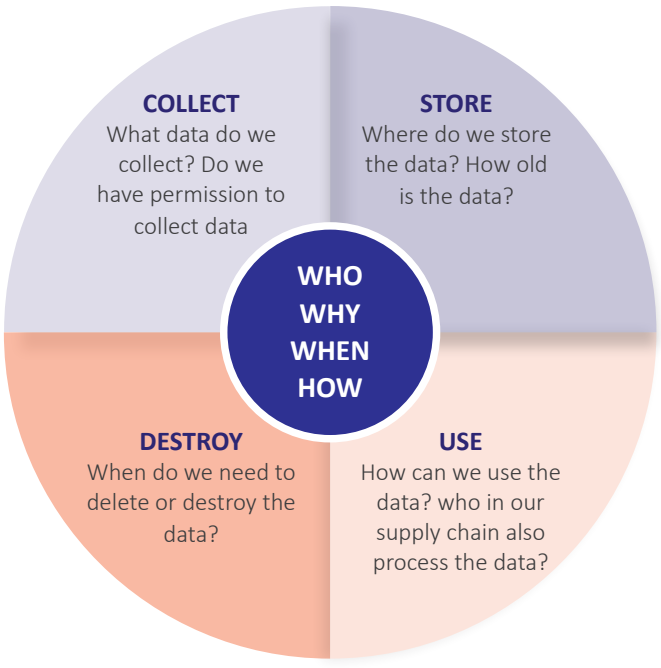
1. Training & Awareness
2. Monitoring
3. Incident Response

Who is affected by data regulations

The Protection of Personal Information Act (RSA): Organisations who decide why and how to process personal information (i.e Responsible Party).

Our POPI Compliance Framework

Owner consent & legal responsibility



The execution of POPIA should be done in a systematic manner beginning with a careful information planning exercise, where individual data which is utilized and handled by the business is assessed and examined mainly from a risk perspective, and the gaps and results are outlined. Thereafter, POPIA policies and related processes that are required can be implemented. After building the necessary strategies, then a carefully constructed project programme can be executed.

Bonutrim Consultancy have drafted a POPIA Template pack. These templates will have to be implemented at various sites and areas within your business. Should you require the full pack or parts of the pack, we are able to assist.

Some of the Templates available in our pack are:

- POPIA Policy
- POPIA summary
- POPIA guideline
- POPIA processing guide
- POPIA section 18 notices
- POPIA contract wording
- Operator agreement
- Trans border guideline
- Document storage and Archiving plan
- Document destruction guide
- Email disclaimer
- Direct marketing guides and opt in forms
- IT policy review and correlation with POPIA requirements
- Job description of the Information officer and required delegations to deputy information officers
- POPIA self-assessment checklist

We are able to supply a full pack, single templates, or a template specifically designed for you. For a quote, please contact us using the buttons below.

Complying with global privacy regulations that govern the use, collection and treatment of individuals' personal information is a significant and growing challenge. Until recently, global privacy compliance has been mostly an issue for large multi-national firms, but with the continued expansion of internet technology, like cloud storage services, global privacy compliance is fast becoming a concern for companies large and small.

The specific configuration of any privacy compliance program depends on the company's unique needs and requirements considering business needs, internal structure and organizational culture. The company's primary business risks must first be determined and then a plan must be crafted to minimize those risks and address compliance in a systematic way.

Privacy requirements typically differ depending on the nature of the company's:

- Industry and business.
- Data and the types of projects or tasks the company conducts.
- Geographic footprint.

To guide the process at the outset, a company should gather basic information regarding:

- The personal information the company collects, including whether it collects:
  - sensitive information, such as Social Security numbers or health information; and
  - information on employees or consumers, or both.
  - How the company collects personal information.
  - The purposes for which it collects personal information.
  - Who has access to the personal information.
  - How the company stores and disposes of data that includes personal information.
  - The greatest risks the company faces to its data.

Geographic issues related to its business operations and data, such as:

- the location of physical facilities, employees, servers or other assets;
- whether the company uses cloud storage for data; and
- the enforcement history of jurisdictions in which it operates or has assets.

Cross-border marketing issues, such as:

- whether the company directly markets products or services to residents of other countries; and
- the language used on its website, any mobile application or any other marketing materials.

Issues related to marketing and use of data, including the:

- types of marketing activities in which the company engages;
- overall collection, use and sharing of information in connection with marketing activities; and
- third parties involved in the marketing activities that collect, share or access data.

Contact us:

Cell: +27 82 478 1505 Email: Memme.Leepile@icloud.com

bonutrim consulting