OUR APPROACH TO POPIA COMPLIANCE

Abstract

The Protection of Personal Information Act (or POPI Act) is South Africa's equivalent of the EU GDPR. It sets some conditions for responsible parties (called controllers in other jurisdictions) to lawfully process the personal information of data subjects (both natural and juristic persons). The POPI Act is important because it protects data subjects from harm, like theft and discrimination. The risks of non-compliance include reputational damage, fines and imprisonment, and paying out damages claims to data subjects. The biggest risk, after reputational damage, is a fine for failing to protect account numbers.

Keywords:

POPIA – Protection of Personal Information Act

ISO – Information Security Officer

ISO27001 – International Standard for Information Security

GDPR – General Data Protection Regulation

ISMS – Information Security Management System

OUR APPROACH TO POPIA COMPLIANCE

In 2020 we decided to achieve POPIA compliance through the ISO27001 certification, which we officially obtained in November 2020. ISO27001 is an international standard that defines how to manage information security in an organization through the implementation of a robust information security management system (ISMS). To this ISMS we added the additional items required to achieve full POPIA (and GDPR) compliance.

How are we meeting POPIA compliance?

This section explains our approach and actions taken to ensure compliance with POPIA. Contact information of our ISO, references to various documents and policies and other critical information are mentioned in the *reference table* at the end of this document.

Summary

We are committed to preserving the confidentiality, integrity and availability of all the physical and electronic information and information-related assets relevant to meet the purpose and goals of the organisation. This includes the handling of personal data or “Personally Identifiable Information” (PII).

Furthermore, we are committed to ensuring compliance with the European Union General Data Protection Regulation (GDPR) and the UK Data Protection Act (DPA) 1998 and any other data protection legislation or regulation relevant to our business operations.

In complying with the above-mentioned legislation and regulation, the organisation makes commitments to implement policies and processes related to that compliance and to make staff and relevant third parties aware of their responsibilities when handling personal data.
More detailed policies and processes support this document, including our Information Security Policy. A GDPR compliance workspace is also maintained in line with Information Commissioner Office recommendations. These are located and managed within our ISMS platform. References to these documents can be found in the *reference table* at the end of this document.

What are our obligations towards you?

We, Headspace Technologies, are obligated to secure any Personal Identifiable Information (PII) provided to us. We will destroy, move and/or modify PII to the needs of the information owner on request to our ISO. We are obligated to adhere to these requests given the authorization of the information owner and the correct processes are followed. We acquire consent from information owners before processing PII and are obligated to request the consent in a timely manner before we plan to use/process the information for different purposes than for previous given consent.
Your PII will be controlled through secure systems and removed from our ownership based on a retention schedule. These schedules acts as audits to ensure that we are not in possession of PII after agreed/consented period. We are obligated to supply information owners' copies of our policies and procedures on request to clarify and/or prove the existence of the same. We must also have an accessible environment for information owners to contact, request or demand actions, procedures and/or information regarding their PII and security related enquiries.

All members of staff have an obligation to report actual or potential data protection weaknesses, events and incidents where compliance may be breached. This allows us to:

- Investigate the failure and take remedial steps if necessary
- Maintain a register of compliance failures
- Notify the Supervisory Authority (SA) of any compliance failures that are material either in their own right or as part of a pattern of failures

The reporting of such weaknesses, events and incidents will be managed through our Information Security Incident Management processes.

What are your obligations towards us?

As the information owners of your PII, you are obligated to supply us with consent before we may process your information. You must follow procedures and processes put in place by Headspace Technologies to request any modification, removal or relocation of your PII.

Reference Table

Policy/Document	Location	Action
Website Privacy Policy	Commspace Website/Legal	Publicly available
Data Protection Policy	Commspace Website/Legal	Publicly available
Information Security Policy	ISMS	Request from ISO
Data Retention Policy	ISMS	Request from ISO
Data Breach Response Plan	ISMS	Request from ISO

Contact our ISO: iso@headspacetech.com.