ThoughtCorp - 2001/028544/07

PoPIA Compliance Manual

01 July 2021

1. Table of Contents

2. Purpose of this Document

This document serves as a manual to ensure ThoughtCorp PoPIA compliance, maintenance, and monitoring, as prescribed in sections 14 and 51 of PAIA.

3. Information Officer

Robert Braune has been registered as the Information Officer for ThoughtCorp.

4. Impact Assessment

A personal information impact assessment is conducted on an annual basis to ensure that adequate measures and standards exist in order to comply with the conditions for the lawful processing of personal information. Based on the assessment, internal measures are developed together with adequate systems to process requests for information or access thereto.

5. Awareness and Training

Internal awareness sessions are conducted at ThoughtCorp on an annual basis to make provision for POPIA, regulations made in terms of POPIA, codes of conduct, or information obtained from the Regulator.

6. Activation of Website Compliance Features

The European Union's Global Data Protection Regulations have required websites to inform consumers about tracking cookies that may be in use, and give them the option to opt-out or accept cookies. This feature will be enabled for ThoughtCorp clients on request and acceptance of a quotation.

Further to this, any ThoughtCorp clients that require changes to their website privacy policy or deletion of client databases will be provided with a quote, and on approval those tasks will be attended to.

ThoughtCorp has also activated a cookie notification and acceptance on its own website, along with access to the ThoughtCorp PoPIA compliance manual.

7. Security Protocols

Physical access controls

Thoughtcorp has implemented reasonable measures to prevent physical access, such as secured access to the office, to prevent unauthorized persons from gaining access to inside the office. Visitors are to sign in at the gate before entry into the office park.

System access controls

Thoughtcorp has implemented reasonable measures to prevent data from being used without authorization. These controls vary based on the nature of the processing undertaken and may include, among other controls, authentication via passwords.

Data access controls

Thoughtcorp has implemented reasonable measures to ensure that data is accessible and manageable only by properly authorised staff. Direct database query access is restricted and application access rights are established and enforced to ensure that persons entitled to use a data processing system only have access to the system to which they have privilege of access.

Transmission controls

Thoughtcorp has implemented reasonable measures to ensure that the transmission of data is secure. All database excel files that are received and/or sent via email is done via a OneDrive link and is password protected. No databases are sent via email attachment.

Input controls

Thoughtcorp has implemented reasonable measures to allow it to check and establish whether and by whom data has been entered into the website, modified or removed.

Data backups

Thoughtcorp has implemented measures to ensure that back-ups of relevant databases are taken on a regular basis, are secured. Backups will be securely deleted or erased when it is no longer needed for a permitted business purpose or termination by the client.

Data segregation

Thoughtcorp has implemented measures to ensure that data from different subscriber environments is segregated on its systems to ensure that data that is collected for different purposes is processed separately.

8. Data Processing Agreement

PoPIA requires a Responsible Party (the party that determines what to do with the personal information) to enter into written agreements with any other parties that will be doing further processing on their behalf. ThoughtCorp is therefore required to have agreements with any sub-contractors that process personal data. This agreement states how these operators will be required to process the personal information. These services will need to be factored into our direct marketing costs for clients.

9. Marketing Consent and Storage

For company and client direct marketing, ThoughtCorp keeps a record of all direct marketing requests and responses, as companies are not allowed to advertise directly to people that have not expressly opted in on these requests. PoPIA guarantees data subjects or the people whose information will be processed the rights of access to, correction, or deletion of their personal information. All such requests are therefore recorded and stored by ThoughtCorp, as well as the action taken.

10. Data Breach

In the event of a data breach, where an unauthorised person accesses and potentially exposes the sensitive data of ThoughtCorp customers, suppliers or employees, ThoughtCorp will respond to this scenario and inform the relevant party via email within 24 hours, and advise on any corrective measures to be taken.