DTE PROJECT MANAGEMENT (PTY) LTD

POPIA ACT POLICY

Effective Date: 08-05-2024

Configuration Status: Final

DOCUMENT TITLE	DOCUMENT NUMBER
POPIA ACT POLICY	**DTEP-MNP-0002**

AUTHORISED BY	NAME	SIGNATURE	DATE
Managing Director	Gavin Schroeder		
Technical Director	Johan Steyn		

REVISION

REV NUMBER	DATE	DESCRIPTION
A	19-08-2023	Draft
B	16-02-2024	Formatting
C	08-05-2024	Final for Review

DTE Project Management (Pty) Ltd (Reg Nr 2005/01074/07)
Physical Address: 1st Floor, Cascade House, Constantia Office Park, Cnr 14th Avenue and Hendrik Potgieter Street, Weltevredenpark, Johannesburg 1709
Tel: +27 (0)11 475 0643 Fax: +27 (0)11 475 0647

Controlled Distribution

The controlled copy of this exists on the **DTE PROJECT MANAGEMENT (PTY) LTD** Server as well as in the master Quality Manual File:

Path
Z:\Data\3_Data\000000 - DTE Procedures Instructions\Quality Management System Documentation\01. Management

Amendments

All Changes must be recorded on the Amendments List below.

Table of Amendment			
Rev. No.	**Pages affected**	**QAR No.**	**Revision Date**
A	Pages 1; 2; 3….9		2023-08-19
B	Pages 1; 2; 3….9		2024-02-16
C	Pages 1; 2; 3….9		2024-05-08

Table of Contents

1. TERMS AND DEFINITIONS

Term	Explanation
Data	Information, which is stored electronically, on a computer, or in certain paper-based filing systems
Data Subjects	For the purpose of this policy, this classification includes all living individuals about whom we hold personal data. All data subjects have legal rights in relation to their personal data.
Information Officer	The Information Officer has a responsibility to establish practices and policies in line with applicable data protection legislation.
Data Controller	The person who determines the purposes and manner in which any personal data is processed.
Data Users	Personnel whose work involves using personal data. Data users have a duty to protect the information they handle by following the Privacy Policy.
Data Processors	Any person who processes personal data on behalf of an Information Officer. Employees are excluded from this definition, but it could include suppliers which handle personal data on our behalf.
Personal Data	Data or information relating to an identifiable natural person. An identifiable natural person is one who can be identified directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, and an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic cultural or social identity of that natural person.
Processing	Any activity that involves use of personal data. It includes obtaining, collecting, recording, or holding the data, or carrying out any operation or set of operations on the data including organizing, amending, retrieving, using, disclosing, erasing, or destroying it. Processing also includes transferring personal data to third parties.
Sensitive Personal Data	Information about a person's racial or ethnic origin, political opinions, religious or similar beliefs, physical or mental health or condition or sexual life, or about the commission of, or proceedings for, any offence committed or alleged to have been committed by that person, the disposal of such proceedings or the sentence of any court in such proceedings. Sensitive personal data can only be processed under strict conditions and will usually require the express consent of the person concerned.
Data	Information, which is stored electronically, on a computer, or in certain paper-based filing systems
PAIA	the Promotion of Access to Information Act 2 of 2000

2. PRIVACY POLICY IN TERMS OF THE PROTECTION OF PERSONAL INFORMATION ACT

2.1 Objective

The objective of this policy is to outline the Company's position on the privacy policy in terms of the protection of personal information. Complying with the law in respect of the data it holds about individuals, follow good practice and to protect the organisation from consequences of a breach of its responsibilities.

2.2 Application

The purpose of this privacy policy is to promote the principles the Company must follow to achieve our data privacy responsibility. The policy summaries what the Company must do when processing personal data at every level within **DTE PROJECT MANAGEMENT (PTY) LTD**. It is intended to:

- Increase awareness of governing, legal and business requirements relating to privacy, which impact how we process personal data.
- Set out the standards that we are dedicated to follow when we process personal data.
- It helps us to meet our governing, legal, and business responsibilities when we process personal data.

This policy applies to all employees, Shareholders, fixed term employees, temporary employees, and contractors. We all have a responsibly to ensure that **DTE PROJECT MANAGEMENT (PTY) LTD** respects the privacy of individuals, that the systems and equipment that is used by **DTE PROJECT MANAGEMENT (PTY) LTD** to process personal data is secure and that personal data is processed in accordance with applicable laws and regulations. Ss

We must obey with privacy and data protection laws which regulate how we can legally collect, use, retain, transfer and store personal data.

Personal data includes any information relating to an individual person who can be identified from that information. This includes an individual's name, passport details or email address.

Within **DTE PROJECT MANAGEMENT (PTY) LTD** we process personal data about our employees, suppliers, clients, customers, and other individuals with whom we work in our daily business activities.

We need to understand the importance of handling information correctly in agreement with privacy laws and regulations which are in place to protect the privacy rights of the individuals whose data we collect and keep. These laws and regulations typically enforced responsibilities on us to ensure that we only process personal data lawfully and fairly, take extra precautions when we process particularly sensitive information about people (for example information about health conditions) and that we create an effective governance framework to ensure we make well-informed decisions about how we use personal data.

2.2.1 Everyone needs to comply with the following Privacy Principles:

- You should only process personal data where you have a lawful reason to do so. When obtaining personal data from an individual you must ensure that you obtain it lawfully, and that you are clear that you have a lawful basis for each of the processing actions you want to use it for. Some of the information is sensitive e.g., information regarding health conditions, racial or ethnic origin can only be lawfully processed in very limited cases, so extra care needs to be taken when you collect this sensitive personal data.
- You should only process data in line with the data subjects' rights. Some data subjects have specific legal rights relating to their personal data e.g., to access their data or to object to certain types of processing action. You need to ensure that you know and understand these rights and respond effectively if an individual chooses to exercise them.

2.2.2 The different data subjects 'rights:

- Data controllers have a legal obligation to respond to requests from data subjects. If it's not possible to fulfil a request, the data controller must state the reason for this. Sometimes data processors receive the requests and may have to help data controllers fulfil them.
- The right to information – Data subjects have a right to be informed about the processing of their data. Data controllers must give clear and concise information in this regard. The information needs to be very easy to understand.

- The right to access – Data subjects have the right to request access to their data. Data controllers must provide this access free of charge and in an accessible format.
- The right to rectification – Data subjects have the right to request rectification of correct information as soon as possible.
- The right to erasure – Data subjects may ask to exercise their right to erasure. Erasure means that the data controller must delete the personal data about the data subject. The right is not absolute, though, and there are times when the data controller does not have to comply.
- The right to data portability – Data subjects have the right to data portability. Portability means that the data controller must transfer the personal data when asked. Data subjects can request that the data be transferred either to themselves or to another controller. The other controller may be a company that provides a service that the data subject wants to use. The controller only must fulfil the request if it's technically possible.
- The right to objection – Data subjects have the right to object to the processing of their data if they have not given their consent. Generally, data controllers must stop processing personal data if this happens. As an exception, processing may continue due to reasons of public interest, such as for scientific research.
- The right to restriction – Data subjects may request restriction. Restriction means that the data controller has to stop processing data for certain things. In other words, the data controller does not have to stop the processing completely.

You should tell the data subject what you will do with their personal data. We should make sure we provide a privacy notice to individuals, preferably at the point at which their personal data is first collected i.e., forms, on websites, in which we explain who we are and what we intend to do with their personal information.

You should only process personal data for the specific purpose(s) for which it was intended. If you want to use the personal data for any purpose beyond the lawful purposes which we originally collected their data, you will need to inform the individual and be satisfied that the additional purposes are also lawful.

You should only collect the personal data which you need for the stated purpose(s) only. You should not ask for more personal data than you need for the lawful purpose(s) for which it is

being collected. (This should not be extreme). If you do not need the data to achieve our intended business objective, you should not process that data.

You should ensure that all personal data you process is accurate and up to date. You should update details once you become aware of changes to an individual's situations. You should be wary of relying on information which may be incorrect because it is out of date. For instance, if you have not had active engagement with the individual for a long period of time, you need to take the necessary steps to contact the individual and update the information.

You should only keep personal data for as long as it is required for the purpose(s) for which it was collect. You should be proactive in deleting personal data where you no longer need to process or keep the data.

You should keep personal data confidential and secure and protect it against accidental and malicious loss, destruction, damage, and unauthorised disclosure. You have a duty to ensure that all data is maintained effectively and kept safe.

No personal data should be shared or transferred to people or organisations except if there is a lawful basis to do so and appropriate measures are in place to protect that personal data. You should ensure that each organisation you intend to share personal data with is able to effectively protect the personal data that is transferred to it.

2.2.3 Working with personal data

You should consider data privacy risk, and act in compliance with the privacy policy when processing personal data. This is particularly important to consider when undertaking any of the following activities which may involve particular privacy risk. Where necessary contact the Information Officer to complete a data protection impact assessment.

- Starting a new personal data processing activity involving the processing of personal data.
- Changing a process or system that currently processes personal data.
- Acquiring or decommissioning systems or applications that process personal data.
- Sharing personal data with any third party – this may include providing a third party with access to personal data, appointing a contractor to provide an outsourced service to the company.
- Engaging in a business activity that involves receiving personal data from a third party.

2.2.4 Data breach incidents

You should notify the Information Officer immediately if you think that personal data may have been lost, disclosed, damaged, or accessed without permission.

2.2.5 Consequences of non-compliance with this policy

Any breach of this policy will be taken seriously and may result in disciplinary action up to and including dismissal.

We do not endure any form of retaliation against employees raising concern in good faith. Allegations of retaliation against or harassment or intimidation of an employee by others as a result of a call to speak up will be investigated and appropriate action taken, including disciplinary action up to and including dismissal of the employee(s) responsible for reprisals.

This manual has been prepared in terms of the section 51 of the Promotion of Access to Information Act 2 of 2000 and to address the requirements of the Protection of Personal Information Act 4 of 2014.