Protection of Personal Information Policy

Table of Contents

1. OVERVIEW

This Protection of Personal Information Policy deals with the specifics of how Tracer use and disclose personal information obtained as required by the Protection of Personal Information Act.

Tracer has access to and/or process information relating to an identifiable living natural person or existing juristic person ("**Personal Information**") of its customers. Tracer undertakes to comply with the applicable provisions of the Protection of Personal Information Act No. 4 of 2013, as amended.

2. PERSONAL INFORMATION SECURITY GOVERNANCE

Tracer is legally obliged to provide adequate protection for the personal information we hold and to stop unauthorized access and use of personal information. We will, on an ongoing basis, continue to review our security controls and related processes to ensure that the personal information in the Tracer system is secure.

Our security policies and procedures cover:

- Physical security;
- Computer and network security;
- Access to personal information;
- Secure communications;
- Governance and regulatory issues;
- Monitoring access and usage of private information;
- Investigating and reacting to security incidents.

3. PERSONAL INFORMATION SECURITY IMPLEMENTATION

Tracer is responsible to:

3.1 Secure the integrity of such Personal Information by taking appropriate, reasonable technical and organisational measures to prevent loss of, damage to or unauthorised destruction of the Personal Information and unlawful access to or processing of the Personal Information;

3.2 have due regard to generally accepted information security practices and procedures which may apply to it generally or be required in terms of specific industry or professional rules and regulations or any legislation;

3.2.1 take reasonable measures to:

3.2.1.1 identify all reasonable foreseeable internal and external risks to Personal Information in its possession or under its control;

3.2.1.2 establish and maintain appropriate safeguards against the risks identified;

3.2.1.3 regularly verify that the safeguards are effectively implemented; and

3.2.1.4 ensure that the safeguards are continuously updated in response to new risks or deficiencies in previously implemented safeguards;

3.2.2 treat Personal Information as confidential and shall not disclose it, unless required by law or in the course of the proper performance of its obligations relating to the licensing, implementation and support of the System;

3.2.3 where there are reasonable grounds to believe that Personal Information has been accessed or acquired by any unauthorised person, immediately notify the applicable customer of same and take the necessary steps to stop such access and prevent any further access or acquisition;

3.2.4 not process, in any manner, the Personal Information in its possession or control unless strictly and specifically necessary for Tracer to perform its obligations in relation to the licensing, implementation and support of the System;

3.2.5 comply with all applicable legislation and any Customer specific instructions and directions relating to the Personal Information in its possession or control.

4. ENFORCEMENT

Refer to the "Tracer Security Strategy" for more detail on ongoing security evaluation and improvements.

5. INCIDENT REPONCE

Refer to the "Tracer Incident Response Policy" for more detail on disclosure in case of Personal Information being compromised.

6. ACKNOWLEDGEMENTS

6.1 Tracer Contributors and Reviewers

Nadine Fouche

Cobus van Graan