DATA PRIVACY POLICY (POPI)

The Protection of Personal Information Act No 4 of 2013 (Republic of South Africa – "POPI") was gazetted on 26 November 2013. As at the date of this policy, it has not yet become fully effective from a compliance perspective, however, implementation is imminent.

As information technology increases the opportunities for collection of personal data, the intention of the legislation is to protect the general public from the misuse of personal particulars furnished to businesses.

Such businesses include telephone companies, retailers, credit bureaus, the health and medical profession, banks and financial institutions, the insurance industry, the direct marketing industry, and public bodies (such as government departments and agencies, educational institutions, local authorities and the police).

Misuse of personal data covers unauthorised disclosure, identity theft and other criminal offences, as well as the proliferation of unsolicited pornography, spam and direct marketing excess.

The failure by a business to protect the personal information of its customers can impede its business activities.

THE EIGHT PRINCIPLES OF DATA PROTECTION :

Collection Limitation Principle

There should be limits to the collection of personal data, data should be obtained by lawful and fair means, and where appropriate, with the knowledge or consent of the data subject.

Data Quality Principle

Personal data should be relevant to the purposes for which they are to be used, and, to the extent necessary for those purposes, should be accurate, complete and kept up-to-date.

Purpose Specification Principle

The purpose for the collection of data should be specified at the time of collection and data should not be used for anything other than its original intention without again notifying the data subject.

Use Limitation Principle

Personal data should not be used for purposes outside of the original intended and specified purpose, except with the consent of the data subject or the authority of the law.

Security Safeguards Principle

Personal data should be protected by reasonable security safeguards against such risks as loss or unauthorised access, destruction, use, modification or disclosure of data.

Openness Principle

There should be a general policy of openness about developments, practices and policies with respect to personal data. Individuals should have easy access to information about their personal data, who is holding it, and what they are using it for.

Individual Participation Principle

An individual should have the right to know if a controller has data about him/her and to have access to that data in an intelligible form for a charge, if any, that is not excessive. An individual should also have the right to challenge a controller for refusing to grant access to his/her data, as well as challenging the accuracy of the data. Should such data be found to be inaccurate, or the business no longer authorised to retain that data, the data should be erased or rectified.

Accountability Principle

Data controllers should be accountable for complying with the measures detailed above.

REPUBLIC OF SOUTH AFRICA : POPI

"Personal information" is defined as that relating to an individual if it/he/she is an identifiable, living natural personal or juristic person and includes :

- Name;
- Identifying number (identity number, email or telephone number);
- Race, gender, sex, pregnancy status, marital status, sexual orientation, nationality, ethnic or social origin, colour, age, physical or mental health, disability, birth, religion, conscience, belief, culture or language;
- Medical history;
- Education and employment history;
- Criminal record;
- Financial transactions;
- Blood type and other biometric information such as fingerprints;
- Opinions, views and preferences;
- Another person's views and opinions of the individual.

There is an Information Protection Regulator ("IPR") to enforce the provisions of the legislation, who will control the purpose and means of processing of such personal data.

POPI PROVISIONS

- The business' CEO or nominee is responsible for compliance. Registration with the IPR is compulsory and personal information to be processed must be registered.
- The purpose of processing information must be specific, explicitly defined and legitimate. It will determine what data a business may collect and process. The time period for which information may be kept is related.
- The business and individual must agree on the collection of the information and the purpose for which the information will be used. The recipients of the information must be disclosed, and the information must be gathered directly unless it is publicly available.
- Further use of personal information cannot be incompatible with the initial purpose for which the information was initially collected.

- The information must be kept accurate, up to date and not misleading.
- The business must advise the individual that the information is being collected, of contact details for the business, whether provision of the information is voluntary or mandatory (and the consequences of not providing it) and if collection is authorised by law, which law is applicable.
- Businesses must have technical and organisational measures to secure the data's integrity and ensure it is not lost, damaged, destroyed or accessed without authorisation. If a loss occurs, the business must advise the affected individual/s and the IPR.
- An individual will be entitled to the particulars of information held by a business as well as details of anyone who has accessed such information. If an individual makes such a request and does not receive a satisfactory response within 60 days, the IPR may make a formal request, and then hand the matter to a magistrate, who may fine or imprison the responsible party (the institution's CEO or nominee) or both.

SUPERVISORY AUTHORITY

The supervisory authority in the Republic of South Africa is the Information Regulator ("IPR"), with contact details as follows :

Email :	inforeg@justice.gov.za
Tel :	+27 12 406 4818
Fax :	(086) 500 3351
Physical address :	SALU Building, 316 Thabo Sehume Street, Pretoria

Our business does not :

1. process data in the European Union ("EU"), or process data of persons residing in the EU;
2. require prior authorisation from any supervisory authority in respect of data protection.

INFORMATION OFFICER (RSA)

Our designated information officer is N S NORVAL, with contact details as follows :

Email :	nicole@NLATeam.com
Tel :	+27 11 704 1563
Physical address :	1st Floor, Block B, Fancourt Office Park, cnr Felstead & Northumberland, Northriding, Gauteng, RSA
Postal address :	P O Box 662, Bromhof, 2154

WHY WE COMPLY

The legislation promotes transparency regarding the personal data collected, which increases customer confidence. Because businesses are required to collect only a minimum amount of data, ensuring accuracy and discarding data not required, the reliability of a business' databases is increased. Businesses are also required to protect data, which reduces the risk of breaches of that data.

PENALTIES : POPI

If a business does not comply with the legislation, a penalty of a fine and/or imprisonment up to 12 months may be imposed. There are instances where the penalty may be imprisonment up to 10 years.