Data Protection

and

Information Sharing Policy

ALTEILE (PTY) LTD

Table of Contents

1. INTRODUCTION

This Data Protection and Information Sharing Policy describes the way that **ALTEILE (PTY) LTD** will meet its legal obligations and requirements concerning confidentiality and information security standards. The requirements within the Policy are primarily based upon the Protection of Personal Information Act number 4 of 2013 ("POPIA"), as that is the key piece of legislation covering security and confidentiality of Personal Information.

Contact Details:

Head of Company/Group:	Llewellyn David Lloyd.
Physical Address:	Unit 2, 43 Harris Street, Edenglen, Edenvale, 1613.
Postal Address:	P.O. Box 9936, Edenvale, 1613.
E-mail:	lew@alteile.co.za
Landline telephone number:	011-452 2087.
Fax number:	N/A.
Cell phone number:	082 784 9198.

Information Officer:	Llewellyn David Lloyd.
Physical Address:	Unit 2, 43 Harris Street, Edenglen, Edenvale, 1613.
Postal Address:	P.O. Box 9936, Edenvale, 1613.
E-mail:	lew@alteile.co.za
Landline telephone number:	011-452 2087.
Fax number:	N/A.
Cell phone number:	082 784 9198.

Deputy Information Officer:	Marie-Louise Brand.
Physical Address:	Unit 2, 43 Harris Street, Edenglen, Edenvale, 1613.
Postal Address:	P.O. Box 9936, Edenvale, 1613.
E-mail:	marie-louise@alteile.co.za
Landline telephone number:	011-452 2087.
Fax number:	N/A.
Cell phone number:	082 853 9017.

2. DEFINITIONS (as defined in the POPIA)

2.1. “Consent” means the voluntary, specific and informed expression of will;

2.2. “Data Subject” means the natural or juristic person to whom the Personal Information relates;

2.3. “Direct Marketing” means approaching a Data Subject personally for the purpose of selling them a product or service, of requesting a donation;

2.4. “Company/Group” means **ALTEILE (PTY) LTD;**

2.5. “POPIA” means the Protection of Personal Information Act, No. 4 of 2013;

2.6. “Personal Information” means information relating to an unidentifiable, living, natural person, or an identifiable, existing juristic person, as defined in POPIA;

2.7. “Processing” means an operation or activity, whether or not by automatic means, concerning Personal Information.

3. SCOPE OF THE POLICY

This policy applies to all Company/Group employees, directors, sub-contractors, agents, and appointees. The provisions of the Policy are applicable to both on and off-site processing of Personal Information.

4. POLICY STATEMENT

The Company/Group collects and uses Personal Information of the individuals and corporate entities with whom it works in order to operate and carry out its business effectively. The Company/Group regards the lawful and appropriate processing of all Personal Information as crucial and essential to successful and safely service delivery and essential to maintaining confidence between the Company/Group and those individuals and entities who deal it. The Group therefore fully endorses, commits to and adheres to the principles of POPIA.

5. PROCESSING OF PERSONAL INFORMATION

5.1. Purpose of Processing

The Company/Group uses the Personal Information under its care in the following ways:

- Conducting credit- and criminal reference checks and assessments;
- Administration of agreements;
- Providing products and services to customers;
- Discounting and asset funding purposes;
- Detecting and prevention of fraud, crime, money laundering and other malpractice;
- Conducting market or customer satisfaction research;
- Marketing and sales;
- In connection with legal proceedings;
- Staff administration;
- Keeping of accounts and records;
- Complying with legal and regulatory requirements;
- Profiling data subjects for the purposes of direct marketing.

5.2. Categories of Data Subjects and their Personal Information

The Company/Group may possess records relating to suppliers, shareholders, contractors service providers, staff and customers:

Entity Type Personal Information Processed (including, but not limited to):

- **Natural Persons as customers:**

-Names;

-Contact details;

-Physical- and postal addresses;

-Date of birth;

-ID number;

-Tax related information;

-Nationality;

-Gender;

-Confidential correspondence.

- **Juristic Persons / -entities as customers:**

-Names of contact persons;

-Name of legal entity;

-Physical- and postal address and contact details;

-Financial information;

-Registration number;

-Founding documents;

-Tax related information;

-Authorised signatories;

-Beneficiaries;

-Ultimate beneficial owners;

-Shareholding information;

-BBBEE information.

- **Contracted Service Providers:**

-Names of contact persons;

-Name of legal entity;

-Physical- and postal address and contact details;

-Financial information;

-Registration number;

-Founding documents;

-Tax related information;

-Authorised signatories;

-Beneficiaries;

-Ultimate beneficial owners;

-Shareholding information;

-BBBEE information.

- **Employees and Directors:**

-Gender;

-Pregnancy;

-Marital status;

-Colour;

-Race;

-Age;

-Language;

-Education information;

-Financial information;

-Employment history;

-ID number;

-Physical- and postal address;

-Contact details;

-Opinions;

-Credit record;

-Criminal record;

-Employee benefits and wellness.

5.3. Categories of Recipients for Processing the Personal Information

The Company/Group may share the Personal Information with its agents, affiliates, and associated companies who may use this information to send the Data Subject information on products and services. The Company/Group may supply the Personal Information to any party to whom the Company/Group may have assigned or transferred any of its rights or obligations under any agreement, and/or to service providers who render the following services:

- Capturing and organising of data;

- Storing of data;

- Sending of emails and other correspondence to customers;

- Conducting due diligence checks;

- Administration of the Medical Aid and Pension Schemes;

- Rendering of outsourced services.

5.4. Actual or Planned Trans-Border Flows of Personal Information

Personal Information may be transmitted trans-border to the Company's/Group's authorised dealers and its suppliers in other countries, and Personal Information may be stored in data servers hosted outside South Africa. Taking note that some countries may not have adequate data protection laws in place, the Company/Group is committed to, as far as reasonably possible, ensure that Personal Data is kept in designations with the necessary security measures in place.

5.5. General Description of Information Security Measures

The Company/Group is committed to ensure the sound integrity of security systems protecting Personal Information, *inter alia* the following:

- Firewalls;
- Virus protection software and update protocols;
- Logical- and physical access control;
- IT software and –hardware security measures;
- The Company/Group will ensure that outsourced service providers who process Personal Information on behalf of the Company/Group have the required security measures in place to protect any and all Data Subjects.

6. ACCESS TO PERSONAL INFORMATION

All individuals and entities as Data Subjects may request access, amendment, or deletion of their own Personal Information held by the Company/Group. Any requests should be directed, on the prescribed form that can be obtained from HR and also attached to this policy as examples, to the Information Officer.

6.1. Remedies available if request for access to Personal Information is refused

6.1.1. Internal Remedies

The matter can be referred to the Company/Group's Information Officer, who will have the final decision on such matters.

6.1.2. External Remedies

A requestor (employee, third party and/or any Data Subject) that is dissatisfied with the Information Officer's refusal to disclose information, may within 30 (thirty) days of notification of the decision, apply to the Information Regulator or an applicable Court for the prescribed relief.

6.2. Grounds for Refusal

The Company/Group may lawfully refuse to grant access to a requested record that falls within a certain category. Grounds on which the Company/Group may refuse access include, *inter alia* the following:

- Protecting personal information that the Company/Group holds about a third person (who is a natural- and/or juristic person), including a deceased person, from unreasonable disclosure;
- Protecting commercial information and or intellectual property that the Company/Group holds about a third party or the Company/Group's own confidential and/or privileged information, which disclosure may have an adverse effect on the rights and interests of the parties concerned in any way whatsoever, *inter alia* trade secrets, financial secrets, commercial information and client lists;
- If disclosure of the requested record would result in a breach of a duty of confidence and/or contract owed to a third party in;
- If disclosure of the record would endanger the life and/or physical safety of an individual, the general public and/or any other Data Subject, *inter alia* transport information, information regarding a witness protection program and/or privileged information (if not duly waived) regarding pending legal cases and/or –proceedings;
- The record is a computer programme;
- The record contains research information carried out by and/or on behalf of third party and/or the Company/Group;
- Records that cannot be found or that is not in existence, which status/case will then be reported to the relevant Data Subject as prescribed.

7. IMPLEMENTATION GUIDELINES

7.1. Training

To assist in the implementation of POPIA and/or its amendments in the workplace and to ensure that all parties concerned, including the Company/Group's current and future employees (also *via* induction) as Data Subjects are fully aware of their status, rights and responsibilities according to POPIA, the Company/Group is committed to ensure that the necessary training- and meeting programs are in place in this regard, which will be minuted and attendance records will be kept.

7.2. Employee Contracts

New employees will sign an Employment Contract containing the relevant consent clauses for the use and storage of employee information, their rights and responsibilities in this regard and a confidentiality undertaking to ensure breaches of confidentiality in relation to any Personal Information are eliminated. Strict disciplinary action will be taken against employees that breaches these rules, which might be grounds for summary dismissal.

Employees currently employed by the Company/Group will be required to sign an addendum to their current contract of employment that will stipulate the *status quo* regarding POPIA compliance to ensure breaches of confidentiality in relation to any Personal Information are eliminated. Strict disciplinary action will be taken against employees that breaches these rules, which might be grounds for summary dismissal.

8. EIGHT PROCESSING CONDITIONS AS PER POPIA

As prescribed by POPIA and to ensure compliance which its goals and reason for its existence, the Company/Group undertakes to abide by the following 8 (eight) principles as quoted in POPIA in all its processing activities:

8.1. Accountability

The Company/Group will at all times ensure compliance with all eight processing conditions through all stages of interaction with Personal Information, not only when processing personal information, but also when deciding what data to process and the reason for processing.

8.2. Processing Limitation

8.2.1. Lawfulness of processing

This condition sets out a principle of minimality, meaning only processing personal information that is relevant and only to the point needed for the stated purpose. The processing of Personal Information is only lawful if, given the purpose of processing, the information is adequate, relevant and not excessive.

The Company/Group may only process Personal Information if one of the following grounds of lawful processing exists:

- The Data Subject, or a competent person where the data subject is a child, consents to the processing;
- Processing is necessary for the conclusion or performance of a contract with the Data Subject;
- Processing complies with a legal responsibility and/or -obligation imposed on the Company/Group;
- Processing protects a legitimate interest of the Data Subject;
- Processing is necessary for the proper performance of a public law duty by a public body;
- Processing is necessary for pursuance of a legitimate interest of the Company/Group and/or a third party to whom the information is supplied.

Special Personal Information includes:

- Religious, philosophical, or political beliefs;
- Race or ethnic origin;
- Trade union membership;
- Health or sex life;
- Biometric information (including blood type, fingerprints, DNA, retinal scanning, voice recognition, photographs);
- Criminal behaviour;
- Information concerning a child.

The Group may only process Special Personal Information under the following circumstances:

- The Data Subject has consented to such processing;
- The Special Personal Information was deliberately made public by the Data Subject;
- Processing is necessary for the establishment of a right or defence in law;
- Processing is for historical, statistical, or research reasons;
- If processing of race or ethnic origin is in order to comply with affirmative action laws.

All Data Subjects have the right to refuse or withdraw their consent to the processing of their Personal Information, and a Data Subject may object, at any time, to the processing of their Personal Information on any of the above grounds, unless legislation provides for such processing. If the Data subject withdraws consent or objects to processing then the Group shall forthwith refrain from processing the Personal Information.

8.2.2. Collection directly from the Data Subject

Personal Information must be collected directly from the Data Subject, unless:

- Personal Information is contained in a public record;
- Personal Information has been deliberately made public by the Data Subject;
- Personal Information is collected from another source with the Data Subject's consent;
- Collection of Personal Information from another source would not prejudice the Data Subject;
- Collection of Personal Information from another source is necessary to maintain, comply with or exercise any law or legal right;
- Collection from the Data Subject would prejudice the lawful purpose of collection;
- Collection from the Data Subject is not reasonably practicable.

8.3. Purpose Specification

The Company/Group will only process Personal Information for the specific purposes/reasons as set out and defined in paragraph 5.1 hereto and the Company/Group will make the data subject aware of this reason and will only retain the personal information for as long as needed to meet this purpose, after which it will be deleted, destroyed or de-identified.

8.4. Further Processing

New processing activity must be compatible with original stated purpose of processing. Further processing will be regarded as compatible with the purpose of collection if:

- Data Subject has consented to the further processing;
- Personal Information is contained in a public record;
- Personal Information has been deliberately made public by the Data Subject;
- Further processing is necessary to maintain, comply with or exercise any law or legal right;
- Further processing is necessary to prevent or mitigate a threat to public health or safety, or the life or health of the Data Subject or a third party.

8.5. Information Quality

The Company/Group will take reasonable steps to ensure that Personal Information is complete, accurate, not misleading and updated. The Company/Group shall periodically review Data Subject records to ensure that the Personal Information is still valid and correct.

Employers should as far as reasonably practicable follow the following guidance when collecting Personal Information:

- Personal Information should be dated when received;
- A record should be kept of where the Personal Information was obtained;
- Changed to information records should be dated;
- Irrelevant or unneeded Personal Information should be deleted or destroyed;
- Personal Information should be stored securely, either on a secure electronic database or in a secure physical filing system.

8.6. Openness

The Company/Group shall take reasonable steps to ensure that the Data Subject is made aware of:

- What Personal Information is collected, and the source of the information;
- The purpose of collection and processing;
- Where the supply of Personal Information is voluntary or mandatory, and the consequences of a failure to provide such information;
- Whether collection is in terms of any law requiring such collection;
- Whether the Personal Information shall be shared with any third party. These details will form part of the Company/Group's Privacy Policy to which the Data Subject agrees when signing a Consent form.

8.7. Security Safeguards

The Group shall ensure the integrity and confidentiality of all Personal Information in its possession, by taking reasonable steps to:

- Identify all reasonably foreseeable risks to information security;
- Establish and maintain appropriate safeguards against such risks;

8.7.1. Written records

- Personal Information records should be kept in locked cabinets, or safes;
- When in use Personal Information records should not be left unattended in areas where non-staff members may access them;
- The Group shall implement and maintain a "Clean Desk Policy" where all employees shall be required to clear their desks of all Personal Information when leaving their desks for any length of time and at the end of the day;
- Personal Information which is no longer required should be disposed of by shredding.

Any loss or theft of, or unauthorised access to, Personal Information must be immediately reported to the Information Officer.

8.7.2. Electronic Records

- All electronically held Personal Information must be saved in a secure database;
- As far as reasonably practicable, no Personal Information should be saved on individual computers, laptops or hand-held devices;
- All computers, laptops and hand-held devices should be access protected with a password, fingerprint or retina scan, with the password being of reasonable complexity and changed frequently;
- The Group shall implement and maintain a "Clean Screen Policy" where all employees shall be required to lock their computers or laptops when leaving their desks for any length of time and to log off at the end of the day;
- Electronic Personal Information which is no longer required must be deleted from the individual laptop or computer and the relevant database. The employee must ensure that the information has been completely deleted and is not recoverable.

Any loss or theft of computers, laptops or other devices which may contain Personal Information must be immediately reported to the Information Officer, who shall notify the IT department, who shall take all necessary steps to remotely delete the information, if possible.

Should the Company/Group make use a third party, called an Operator, to process personal information, the Company/Group will ensure the Operator complies with all the prescriptions of the POPIA.

In the unlikely event that a data breach occurs, the Company/Group will follow its own policy and procedure in this regard and further inform the Information Regulator and, if known, the relevant data subjects as soon as possible, unless law enforcement officials instruct the Company/Group to delay doing so or to not do so at all.

8.8. Data Subject Participation

Data Subject have the right to request access to, amendment, or deletion of their Personal Information. All such requests must be submitted in writing to the Information Officer. Unless there are grounds for refusal as set out in herein mentioned paragraph 6.2, the Company/Group will disclose the requested Personal Information:

- On receipt of adequate proof of identity from the Data Subject, or requester;
- Within a reasonable time;
- On receipt of the prescribed fee, if any;
- In a reasonable format.

The Company/Group shall not disclose any Personal Information to any party unless the identity of the requester has been verified.

9. DIRECT MARKETING

Direct Marketing communications will be subject to the prescriptions that it must contain the Company/Group's details and an opt-out-option. If a recipient of such marketing material indicates the wish to opt-out, marketing to such a recipient will seize with immediate effect.

Direct Marketing by electronic means to existing customers and/or employees is only permitted when consent has been obtained by such a recipient (and/or data subject), which consent can only be obtained once, and/or:

- If the customer's details were obtained in the context of a sale or service;
- For the purpose of marketing the same or similar products;
- If the Company/Group is already in possession of the Data Subject's Personal Information;
- If the Company/Group procured the recipient of marketing's Personal Information that was already made public by such a recipient.

Relating to consent, the Company/Group will ensure that proper and accurate records are kept regarding:

- Date of consent;
- Wording of the consent;
- Who obtained the consent;
- Proof of opportunity to opt-out on each marketing contact;
- Record of opt-outs.

10. DESTRUCTION OF PERSONAL INFORMATION

Documents may be destroyed as indicated in this policy or on direction of the Company/Group by the relevant department and/or the Company/Group. Regular internal audits are done to determine which records are being retained that are eligible for destruction, bearing in mind that original document/s will be returned to its owners or the Company/Group for safe keeping purposes. Regarding Personal Information stored in document form, destruction of same by the Company/Group and/or appointed document disposal service provider to ensure that it cannot be re-identified. Regarding Personal Information stored in electronic records, destruction of same will be done by the Company/Group and/or appointed IT service provider to ensure that same cannot be re-identified.

11. RETENTION PERIODS

The Company is committed to only retain processed Personal Information for as long as it is required relating to the purposes for its collection, any contractual obligations, statutory required obligations and/or as prescribed by any relevant legislation of the Republic of South Africa, after which it will be destroyed in such a manner in which it will not be possible to re-identify same. Should there be any queries regarding the length of retention and/or different legislation that prescribes retention periods, all parties are motivated and required to contact the Information Officer in this regard.

12. DATE OF APPLICATION

This policy will be effective and enforceable as from the date of signing.

SIGNED BY _____ ON THIS THE _____ DAY OF _____ 20_____.

_____

Information Officer