STUTT GROUP HEAD OFFICE
Ground Floor, Chestnut House, Palm Square Business Park
Bonza Bay Road, Beacon Bay, East London, 5241
PO Box 197, Stutterheim, 4930

PROTECTION OF PERSONAL INFORMATION & PROMOTION OF ACCESS TO INFORMATION POLICY

Introduction

The company is obliged to comply with the Protection of Personal Information Act (No. 4 of 2013) ("POPI") as well as the Promotion of Access to Information Act (No. 2 of 2000) ("PAIA"), given that it processes the personal information of its employees, suppliers, clients and other data subjects from time to time as well as that there may be requesters of information relating to the company and its operations.

The company guarantees its commitment to protecting data subject' privacy as well as ensuring that their personal information is used appropriately, transparently, securely and in accordance with applicable laws. This is in line with the Constitutional provisions.

POPI requires the company to inform its data subjects as to how their personal information is collected, processed, secured, disclosed and destroyed. This Policy sets out the manner in which the Company deals with such personal information as well as stipulates the general purpose for which such information is used. It also addresses the standards expected of employees of the company in respect of their conduct in this regard.

Appropriate stakeholders should be made aware of the contents of this Policy when their consent is requested for the processing of their personal information or when there are interactions with data subjects. The provisions of this policy must be read along with the relevant practices and procedures that are used to operationalise the purpose hereof.

Collection of personal information

The company collects stores and processes personal information pertaining to data subjects including its employees, suppliers, clients and other stakeholders. The type of information collected and processed will depend on the purpose for which it is collected and will be processed for that scope of application only.

Whenever appropriate, the company will inform the data subject of the information required, the purpose thereof, the rights of participation and the other relevant provisions contained at law.

The company must indicate to the data subject the consequence of failing to provide such personal information. For example, the company may not be able to employ an individual without certain personal information relating to that individual or the company may not be in a position to render services to a client in the absence of certain information which is required.

Examples of the personal information the company collects includes, but is not limited to: information relating to an identifiable, living, natural person, and where it is applicable, an identifiable, existing juristic person –

a) information relating to the race, gender, sex, pregnancy, marital status, national, ethnic or social origin, colour, sexual orientation, age, physical or mental health, well-being, disability, religion, conscience, belief, culture, language and birth of the person;

b) information relating to the education or the medical, financial, criminal or employment history of the person;

c) any identifying number, symbol, e-mail address, physical address, telephone number, location information, online identifier or other particular assignment to the person;

d) the biometric information of the person;

e) the personal opinions, views or preferences of the person;

f) correspondence sent by the person that is implicitly or explicitly of a private or confidential nature or further correspondence that would reveal the contents of the original correspondence;

g) the views or opinions of another individual about the person; and

h) the name of the person if it appears with other personal information relating to the person or if the disclosure of the name itself would reveal information about the person.

Collection of employee information

For the purposes of this Policy, “employees” include potential, past and existing employees of the company.

The company will, when appointing new employees, require information, including, but not limited to that listed above, from the prospective employee in order to process the employee’s information on the company’s system.

Such information is reasonably necessary for the company’s record purposes as well as to ascertain if the prospective employee meets the requirements for the position to which he or she is being appointed and is suitable for such appointment.

The company will use and process such employee information, as set out below, for purposes including, but not limited to, its employment records and to make lawful decisions in respect of that employee and its business.

Use of employee information

Employees' personal information will only be used for the purpose for which it was collected and intended. This would include, but is not limited to:

- ✓ submissions to the Department of Employment and Labour
- ✓ submissions to the Receiver of Revenue
- ✓ for audit and recordkeeping purposes
- ✓ in connection with legal proceedings
- ✓ in connection with and to comply with legal and regulatory requirements
- ✓ in connection with any administrative functions of the Company
- ✓ disciplinary action or any other action to address the employee's conduct or capacity
- ✓ in respect of any employment benefits that the employee is entitled to
- ✓ pre-and post employment checks and screening
- ✓ any other relevant purpose to which the employee has been notified of any compliance requirements at law.

Should information be processed for any other reason that is not in the legitimate interests of the employee, the company will inform the employee accordingly.

The company acknowledges that personal information may only be processed if certain conditions are met which, depending on the merits include -

- ✓ The employee consents to the processing
- ✓ The processing is necessary to attend to justifiable rights and obligations, for example contractual fulfilment
- ✓ The processing complies with an obligation imposed by law on the company
- ✓ Processing protects a legitimate interest of the employee
- ✓ Processing is necessary for pursuing the legitimate interests of the company or of a third party to whom information is supplied.,

Collection of client and/ or supplier information

For purposes of this Policy, clients include potential, past and existing clients. The company collects and processes its clients' personal information, such as that mentioned hereunder. The type of information will depend on the need for which it is collected and will be processed for that purpose only. Further examples of personal information collected from clients include, but is not limited to:

- ✓ The client's identity number, name, surname, address, postal code
- ✓ The client's residential and postal address

- ✓ Contact information
- ✓ Banking details
- ✓ Company registration number
- ✓ Full name of the legal entity
- ✓ Tax and/or VAT number
- ✓ Details of the person responsible for the client's account

The company also collects and processes clients' personal information for marketing purposes in order to ensure that our products and services remain relevant to our clients and potential clients.

Use of client and supplier information

The client's personal information will only be used for the purpose for which it was collected and as agreed, if any such agreement is required at law. This may include, but not be limited to:

- ✓ Providing products and/ or services to clients
- ✓ In connection with sending accounts and communication in respect of services rendered
- ✓ Referral to other service providers
- ✓ Confirming, verifying and updating client details
- ✓ Conducting market or customer satisfaction research
- ✓ For audit and record keeping purposes
- ✓ In connection with legal proceedings
- ✓ In connection with and to comply with legal and regulatory requirements or when it is otherwise allowed by law

The company acknowledges that personal information may only be processed if any of the conditions set out hereunder are met:

- ✓ Client consents to the processing
- ✓ The processing is necessary to attend to rights and obligations that are justifiable, including fulfilling contractual provisions
- ✓ The processing complies with an obligation imposed by law on the company
- ✓ Processing protects a legitimate interest of the party
- ✓ Processing is necessary for pursuing the legitimate interests of the company or of a third party to whom information is supplied.

Disclosure of personal information

Subject to legislative provisions providing the contrary, the company may share data subject's personal information with third parties as well as obtain information from such third parties for reasons set out above.

The Company may also disclose data subject's information where there is a duty or a right to disclose in terms of applicable legislation, a contractual obligation, the law or where it may be necessary to protect the company's rights.

Safeguarding personal information and consent

It is a requirement of POPI to adequately protect the personal information the company holds and to avoid unauthorised access and use of personal information.
The company shall review its technical and operational security controls and processes on a regular basis to ensure that personal information is secure.

The Company shall appoint an Information Officer who is responsible for the encouragement of compliance with the conditions of the lawful processing of personal information and other provisions of POPI and PAIA.

Information Officer details

Name:	Odette Le Roux
Telephone number:	043 101 0146
Fax number:	043 748 3285
Postal Address:	P.O. Box 15213, Beacon Bay, East London
Physical address:	Ground Floor, Chestnut House, Palm Square Business Park, Bonza Bay Road, Beacon Bay, East London.
Email address:	popi@stuttgroup.co.za

Each new employee will be required to sign an employment contract containing relevant consent clauses for the use and storage of employee information, or any other action so required, in terms of POPI.

Every employee currently employed within the Company will be required to sign an addendum to their employment contract containing relevant consent clauses for the use and storage of employee information, or any other action so required, in terms of POPI.

The Company's suppliers who fall within the definition of "operators" will be required to enter into a written agreement guaranteeing their commitment to the Protection of Personal Information.

Consent to process client information is obtained from data subjects (or a person who has been given authorisation from the client to provide the client's personal information) during the introductory, appointment and needs analysis stage of the relationship.

Security breaches

Should the company detect a security breach on any of its systems that contain personal information, the company shall take the required steps to assess the nature and extent of the breach in order to ascertain if any information has been compromised.
The company shall activate its **Incident Response Plan** which includes the notification of the affected parties and the Information Regulator should it have reason to believe that personal information has been compromised. Such notification shall only be made where the company can identify the data subject to which the information relates. Where it is not possible it may be necessary to consider website publication and whatever else the Information Regulator prescribes.

Notification will be provided in writing by means of either:

- ✓ email
- ✓ registered mail
- ✓ place on our website.

The notification shall provide the following information where possible:

- ✓ description of possible consequences of the breach
- ✓ measures taken to address the breach
- ✓ recommendations to be taken by the data subject to mitigate adverse effects
- ✓ the identity of the party responsible for the breach.

In addition to the above, the company shall notify the Regulator of any breach and/or compromise to personal information in its possession and work closely with and comply with any recommendations issued by the Regulator.

The following provisions will apply in this regard –

- The Information Officer will be responsible for overseeing the investigation;
- The Information Officer will be responsible for reporting to the Information Regulator within 2 working days of a breach/ compromise to personal information;
- The Information Officer will be responsible for reporting to the Data Subject(s) within 2 working days of a breach/ compromise to personal information;
- The timeframes above are guidelines and depending on the merits of the situation may require earlier or later reporting.

Access and correction of personal information

Data subjects have the right to request access to any personal information that the company holds about them.

Data subjects have the right to request the Company to **update, correct or delete** their personal information on reasonable grounds. Such requests must be made to the company's Information Officer (see details above) or to the Company's head office (see details below) or submitted via the email address provided. The company is in the process of developing a portal on our company website where all POPI and PAIA related queries can be submitted for the attention of the Information Officer.

Where an employee or client objects to the processing of their personal information, the Company may no longer process said personal information. The consequences of the failure to give consent to process the personal information must be set out before the employee or client confirms his/her objection. The data subject must provide reasons for the objection to the processing of his/her personal information.

Head office details

Name:	Stutt Group (Pty) Ltd
Telephone number:	043 101 0146
Fax number:	043 748 3285
Postal address:	P.O. Box 15213, Beacon Bay, East London
Physical address:	Ground Floor, Chestnut House, Palm Square Business Park, Bonza Bay Road, Beacon Bay, East London.
Email address:	popi@stuttgroup.co.za

Retention of records

The company shall ensure the safeguarding and protection of all personal information or data. The company is obligated to retain certain information as prescribed by law. This includes but is not limited to the following:

With regard to the Companies Act, No. 71 of 2008 and the Companies Amendment Act No 3 of 2011, hard copies of the documents mentioned below must be retained for 7 years:

- ✓ Any documents, accounts, books, writing, records or other information that a company is required to keep in terms of the Act
- ✓ Notice and minutes of all shareholders meetings, including resolutions adopted and documents made available to holders of securities
- ✓ Copies of reports presented at the annual general meeting of the company
- ✓ Copies of annual financial statements required by the Act and copies of accounting records as required by the Act.

The Basic Conditions of Employment No. 75 of 1997, as amended requires the Company to retain records relating to its staff for a period of no less than 3 years.

Amendments to this policy

Amendments to this Policy will take place from time to time subject to the discretion of the Company and pursuant to any changes in the law. Such changes will be brought to the attention of employee's clients where it affects them.

Standards of conduct required of employees

In addition to the provisions contained within this POPI policy, the employment contract, the disciplinary code, the electronic communications and social media policy as well as any other document relating to employees, the following standards of conduct and practice and their accompanying underlying principles must be complied with at all times and a breach thereof may result in serious disciplinary action and even dismissal for a first offence.

1. Physical records and assets

All physical records containing personal information (PI) as well as any hardware, devices or similar equipment must always be protected from unauthorised access and/ or damage and/ or loss and/ or other prejudice.

2. Systems and platforms

Compliance with security requirements in respect of, for example, the following areas is crucial –

2.1 Changing, storage and sharing of usernames and passwords;
2.2 Data back-ups and protection;
2.3 Limitations on the use of personal devices such as external hard drives or similar storage options, mobile phones and the like

3. Internal and external posting of personal information of company data subjects

A prohibition on the sharing and/ or posting of PI on any platforms outside of those that are company approved under specific conditions as well as a total ban on posting and/ or transmitting PI outside of the company on social media and/ or any other similar platform.

4. Conditions to be observed when collecting or processing PI

The following principles must be complied with when dealing with PI and if there is any doubt, the written authority of the Information Officer must be obtained by the employee prior to the said processing –

Accountability
The employee must ensure that the conditions and all the measures that give effect to such conditions are complied with at the time of the determination of the purpose and means of the processing and during the processing itself.

Processing limitation

Personal information must be processed

(a) lawfully; and

(b) in a reasonable manner that does not infringe the privacy of the data subject.

This includes considerations of minimality and adequacy given the purpose for which it is intended. In addition –

- The data subject or a competent person (data subject is a child) consents to the processing; or/ and
- The purpose is to carry out actions for the conclusion or performance of a contract; or/ and
- Processing complies with an obligation imposed by law on the responsible party; or/ and
- Processing protects a legitimate interest of the data subject; or/ and
- Processing is necessary for the proper performance of a public law duty by a public body; or/ and
- Processing is necessary for pursuing the legitimate interests of the responsible party or of a third party to whom the information is supplied; or/ and
- Collection must be directly from the data subject, except as otherwise provided for unless the information is contained in or derived from a public record or has deliberately been made public by the data subject.

Purpose specification

PI is collected for a specific, explicitly defined and lawful purpose related to a function or activity of the responsible party.

Further processing limitation

Further processing of personal information must be compatible with the purpose for which it was collected and consider -

(a) the consequences of the intended further processing for the data subject

(b) the manner in which the information has been collected; and

(c) any contractual rights and obligations between the parties.

Security Safeguards

Employees must secure the integrity and confidentiality of personal information in their possession or under their control by taking appropriate, reasonable technical and organisational measures to prevent—

(a) loss of, damage to or unauthorised destruction of personal information; and

(b) unlawful access to or processing of personal information.

Employees must take reasonable measures to—

(a) identify all reasonably foreseeable internal and external risks to personal information in its possession or under their control;

(b) establish and maintain appropriate safeguards against the risks identified;
(c) regularly verify that the safeguards are effectively implemented; and
(d) ensure that the safeguards are continually updated in response to new risks or deficiencies in previously implemented safeguards.

Employees must have due regard to **generally accepted information security practices and procedures** which may apply to the situation generally or be required in terms of specific industry or professional rules and regulations.