# POPI POLICY

| | | | |
|---|---|---|---|
| **Policy Owner** | Human Resources (HR) | | |
| **Effective date** | 28 June 2021 | | |
| **Authorized by** | CEO |  Signature | 28/6/2021 Date |
| | Human Resources Manager |  Signature | 28/6/2021 Date |
| **Note** | George Stott and Company (Pty) Ltd reserves the right to amend the contents of this policy as and when required. The policy currently in effect will apply to all employees regardless of the policy that applies at the time of employment. | | |

## 1. Scope and objective of the policy

1.1 The Protection of Personal Information (POPI) policy is intended to ensure the legitimate concerns of individuals/companies about the ways in which their data may be used.

1.2 The Personal information Act, 4 of 2013 (signed into law in November 2013) has the following aims:

1.2.1 to promote the protection of personal information processed by organisations in the public and private sectors.

1.2.2 to establish minimum requirements for the processing of personal information.

1.2.3 to establish an Information Regulator with powers.

1.2.4 to provide for the issuing of codes of conduct.

1.2.5 to protect the rights of people regarding unsolicited electronic communications and automated decision making.

1.2.6 to regulate the transborder flow of information.

1.2.7 to provide for connected matters.

1.3 This policy has been developed in line with the Personal Information (POPI) Act, 4 of 2013 and aims to ensure that the processing of personal information & special/sensitive personal information adhere to the conditions for lawful processing as set out in Chapter 3 of the POPI Act.

1.4 The POPI Act and this policy does not apply to the processing of personal information of a deceased person.

1.5. The POPI act includes identifiable, existing jurisdic person (where applicable) in its definition of personal information. The processing of personal information of the directors of companies or partners in business partnerships, for example, falls within the parameters of the POPI Act and this policy.

## 2. Definitions

2.1 **"competent person"** - means any person who is legally competent to consent to any action or decision being taken in respect of any matter concerning a child;

2.2 **"Consent"** - means any voluntary, specific and informed expression of will in terms of which permission is given for the processing of personal information;

2.3 **"Company"** - a legal registered entity.

2.4 **"Privacy"** - is about ensuring that both individuals and juristic entities are aware of what is being done with their personal information.

2.5 **"Personal information"** means information relating to an identifiable, living, natural person, and where it is applicable, an identifiable, existing, juristic person, including, but not limited to:

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[1].

The definition of personal information includes *special* or *sensitive* personal information. These categories refer to sensitive areas which a person would not like published.

2.6 "**Special personal information**" relates to the religious or philosophical beliefs, race or ethnic origin, trade union membership, political persuasion, health or sex life or the biometric information of a data subject. It also relates to the criminal behaviour of a data subject regarding the alleged commission of an offence or any proceedings in respect of any offence allegedly committed by the data subject or the disposal of such proceedings; a history of a person's education, medical, financial, criminal or employment history; and/or the processing of biometric information of a person.

## 3. Legal Principles

The following legislation is applicable to this policy:

3.1 the Constitution of South Africa act 108 of 1996.

3.2 The Personal Information Act, Act 4 of 2013.

3.3 Regulation of Interception of Communications & Provision of Communication-related Information Act, 70 of 2002.

3.4 Electronic Communications & Transactions Act, 25 of 2002.

3.5 National Credit Act, 34 of 2005.

3.6 The Cybercrimes and Cybersecurity Bill and relevant proposed Bills.

[1] The POPI act s 1.

3.7 The Spatial Data Infrastructure Act 54 of 2003.

3.8 Codes of Conduct published by industries/bodies (e.g. Advertising Standards Authority of South Africa).

## 4. Policy

4.1 The policy applies to any information regarding clients, suppliers and employees including contact details and correspondence. Human Resources and payroll data, curricula vitae, applications for employment, CCTV records, performance reviews and internal e-mail records of the employee, customers, and George Stott and Company (Pty) Ltd.

4.2 The policy applies to any form of recorded information, regardless of the form of medium and include, but is not limited to information on:

- 4.2.1 Tape recorder
- 4.2.2 Computer
- 4.2.3 Labels
- 4.2.4 Markings
- 4.2.5 Books
- 4.2.6 Maps
- 4.2.7 Photographs
- 4.2.8 Films
- 4.2.9 Negative type/other devices.

4.2 The policy conditions impact technology, processes, and the way George Stott and Company (Pty) Ltd process personal information.

4.3 Personal information may only be used for the purpose agreed with your customers, clients, and employees.

4.4 Marketing by means of unsolicited e-mail is prohibited unless certain provisions apply – George Stott and Company (Pty) Ltd to implement opt-in and opt-out strategies.

4.5 Personal information may only be retained for as long as necessary – George Stott and Company (Pty) Ltd to specify retention periods.

4.6 George Stott and Company (Pty) Ltd shall not process more personal information than is necessary.

4.7 Processing of special personal information is prohibited unless provisions stipulated in this policy apply.

4.8 Personal information of employees, clients, customers and George Stott and Company (Pty) Ltd will be sufficiently protected and used in a manner that facilitates transparency around the following:

4.8.1 what is done with the personal information;

4.8.2 why and how it is processed (i.e. this covers all phases of a typical information management life cycle – from collection, to usage, sharing, disposal, archiving, etc);

4.8.3 who the personal information is shared with (i.e. third parties – both locally and internationally, other legal entities – sometimes within the same group or company, etc);

4.8.4 what types of personal information is processed and for what purpose.

4.9 Personal Information of the employees, clients, and customers includes:

4.9.1 contact details;

4.9.2 demographic information;

4.9.3 personal history, criminal record;

4.9.4 email addresses, date of birth and age;

4.9.5 education information physical address; and

4.9.6 financial information as well as communication records.

4.10 Personal information (PI) of George Stott and Company (Pty) Ltd includes:

4.10.1 financial information;

4.10.2 intellectual property (processes, methods);

4.10.3 ICT systems/ programmes; and

4.10.4 CCTV surveillance and guard monitoring systems

## 5. Procedure

5.1 George Stott and Company (Pty) Ltd is expected to identify what they classify as Personal Information and take reasonable measures to protect the data. This will likely reduce the risk of data breaches and avoid legal ramifications for George Stott and Company (Pty) Ltd

5.2 George Stott and Company (Pty) Ltd, therefore, must receive consent from individuals before they can obtain and retain personal information for communication or any other purpose.

5.3 The employee, clients, customers, and George Stott and Company (Pty) Ltd will be kept updated of what is being done with their information and the associated reasoning.

5.4 In accordance with the Protection of Personal Information Act, as soon as a privacy breach is detected and established, it must be reported to the regulator and to the party whose information was accessed.

5.5 All responsible parties need to know and be able to explain how the breach occurred, what has been done to contain any harm and how will any such breach be prevented in the future.

5.6 Should employees for any given reason no longer service the organisation; information prescribed as personal (financial information, intellectual property) as according to George Stott and Company (Pty) Ltd policy should not be disclosed to the public (i.e. companies operating in the same industry). The same principal applies to George Stott and Company (Pty) Ltd.

5.7 Those concerned (George Stott and Company (Pty) Ltd the employee, and clients) have the right to complain and escalate any issues related to privacy, especially if they believe that their right to information privacy has been violated.

5.8 Employees are expected to protect the private information of George Stott and Company (Pty) Ltd e.g.:

5.8.1 confidential files are expected to be put in a secure area (locked draws); and

5.8.2 personal login details to George Stott and Company (Pty) Ltd's ITC systems are expected to be kept confidential to avoid unauthorized access to private systems.

5.9 Failure to comply with the requirements of the policy will result in immediate dismissal, fine or severe legal consequences.

## 6. Relevant Policies

6.1 Code of Conduct

6.2 PAIA/Section 51 Manual

6.3 Data Breach Policy

## 7. Relevant Documents

7.1 Information Officer – Appointment letter.

7.2 Deputy Information Officer – Appointment letter.