

SOLID GREEN CONSULTING (PTY) LTD

PROTECTION OF PERSONAL INFORMATION POLICY

Revision History

Revision	Date	Author	Description
Version 1	07/03/2024	J Hattingh	Created

1. POLICY STATEMENT

The development of a standard operating procedure to ensure adequate protection of personal client information which becomes available to Solid Green Consulting and its personnel is of utmost importance for the effective operations and risk management of the company. Moreover, internal control mechanisms to constantly review and measure adherence to procedure are important risk management tools and assist the company in treating our clients fairly. The absence of policy and procedure will expose the company to unnecessary risk and create a burden in respect of financial and other regulatory requirements.

The purpose of this policy is to format, approve, update and document management, relating to the protection of client data as prescribed in the protection of personal information act and augmented by the company's stance on the fair treatment of customers.

Solid Green Consulting subscribes to the principles espoused in the Protection of Personal Information Act and the Constitution of South Africa in respect of:

- The lawful processing of client data by Solid Green Consulting - acting as a responsible corporate citizen; and
- The identification and allocation of accountability, where personal data is processed contrary to the prescripts of the Act.

2. MEANING/DEFINITIONS

- “Act”** means the Protection of Personal Information Act – 4/2013;
- “Data subject”** means the person to whom personal information relates;
- “Policy”** means this policy on the lawful processing and protection of client information;
- “Procedure”** means a statement or number of statements, contained in a separate yet linked document, the effect of which is to prescribe those things that must be done or omitted in order to ensure adherence with this policy and the Act;
- “Processing”** means any operation or activity or any set of operations, whether or not by automatic means, concerning personal information, including-
- a) the collection, receipt, recording, organisation, collation, storage, updating or modification, retrieval, alteration, consultation or use;
 - b) dissemination by means of transmission, distribution or making available in any other form; or
 - c) merging, linking, as well as restriction, degradation, erasure or destruction of information;
- “Responsible Committee”** means the Executive committee of Solid Green Consulting.
- “POPIA Policy”** means policy on the lawful processing and protection of client information.

3. SCOPE AND APPLICATION

This policy shall apply in respect of:

3.1 The Lawful Processing of Personal Information

In that the following conditions for processing of personal information must be met prior to any processing of personal data:

- 3.1.1 The purpose of use of the data and the manner in which data was obtained are lawful;
- 3.1.2 The use of the data does not infringe on the privacy of the client;
- 3.1.3 The extent of the data obtained is commensurate with the purpose for which it is being processed; and
- 3.1.4 The data subject's consent was obtained, or processing is otherwise necessitated to comply with laws;
- 3.1.5 We shall obtain data directly from the data subject unless required by law to obtain data from another source; and
- 3.1.6 Where we obtain data from another source such as third-party processors, we shall have a written agreement in place with such providers:

Bearing in mind that the data subject may at any time object to our processing of such data, in which case we must stop unless precluded to do so by law.

3.2 Collection and Retention of Quality Data for a Specific Purpose

In that we have to ensure that we collect data only if:

- 3.2.1 We have a defined specific purpose that relates to our business;
- 3.2.2 The data subject has been made aware of our data collection activities and purpose and does not object thereto, or the data is in the public domain;
- 3.2.3 Data collected by us are of the highest quality in the circumstances so as to avoid unnecessary mistakes and/or inconvenience to the data subject;
- 3.2.4 We retain records only for as long as reasonable for the original purpose of longer if required by law or purely for historical analysis purposes;
- 3.2.5 and destroy records in a comprehensive and responsible manner when they are no longer required to be kept.

3.3 Transparency of our Activities

In that we must ensure that data subjects, prior to the collection of data:

- 3.3.1 Are able to, based on information provided by us in our manual published under the Promotion of Access to Information Act, assess the type of information we collect and hold on them;
- 3.3.2 Are informed by us that we, as SOLID GREEN CONSULTING, are the responsible party collecting and holding data about them as well as our reason for doing so;
- 3.3.3 Are informed whether they are obliged, under any law, or otherwise voluntarily disclose the data to us and any other rights they may have, including the right to object and to lodge a complaint with the Regulator appointed under the Act.

3.4 Protection of Data

- 3.4.1 We shall ensure that data in our possession is secure and confidential so as to protect us against loss, unlawful access or accidental destruction of data.
- 3.4.2 In so doing, we shall take measures to incorporate data protection in our risk management framework and adapt our risk management practices so as to align them, insofar as data protection is concerned, with generally accepted data security practices and procedures.
- 3.4.3 We shall ensure that any service provider to whom we outsource any aspect relating to data collection abides by the terms of this policy.
- 3.4.4 We shall ensure, in the event of a breach of security regarding data that we notify the Regulator and the affected data subjects as soon as reasonably possible, by such means and media as are appropriate in the circumstances to enable them to take steps to protect their interests.
- 3.4.5 We shall ensure, when requested to transfer data across the borders of South Africa, that we do so only with the consent of the data subject and thereafter only to a jurisdiction which has rules on the protection of data substantially similar to those contained in this policy and the Protection of Personal Information Act.

3.5 Access to Information

- 3.5.1 We shall ensure that data subjects have access to such information as we may hold on them.
- 3.5.2 We shall modify data held at the request or instruction from a data subject.

3.5.3 We shall not process information regarding a data subject in respect of:

3.5.3.1 the religious or philosophical beliefs, race or ethnic origin, trade union membership, political persuasion, health or sex life or biometric information;

3.5.3.2 the criminal behaviour of a data subject to the extent that such information relates to-

(i) the alleged commission by a data subject of any offence; or

(ii) any proceedings in respect of any offence allegedly committed by a data subject or the disposal of such proceedings, unless the data subject has authorised such processing or unless otherwise required by law.

3.5.4 We shall not process data regarding children unless authorised by such children's guardian or otherwise as required by law.

3.6 Information Officer

We shall appoint an Information Officer, the purpose of which is to ensure compliance with this policy. The Information Officer shall be the CEO. The CEO may appoint Deputy Information Officers to assist with the performance of his/her duties.

4. STANDARDS AND APPLICATION

In adopting the processes required to give effect to this policy, we shall at all times adhere to the highest standards set by the South African regulatory authority and failing that, by the European Commission.

This policy document shall be circulated to all heads of departments with a view of them assessing the extant process requirements and making recommendations to the Head: Compliance in respect of any changes required to meet the demands of this policy.

5. REVIEW AND TRAINING

This policy content shall be reviewed bi-annually by the CIO or more frequently in the event of material amendments to the regulatory environment.

Compliance with this policy shall be reviewed annually and reported on by the CIO to the Board.

POPI training will be conducted as often as possible, but no less than on an annual basis.

6. AUTHORITY

The CIO is hereby appointed to act in terms of this policy and is specifically furnished with the power to delegate any functions to one or more deputies.

This policy must initially be approved by the Board and may thereafter be amended by the Executive Committee of SOLID GREEN CONSULTING.

I, the undersigned, hereby commit myself and agree to abide by the statutes as described in the Protection of Personal Information Policy.



SOLID GREEN CONSULTING
Marloes Reinink
Director