## 1. INTRODUCTION

This policy describes the way that Compliance Hub Consulting (Pty) Ltd will meet its legal obligations and requirements concerning confidentiality and information security standards.

Given the importance of privacy and the fact that the right to privacy is an integral human right recognized and protected in the South African Constitution and in the Protection of Personal Information Act 4 of 2013 ("POPIA), Compliance Hub Consulting is committed to effectively managing personal information in accordance with POPIA's provisions.

## 2. DEFINITIONS

| | | |
|---|---|---|
| 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. |
| 2.4 | **Company** | means Compliance Hub Consulting (Pty) Ltd (Registration Number: 2014/077263/07), a private company with limited liability duty registered and incorporated in terms of the company laws of the Republic of South Africa and having its current principal place of business at **186 Rigel Avenue Waterkloof Pretoria** |
| 2.5 | **POPI** | 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 POPI. |
| 2.7 | **Processing** | means an operation or activity, whether or, not, by automatic means, concerning Personal Information. |

## 3. SCOPE OF POLICY

The policy applies to all company 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 collects and uses Personal Information of the individuals and entities with whom it works to operate and carry out its business effectively.

The company regards the lawful and appropriate processing of all Personal Information as crucial to successful service delivery and essential to maintaining confidence between the company and those individuals and entities who deal it.

The company therefore fully endorses and adheres to the principles of the Protection of Personal Information Act ("POPI").

## 5. PROCESSING OF PERSONAL INFORMATION

### a. Purpose of processing

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

- Administration of agreements
- Providing products and services to clients
- 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

### b. Categories of Data Subjects and their Personal Information

The company may possess records relating to suppliers, shareholders, contractors service providers, staff, and clients:

| ENTITY TYPE | PERSONAL INFORMATION PROCESSED |
|---|---|
| Clients: Natural Persons | Names; contact details; physical and postal addresses; date of birth; ID number; tax related information; nationality; gender; confidential correspondence. |
| Clients – Juristic Persons / Entities | Names of contact persons; name of legal entity; physical and postal address and contact details; financial information; registration number; founding documents; tax related |

| | |
|---|---|
| | information; authorized 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; authorized signatories; beneficiaries; ultimate beneficial owners; shareholding information; BBBEE information. |
| Employees / Directors | Gender; pregnancy; marital status; color, race; age; language; education information; financial information; employment history; ID number; physical and postal address; contact details; opinions; criminal record; well-being. |

c. Categories of Recipients for Processing the Personal Information

The Company 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 may supply the Personal Information to any party to whom the Company 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 organizing of data.
- Storing of data.
- Conducting due diligence checks.

d. Actual or Planned Transborder Flows of Personal Information

Personal Information may be transmitted transborder to the company's authorized suppliers in other countries, and Personal Information may be stored in data servers hosted outside South Africa, which may

not have adequate data protection laws. The company will endeavor to ensure that its suppliers will make all reasonable efforts to secure said data and Personal Information.

### e. Retention of Personal Information Records

The Company may retain Personal Information records indefinitely unless the Data Subject objects thereto. If the Data Subject objects to indefinite retention of its Personal Information the Company shall retain the Personal Information records to the extent permitted or required by law.

### f. General Description of Information Security Measures

The Company employs up to date technology to ensure the confidentiality, integrity, and availability of the Personal Information under its care. Measures include:

- Firewalls
- Virus protection software and update protocols
- Logical and physical access control.
- Secure setup of hardware and software making up the IT infrastructure.
- Outsourced Service Providers who process Personal Information on behalf of the company are contracted to implement security controls.

## 6. ACCESS TO PERSONAL INFORMATION

All individuals and entities may request access, amendment, or deletion of their own Personal Information held by the Company. Any requests should be directed, on the prescribed form, to the Information Officer.

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

#### i. Internal Remedies

The Company does not have internal appeal procedures. As such, the decision made by the Information Officer pertaining to a request is final, and requestors will have to exercise such external remedies at their disposal if a request is refused, and the requestor is not satisfied with the response provided by the information officer.

#### ii. External Remedies

A requestor that is dissatisfied with the information officer's refusal to disclose information, may within 30 days of notification of the decision, apply to a court for relief. Likewise, a third party

dissatisfied with the information officer's decision to grant a request for information, may within 30 days of notification of the decision, apply to a court for relief. For purposes of the Act, courts that have jurisdiction over these applications are the Constitutional Court, the High Court, or another court of similar status.

b. Grounds for Refusal

The Company may legitimately refuse to grant access to a requested record that falls within a certain category. Grounds on which the Company may refuse access include:

- Protecting personal information that the Company holds about a third person (who is a natural person) including a deceased person, from unreasonable disclosure.
- Protecting commercial information that the Company holds about a third party or the Company (for example trade secret: financial, commercial, scientific, or technical information that may harm the commercial or financial interests of the organization or the third party).
- If disclosure of the record would result in a breach of a duty of confidence owed to a third party in terms of an agreement.
- If disclosure of the record would endanger the life or physical safety of an individual.
- If disclosure of the record would prejudice or impair the security of property or means of transport.
- If disclosure of the record would prejudice or impair the protection of a person in accordance with a witness protection scheme.
- If disclosure of the record would prejudice or impair the protection of the safety of the public.
- The record is privileged from production in legal proceedings unless the legal privilege has been waived.
- Disclosure of the record (containing trade secrets, financial, commercial, scientific, or technical information) would harm the commercial or financial interests of the Company.
- Disclosure of the record would put the Company at a disadvantage in contractual or other negotiations or prejudice it in commercial competition.
- The record is a computer program; and
- The record contains information about research being carried out or about to be carried out on behalf of a third party or the Company.

*Records that cannot be found or do not exist.*

If the Company has searched for a record and it is believed that the record does not exist or cannot be found, the requester will be notified by way of an affidavit or affirmation. This will include the steps that were taken to try to locate the record.

## 7. IMPLEMENTATION GUIDELINES

### a. Training & Dissemination of Information

This policy has been put in place throughout the Company, training on the Policy and POPI will take place with all the affected employees.

All new employees will be made aware at induction, or through training programs, of their responsibilities under the terms of this Policy and POPI.

Modifications and updates to data protection and information sharing policies, legislation, or guidelines will be brought to the attention of all staff.

### b. Employee Contracts

Each new employee will sign an Employment Contract containing the relevant consent clauses for the use and storage of employee information, and a confidentiality undertaking as part and will be personally responsible for ensuring there are no breaches of confidentiality in relation to any Personal Information, however it is stored. Failure to comply will result in the instigation of a disciplinary procedure.

Each employee currently employed within the Company will sign an addendum to their Employment Contract containing the relevant consent clauses for the use and storage of employee information, and a confidentiality undertaking as part and will be personally responsible for ensuring there are no breaches of confidentiality in relation to any Personal Information, however it is stored. Failure to comply will result in the instigation of a disciplinary procedure.

## 8. PROCESSING CONDITIONS

POPI is implemented by abiding by eight processing conditions. The Company shall abide by these principles in all its possessing activities.

### a. Accountability

The Company shall ensure that all processing conditions, as set out in POPI, are complied with when determining the purpose and means of processing Personal Information and during the processing itself. The Company shall remain liable for compliance with these conditions, even if it has outsourced it processing activities.

### b. Processing Limitation

#### i. Lawful grounds

The processing of Personal Information is only lawful if given the purpose of processing, the information is adequate, relevant, and not excessive.

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

- The Data Subject 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 imposed on the Company.
- Processing protects a legitimate interest of the Data Subject. Processing is necessary for pursuance of a legitimate interest of the Company, 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 behavior.
- Information concerning a child.

The Company may only possess 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 defense in law.
- Processing is for historical, statistical or research reasons.
- If processing of race or ethnic origin is 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 Company shall forthwith refrain from processing the Personal Information.

ii. 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.

c. Purpose Specification

The Company shall only process Personal Information for the specific purposes as set out and defined above at paragraph 5.1.

d. Further Processing

New processing activity must be compatible with original 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.

e. Information Quality

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

Employees should as far as reasonably practicably 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.

f. Openness

The Company 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.

g. 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 paragraph 6,2, above, the Company shall 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 shall not disclose any Personal Information to any party unless the identity of the requester has been verified.

8.1 Security Safeguards

The Company 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.

8.1.1 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 Company 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 unauthorized access to, Personal Information must be immediately reported to the Information Officer.

### 8.1.2 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 Company 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.
- Electronical 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.

## 9. DIRECT MARKETING

All Direct Marketing communications shall contain the Company's details, and an address or method for the customer to opt-out of receiving further marketing communication.

### a. Existing Clients

Direct Marketing by electronic means to existing clients is only permitted:

- If the client's details were obtained in the context of a sale or service; and
- For the purpose, of marketing the same or similar products.

The client must be given the opportunity to opt-out of receiving direct marketing on each occasion of direct marketing.

b. Consent

The Company may send electronic Direct Marketing communication to Data Subjects who have consented to receiving it. The Company may approach a Data Subject for consent only once.

c. Record Keeping

The Company shall keep record of:

- 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 DOCUMENTS

Documents may be destroyed after the termination of the retention period specified herein, or as determined by the Company from time to time.

Each department is responsible for attending to the destruction of its documents and electronic records, which must be done on a regular basis. Files must be checked to make sure that they may be destroyed and to ascertain if there are important original documents in the file. Original documents must be returned to the holder thereof, failing which, they should be retained by the Company pending such return.

The documents must made available for collection by the Shred-It, or other approved document disposal company.

Deletion of electronic records must be done in consultation with the IT Department, to ensure that deleted information is incapable of being reconstructed and/or recovered.

11. STATUTORY RETENTION PERIODS

| LEGISLATION | DOCUMENT TYPE | PERIOD |
|---|---|---|
| COMPANIES ACT | • Any documents, accounts, books, writing, records, or other information that a company is required to keep in terms of the Act.<br>• Notice and minutes of all shareholders meeting, including resolutions adopted and documents made available to holders of securities.<br>• Copies of reports presented at the annual general meeting of the company.<br>• Copies of annual financial statements required by the Act.<br>• Copies of accounting records as required by the Act.<br>• Record of directors and past directors, after the director has retired from the company.<br>• Written communication to holders of securities and<br>• Minutes and resolutions of directors' meetings, audit committee and directors' committees. | 7 YEARS |
| | • Registration certificate.<br>• Memorandum of Incorporation and alterations and amendments.<br>• Rules.<br>• Securities register and uncertified securities register.<br>• Register of company secretary and auditors and<br>• Regulated Companies (companies to which chapter 5, part B, C and Takeover Regulations apply) – Register of disclosure of person who holds beneficial interest equal to or more than 5% of the securities of that class issued. | INDEFINITELY |

| | | |
|---|---|---|
| CONSUMER PROTECTION ACT | • Full names, physical address, postal address, and contact details.<br>• ID number and registration number.<br>• Contact details of public officer in case of a juristic person.<br>• Service rendered.<br>• Cost to be recovered from the consumer.<br>• Frequency of accounting to the consumer.<br>• Amounts, sums, values, charges, fees, remuneration specified in monetary terms.<br>• Conducting a promotional competition refer to Section 36(11)(b) and Regulation 11 of Promotional Competitions. | 3 YEARS |

| | | |
|---|---|---|
| FINANCIAL INTELLIGENCE CENTRE ACT | • Whenever a reportable transaction is concluded with a customer, the institution must keep record of the identity of the customer.<br>• If the customer is acting on behalf of another person, the identity of the person on whose behalf the customer is acting and the customer's authority to act on behalf of that other person.<br>• If another person is acting on behalf of the customer, the identity of that person and that other person's authority to act on behalf of the customer.<br>• The way the identity of the persons referred to above was established.<br>• The nature of that business relationship or transaction.<br>• In the case of a transaction, the amount involved and the parties to that *transaction*.<br>• All accounts that are involved in the transactions concluded by that accountable institution during that business relationship and that single transaction.<br>• The name of the person who obtained the identity of the person transacting on behalf of the accountable institution.<br>• Any document or copy of a document obtained by the accountable institution. | 5 YEARS |

| | | |
|---|---|---|
| COMPENSATION FOR OCCUPATIONAL INJURIES AND DISEASES ACT | Register, record or reproduction of the earnings, time worked, payment for piece work and overtime and other prescribed particulars of all the employees. | 4 YEARS |
| | Section 20(2) documents:<br>• Health and safety committee recommendations made to an employer in terms of issues affecting the health of employees and of any report made to an inspector in terms of the recommendation.<br>• Records of incidents reported at work. | 3 YEARS |
| | Asbestos Regulations, 2001, regulation 16(1):<br>• Records of assessment and air monitoring, and the asbestos inventory.<br>• Medical surveillance records.<br>• Hazardous Biological Agents Regulations, 2001, Regulations 9(1) and (2):<br>• Records of risk assessments and air monitoring.<br>• Medical surveillance records.<br>• Lead Regulations, 2001, Regulation 10:<br>• Records of assessments and air monitoring.<br>• Medical surveillance records<br>• Noise - induced Hearing Loss Regulations, 2003, Regulation 11:<br>• All records of assessment and noise monitoring.<br>• All medical surveillance records, including the baseline audiogram of every employee. | 40 YEARS |
| | Hazardous Chemical Substance Regulations, 1995, Regulation 9:<br>• Records of assessments and air monitoring.<br>• Medical surveillance records | 30 YEARS |

| | | |
|---|---|---|
| BASIC CONDITIONS OF EMPLOYMENT | Section 29(4):<br>• Written particulars of an employee after termination of employment.<br>Section 31:<br>• Employee's name and occupation.<br>• Time worked by each employee. | 3 YEARS |

| | | |
|---|---|---|
| | • Remuneration paid to each employee.<br>• Date of birth of any employee under the age of 18 years. | |
| EMPLOYMENT EQUITY ACT | • Records in respect of the company's workforce, employment equity plan and other records relevant to compliance with the Act.<br>• Section 21 report which is sent to the Director General. | 3 YEARS |
| LABOR RELATIONS ACT | Records to be retained by the employer are the collective agreements and arbitration awards. | 3 YEARS |
| | • An employer must retain prescribed details of any strike, lock-out or protest action involving its employees.<br>• Records of each employee specifying the nature of any disciplinary transgressions, the actions taken by the employer and the reasons for the actions. | INDEFINITE |
| UNEMPLOYMENT INSURANCE ACT | Employers must retain personal records of each of their current employees in terms of their names, identification number, monthly remuneration and address where the employee is employed. | 5 YEARS |
| TAX ADMINSISTRATION ACT | <u>Section 29 documents which:</u><br>• Enable a person to observe the requirements of the Act.<br>• Are specifically required under a Tax Act by the Commissioner by the public notice.<br>• Will enable SARS to be satisfied that the person has observed these requirements. | 5 YEARS |

| | | |
|---|---|---|
| INCOME TAX ACT | • Amount of remuneration paid or due by him to the employee.<br>• The amount of employee's tax deducted or withheld from the remuneration paid or due.<br>• The income tax reference number of that employee.<br>• Any further prescribed information.<br>• Employer Reconciliation return. | 5 YEARS |
| VALUE ADDED TAX ACT | • Where a vendor's basis of accounting is changed the vendor shall prepare lists of debtors and creditors showing the amounts owing to | 5 YEARS |

| | | |
|---|---|---|
| | the creditors at the end of the tax period immediately preceding the changeover period.<br>• Importation of goods, bill of entry, other documents prescribed by the Custom and Excise Act and proof that the VAT charge has been paid to SARS.<br>• Vendors are obliged to retain records of all goods and services, rate of tax applicable to the supply, list of suppliers or agents, invoices and tax invoices, credit and debit notes, bank statements, deposit slips, stock lists and paid cheques.<br>• Documentary proof substantiating the zero rating of supplies.<br>• Where a tax invoice, credit, or debit note, has been issued in relation to a supply by an agent or a bill of entry as described in the Customs and Excise Act, the agent shall maintain sufficient records to enable the name, address, and VAT registration number of the principal to be ascertained. | |