POPI POLICY

Table of Contents

1. INTRODUCTION

1.1. This policy is prepared with respect to S4 Integration (Pty) Ltd as well as any companies trading within the S4 Group of Companies (hereinafter referred to as the "Company").

1.2. This Protection of Personal Information Act – Policy and Compliance (hereinafter referred to as the "Policy") serves to:

1.2.1. Indicate the method in which the Company will meet and fulfil its legal obligations and requirements concerning the protection, processing, and disclosure of personal and confidential information; and

1.2.2. Indicate the method in which the Company will meet and fulfil its legal obligations and requirements concerning confidentially and information security standards.

1.3. This Policy is based broadly on the Protection of Personal Information Act 4 of November 2013, as may be amended from time to time and in respect whereof regulations and guidelines may be issued (hereinafter referred to as the "Act").

1.4. The Company is committed to ensuring it complies and adheres to the requirementsas set out in the Act.

1.5. This Policy must be read together with the S4 Private Policy (https://www.s4.co.za/privacy-policy).

1.6. The Company contact details are:

1.6.1.	Head of the Company:	Andrew White
1.6.2.	Information Officer:	Louise van Schalkwyk
1.6.3.	Postal Address:	PO Box14248 Sidwell *Gqeberha* 6061
1.6.4.	Registered Address:	150 Mimosa Road Fairview *Gqeberha* *6065*
1.6.5.	Telephone Number:	+27 41 451 1250
1.6.6.	Email Address:	louise.vanschalkwyk@s4.co.za

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, of requesting a donation.

2.4. **POPI**
means the Protection of Personal Information Act, No. 4 of 2013.

2.5. **Personal Information**
means information relating to an unidentifiable, living, natural person, or an identifiable, existing juristic person, as defined in POPI.

2.6. **Processing**
means an operation or activity, whether or not by automatic means, concerning Personal Information.

2.7. **S4 Group of Companies**
S4 Integration, S4 Automation, S4 Devserv, S4 Corporate Services

3. REQUIREMENTS

3.1. In terms of the Act, the Company is required to inform any and all data subjects of the purpose for which their personal information is collected and will be processed,stored, and/or used.

3.2. In terms of the Act, the Company is required to protect any and all information assets from all internal and external threats.

4. INFORMATION OFFICER

4.1. The Information Officer shall be responsible for:

4.1.1 Conducting a preliminary assessment;
4.1.2 Implementing, monitoring, and adjustment of this Policy;
4.1.3 Ensuring sufficient and appropriate documentation is available to support this Policy;

4.1.4 Ensuring that all documentation in connection with this policy is relevant and up to date; and

4.1.5 Ensuring this Policy, and any subsequent amendments and/or replacements and/or updates thereto, are communicated to all relevant parties.

5 PRINCIPLES

The Company collects and uses Personal Information of individuals and corporate entities with whom it works in order 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 it deals with. The Company therefore fully endorses and adheres to the principles of the Protection of Personal Information Act ("POPI").

5.1 Accountability:

5.1.1 The Company will take reasonable steps that personal information obtained from data subjects is stored in a safe and secure manner.

5.2 Processing limitation:

5.2.1 The Company undertakes to, as far as reasonably possible, collect personal information directly from the data subject or any party authorised by them to release such information.

5.2.2 Personal information may be collected by the Company from a source other than the data subject, provided that:

5.2.2.1 The personal information is obtained from a public record;

5.2.2.2 The personal information was made public by the data subject in a deliberate manner;

5.2.2.3 The personal information is collected from another source with the data subject's consent;

5.2.2.4 The collection of the personal information from another source does not have any reasonable possibility of prejudicing the data subject;

5.2.2.5 The collection of the personal information from another source is required to comply with any law;

5.2.2.6 The collection of the personal information from another source is required to maintain or exercise any legal right;

5.2.2.7 The collection of the personal information from the data source would prejudice the lawful purpose of the collection; or

5.2.2.8 The collection of personal information from the data source is not reasonably practical.

5.2.3 The Company undertakes, as far as reasonably possible, to process and disclose any personal information received from a data subject only with the consent of the data subject, or if required to so release the informationby law.

5.2.4 Where the Company is required to disclose any personal information by law, it will take reasonable steps to inform the data subject of suchdisclosure.

5.3 Specific purpose:

5.3.1 The Company undertakes to collect personal information from data subjects insofar as such information is required for any and all activities related to and/or incidental to its business operations, including, but not limited to the supply of products, the rendering of services, the registering of learnerships with the relevant bodies, the supplying of information to bodies requiring such information under any law, and the direct marketing of services to clients and students through electronic communication

5.3.2 The Company may only process special personal information if:

5.3.2.1 The data subject has consented to such processing;

5.3.2.2 The special personal information was made public by the data subject in a deliberate manner;

5.3.2.3 The processing of the special personal information is required for the establishment of a right or defense in law;

5.3.2.4 The processing of the special personal information is for statistical, historical or research purposes; or

5.3.2.5 If the special personal information relates to race or ethnic origin, such special personal information must be processed tocomply with affirmative action laws.

5.4 Limitation of further processing:

5.4.1 The Company shall not be entitled to process personal information in a manner which is incompatible with the purpose wherefore the information was initially collected, as set out in Clause 5.3 hereof.

Further processing will be compatible with the purpose set out in Clause 5.3 hereof if:

5.4.1.1 The data subject has consented to such further processing;

5.4.1.2 The personal information is obtained in a public record;

5.4.1.3 The personal information was made public by the data subjectin a deliberate manner;

5.4.1.4 The collection of the personal information from another sourceis required to comply with any law;

5.4.1.5 The collection of the personal information from another sourceis required to maintain or exercise any legal right; or

5.4.1.6 Such further processing is required to prevent or mitigate a threat to public health or safety or the life or health of the data subject or a third party.

5.5 Information quality:

5.5.1 The Company will ensure that all reasonable measures are taken to ensurea data subject's personal information is complete, up to date, and accurate before such personal information is used.

5.5.2 To ensure that any and all personal information is complete, up to date andaccurate, the Company may request a data subject, from time to time, to update the personal information and to confirm the same is still relevant.

5.5.3 Should the Company be unable to reach a data subject for the purposes of confirming the personal information held for the said data subject, the Company is entitled to permanently remove and/or delete such personal information from its records.

5.6 Transparency and openness:

5.6.1 The Company will reasonably endeavour to ensure that a data subject is aware of the following where any personal information relating to said data subject was collect from any source other than the data subject directly:

5.6.1.1 That the data subject's personal information is being collected;

5.6.1.2 Who is collecting the data subject's personal information; and

5.6.1.3 The reason for which the data subject's personal information has been collected.

5.7 Security safeguards:

5.7.1 The Company will ensure that all reasonable technical and organisational measures have been taken to secure the integrity of data subject's personal information, and to guard against the risk of loss, damage and/or destruction thereof.

5.7.2 The Company will ensure that all reasonable measures are taken to protectagainst the unauthorised and/or unlawful access, processing and/or use of a data subject's personal information.

5.7.3 The Company will ensure that all reasonable measure are taken to ensure that a data subject's personal information is only used for legitimate purposes by authorised persons as consented to by the data subject.

5.8 Participation of data subjects:

5.8.1 Any and all data subjects are entitled to know the particulars of the personal information held by the Company in so far the said personal information relates to the particular data subject.

5.8.2 Any and all data subjects are entitled to know the identity of any authorisedperson of the company who has had access to the personal information insofar the personal information relates to the particular data subject.

5.8.3 Any and all data subjects are entitled to correct any and all personal information held by the Company insofar the personal information relates to the particular data subject.

6 CONSIDERATIONS

6.1.1 The Directors of the Company in general, and the Information Officer in particular, are responsible for administering and overseeing the implementation of this Policy and any supporting guidelines, standard operating procedures, notices, consents, and related documentation and processes, if applicable.

6.1.2 The Company undertakes to reasonably train any and all authorised persons, in accordance with the relevant function of such person, in the requirements, policies, guidelines and regulations governing the protection of personal information.

6.1.3 The Company will undertake periodic reviews and audits to ensure compliance with this policy and guidelines, if and when required andapplicable.

6.2 Operating controls:

6.2.1 The Company will take all reasonable steps to establish appropriate standard operating procedures which are consistent with this Policy and theregulatory environment, including:

6.2.1.1 The allocation of information security responsibilities;

6.2.1.2 The establishment of incident reporting and management;

6.2.1.3 The introduction of user identification;

6.2.1.4 Information security training and education; and

6.2.1.5 Data backup.

6.3 Policy compliance:

6.3.1 Any and all breaches of this Policy may result in disciplinary action and the possible termination of employment.

7 PROCESSING OF PERSONAL INFORMATION

7.1 The Company may use any and all personal information in its possession for the following purposes:

7.1.1 Conducting credit reference checks and assessments;

7.1.2 The administration of agreements;

7.1.3 Providing products and services to customers;

7.1.4 Discounting and asset funding purposes;

7.1.5 The detection and prevention of fraud, crime, money laundering and otherunlawful practices;

7.1.6 The conducting market or customer satisfaction research;

7.1.7 Marketing and sales;

7.1.8 In connection with legal proceedings;

7.1.9 Staff administration;

7.1.10 The maintenance of accounts and records;

7.1.11 Ensuring compliance with legal and regulatory requirements;

7.1.12 Registering students with the relevant bodies for learnerships;

7.1.13 Sharing data cross-border with affiliated companies;

7.1.14 Profiling data subjects for the purposes of direct marketing; and

7.1.15 Any other and/or further activities which relate directly or indirectly or are incidental to the Company's business activities.

7.2 The Company may possess the following records relating to supplier, employees, directors, service providers, contractors and customers:

Customers: Natural persons	Full names; Contact details; Physical and postal addresses; Date of birth; Identity number; Tax related information; Nationality; Gender; Confidential correspondence; and Any further information voluntarily supplied by the customer
Customers: Juristic persons	Names of contact persons; Registered name of the legal entity;Physical and postal address; Contact details; Financial information; Registration number; Founding documents; Tax related information; Authorised signatories; Beneficiaries; Ultimate beneficial owners;Shareholding information; BBBEE information; Confidential correspondence; and Any further information voluntarily supplied by the customer
Service providers/contractors	Names of contact persons; Registered name of the legal entity; Physical and postal address; Contact details; Financial information; Registration number; Founding documents; Tax related information; Authorised signatories; Beneficiaries; Ultimate beneficial owners; Shareholding information; BBBEE information; Confidential correspondence; and Any further information voluntarily supplied by the service provider/contractor
Employees and directors	Gender; Race; Age; language; Education information; Financial information; Employment history; Identity number; Physical and postal address;Contact details; Criminal record; Mental and physical well-being; and Any further information voluntarily supplied by the employee/director
Students	Full names; Contact details; Physical and postal addresses; Date of birth; identity number; Nationality; Gender; Confidential correspondence; and Any further information voluntarily supplied by the customer

8 AGREEMENT

8.1 The submission of any documentation, contract, agreement, proposal, contactrequest, and/or the sending of any correspondence by a data subject whereby any personal information is disclosed and/or provided to the Company, such data subjectacknowledges that:

8.1.1 The data subject has read and understood this Policy;

8.1.2 The data subject accepts the terms contained in this policy;

8.1.3 The data subject has no objection to the personal information provided being used by the Company as described in Clause 5 of this Policy;

8.1.4 The personal information which has been provided is true, correct, and up to date.

8.2 All data subjects retain the right to, at any time, refuse consent and/or to withdraw consent to the processing of personal information in terms of this Policy insofar thepersonal information relates to that data subject.

8.3 All data subjects retain the right to, at any time, object to the processing of personalinformation on any of the grounds set out in Clause 5 of this Policy insofar the personal information relates to that data subject unless the processing of the personal information is required by law.

8.4 If the data subject withdraws consent to the processing of personal information in so far the personal information relates to that data subject, the Company shall refrain from any further processing of such personal information.

8.5 Upon the signing of a contract of employment with the Company, all employees acknowledge and agree that they become a data subject of the Company and that the Company shall be entitled to collect and process their personal information in line with Clause 7.2.4 of this Policy.

8.6 The employees of the Company, as data subjects agree and consent to certain of their personal information, including, but not limited to their contact details, full names, identity numbers, and date of birth being processed and provided to customers for the purpose of the tender process and/or ensuring the customer is able to communicate effectively with the employee.

9 CROSS-BORER DATA TRANSFER

9.1 The Company reserves the right to provide any information, whether such information is personal or not, to ESRI Inc. insofar such a transfer is required by anyAgreement between the Company and ESRI Inc. or by any laws governing the relationship between ESRI Inc. and the Company.

9.2 The Company shall be required to ensure that any and all information, whether suchinformation is personal or not, that is transferred to ESRI Inc. is sorted, maintained and/or processed in terms of the relevant law governing such storage, maintenanceand/or processing.

10 WEBSITE PRIVACY POLICY

10.1.1 Please refer to the Company's website where the Website Privacy Policy is published.

https://www.s4.co.za/privacy-policy

11 GENERAL

11.1.1 The Company reserves the right to alter and/or amend and/or substitute and/or replace this Policy at any time without the need to explicitly inform any current and/orfuture data subjects of such alteration, amendment, substitution and/or replacement.

11.1.2 Clause 9.1 shall apply regardless of whether such alteration and/or amendment and/or substitution and/or replacement relates to any particular Clause, provision and/or part of this Policy or to the Policy as a whole.

11.1.3 The Company confirms that it will retain any and all information, whether personal or otherwise, relating to a data subject for as long as its relationship with the said data subject shall continue.

11.1.4 Despite any provision in any law prescribing a minimum retention period for any information, whether personal or otherwise, the Company may, in its sole discretion,retain any and all such information which is deemed to be worth retaining for any period of time which is longer than the prescribed minimum retention period.

11.1.5 The Company undertakes to take reasonable measures to ensure that any and all information, whether personal or otherwise, which is retained after the termination of the relationship between it and a data subject shall be stored and kept in a mannerwhich is consistent with the provisions of the Act.

12 SECURITY SAFEGUARDS

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

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

12.2.1 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 wherenon-staff members may access them;
- 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.

12.2.2 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 individualcomputers, laptops or hand-held devices;
- Electronical Personal Information which is no longer required must be deleted from theindividual 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 Informationmust 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.

13 DIRECT MARKETING

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

13.1.1 Existing Customers

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

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

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

13.1.2 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.

13.1.3 Record Keeping

The Company shall keep record of:

13.1.3.1 Date of consent
13.1.3.2 Wording of the consent
13.1.3.3 Who obtained the consent
13.1.3.4 Proof of opportunity to opt-out on each marketing contact
13.1.3.5 Record of opt-outs

14 DESTRUCTION OF DOCUMENTS

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

14.2 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 in order to make sure that they may be destroyed and also 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.

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

14.4 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.

15 STATUTORY RETENTION PERIODS

The Company confirms that, once its relationship with a data subject has ended, it will retain any and all information, whether personal or otherwise, relating to the said data subject for the minimum period prescribed by law:

Legislation	Document Type	Period
Companies Act	Any documents, accounts, books, writing, records or other information that a company isrequired to keep in terms of the Act; Notice and minutes of all shareholders meeting, including resolutions adopted anddocuments made available to holders of securities; Copies of reports presented at the annualgeneral meeting of the company; Copies of annual financial statements requiredby the Act; Copies of accounting records as required bythe Act; Record of directors and past directors, after the director hasretired from the company; Written communication to holders ofsecurities and Minutes and resolutions of directors' meetings, audit committee and directors'committees.	7 Years
	Registration certificate; Memorandum of Incorporation andalterations and amendments; Rules; Securities register and uncertifiedsecurities register; Register of company secretary andauditors and Regulated Companies (companies to whichchapter 5, part B, C and Takeover Regulations apply) – Register of disclosure of person who holds beneficial interest equal to or in excess of 5% of the securitiesof that class issued.	Indefinitely

Consumer Protection Act	Full names, physical address, postaladdress and contact details; ID number and registration number; Contact details of public officer in case of ajuristic person; Service rendered; Cost to be recovered from the consumer; Frequency of accounting to the consumer; Amounts, sums, values, charges, fees, remuneration specified in monetary terms; Conducting a promotional competitionrefer 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 institutionmust keep record of the identity of the customer; If the customer is acting on behalf of another person, the identity of the person on whose behalf the customer is acting andthe customer's authority to act on behalf of that other person; If another person is acting on behalf of thecustomer, the identity of that person and that other person's authority to act on behalf of the customer; The manner in which the identity of the persons referred to above was established; The nature of that business relationship ortransaction; In the case of a transaction, the amount involved and the parties to that transaction; All accounts that are involved in the transactions concluded by that accountableinstitution in the course of that business relationship and that single transaction; The name of the person who obtained the identity of the person transacting on behalfof the accountable institution; 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 piecework and overtime and other prescribed particulars of all the employees.	4 years
	Section 20(2) documents : -Health and safety committee recommendations made to an employer interms of issues affecting the health of employees and of any report made to an inspector in terms of the recommendation; -Records of incidents reported at work.	3 years
	Asbestos Regulations, 2001, regulation 16(1): -Records of assessment and air monitoring, and the asbestos inventory; -Medical surveillance records; Hazardous Biological Agents Regulations, 2001, Regulations 9(1) and (2): -Records of risk assessments and airmonitoring; -Medical surveillance records. Lead Regulations, 2001, Regulation 10: -Records of assessments and airmonitoring; -Medical surveillance records Noise - induced Hearing Loss Regulations,2003, Regulation 11: -All records of assessment and noisemonitoring; -All medical surveillance records, including the baseline audiogram of every employee.	40 years
	Hazardous Chemical Substance Regulations, 1995, Regulation 9: -Records of assessments and air monitoring; -Medical surveillance records	30 years

Basic Conditions of Employment Act	Section 29(4): -Written particulars of an employee after termination of employment; Section 31: -Employee's name and occupation; -Time worked by each employee; -Remuneration paid to each employee; -Date of birth of any employee under the age of 18 years.	3 years
EmploymentEquity Act	Records in respect of the company's workforce, employment equity plan and other records relevant to compliance withthe Act; Section 21 report which is sent to the Director General	3 years
Labour Relations Act	Records to be retained by the employer are the collective agreements and arbitration awards.	3 years
	An employer must retain prescribed detailsof any strike, lock-out or protest action involving its employees; Records of each employee specifying the nature of any disciplinary transgressions, the actions taken by the employer and thereasons 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 Administration Act	Section 29 documents which: -Enable a person to observe the requirements of the Act; -Are specifically required under a Tax Act by the Commissioner by the public notice; -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; The amount of employees tax deducted or withheld from the remuneration paid or due; The income tax reference number of that employee; Any further prescribed information; 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 the creditors at the end of the tax period immediately preceding the changeover period; 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; 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; Documentary proof substantiating the zero rating of supplies; 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.	5 years