PURESAN©

Environmentally +

Protection of Personal Information Policy

This Policy was prepared in accordance with Section 51 of the Promotion of Access to Information Act, 2000 and to address the requirements of the Protection of Personal Information Act, 2013.

July 2021

Contents

Page

1 INTRODUCTION

The purpose of this document is to provide a concise policy statement regarding the Data Protection obligations of Puresan (Pty) Ltd (Puresan). This includes obligations in dealing with personal data, in order to ensure that Puresan (Pty) Ltd complies with the requirements of the relevant and applicable Personal Information Protection Act 26 November 2013 (and amendments).

Puresan (Pty) Ltd is required to collect, process and use certain information about individuals which includes but is not limited to customers, suppliers, business contacts, employees and other persons Puresan may need to contact.

This policy lists how this data/information must be collected, handled and stored in order to meet Puresan' data protection standards whilst also complying with the data privacy requirements as prescribed by the POPI Act of 2013.

Why this Policy Exists

This data protection policy ensures that Puresan:

- Complies with data protection law and follows good practise;
- Protects the rights of staff, customers and 3rd Parties;
- Is open about how is stores and processed individual's data;
- Protects itself from the risks of a data/information breach.

Contact Details:
Operations Director: J L Penrose
Address: Unit 2, Gate 1
11 Engwena Road
Sebenza
Edenvale
1609
Postal Address: P O Box 1062
Bedfordview
2008
Telephone Number: +27 (0)11 609 0314
Email: info@puresan.net

Head of Body: I Wegrostek
Address: 190 Longleat Avenue
Chartwell
2055
Postal Address: P O Box 2960
Ditropan
2058
Telephone Number: +27 (0)11 609 0314
Email: info@puresan.net

Information Officer: J L Penrose
Address: Unit 2, Gate 1
11 Engwena Road
Sebenza
Edenvale
1609
Postal Address: P O Box 1062
Bedfordview
2008
Telephone Number: +27 (0)11 609 0314
Email: info@puresan.net

Deputy Information Officer: J Dawes
Address: Unit 2, Gate 1
11 Engwena Road
Sebenza
Edenvale
1609
Postal Address: P O Box 1062
Bedfordview
2008
Telephone Number: +27 (0)11 609 0314
Email: info@puresan.net

2 DEFINITIONS

The following definitions will apply to this policy, if there is any doubt the definitions as described in the Act should be used:

Data Subject – means the person from whom the Personal Data/ Information is required

Personal Data/ Information – means any and all information pertaining to either a natural or juristic person by which they can be identified.

Processing - means any operation or activity or any set of operations whether or not by automated means, concerning Personal information, including –

(a) The collection, receipt, recording, organisation, collation, storage, updating or modifications, retrieval, alteration, consultation, or use;
(b) Decimation 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."

Record - means any type of record whether it be written, stored on a computer, generated by a computer, on tape, camera, films, photographs; any way that Personal information can be stored.

Responsible Party - means a public or private body or any other person which, alone or in conjunction with others, determines the purpose of a means for processing Personal information.

3 POLICY SCOPE

This policy applies to:

- Puresan (Pty) Ltd (Puresan)
- All staff of Puresan
- All contractors, suppliers and other service providers
- It applies to all information that Puresan holds relating to identifiable individuals, even if that information technically falls outside of the Protection of Personal Information Act of 2013. This can include but not limited to:
    - Names of individuals;
    - Identity Numbers;
    - Physical Addresses;
    - Postal Addresses;
    - Email Addresses;
    - Telephone Numbers;
    - Any other information relating to individuals

4 PROTECTION OF PERSONAL INFORMATION ACT

4.1 The Protection of Personal Information Act 2013, ("POPI") describes how organisations including APWS must collect, handle and store Personal Data / Information.

4.2 These rules apply regardless of whether data is stored electronically, on paper or on other materials.

4.3 To comply with the law, Personal Data / Information must be collected and used fairly, stored safely and not disclosed unlawfully.

4.4 The Protection of Personal Information Act is underpinned by eight important conditions which together constitute the lawful processing of information, namely:

4.4.1 Accountability – The person or entity collecting the data / information has an obligation to ensure that there is compliance with POPI in respect of the processing of Personal Data / Information.

4.4.2 Processing Limitations – Personal Data /Information must be collected directly from the person to the extent that such data / information is necessary; must only be processed with the consent of the data subject; where such consent is necessary and must only be used for the purposes for which it is obtained.

4.4.3 Purpose Specification – Personal Data / Information must only be processed for the specific purpose for which it is obtained and must not be kept for any longer than is needed to achieve such purpose.

4.4.4 Further Processing Limitations – Further processing of Personal Data / Information must be compatible with the initial purpose for which the data / information was collected.

4.4.5 Information Quality – The Responsible Party must ensure that the Personal Data / Information held is accurate and updated regularly and that the integrity of the Personal Data / Information is maintained by appropriate security measures.

4.4.6 Openness – There must be transparency between the Data Subject and the Responsible Party.

4.4.7 Security Safeguards – A Responsible Party must take reasonable steps to ensure that adequate safeguards are in place to ensure that Personal Data / Information is being processed responsibly and it not unlawfully accessed.

4.4.8 Data Subject Participation – The Data Subject must be made aware that their Personal Data / Information is being processed and must have provided their informed consent to such processing.

5 PURPOSE OF PROCESSING PERSONAL INFORMATION

5.1 The purpose for which Puresan processes information is set out in **Annexure A** hereto.

5.2 Puresan will evaluate the information it needs on an annual basis to ensure that the information it requires in order to operate its business is still relevant.

5.3 Puresan will never request any information from a data subject that is not relevant to it fulfilling its business operation requirements.

6 CATEGORIES OF DATA SUBJECTS AND THEIR PERONSAL INFORMATION

6.1 Puresan has the following categories of Data subjects as listed in **Annexure B** hereto.

7 DATA SUBJECT PARTICIPATION TRANSPARENCY

7.1 Puresan will take all necessary steps to ensure the Data subject is aware of the following:

7.1.1 That Personal Data/ Information is needed from them.

7.1.2 Of their right to have their Personal Data/ Information processed in line with the conditions of lawful processing.

7.1.3 Of their right to refuse to have their Personal Data/ Information processed and the consequences thereof.

7.1.4 Of their right to be notified that their Personal Data/ Information has been accessed or acquired by an unauthorised person.

8 DATA SUBJECT PARTICIPATION RIGHT TO REQUEST /AMEND OR DELETION OF PERSONAL INFORMATION

8.1. Puresan will take all necessary steps to ensure the Data subject is aware of the following:

8.1.1 Their right to ask whether a Responsible Party holds Personal Data /Information about him and to request access to such information.

8.1.2 Their right to ask, if necessary, for the correction, destruction or deletion of his Personal Data / Information.

8.1.3 Their right to object, on reasonable grounds relating to his individual situation, to the processing of his Personal Data /Information.

8.1.4 The right to object to the processing of his Personal Data / Information –
(i) At any time for the purposes of direct marketing.

8.1.5 The right not to have his Personal Data /Information processed for the purposes of direct marketing by means of unsolicited electronic communications except as provided for in s69(1).

8.1.6 The right not to be subject, under certain conditions, to a decision based solely on the basis of automated processing of his Personal Data / Information intended to provide a profile of such a person as provided for in section 71.

8.1.7 The right to lodge a complaint with the Regulator regarding the alleged interference with the protection of the Personal Data / Information of any Data Subject or to submit a complaint to the Regulator in respect of a determination of an adjudicator as provided for in s74.

8.1.8 The right to institute civil proceedings regarding the alleged interference with his personal information as provided for in s99.

8.2 The Information Officer or the delegated official is to ensure that all documentation in which all personal information is requested must contain clauses to this effect.

9 DATA ACCURACY

9.1 The law requires Puresan to take reasonable steps to ensure data is kept accurate and up to date.

9.2 The more important the Personal Data /Information, the greater the effort Puresan should put into ensuring its accuracy.

9.3 It is the responsibility of all employees who work with data to take reasonable steps to ensure it is kept as accurate and up to date as possible.

9.4 This will include but not be limited to the following:

9.4.1 Where documents are completed physically in writing by the person that the handwriting is legible.

9.4.2 Where documents are completed on behalf of someone for whatsoever reason that they are legible, and the spelling is correct.

9.4.3 Where photocopies or scans are made of any documents or proof of identity that the copies / scans are legible.

9.4.4 Where the information obtained has to be uploaded on to a computer system that such is done with the proper care and accurately.

9.4.5 All employees are to check that any clients' / suppliers' details that are already on record are up to date should that client / supplier phone or attend Puresan.

9.4.6 Data / Information should be updated as inaccuracies are discovered. For instance, if a customer can no longer be reached on their stored telephone number, it should be removed from the database.

10 PROCESSING OF PERSONAL INFORMATION

10.1 Nominated person/s working for Puresan has responsibility for ensuring Personal Data / Information is collected, stored, and handled appropriately.

10.2 Such nominated person/s who handle Personal Data / Information must ensure that it is handled and processed in line with this policy and data protection principles. However, the positions listed hereunder have key areas of responsibility:

10.2.1 The Information Officer

The Information Officer is ultimately responsible for ensuring that Puresan meets its legal obligations.

10.2.2 The Information Officer

J L Penrose is responsible for:

- Keeping the Company Representative / Director updated about data protection responsibilities, risks, and issues.
- Reviewing all data protection procedures and related policies, in line with an agreed schedule.
- Arranging data protection training and advice for the people covered by this policy.
- Handling data protection questions from staff and anyone else covered by this policy.
- Dealing with requests from individuals to see the data that APWS holds about them (also referred to as 'subject access requests').
- Checking and approving any contracts or agreements with third parties that may handle the Company's sensitive data.
- Ensuring all systems, services and equipment used for storing data meet acceptable security standards.
- Performing regular checks and scans to ensure security hardware and software is functioning properly.
- Evaluating any third-party services the Company is considering using to store or process data. For instance, cloud computing services.
- Approving any data protection statements attached to communications such as emails and letters.
- Addressing any data protection queries from journalists or media outlets such as newspapers.
- Where necessary, working with other staff to ensure marketing initiatives abide by data protection principles.

10.2.3 General Staff Guidelines

The Company Representative, is responsible for:

The only people able to access the Personal Data / Information covered by this policy should be those who need it for their work.
Data should not be shared informally. When access to confidential information is required, employees can request it from their line managers.
Puresan will provide training to all employees to help them understand their responsibilities when handling data / information.
Employees should keep all data secure, by taking sensible precautions and following the guidelines below.
In particular, strong passwords must be used, and they should never be shared.
Personal Data / Information should not be disclosed to unauthorised people, either within the Company or externally.
Data / Information should be regularly reviewed and updated it is found to be out of date. If no longer required, it should be deleted and disposed of.

Employees should request help from their line manager or the data protection officer if they are unsure about any aspect of data protection.

11 THIRD-PARTY PROCESSORS AND SERVICE PROVIDERS

11.1 Puresan may engage the services of Third-Party Processors and Service Providers to process Personal Data / Information on its behalf from time to time.

11.2 In this case a formal written contract is in place with the Processor, outlining their obligations in relation to the Personal Data / Information, the specific purpose or purposes for which they are engaged, and an understanding that they will process the data in compliance with the POPI Act 26 of November 2013 and amendments.

11.3 The following categories of data processors are used in the course of business:

- Cloud web hosting services with providers to do analytics, forms and scheduling.
- Business administration services that do document management, accounting and document verification.
- Payment service providers including the bank and payment processors.
- Location and CCTV monitoring tools.
- Video and voice recording tools.
- Social media platforms.

These categories may be updated from time to time and for an updated list of categories of data processors, please contact the information officer.

12 FURTHER PROCESSING

12.1 Personal Data / Information that has been collected will only be processed again if such is compatible with the original purpose for which it was collected and under the following conditions:

12.1.1 The Data Subject has consented to further processing.

12.1.2 Further processing is necessary to maintain, comply with or exercise any law or legal right.

12.1.3 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.

12.1.4 Further processing is necessary to prevent a

12.1.5 The Data Subject

13 DATA STORAGE AND DESTRUCTION

13.1 Paper

13.1.1 When data is stored on paper, it should be kept in a secure place where unauthorised people cannot see it.

13.1.2 These guidelines also apply to data that is usually stored electronically but has been printed out for some reason:

- When not required, the paper or files should be kept in a locked drawer or filing cabinet.
- Employees should make sure paper and printouts are not left where unauthorised people could see them, such as for instance, on a printer.

- Data printouts should be shredded and disposed of securely when no longer required.
- Data printouts, photocopies or scans that have been made and are defective must be shredded immediately.

13.2 Electronic Storage

13.2.1 When data is stored electronically, it must be protected from unauthorised access, accidental deletion, and malicious hacking attempts:

- Data should be protected by strong passwords that are changed regularly and never shared between employees.
- If data is stored on removable media (such as a CD or DVD), these should be kept locked away securely when not being used.
- Data should only be stored on designated drives and servers and should only be uploaded to an approved cloud computing service/s.
- Servers containing personal data should be kept in a secure location, away from general office space.
- Data should be backed up frequently. Those backups should be tested regularly, in line with the Company's standard backup procedures.
- Data should never be saved directly to laptops or other mobile devices such as tablets or smart phones.
- All servers and computers containing data should be protected by approved security software and a firewall.
- When working with personal data, employees should ensure the screens of their computers are always locked with left unattended.
- Personal data should not be shared informally.
- Data must be encrypted before being transferred electronically.
- Personal data must never be transferred outside of the borders of South Africa, unless contractually obligated to do so.

14 DATA SUBJECT ACCESS REQUESTS

14.1 All individuals who are subjects of personal data held by Puresan are entitled to:

14.1.1 Ask for information the Company holds about them and why.

14.1.2 Ask how to gain access to it.

14.1.3 Be informed how to keep it up to date.

14.1.4 Be informed on how Puresan is meeting its data protection obligations.

14.2 Should an individual request such information, this will be in compliance with the PAIA Act, and a nominal fee can be charged at the discretion of the Information Officer.

15 DISCLOSING DATA FOR OTHER REASONS

15.1 In certain circumstances, the Protection of Personal Information Act allows Personal Data / Information to be disclosed to law enforcement agencies without the consent of the data subject.

15.2 Under these circumstances Puresan will disclose requested data. However, the Information Officer will ensure the request is legitimate, seeking assistance from the Company Representative / Director and from the Company's legal advisers where necessary.

16 CROSS-BORDER FLOW OF PERSONAL INFORMATION

16.1 Section 72 of POPI provides that Personal Information may only be transferred out of the Republic of South Africa:

16.1.1 If the recipient country can offer such data an "adequate level" of protection. This means that its data privacy laws must be substantially like the Conditions for Lawful Processing as contained in POPI; or

16.1.2 If the Data Subject consents to the transfer of their Personal Information; or

16.1.3 If the transfer is necessary for the performance of a contractual obligation between the Data Subject and the Responsible Party; or

16.1.4 If the transfer is necessary for the performance of a contractual obligation between the Responsible Party and a third party, in the interests of the Data Subject; or

16.1.5 If the transfer is for the benefit of the Data Subject, and it is not reasonably practicable to obtain the consent of the Data Subject, and if it were, the Data Subject would like provide such consent.

16.2 Puresan does do Cross-Border transfers of any Personal Information relating to employees, clients, companies or organisation/s.

17 DATA BREACH NOTIFICATION

17.1 If a Data Subject becomes aware of a Data Breach, then the Data Subject is encouraged to contact the Information Officer immediately with all known information.

17.2 Where there are reasonable grounds to believe that the Personal Data / Information of a Data Subject has been accessed or acquired by any unauthorised person, Puresan must notify –

(a) The Regulator, and;

(b) The Data Subject unless the identity of the Data Subject cannot be established.

17.3 The notification will be made as soon as is reasonably possible after the discovery of the compromise, taking into account –

(a) The legitimate needs of law enforcement;

(b) Any measures necessary to determine the scope of the compromise

(c) To restore the integrity of the responsible person's information system.

17.4 The Responsible Party may only delay the notification to the Data Subject if a public body responsible for the prevention, detection, or investigation of offences, or the Regulator, determines that notification will impede a criminal investigation by a public body concerned.

17.5 Notification to the Data Subject will be in the manner as described by the Act.

17.6 The notification will provide sufficient information to allow the Data Subject to take protective measures against the potential consequences of the compromise, including –

(a) A description of the possible consequences of the breach;

(b) A description of the measures that the Responsible Party intends or has taken to address the breach;

(c) A recommendation with regards to the measures to be taken by the Data Subject to mitigate the possible consequences of the breach;
(d) If the Responsible Party knows the identity of the unauthorised person who may have accessed the personal information.

18 RETENTION OF PERSONAL INFORMATION RECORDS

18.1 Puresan will retain the Personal Data / Information in accordance with Annexure C hereto, where the relevant Acts are clear on data retention. Where the Acts remain silent, such information will be retained only for as along as such personal information is required.

18.2 Where the Personal Data / Information is of historical, scientific or research purposes, same will be retained indefinitely.

ANNEXURE A

PURPOSE OF PROCESSING

Puresan uses personal information under its care in the following manner:

1) Administration;
2) Rendering services according to its obligations under the Acts already aforementioned;
3) Staff administration;
4) Complying with tax laws;
5) Keeping of accounting records.

ANNEXURE B

CATEGORIES OF DATA SUBJECTS AND THEIR PERSONAL INFORMATION

ENTITY TYPE	PERSONAL INFORMATION PROCESS
Customers: Natural Persons	Names, contact details, physical and postal address, date of birth, identity number.
Customers: 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, authorised signatories, beneficiaries, ultimate beneficial owners.
Contracted Service Providers	Names of contact persons, name of legal entity, physical and postal address and contact details, financial information, registration number, tax related information, authorised signatories, beneficiaries.
Employees	Gender, pregnancy, marital status, colour, race, age, language, educational information, financial information, employment history, ID number, physical and postal address, contact details, criminal record, wellbeing.

ANNEXURE C

LEGISLATION LIST

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; Notice and minutes of all shareholders meeting, including resolutions adopted and documents made available to holders of securities; Copies of reports presented at the annual general meeting of the SPCA; Copies of annual financial statements required by the Act; Records of directors and past directors, after the director has retired from the company; Written communication to holders of securities and Minutes and resolutions of directors' meetings, audit committee meetings and Directors' committees.	7 years
	Registration certificate; Memorandum of Incorporation and alternations and amendments; Rules; Securities register and uncertified securities register; Register of company secretary and auditors and 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 in excess of 5% of the securities of that class issued.	Indefinitely
Consumer Protection Act	Full names, physical address, postal address and contact details; ID number and registration number; Contact details of public officer in case of a juristic 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 competition refer to Section 36(11)(b) and Regulation 11 of Promotional Competitions.	3 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
	<u>Section 20(2) documents:</u> - 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; - Records of incidents reported at work	3 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

Employment Equity Act	Records in respect of the company's workforce, employment equity plan and other records relevant to compliance with the 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 details of 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 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 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

POLICY REVIEW

Puresan (Pty) Ltd will continue to review the effectiveness of this policy to ensure it is achieving its stated objectives on at least an annual basis and more frequently if required, taking into account changes in the law and organisational or security changes.

SIGNED : 

DATE: 11/7/21

J L PENROSE
OPERATIONS DIRECTOR