

**Venco Fruit Processors (Pty) LIMITED T/A
Venco**

**POPI COMPLIANCE MANUAL
in terms of
FOR THE IMPLEMENTATION OF THE
PROTECTION OF PERSONAL INFORMATION ACT
OF 2013
(the "ACT")**

Date of Compilation – 10 June 2021

Registration Number of Company: 2012/193965/07

INDEX

1.	BACKGROUND TO THE ACT.....	1
1.1.	Definitions	1
1.2.	Purpose.....	1
2.	INTRODUCTION TO VENCO FRUIT PROCESSORS (PTY) LIMITED	1
3.	PARTICULARS OF COMPANY	2
4.	RESPONSIBILITIES OF INFORMATION OFFICERS [Section 55-56].....	2
5.	PROTECTION OF PERSONAL INFORMATION PROCESSED BY VENCO.....	3
5.1.	Part A Processing of personal information in general	3
5.2.	Part B Processing of special personal information [Section 26-33]	4
5.3.	Part C Processing of personal information of children [Section 34-35].....	5
6.	PURPOSE OF THE PROCESSING OF PERSONAL INFORMATION	5
6.1.	Categories of Data Subjects and reasons Personal Information processed.....	5
6.2.	Categories of Data Subjects and types of Personal Information processed.....	7
6.3.	Categories of Recipients with whom Personal Information is Shared	8
7.	CIRCUMSTANCES REQUIRING PRIOR AUTHORISATION [Section 57-59]	8
8.	CROSS-BORDER FLOWS OF PERSONAL INFORMATION [Section 72]	9
9.	SECURITY MEASURES AND SAFEGUARDS.....	9
10.	BREACHES [Section 22].....	12
11.	DIRECT MARKETING [Section 69-71]	13
12.	COMPLAINTS [Section 74]	13

1. BACKGROUND TO THE ACT

1.1. Definitions

Data subject means the person to whom the personal information relates.

Operator means a person who processes personal information for a responsible party in terms of a contract or mandate, without coming under the direct authority of that party.

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

1.2. Purpose

The purpose of POPIA is, amongst others, to give effect to the constitutional right to privacy by safeguarding personal information when processed by a responsible party.

The Protection of Personal Information Act (POPI) is intended to balance 2 competing interests.

These are:

1. Our individual constitutional rights to privacy (which requires our personal information to be protected); and
2. The needs of our society to have access to and to process (work with) our personal information for legitimate purposes, including the purpose of doing business.

POPIA applies to the processing of personal information: entered in a record by or for a responsible party by making use of automated or non-automated means provided that when the recorded personal information is processed by non-automated means, it forms part of a filing system or is intended to form part thereof.

This manual sets out the framework for Venco's compliance with POPI.

This POPI Manual of Venco Fruit Processors is available at its premises:

2. INTRODUCTION TO VENCO FRUIT PROCESSORS (PTY) LIMITED

Venco Fruit Processors (Pty) Limited ("Venco") is a fruit juicing company based in the Sundays River Valley. Venco is classified as a "private body" within the definition of Section 1 of the Act. Venco is involved in the processing of oranges, lemons and softs into concentrated juice for both local and export markets. Venco also harvests citrus oils and aromas from the fruit.

3. PARTICULARS OF COMPANY

Company contact details

Company Name	Venco Fruit Processors (Pty) Limited
Business Address	Farm Commando Kraal 113 (remaining portion 38), Addo/ Sunland Road (R336), Sundays River Valley, Eastern Cape, 6105
Phone number	042 233 0438
Fax number	042 233 0457
Email Address	andre@vencofruit.co.za
Website Address	www.vencofruit.co.za

4. RESPONSIBILITIES OF INFORMATION OFFICERS [Section 55-56]

Venco's information officer's responsibilities include the following:

- ensuring compliance by Venco with the provisions of the POPI Act
- encouraging compliance with the lawful processing of personal information conditions;
- dealing with requests made to Venco;

Venco has appointed an Information Officer to take up the duties/responsibilities information in terms of the POPI Act. The information officer, details given below, has been registered with the regulator.

Information Officer	Andre Swart
Business Address	Farm Commando Kraal 113 (remaining portion 38), Addo/ Sunland Road (R336), Sundays River Valley, Eastern Cape, 6105
Phone number	042 233 0438
Fax number	042 233 0457
Email Address	andre@vencofruit.co.za

5. PROTECTION OF PERSONAL INFORMATION PROCESSED BY VENCO

Chapter 3 of POPIA regulates the processing of personal information through compliance with the eight (8) conditions for the lawful processing of personal information, the processing of special personal information and the processing of personal information of children.

5.1. Part A Processing of personal information in general

The eight (8) conditions for the lawful processing of personal information with which Venco complies, are the following:

Accountability	Venco will ensure that the conditions and all the measures set out in the Act that give effect to such conditions are complied with at the time of determining the purpose and means of the processing.
Processing Limitation	Personal information will only be processed fairly and lawfully and only with the data subject's consent.
Purpose Specific	Personal information will only be processed for specific, explicitly defined and legitimate reasons.
Further Processing Limitation	Personal information will not be processed for a secondary purpose unless compatible with the original purpose.
Information Quality	Venco will take reasonable steps to ensure that the personal information collected is complete, accurate, not misleading and updated where necessary.
Openness	Venco will ensure that the data subject is aware that Venco is collecting their personal information and for what purpose the information will be used.
Security Safeguards	Personal information will be kept secure against the risk of loss, unlawful access, interference, modification, unauthorised destruction and disclosure.
Data Subject Participation	Data subjects may request whether their personal information is held, as well as the correction and/or deletion of any personal information held about them.

Rights of data subjects

A data subject has the right to have their personal information processed in accordance with the conditions for the lawful processing of personal information.

Data Subjects have the right to:

- (a) be notified that their Personal Information is being collected by Venco.
- (b) be notified if their data has been accessed/acquired by an unauthorised person;
- (c) know whether Venco holds their Personal Information and to access that information;
- (d) request the correction or deletion of inaccurate, irrelevant, excessive, out of date, incomplete, misleading or unlawfully obtained personal information [Regulations: Form 2];
- (e) object on reasonable grounds to use of their Personal Information and request the deletion of such Personal Information [POPI Regulations: Form1];
- (f) object to the processing of Personal Information for purposes of direct marketing using unsolicited electronic communications; and
- (g) not to be subject, under certain circumstances, to a decision which is based solely on the basis of the automated processing of their personal information
- (h) complain to the Information Regulator regarding an alleged interference of any of the rights protected under POPI and to institute civil proceedings regarding the alleged interference with the protection of his, her or its personal information.

5.2. Part B Processing of special personal information [Section 26-33]

Special rules apply to the collection and use of information relating to a:

- person's religious or philosophical beliefs,
- their race or ethnic origin,
- their trade union membership,
- their political persuasion,
- their health or sex life,
- their biometric information,
- or their criminal behaviour.

Venco will not process any of this Special Personal Information:

- without the client's consent,
- or where this is necessary for the establishment, exercise or defence of a right or an obligation in law.
- processing is necessary to comply with an obligation of international public law;
- information has deliberately been made public by the data subject.

5.3. Part C Processing of personal information of children [Section 34-35]

Venco will only process the personal information of a child if:

- we have the consent of the child’s parent or legal guardian
- necessary for the establishment, exercise or defence of a right or obligation in law
- necessary to comply with an obligation of international public law;
- of personal information which has deliberately been made public by the child with the consent of a competent person.

6. PURPOSE OF THE PROCESSING OF PERSONAL INFORMATION

Personal Information may only be processed for a specific purpose.

Venco processes personal information for several reasons, including but not limited to the following:

- to perform services and conduct business operations;
- to maintain records;
- for employment purposes;
- for health and safety purposes;
- to comply with relevant laws
- to detect and prevent fraud and corruption.

See Table 1 below for a detailed listing of the reasons to process data subjects personal information

6.1. Categories of Data Subjects and reasons Personal Information processed

Table 1

Data Subject	Reason for processing of personal information
Customers	<ul style="list-style-type: none">– Performing duties in terms of any agreement/contract with customers– Processing credit applications concerning customers– Operate and manage Customers’ accounts and manage any application, agreement or correspondence customers may have with Venco– Communicating with customers by email, SMS, letter, telephone or in any other way about Venco’s products and services, unless customers indicate otherwise– Performing other administrative and operational purposes including the testing of systems– Recovering any debt customers may owe the Venco– Complying with Venco’s regulatory and other legal obligations– Verifying and updating information Any other reasonably required purpose relating to the Venco business

<p>Employees:</p>	<p>Verification of applicant employees' information during the recruitment process</p> <ul style="list-style-type: none"> • Name and surname • Identification numbers • Employment history • Other additional information provided on an employee's resume' <p>Additional records of employment information related to employees:</p> <ul style="list-style-type: none"> • Address • Contact details (Phone number, email address) • Disciplinary action • Employment contract • Employment equity-related information • Leave records • Medical aid • Payroll • Pension • Training and SETA • SARS records <p>Any other reasonably required purpose relating to the employment or possible employment relationship.</p>
<p>Vendors/suppliers</p>	<p>Necessary information in order to conduct business;</p> <ul style="list-style-type: none"> • Bank details • Company or individuals name • Registration number or I.D. numbers <p>Processing of invoices for financial records or payment;</p> <p>Complying with Venco's regulatory and other obligations; and</p> <p>Any other reasonably required purpose relating to the Venco business.</p>
<p>Visitors or others on Venco premises</p>	<p>Physical access records</p> <p>Electronic access records</p> <p>Surveillance records</p> <p>Any other reasonably required purpose relating to the Venco business.</p>

6.2. Categories of Data Subjects and types of Personal Information processed

Table 2

Data Subject/Category	Personal information processed
Employees	<ul style="list-style-type: none"> • Age • Banking and financial details • Details of payments to third parties (deductions from salary) • Disciplinary records • Employment contracts • Employment equity plans • Employment history and references • Ethnic group • Gender • Language • Identity number and identity documents including passports • Leave records • Marital status • Medical aid records • Name and contact details • Nationality • Pension Fund records • Performance appraisals • Postal and/or street address • Remuneration/salary records • Training records
Customers	<ul style="list-style-type: none"> • Contact numbers and/or e-mail address • Company registration number or identification number • Company or individuals name • Financial information (Bank account information, credit history) • Language • Nationality • Postal and/or street address
Vendors/suppliers	<ul style="list-style-type: none"> • Banking and financial information • Identity and/or company information and directors' information • Information about products or services • Name and contact details • Other information not specified, reasonably required to be processed for business operations

6.3. Categories of Recipients with whom Personal Information is Shared

In performing normal functions/operations of conducting business, Venco may have to share personal information with other recipients. These include Joint Venture partners, Venco service providers, consultants and agents who perform services on behalf of Venco.

Venco does not share personal information with third parties, except if:

- Venco is obliged to provide such information for legal, regulatory purposes or to governmental authorities;
- Venco is involved in the prevention of fraud, loss, bribery or corruption;
- The third-party processes personal information on behalf of the Venco;
- Third parties to whom payments are made on behalf of employees;
- Any firm, organisation or person that Venco uses to collect payments and recover debts or to provide a service on its behalf;
- Financial institutions from whom payments are received on behalf of data subjects;
- Any other operator not specified.

Venco will only send our data subjects notifications or communications if Venco is obliged by law, or required to do so in terms of an agreement.

Venco will only disclose personal information to government authorities if required to do so by law. All employees of Venco are required to adhere to data privacy and confidentiality principles and attend to data privacy training:

7. CIRCUMSTANCES REQUIRING PRIOR AUTHORISATION [SECTION 57-59]

1. In the following circumstances, we will require prior authorisation from the Information Regulator before processing any personal information:
 - 1.1 If we intend to utilise any unique identifiers of clients for any purpose other than the original intention, or to link the information with information held by others;
 - 1.2 processing information on criminal behaviour or unlawful or objectionable conduct;
 - 1.3 processing information for credit reporting
 - 1.4 transferring special personal information or the personal information of children, to a third party in a foreign country, that does not provide adequate protection of that personal information.

8. CROSS-BORDER FLOWS OF PERSONAL INFORMATION [SECTION 72]

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

- a. the third party can provide an adequate level of protection effectively upholds principles for reasonable processing of the information that is substantially similar to the conditions for the lawful processing of personal information relating to a data subject; or
- b. Data Subject consents to the transfer of their Personal Information; or
- c. transfer is necessary for the performance of a contractual obligation between the Data Subject and the Responsible Party; or
- d. 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
- e. 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 in all likelihood provide such consent.

Policy regarding cross border transfers of Personal Information

Personal Information may be transmitted trans-border to Venco's 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. Venco will endeavour to ensure that its customers and suppliers will make all reasonable efforts to secure said data and Personal Information.

9. SECURITY MEASURES AND SAFEGUARDS

Venco takes reasonable measures, on an annual basis, to

- identify all reasonably foreseeable internal and external risks to personal information in its possession or under its control;
- establish and maintain appropriate safeguards against the risks identified;
- regularly verify that the safeguards are effectively implemented; and
- Stay up to date on generally accepted information security practices and procedures required in terms of a specific industry or professional rules and regulations.

All operators processing personal information on behalf of Venco will be required

- process such information only after authorisation has been received from Venco;
- treat personal information as confidential;
- to sign a written contract to ensure that the operator which processes personal information for Venco establishes and maintains the security measures.

To prevent loss of, damage to or unauthorised destruction; and unlawful access to or processing of personal information. Venco has the following technical and organisational measures in place:

Technical

- Physical Access
 - Business premises where records data processing equipment are kept protected by security and physical locks.
 - Archived files stored behind locked doors and access control to these storage facilities implemented.
 - CCTV, security lighting and alarms in place.
- Logical access
 - Venco shall implement suitable measures to prevent unauthorized input into data memory and the unauthorised reading, alteration or deletion of data.
 - Venco represents that the persons entitled to use Venco's data processing system are only able to access the data within the scope and to the extent covered by their respective access permissions (authorisation).
 - All the user terminals on our internal computer network and our servers are protected by passwords and changed regularly.
- Disposal
 - Correct disposal of paperwork and devices.
 - Shredding and certified disposal of hard-copy records for personal data.
 - IT disposal is done by a knowledgeable person to guarantee effective and complete erasure of any personal data or access
 - The employees' digital work profiles and privileges who have left out employ are properly terminated.
 - The personal information of clients and staff must be destroyed timeously in a manner that de-identifies the person.
- Cyber Security on all devices and networks
 - Firewalls, anti-virus protection and patches and updates.

Organisational

- Policies and Procedures
 - The processing of personal information must take place in accordance with the rules contained in the relevant labour legislation.
 - All employees informed of the policies and procedures regarding IT security.
 - All employees to maintain security measures and full confidentiality in respect of all of our data subjects' affairs, including our data subjects' personal information;
 - All employees to notify their manager/supervisor immediately if there are reasonable grounds to believe a breach has occurred
- Business Continuity/Disaster recovery plan
 - Protocols and measures in place to back up data and ensure that it can be recovered and maintained in the event of a disaster.
- Risk Assessment
 - Assessing high-risk data and processing activities and developing mitigating solutions to prevent or reduce risks as a preventative measure.
 - Vulnerability assessments carried out on our digital infrastructure annually to identify weaknesses in our systems and to ensure adequate safeguards in place.
- Management Information & Reporting
 - Regular reports and information passed to management to ensure adequate resources and funding are available and for accountability at all levels.
- Reviews & Audits
 - Reviewing and auditing functions, activities and systems against procedures and regulations helps to know if they are still effective and fit for purpose
- Awareness & Training
 - Security and data protection awareness for all employees and any third parties to know what is expected of them and how to maintain compliance.
 - Regular and ongoing training sessions to ensure that the latest information, guidance, legislation and regulations are known and understood
 - Staff have ongoing training to carry out their duties in compliance with POPI.
- Due Diligence
 - Due diligence checks on suppliers, service providers, employees and customers.

10. BREACHES [SECTION 22]

Where there are reasonable grounds to believe that the personal information of a data subject has been accessed or acquired by any unauthorised person, Venco will notify

- the Regulator; and
- the data subject, unless the identity of such data subject cannot be established.

The notification will be made as soon as reasonably possible after the discovery of the compromise, taking into account the legitimate needs of law enforcement or any measures reasonably necessary to determine the scope of the compromise and to restore the integrity of the responsible party's information system.

The notification to a data subject will be communicated in writing to the data subject in at least one of the following ways:

- Mailed to the data subject's last known physical or postal address;
- sent by e-mail to the data subject's last known e-mail address;
- placed in a prominent position on the website of the responsible party;
- published in the news media;
- or as directed by the Regulator.

The notification will provide sufficient information to allow the data subject to take protective measures against the potential consequences of the compromise, including

- a description of the possible consequences of the security compromise;
- a description of the measures that Venco intends to take or has taken to address the security compromise;
- a recommendation with regard to the measures to be taken by the data subject to mitigate the possible adverse effects of the security compromise; and
- if known to Venco, the identity of the unauthorised person who may have accessed or acquired the personal information.

11. DIRECT MARKETING [SECTION 69-71]

Venco will carry out direct marketing (using any form of electronic communication) if:

- the data subject has given their consent to the processing or is a customer of Venco; and
- who has not previously withheld such consent
- For customers
 - the personal information Venco obtained in the context of providing services/products and,
 - for direct marketing of Venco's own similar products or services; and
 - they were given an opportunity to object to receiving direct marketing material by electronic communication at the time that their personal information was collected; and
- For other data subjects (non-customers)
 - The data subject has given consent
 - The data subject has not previously withheld such consent
- A request for consent to receive direct marketing must be made in the prescribed manner and form POPI Regulations: Form 4.
- All direct marketing communications must disclose Venco's identity and contain an address or other contact details to which the recipient may send a request that the communications cease.

12. COMPLAINTS [Section 74]

Any person may submit a complaint to the Regulator in the prescribed manner and form alleging interference with the protection of the personal information of a data subject [POPI Regulations: Form 5].