



HUMAN RESOURCES

Reference: HRP 1.2
Revision: 0
Date: 2022-01-11
Page: 1/17
Owner: Human Resources

POPI POLICY

DISCLAIMER

The information contained in this document has been prepared exclusively for internal use by Air Liquide Southern Africa. Since this document is confidential and proprietary to Air Liquide, third parties are not entitled to rely on it in any way. With regard to third parties, Air Liquide does not hold itself out as recommending the use of the information contained herein or reliance thereon in any way without its prior approval and Air Liquide does not give any warranties on the information contained in this document and assumes no liability or responsibility in connection with the information or suggestions herein contained. Air Liquide makes no representations or warranties as to the completeness of this document and DISCLAIMS ALL WARRANTIES, EXPRESS OR IMPLIED INCLUDING, BUT NOT LIMITED TO, THE WARRANTY OF MERCHANTABILITY AND THE WARRANTY OF FITNESS FOR A PARTICULAR USE OR PURPOSE.

This document supersedes the following document(s):

--	--	--	--

Rev	Date	Prepared by	Verified by	Approved by	Changes
0	1 November 2022	Karabo Dube	Laressa Thavarin / Thobeka Mbatha	Natasha Naidoo	New Policy

FRAMEWORK AND POLICY ON THE PROTECTION OF PERSONAL INFORMATION ACT NO 4 OF 2013

Continuous Oxygen Suppliers trading as VitalAire (Pty) Ltd (the “Company”) is a private company incorporated and registered in accordance with the laws of the Republic of South Africa. The Company supplies medical products and services to patients at home. The portfolios the Company covers is oxygen, sleep apnea and diabetes across South Africa.

1. INTRODUCTION

The Protection of Personal Information Act 4 of 2013, (“POPIA/The Act”) and the Regulations promulgated thereunder give effect to the right to privacy provided by section 14 of the Bill of Rights of the Constitution of the Republic of South Africa 1996.

The Act and Regulations require the Information Officer of the responsible person as defined under the Act to develop, implement, monitor and maintain a compliance framework, (Regulation 4 of Regulations published under GG number 42110 dated 14 December 2018 (“POPI Regulations”).

The Company has developed this policy in order to comply with the aforesaid requirements and to further demonstrate commitment to the spirit of the Act in respecting the rights of Data Subjects to have their Personal Information protected as set out in the Act.

Forms 1, 2 and 4 of the POPI Regulations are attached to this Policy.

This Policy aligns with, and flows from the Air Liquide [Group Privacy policy DS_GP03](#).

2. SCOPE

This policy applies to all employees and office bearers of the Company and anyone who may process Personal Information for and on behalf of the Company.

This policy applies to all situations and business processes where Personal Information is processed, and where such information may be made accessible to third parties. This policy must be read together with the Company’s PAIA Manual.

This policy also outlines how patient personal- and health information is processed by the Company.



HUMAN RESOURCES

Reference: HRP 1.2

Revision: 0

Date: 2022-01-11

Page: 2/17

Owner: Human Resources

POPI POLICY

3. DEFINITIONS

- 3.1. **“Applicable Legislation”** means all legislation applicable to the Company including the POPIA, the Medicines and Related Substances Act 101 of 1965; the National Health Act 61 of 2003; the National Archiving Act, Income Tax Act 58 of 1962; Value Added Tax Act 89 of 1991; Labour Relations Act 66 of 1995; Basic Conditions of Employment Act 75 of 1997; Disaster Management Act 75 of 200; Employment Equity Act 55 of 1998; Skills Development Levies Act 9 of 1999; Unemployment Insurance Act 63 of 2001; Electronic Communications and Transactions Act 25 of 2002; Telecommunications Act 103 of 1996; Electronic Communications Act 36 of 2005; Consumer Protection Act 68 of 2008; National Credit Act 34 of 2005; and all regulations issued thereunder, and all legislation as listed under the Company PAIA Manual.
- 3.2. **“Data subject”** means the person to whom personal information relates as defined under the Act;
- 3.3. **“Employee”** means, for the purposes of this policy, any person employed permanently (full- or part-time), temporary, or on a fixed-term contract, and include contractors that may come into contract with, use, process or otherwise deal with Personal Information.
- 3.4. **“Office-bearer”** means the members of the Board of Trustees, the Principal Officer, members of Committees of the Scheme, governance secretaries and persons in similar positions.
- 3.5. **“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.
- 3.6. **“Personal information”** shall mean, for purposes of this policy and as defined under the Act, information about an identifiable, natural person, and in so far as it is applicable, an identifiable, juristic person, including, but not limited to:
- 3.6.1. information relating to the race, gender, sex, pregnancy, marital status, nationality,
 - 3.6.2. ethnic or social origin, colour, sexual orientation, age, physical or mental health,
 - 3.6.3. well-being, disability, religion, conscience, belief, culture, language and birth of the person;
 - 3.6.4. information relating to the education or the medical, criminal or employment history of the person or information relating to financial transactions in which the person has been involved;
 - 3.6.5. any identifying number, symbol or other particular assigned to the person;
 - 3.6.6. the address, fingerprints or blood type of the person;
 - 3.6.7. the personal opinions, views or preferences of the person, except where they are about another individual or about a proposal for a grant, an award of a prize to be made to another individual;
 - 3.6.8. correspondence sent by the person that is implicitly or explicitly of a private or confidential nature or further correspondence that would reveal the contents of the original correspondence;
 - 3.6.9. the views or opinions of another individual about the person;
 - 3.6.10. the views or opinions of another individual about a proposal for a grant, an award or a prize to be made to the person, but excluding the name of the other individual where it appears with the views or opinions of the other individual; and



HUMAN RESOURCES

Reference: HRP 1.2

Revision: 0

Date: 2022-01-11

Page: 3/17

Owner: Human Resources

POPI POLICY

3.6.11. the name of the person where it appears with other personal information relating to the person or where the disclosure of the name itself would reveal information about the person;

3.6.12. but excludes information about a natural person who has been dead, or a juristic person that has ceased to exist, for more than 20 years.

3.7. **“Policy”** means this policy developed in terms of the POPIA;

3.8. **“POPIA”** means the Protection of Personal Information Act, 2013 and the Regulations thereto;

3.9. **“Processing”** means any operation or activity or any set of operations, whether or not by automatic means, concerning personal information, including:

3.9.1. the collection, receipt, recording, organisation, collation, storage, updating or modification, retrieval, alteration, consultation or use;

3.9.2. dissemination by means of transmission, distribution or making available in any other form; or

3.9.3. merging, linking, as well as restriction, degradation, erasure or destruction of information.

3.10. **“Purpose”** means the Company’s purpose for processing of Personal Information as set out under the Company’s [PAIA Manual](#).

3.11. **“Responsible Party”** means, for the purpose of this Policy, VitalAire (Pty) Ltd, and Includes all persons to whom this policy applies, whom, whether alone or in conjunction with others, determines the purpose and means of processing Personal Information;

3.12. **“SAHPRA”** means the South African Health Products Regulatory Authority, an entity of the National Department of Health;

3.13. **“Special Personal Information”** means information relating to a person’s (a) religious or philosophical beliefs, race or ethnic origin, trade union membership, political persuasion, health or sex life or biometric information of a data subject; or (b) criminal behavior, as defined under the Act.

4. PRINCIPLES SET BY THE AIR LIQUIDE GROUP POLICY

Air Liquide has adopted 10 golden rules when the personal information of any person is processed:

1. Personal data must be collected for specific, explicit and legitimate purpose
2. Ensure that there is a legal ground for the processing of personal data
3. Ensure that only adequate, relevant and limited personal data is collected and retained for a limited period of time
4. Be transparent to individuals on how their personal data will be used
5. Ensure that the processing of sensitive personal data is allowed
6. Uphold rights of individuals
7. Ensure that individuals are able to object to direct marketing communications
8. Prevent solely automated individual decision-making, including profiling
9. Ensure security and confidentiality of personal data



HUMAN RESOURCES

Reference: HRP 1.2

Revision: 0

Date: 2022-01-11

Page: 4/17

Owner: Human Resources

POPI POLICY

10. Implement appropriate measures for transfers of personal data outside of Air Liquide

5. THE COMPANY REQUIREMENTS FOR PROCESSING PERSONAL INFORMATION: CONSENT OR NOTIFICATION

All Processing of Personal Information must be done:

- 5.1. Only if relevant to VitalAire activity; and
 - 5.1.1. After a written and signed consent in a form (Ops/51) developed and approved form by the Company, has been received from the Data Subject, or
 - 5.1.2. Where there is a legal requirement to disclose Personal Information for example to the scheme itself, to authorities, operators, etc., the Data Subject must still be notified of such disclosure, unless the Applicable Law provides otherwise; or
- 5.2. For the purposes of entering into and for implementing a contract; or
- 5.3. When required by law enforcement, regulatory processes and such purposes as allowed by law.

6. NOTIFICATIONS

- 6.1. The Company will inform all persons whose information is being processed, of that fact.
- 6.2. This is done via the Company's Terms and Conditions, on specific consents to disclosure, and, where bulk-mailers or communications are sent out, with a statement relating to the rights of the Data Subject, attached thereto.
- 6.3. The rights of Data Subjects are as follows:
 - 6.3.1. Notification when personal information is being collected, the type of information collected, for what purpose, whether the information is to be supplied voluntarily or is collected mandatory, and whether the information would be transferred to a third country and the protections afforded there;
 - 6.3.2. Notified if there has been unlawful access or acquisition of his/her/its personal information;
 - 6.3.3. Request a record of your Personal Information;
 - 6.3.4. Request the correction, deletion and/or destruction of your Personal Information;
 - 6.3.5. Object to the processing of your Personal Information;
 - 6.3.6. Exercise the right to withdraw the consent to processing, if voluntarily given;
 - 6.3.7. Not be subjected to unsolicited electronic communication, unless the you are our customer and we have sold goods or services to you, or where you have consented to the communication and you had and have the opportunity to object to the communication;
 - 6.3.8. Not to be subjected to automated decision-making based on the personal information in contravention of section 71, POPI Act;
 - 6.3.9. Submit a complaint to the Information Regulator at <https://www.justice.gov.za/inforeg/>; and
 - 6.3.10. Institute civil proceedings regarding an alleged interference with his/her/its personal information in terms of section 99, POPI Act.



HUMAN RESOURCES

Reference: HRP 1.2

Revision: 0

Date: 2022-01-11

Page: 5/17

Owner: Human Resources

POPI POLICY

6.4. The details of the Information Officer, or the responsible Deputy Information Officer will also be included in all Notifications, and also appear on the PAIA Manual / PAIA Guide.

7. COLLECTION OF PERSONAL INFORMATION

The Company collects Personal Information from various Data Subjects for varying purposes, but mainly from its customers, employees, the regulator, its contractors and industry associates / stakeholders. Such information must be collected in accordance with the provisions of the Act and this policy. The processing of personal information of employees is subject to contractual provisions (either in the form of an addendum or incorporated into an employment contract and all processing is subject to the Air Liquide Human Resources "Protection of Employee Personal Data and Privacy".

8. INDIRECT COLLECTION OF PERSONAL INFORMATION

Where the collection of personal data is performed indirectly (e.g. from a business partner, a recruitment agency, an entity selling contact lists, etc.), the concerned individual must be informed of their information being passed on to Air Liquide and VitalAire and from which source the personal data originate. Such third party entity must obtain the individual's consent or do so under legislative authority, which allows the passing on of such personal information.

9. SENSITIVE / SPECIAL INFORMATION

9.1. Sensitive / special information includes information on health, politics, the information of children, biometrics, criminal record/history, etc., as described in the POPI Act may not be processed at all, unless the provisions of the POPI Act as set out in sections 26 to 33 are followed.

9.2. In some instances, such as that pertaining to credit records, criminal records, reprocessing of personal identifiers, etc. the Information Regulator may require that special permission be obtained from it before processing is permitted, which will be undertaken should credit checks or other activities, as set out in chapter 6 to the POPIA.

9.3. Always seek the advice of the Information Officer and/or Legal before proceeding with the processing of sensitive information.

9.4. As a Company that supplies products directly to consumers (patients), and as such supply necessitates the company to process health information, such as:

9.4.1. patient diagnosis and health condition,

9.4.2. health information such as health behaviours,

9.4.3. medical scheme details (number, plan options, etc.), including main member and beneficiary details,

9.4.4. reimbursement information, such as motivations by medical practitioners, etc.

9.4.5. financial information, whether medical scheme-related or of cash-paying persons,

9.4.6. contracts and interaction with healthcare professionals, such as prescribers, sleep labs and the likes

9.4.7. patient identity number and residential addresses, so as to effect delivery of orders, accounts / invoicing, and/or the delivery or pick-up of equipment, where applicable,



HUMAN RESOURCES

Reference: HRP 1.2

Revision: 0

Date: 2022-01-11

Page: 6/17

Owner: Human Resources

POPI POLICY

9.4.8. information on nurses trained and bound by relevant regulatory / statutory body

Apart from this overarching Policy, these interactions are governed by POPI-compliant consents or notifications where processing is mandated by law, which are included in terms and conditions signed by patients, a specific document retention, archiving and destruction policy, SOPs and protocols applicable to staff dealing with these matters in various contexts – reception, medical scheme staff, nursing staff, financial staff, logistics and supply staff, etc.

10. PROHIBITION ON AUTOMATED PROCESSING

- 10.1. Where processing is undertaken without human intervention (automated processing), this may not be done if such processing has a negative impact on a person's rights.
- 10.2. All automated processing of personal information will be scrutinized before implemented or commenced, and the advice of the Information Officer and Legal will be sought if it is not clear whether an individual's rights could be affected.

11. CONDITIONS OF LAWFUL PROCESSING OF PERSONAL INFORMATION

Section 4(1) of the POPIA requires that all Processing of Personal Information be done in a lawful manner. Anyone who processes Personal Information for and on behalf the Company must do so in terms of the below conditions in order to ensure compliance with the Act:

- 11.1. Ensure that all the conditions and measures giving effect to conditions of the lawful processing of Personal Information as set out in the Act and this policy are complied with at the time of the determination of the purpose and means of the Processing and during the Processing.
- 11.2. Personal Information must only be processed with the consent of the Data Subject, for a specific, explicit and lawfully defined purpose, related to the functions and activities of the Company or if under a statutory obligation, with a notification to the person of the specific statutory mandate (quote Act, section and/or Regulation and number thereof).
- 11.3. All **consents to processing** and/or **notifications of processing** will be reviewed by responsible employees or office bearers to ensure that it is specific. In cases of uncertainty, the Information Officer or one of his/her deputies will be contacted for support. Where standard consents or notifications have been developed, employees and office-bearers are obligated to use those.
- 11.4. In the event of a requirement to use Personal Information outside the initial consented or legislated purpose, ("**further processing**"), then a further consent for the further processing must be obtained from the Data Subject prior to such further processing.
- 11.5. Personal Information must be **collected directly from the Data Subject**, or, if the data subject is unable to consent, a person authorised in terms of the National Health Act, can provide such consent (such as a spouse/partner, parent, adult child etc.). should there be a need to collect the information from another source, and the consent of the Data Subject or authorised person must be obtained prior thereto. Where databases



HUMAN RESOURCES

Reference: HRP 1.2
 Revision: 0
 Date: 2022-01-11
 Page: 7/17
 Owner: Human Resources

POPI POLICY

are bought or provided by a third party, a **warranty** must be included in the contract that such databases have been compiled and are sold in compliance with POPIA (i.e. with the necessary consent or statutory mandate).

11.6. Only up to date, accurate and correct Personal Information can be processed and there is a duty to ensure that personal information is always up to date and accurate. Data Subjects may request the **correction or deletion** (if possible) of their Personal Information on **Form 2** as set out in Regulations published under GG number 42110 dated 14 December 2018. All consents, notifications and contracts must include a hyperlink or attach Form 2.

11.7. The Information Officer and his/her deputies must ensure that the **security measures** put in place by the Company for every database and type/category of personal information processed, to protect against:

11.7.1. **Unauthorised access**, which means that access privileges must be stipulated, and where applicable, indicated in documents, minutes, etc. as follows:

Accessible by:	Type of Information
In-House Legal Counsel, Company Secretary, Directors, Duly authorised Prescribed Officers and/or personnel	<ul style="list-style-type: none"> ● Board of Directors' or Shareholders' resolutions or minutes of meetings; ● Personal information, documents or details of the Board directors or shareholders' and their representatives; ● Board Committees' or subcommittees' recommendations or minutes of meetings, committee members' personal information, documents or details; ● Statutory Company records related to its incorporation, register of directors and/or shareholders; ● Delegations of Authority of members of the executive committee/top management or powers of attorney; ● Litigations and claims, including that against clients (patients) and third parties (such as funders of healthcare).
Designated and duly authorised personnel from Finance, and Legal department, Executive committee members and Prescribed Officers	<ul style="list-style-type: none"> ● Annual financial statements, financial reports, economic projections, strategic business plans, internal and external audit reports, opinions or recommendations, accounting and tax consultants' opinions, and the like; ● Statutory declarations by the Board of Directors, and/or Prescribed Officers; ● Notarial land lease agreements and notarial deeds; ● Litigations and claims.



HUMAN RESOURCES

Reference: HRP 1.2

Revision: 0

Date: 2022-01-11

Page: 8/17

Owner: Human Resources

POPI POLICY

Designated and duly authorised HR, and Quality Personnel	<ul style="list-style-type: none"> All Company operating policies, procedures, standards, and/or permits, or licences.
Designated Training and Skills Development Personnel	<ul style="list-style-type: none"> Personal Information of employees engaged in internal and/or external training and skills development programmes inclusive of Training Requests, Enrolment Forms and support information, Results Statements, Certificates, Skills Development Funding Agreements where applicable, Skills Development Records, Performance Reviews and Curriculum Vitae if this is a programme requirement.
Duly appointed Committee Members	<ul style="list-style-type: none"> Confidential information and/or documentation related to the respective committee meetings such as minutes, reports or presentations; Personal Information recorded on attendance registers, or Personal Information reviewed for purposes of implementation of the Employment Equity and Skills Development or Transformation Committee statutory objectives.
Duly appointed and authorised third party, members of the Executive committee, HR, Legal, Finance, and Procurement personnel, and Prescribed Officers	<ul style="list-style-type: none"> Information related to B-BBEE annual targets per B-BBEE Category inclusive of required financial information and employee demographic information. Payroll information shared as/and where required for the elements of Skills Development and Management Control; Shared third party - Supplier information such as company registration documents and B-BBEE Certificate for the Procurement Category, Skills Development, Enterprise and Supplier Development and Socio-economic Development; Statutory Company registration records including the directors and shareholders registers. Financial records, debt management, etc.
Designated and duly authorised personnel from Sales & Marketing, Credit/Debit, Accounts Payable, Finance, and Legal department.	<ul style="list-style-type: none"> Personal information of customers for purposes of execution of credit facility applications, supply agreements, agency or distributor agreements, acknowledgement of debt or settlement agreements, delivery notes; Accounts or financial information for purposes of issuing tax invoices and statements, notices of default.



HUMAN RESOURCES

Reference: HRP 1.2
 Revision: 0
 Date: 2022-01-11
 Page: 9/17
 Owner: Human Resources

POPI POLICY

<p>Executive committee members, designated and duly authorised personnel from the Procurement, Legal, HR, and Finance department, and operations</p>	<ul style="list-style-type: none"> • Executed copies of Supply Framework Agreements with third party suppliers, Purchase Orders, and tax invoices; • Third party - Supplier information such as company registration documents, proposals or responses to issued requests for proposals/quotations (“RFP/Q”), operating permits or licences, B-BBEE Certificate for the Procurement Category; • Information or documentation related to the Company’s Enterprise Development and Supplier Development initiatives, projects or agreements with third parties.
<p>On-site medical doctor, and nurse</p>	<ul style="list-style-type: none"> • Personal information of employees related to medical records, reporting of incidents and/or accidents at the workplace or while performing work duties, residential address, contact details, and the like.
<p>Designation and duly authorised HSEQ personnel</p>	<ul style="list-style-type: none"> • Personal information of employees or third party contractors related to HSEQ events. The electronic systems utilized such as the ERP system, PDA and SAP and the respective individuals to have access to them, and, where applicable subject to event attendees having consented to inclusion in a database or event record.

11.7.2. **Loss and/or damage of personal information**, is safeguarded through back-ups off-site, remote wiping of computers and devices stolen / lost), IT protections against file corruption, version control system.

11.7.3. **Archiving and Destruction** will only take place in accordance with the Company’s Document Retention and Destruction policy and guide, and all archiving and destruction will be documented in the registers kept with the BIS Information Technology Department.

11.8. No Company database, list, personal information of any person in its, or any staff member or office bearer’s possession may be used, made known and/or distributed without the concerned Data Subjects’ consent. In case of doubt, the advice of the Information Officer or his/her Deputies will be sought. Even casual provision of contact details to a third party could constitute a breach of the POPI Act.

11.9. Only relevant Personal Information required for the specified purpose should be collected - nothing in excess of that and the information may only be used for that purpose (i.e. subject to the further processing limitation). The data fields (see definition of “personal information” and “special information”) in all existing and new databases and types of information (e.g. contracts, financial information, marketing lists, etc.) will be evaluated as to whether that specific data field is:

11.9.1. Necessary, given the specific purpose for which the personal information will be used.



HUMAN RESOURCES

Reference: HRP 1.2

Revision: 0

Date: 2022-01-11

Page: 10/17

Owner: Human Resources

POPI POLICY

11.9.2. Relevant for that purpose.

Red flag data fields are titles (relevant for communication, but not necessarily for the allocation of benefits), family relation (relevant for medical scheme membership, but not for communication, etc.), information on race, gender, ethnicity (unless required by the B-BBEE Act, EEA, SDA or other law), physical address, views / opinions of persons, contact details (only was person consented to and what is relevant for that database should be kept), etc. The physical address of an employee, a patient (for delivery of goods) is necessary, but the address of a payment clerk at a customer or vendor is not required.

- 11.10. All communications of a **marketing or general communications nature** (e.g. disease awareness campaigns or announcements of a general nature) must be subject to an “opt out” functionality, which has to be adhered to strictly by the Company or anyone processing Personal Information for and on behalf of the Company. The Data Subject’s consent must be obtained on **Form 4** as set out in the Regulations published under GG number 42110 dated 14 December 2018. Information related to changes to company policies, etc. or any right or legitimate expectation of a staff member or a supplier / vendor cannot opt out of. Neither can they opt out of statements and similar information directly related to their contractual or other legal relationship with the Company.
- 11.11. All requests for Personal Information and other information from any person or entity whatsoever shall be dealt with in accordance with the provisions of the Company PAIA Manual and in line with this policy.
- 11.12. The Data Subject must be provided access to their Personal Information related upon written request and other requests for access to personal and other information from any person or entity must be dealt with in terms of The Company PAIA Manual and in line with this policy.
- 11.13. All processing of Personal Information must immediately cease, in the event that the Data Subject withdraws its consent to the processing or objects to the processing of Personal Information in the manner prescribed by law, except where the Company is by law obliged to continue with such processing. Such requests must be made to the scheme on **Form 1** of the POPI Regulations.
- 11.14. Personal Information must be corrected or deleted upon request contained in **Form 2** by the Data Subject to do so.

12. SECURITY AND ACCESS

The Company uses the following security measures to secure Personal Information in its possession:

- 12.1. Electronic information is secured by firewalls, anti-virus and password secured access, set out in the Company’s IT standards used¹.
- 12.2. Electronic information on shared drives operate on access control and permissions, accidental access must be reported to the Information Officer and IT immediately.

¹ which include but are not limited to policies on Digital Solutions and Cloud Infrastructure, Digital Security, Digital Protection, Computer Management, Passwords, Internet and Network Access, Anti Virus, Digital Access Management, etc.



HUMAN RESOURCES

Reference: HRP 1.2

Revision: 0

Date: 2022-01-11

Page: 11/17

Owner: Human Resources

POPI POLICY

- 12.3. No information, including personal information, may be downloaded from shared drives onto device hard drives or any external device.
- 12.4. Physical records are kept in accordance with the Company's Document Retention Policy.
- 12.5. There are security cameras by the site entrance areas, notices are put up to this effect and staff contracts include such surveillance as part of the conditions of employment. All such recordings are stored off-site and will only be accessed in cases of alleged breaches of processing, including unlawful access or destruction of personal information.
- 12.6. A few of our operational sites and office buildings are accessed through a biometrics system for employees, as well as a sign-in system with security personnel and boom gate for visitors, which is guarded and locked at night. The security company acts as an Operator and an Operator agreement is in place, ensuring that no personal information provided is stored for longer than necessary and is permanently destroyed after its use. Frequent visitor information is stored indefinitely at the security company in full compliance with the provisions of the POPI Act, or until a contract or assignment comes to an end. The instruction for destruction of such information to the security company is provided by the Group Security Manager.
- 12.7. All persons responsible for sign-in lists, forms and registers, irrespective of the premises or unit where those are used, will ensure that:
- 12.7.1. the information of previous entries are not visible to a current entrant, by keeping a blank sheet clipped over such information, or, where possible, redesigning access forms so that previous entrants' information is not visible.
 - 12.7.2. the form / list / register is never left unattended, and is, in such cases, locked safely before being left at a station / desk.
 - 12.7.3. visitors / attendees, when asking, are informed that their personal information is collected for security / presence / attendance record purposes, and will only be used for those purposes, and be archived and destroyed after a stipulated period, unless it forms part of an investigation.
 - 12.7.4. the collection of this information protects both the company and visitors, as it also ensures the security of visitors and that, should an incident (e.g. a fire) occur, all employees and visitors can be tracked.
- 12.8. Sign-in lists, forms and registers are kept in accordance with the period stipulated in the Company's [Document Retention Policy](#).
- 12.9. Where a visitor returns the visitor permit, the permit is filed and stored in a secured cupboard and after three (3) years is destroyed by way of shredding. An Operator Agreements is in place with the third party who renders the services of collecting and disposing of the shredded Personal Information.
- 12.10. Records that have a regulatory impact, i.e. for products, equipment or processes subject to the accreditation of SAHPRA and International Organization for Standardization, or fall under the Hazardous Substances



HUMAN RESOURCES

Reference: HRP 1.2

Revision: 0

Date: 2022-01-11

Page: 12/17

Owner: Human Resources

POPI POLICY

Control Act, Conformity Assessment, Calibration and Good Laboratory Practice Act, etc are processed, retained and destroyed in accordance with the requirements of regulators and under the oversight of the Industrial Regulatory Compliance and Risk Department

- 12.11. Regular verification that the safeguards in place are effectively implemented and continually updated in response to any new risks or deficiencies;
- 12.12. Notification in writing to the affected Data Subjects and reporting to the Information Regulator, should the Personal Information relating to the Data Subject be compromised or should there be a suspicion that the Personal Information is compromised. Notification may have to be made to the Information Regulator. All security and access breaches or suspected or potential breaches of personal information must be reported to the Information Regulator or his/her designated Deputy immediately after such breach or potential; breach becomes known.

13. TRANSBORDER DATA TRANSFER

- 13.1. All Air Liquide entities worldwide which have signed the “IntraGroup Agreement on Binding Corporate Rules”. These rules are recognized in section 72 of the POPI Act, and are binding. It ensures that where transborder data transfer takes place, such processing is in line with principles at par with, or stricter than local law (i.e. the POPI Act). Consideration must be had where the information of citizens of the EU’s information is processed.
- 13.2. The Company uses servers and systems that are based in South Africa for some of the personal information that it processes. However, as the Company is part of a global group of companies (the “Group”), certain employee personal information is stored on a server that is hosted outside of South Africa’s borders. These entities are complying with rules that are similar to the POPI Act. Performance records can be accessed through the Group’s Talent Management System. Such information can only be accessed by local human resource personnel so authorised, and by overseas duly authorised central HR Administrators for purposes of technical support, Key Performance Indicators consolidation, and maintenance. Excluded from these records that can be accessed by overseas designated employees of the Company, are Goals details, Performance records, career development wishes, development plans, transcripts, Curriculum Vitae.

14. RETENTION, STORAGE AND DESTRUCTION

- 14.1. All Personal Information in the possession of the Company must be stored, retained and destroyed in accordance with the legislation applicable to the specific information and according to the Company [Document Retention and Destruction Policy](#).
- 14.2. According to POPIA, personal Information shall not be retained longer than required to fulfil the purpose for the Processing or longer than required by Applicable Legislation.
- 14.3. Once the purpose for Processing or the retention period has lapsed, or provided under Applicable Legislation expires, the Personal Information must be destructed and/or deleted and/or returned to the Data Subject, as may be required by the Applicable Law and in a manner that complies with such Applicable Law.



HUMAN RESOURCES

Reference: HRP 1.2

Revision: 0

Date: 2022-01-11

Page: 13/17

Owner: Human Resources

POPI POLICY

14.4. Retention periods, and the destruction of personal information, must be specified in consents and notifications.

15. PURPOSE AND USE OF PERSONAL INFORMATION

When Processing Personal Information as part of any activity, the Responsible Party must:

- 15.1. Identify the nature and extent to which one will deal with (a) Personal Information and (b) Special Personal Information (i.e. measure the data fields through which information it is collecting to assess whether it is **relevant, necessary and not excessive**), and then amend its processing accordingly.
- 15.2. Identify the **types of processing** that will take place (e.g. collection, collation, manipulation, dissemination and destruction, or collection, recording and storage, etc.).
- 15.3. Identify the **purpose** for which the specific processing is undertaken, clearly indicating whether such purpose is permitted by a law (e.g. invoicing requiring a name on the invoice and an email address to which it is to be sent).
- 15.4. Confirm that **consent** has been obtained from Data Subjects, which consent shall constitute a contract between The Company and the Data Subject and shall describe:
 - 15.4.1. the purpose of the Processing or further processing of the Personal Information;
 - 15.4.2. the type of Processing of the Personal Information;
 - 15.4.3. timelines related to the Processing;
 - 15.4.4. the destruction or storage of the personal information; and
 - 15.4.5. the security assurances and measures undertaken by The Company to protect the data and Personal Information.
- 15.5. If processing is mandated by law, describe in a notification what that specific law says, and how processing will take place.
- 15.6. **Personal Information about children and special personal information**
 - 15.6.1. The Company does hold the personal information of children (persons up till the age of 18) for purposes the identification of child dependents for medical aid benefits, and/or life insurance purposes.
 - 15.6.2. The Company also has information of “child-dependents” older than 18, but who are still dependent on their parents – such persons are handled, for POPIA purposes as well as the purposes identified in paragraph 11.6.1 above, the same as any adult dependent.
 - 15.6.3. The Company will take all reasonable measures to protect the confidentiality of family members of employees identified as beneficiaries to pension / provident fund arrangements, medical schemes, HR agencies, insurers, etc. Third parties to whom information is passed and who act as Operators, will be contractually bound to ensure compliance with the POPIA.



HUMAN RESOURCES

Reference: HRP 1.2

Revision: 0

Date: 2022-01-11

Page: 14/17

Owner: Human Resources

POPI POLICY

16. OPERATORS

- 16.1. Operators (Data processors in other jurisdictions) are entities processing personal information on behalf of the Company.
- 16.2. There must be an Agreement between the Company and the Operator, which aligns with the [Company Template](#) and which must include, amongst others:
 - 16.2.1. The specific security measures taken by the Operator;
 - 16.2.2. Who are responsible from the Operator and the Company for what functions in relation to the processing of personal information;
 - 16.2.3. Reporting measures and accountability.

17. ETHICS COMPLIANCE

- 17.1. The Company, in its commitment to conducting its professional activities with the utmost integrity and transparency, has an Ethicall telephonic and online system for the purpose of reporting ethical violations; the report or complaint may be logged anonymously.
- 17.2. The Ethicall system is strictly confidential and managed on behalf of the Group by an external company that complies with rules that are similar to the POPI Act.
- 17.3. The incident report or complaint logged by an employee (or third party) are automatically received at the Group's head office in Paris by the duly authorised Head of Ethics and/or Group HR Director. The incident report or complaint is thereafter accordingly assigned to either Hub, Cluster or Entity level for investigation by the appointed Ethics Officer. Once the Ethics Officer has conducted and completed his/her independent investigation, he/she submits his/her report and recommendation to the Entity or Cluster or Hub HR Director or duly authorised Prescribed Officers, for further consideration and conclusion.
- 17.4. All logged reports or complaints are reviewed on a quarterly basis at Cluster, Hub and Group level by the duly authorised personnel. In addition, the status of closure or remedy of the logged reports or complaints are from time to time discussed at the Southern African Ethics and Social Committee during its quarterly meetings.

18. EMPLOYEE WELLNESS PROGRAMME

- 18.1. The Company has an employee wellness programme in place to support its employees (and/or their immediate family members) with psychosocial issues that they may be experiencing. This employee wellness programme is coordinated, monitored and rendered by a third party who is an Operator insofar as it relates to the Company's Personal Information or where the Company duly provides to the third party its employees Personal Information. In all other instances where the third party collects the employees' Personal Information directly from the employees, the third party remains the Responsible Party. The Company and the third party further have an existing Operator Agreement in place.



HUMAN RESOURCES

Reference: HRP 1.2

Revision: 0

Date: 2022-01-11

Page: 15/17

Owner: Human Resources

POPI POLICY

18.2. The collected Personal Information of employees is limited to the employee's name, surname, telephone and cell phone numbers, email address, and age.

19. REVIEW AND AMENDMENT

This policy shall be reviewed every two years or more frequently as may be required and may be amended from time to time as may be required by law, for corrections of material errors, as the case may be.

20. TRAINING AND COMMUNICATION

At least once a year, a refresher training on this Policy, the POPIA, PAIA shall be scheduled for all interested parties. All existing Employees, contractors, vendors, Committee members and any person who may Process Personal Information for and on behalf of the Company (i.e. Operators), shall be trained on an annual basis on this policy and underlying legal sources on which it is based. The training will also form part of new employee induction.

21. COMPLIANCE

21.1. The Information Officer NATASHA NAIDOO shall maintain a report in relation to POPI and PAIA regarding the above implemented measures, which report shall be available to all interested parties.

21.2. Remedial steps that could be taken in instances of non-compliance may include, amongst others:

21.2.1. Rewording of consents, standard clauses and notifications.

21.2.2. Reporting loss, breach and/or unauthorized access of Personal Information to relevant authorities, recommending disciplinary action, etc.

21.2.3. The destruction of personal information.

21.2.4. The de-identification of personal information.

21.2.5. The implementation of specific security measures.

21.2.6. The implementation of (additional or new) access control measures.

21.2.7. The implementation of consents or notifications *ab initio*.

21.2.8. Research and verification of legislative mandates.

21.2.9. Addenda to contracts and service level agreements within business activities and/or with third parties and contractors.

21.2.10. Amendments to contract templates.

21.2.11. Disciplinary action against employees violating this policy.

21.2.12. Action against office bearers violating this policy, in conjunction with the Board of Trustees.

21.2.13. Requirements on the submission of (regular) progress reports.

21.2.14. Obtaining expert assistance, where required.

21.2.15. Undergoing additional or further training on POPI and PAIA.

22. INFORMATION OFFICE

22.1. This office houses the Information Officer and his deputies: 4 Skeen Boulevard, Bedfordview, Germiston

22.2. The following may be directed to the Information Officer in writing to natasha.naidoo@airliquide.com



HUMAN RESOURCES

Reference: HRP 1.2
Revision: 0
Date: 2022-01-11
Page: 16/17
Owner: Human Resources

POPI POLICY

23. COMPLAINTS

- 23.1. Any complaints by any person including members and beneficiaries, employees, office-bearers, third parties or any regulator, on any allegation or actual violation of this policy or data privacy, may be directed to the Information Officer [or a designated Deputy], who will handle the complaint in line with the principles of natural justice, and apply this policy, as well as the applicable laws and related policies of the Companies, when doing so.
- 23.2. The Information Office may constitute a Committee to investigate the matter, and to make findings on the complaint, and recommend action by the relevant departments, units or structures of the Scheme.

24. POPI ACT: OBJECTIONS, WITHDRAWALS, AMENDMENTS AND DELETIONS

- 24.1. Any person can object to processing of Personal Information, withdraw a consent to processing, request amendment or deletion of personal Information.
- 24.2. The forms to object, consent to marketing, change or request destruction of personal information must use the forms attached to the Policy, as prescribed by the Regulations to the POPI Act.

25. INSPECTIONS BY THE REGULATOR

- 25.1. The Company's Policy applicable to inspections, dawn raids and search and seizure orders will be followed in the event of an unscheduled inspection by the Information Regulator.

26. EFFECTIVE DATE

- 26.1. This Policy is in effect from 30 June 2021, with consideration of the fact that the POPIA will be in full force and effect from 1 July 2021.

27.0 REFERENCES AND ASSOCIATED DOCUMENTS

- AL Template Operator Agreement 2021
- FORM 1 - Objection To The Processing Of Personal Information In Terms Of section 11 (3) of The Protection Of Personal Information Act, 2013 (Act no. 4 Of 2013), Regulations Relating To The Protection Of Personal Information, 2018 [Regulation 2.]
- FORM 2 - Request For Correction Or Deletion Of Personal Information Or Destroying Or Deletion Of Record Of Personal Information In Terms Of section 24 (1) of The Protection Of Personal Information Act, 2013 (ACT NO. 4 OF 2013), Regulations Relating To The Protection Of Personal Information, 2018 [Regulation 3.]
- VitalAire PAIA Manual

28.0 IMPROVEMENT

All noncompliance to this procedure shall be governed by MS Nonconformity & Corrective Action and MS Continual Improvement.



HUMAN RESOURCES

Reference: HRP 1.2

Revision: 0

Date: 2022-01-11

Page: 17/17

Owner: Human Resources

POPI POLICY

29.0 DOCUMENTED INFORMATION

This procedure shall be updated, controlled and distributed in accordance with MS Control of Documented Information.