Data Protection and Information Sharing Policy of African Group Lubricants (Proprietary) Limited

African Group Lubricants (Pty) Ltd
Cnr. Paul Smit Street and Main Road,
Anderbolt, Boksburg, 1459

Reg No: 2014/176422/07
Tel: +27 11 824 0560
Directors: M Kerwan, J Govender, U Lebuso

VAT No: 4250267335
www.aglubricants.co.za

1. BACKGROUND

This is the Data Protection and Information Sharing Policy of African Group Lubricants (Proprietary) Limited ("AGL"). This policy is to explain how AGL intend to meet their legal obligations concerning confidentiality and information security standards. The parameters of the policy are defined by the **Protection of Personal Information Act, No 4 of 2013.**

2. CONTACT DETAILS

2.1 Information Officer

Name	Mark Kerwan
Physical Address:	177 Paul Smit Street, Anderbolt, Boksburg, 1459
Telephone Number	+27(11) 824 0560
Email	mark.kerwan@aglubricants.co.za
Information regulator Reference number	00952/2022-2023/IRRTT

2.2 Deputy Information Officers

Name	Tessa Meyer
Physical Address:	177 Paul Smit Street, Anderbolt, Boksburg, 1459
Telephone Number	+27(11) 824 0560
Email	tessa.meyer@aglubricants.co.za
Information regulator Reference number	00952/2022-2023/IRRTT

3. DEFINITIONS

3.1 **"Consent"** means the voluntary, specific and informed expression of will;

3.2 "**Data Subject"** means the natural or juristic person to whom the Personal Information relates;

3.3 "**POPI"** means the **Protection of Personal Information Act, No. 4 of 2013**;

3.4 "**Personal Information"** means as defined in POPI which includes, but is not limited to:

3.4.1 Race, gender, sex, pregnancy, marital status, nationality, ethnic or social origin, sexual orientation, age, physical or mental health, well-being, disability, religion, conscience belief, culture, language, birth;

3.4.2 Historical information such as education, medical, financial, criminal, employment;

3.4.3 Any identifiers such as a number (for example: ID or passport), symbols, e-mail address, physical address, telephone numbers, location, online ID or other assignment unique to a person (for example an Employee code, tax number; registration number with any governing authority);

3.4.4 Biometric information digitally stored being a physical characterization which may be used, for example in access control to any AGL facility, fingerprints, retinal scanning, voice recognition or any other information contained in a human resource record, medical report or examination which the Company may from time to time have sight of as a consequence of the Employer/Employee relationship;

3.4.5 Personal opinion views or preferences;

3.4.6 Correspondence implicitly or explicitly of a private and confidential nature;

3.4.7 Views or opinions of another individual;

3.4.8 The name of the person with other information or the name alone

3.5. "**Processing"** means an operation or activity, concerning Personal Information, including Personal Information, whether or not by automatic means through the: -

3.5.1 Collection, receipt, recording, organizing, collation, storage, updating, modification, retrieval and/or alteration;

3.5.2 Circulation by means of transmission distribution or making available to others and;

3.5.3 Deletion, erasure and destruction.

3.6 "**Responsible Party"** means the entity which, alone or in conjunction with others, determines the need for the personal information, the reason why it is collected and purpose for which it will be used and processed. In this case the Responsible Party is AGL.

3.7 "**Operator"** means a person who processes personal information for The Responsible Party, in terms of a contract or mandate, but does not come under the direct authority or control of the responsible party such a credit bureau, credit insurer, financial institution, human resource service provider, consultant or risk manager.

3.8 **"Record"** means any recordal of personal information whether or not by automated means. A record includes, but is not limited to manuscript notes, digitally transmitted communications, images, tape recording, video, application forms and documents.

3.9 **"De-identify/ied"** means to delete any information which identifies a Data Subject or any information if interpreted and examined could lead to the identification of a Data Subject.

4. SCOPE OF THE POLICY

The Policy applies to all persons who AGL interact with and whose personal information is processed, users of the AGL website, AGL's Executive Employees, Branches, Departments and Divisions, all Employees or other persons acting on behalf of AGL or on the instruction of AGL. This Policy does not apply where personal information has been de-identified.

5. POLICY STATEMENT

AGL collects and uses Personal Information of individuals and corporate entities with whom it transacts, in order to operate and carry out its business effectively. AGL understands that the lawful and appropriate processing of all Personal Information is crucial to successful service delivery and essential to maintaining confidence between AGL and those individuals and entities who deal it, internally and externally. AGL therefore fully endorses and adheres to the principles of POPI, in as far as it is required.

6. PROCESSING OF PERSONAL INFORMATION

6.1. **Purpose of Processing**

AGL uses the Personal Information under its care in the following ways:

6.1.1 Conducting credit reference checks and assessments;

6.1.2 Preparation and administration of agreements, contracts and legal binding documents;

6.1.3 Providing products and services to customers;

6.1.4 Engaging and contracting with Suppliers and Service Providers;

6.1.5 Discounting, consignment and/or supply funding purposes with Operators and Financial institutions;

6.1.6 Detecting and prevention of fraud, crime, money laundering and other such unlawful practice;

6.1.7 Conducting market research in the course of engaging with its Suppliers, Customers and Service providers.

6.1.8 Conduct marketing, sales and due diligence exercises with potential business partners;

6.1.9 In connection with legal proceedings and in complying with legal and regulatory requirements;

6.1.10 Staff administration including the interview and appointment of new staff members, performance evaluation, operating its payroll, processing of leave applications, disciplinary action which could result in the termination of services of a current employee, processing of information to meet the obligations of AGL to the South African Revenue Services, Unemployment Fund and other such statutory bodies, the administration of benefits schemes such as the company Provident Fund and Bonus Schemes and general maintenance of Human Resource records;

6.1.11 Keeping of accounts and records and the preparation of Audited Financial Statements.

6.1.12 Using a data subjects' details when it uses the AGL website, apps and or when it corresponds with AGL by email.

6.2. **Categories of Data Subjects and their Personal Information**

Customers (natural and juristic)	Service Providers and Suppliers	Employees, Directors and Shareholders
•Names; contact details; physical and postal addresses; date of birth; ID number; tax related information; nationality; gender; confidential correspondence •Names of contact persons; name of legal entity; physical and postal address and contact details; financial information; registration number; founding documents; tax and banking related information; authorised signatories; beneficiaries; ultimate beneficial owners; shareholding information; BBBEE information	•Names of contact persons; name of legal entity; physical and postal address and contact details; financial information; registration number; founding documents; tax and banking related information; authorised signatories; beneficiaries; ultimate beneficial owners; shareholding information; BBBEE information.	•Gender; pregnancy; marital status; colour, race; age; language; education information; financial information; employment history; ID number; •physical and postal address; contact details; opinions; criminal record; well-being •tax and banking related information •Confidential correspondence •reference checks and background information verification

7. RIGHTS OF DATA SUBJECT

AGL shall ensure that those, to whom this policy, is applicable are made aware of the rights conferred upon them as Data Subjects.

The general rights of Data Subjects all summarized as follows: -

7.1 **The right to access personal information**:
AGL recognizes that the Data Subject has the right to establish what personal information related to him or her is held by AGL, and also has the right to access that personal information.

7.2 **The right to have personal information corrected or deleted:**
The Data Subject has the right to request that his or her personal information be corrected or deleted (deidentification of personal information occurs where AGL is no longer authorized to retain such personal information).

7.3 **The right to object to the processing of personal information:**
The Data Subject has the right upon reasonable grounds to object to the processing of his or her personal information, or to retract prior consent given to process his/her personal information. Where such objection/retraction is received, AGL may cease to disclose the Data Subject's personal information, subject to any other statutory or contractual record keeping requirements and may also approve that such personal information be de- identified.

7.4 **The right to complain to the Information Regulator: -**
The Data Subject has the right to submit a complaint to the information regulator regarding any alleged infringements of the rights protected under POPI, if AGL does not address the Data Subject's complaint. Complaints are to be made in writing on the POPI Complaint form. The Details of the Information Regulator can be found at:

The Information Regulator of South Africa is based at: JD House, 27 Stiemens Street, Braamfontein, Johannesburg, 2001.
P.O Box 31533, Braamfontein, Johannesburg, 2017

General enquiries: enquiries@inforegulator.org.za.
Complaints (complete POPIA/PAIA form 5):
PAIAComplaints@inforegulator.org.za - should your PAIA request be denied or there is no response from a public or private bodies for access to records you may use this email address to lodge a complaint.
POPIAComplaints@inforegulator.org.za – should you feel that your personal information has been violated, you may use this e-mail address to lodge a complaint.
Manual registration of Information Officers: Registration.IO@inforegulator.org.za
Compliance: POPIACompliance@inforegulator.org.za or PAIACompliance@inforegulator.org.za

8. POPI INFORMATION PROCESSING CONDITIONS

Under POPI this Policy abides by eight information processing.

These are: -

8.1. **Accountability**

AGL shall insure that all processing conditions, are complied with when determining the purpose and means of processing Personal Information and during the processing itself.

8.2. **Processing Limitation**

8.2.1 Personal Information must be collected and processed lawfully in a reasonable manner without infringing on the privacy of a Data Subject. The Personal Information shall be limited to that which is adequate, relevant, and not excessive. Requests should be confined only to those elements of personal information which are essential to AGL achieving its objectives;

8.2.2 Personal Information processing requires written Data Subject consent, unless it is:

(i) necessary to do so for the conclusion or performance of a contract;
(ii) an obligation in terms of law;
(iii) to protect the legitimate interest of the Data Subject; and
(iv) or to pursue a legitimate interest of the Responsible Party.

8.2.3 Personal Information must be collected directly from the Data Subject unless it is: -

(i) contained in a public record;
(ii) has been deliberately made public by the Data Subject;
(iii) is collected from another source with the Data Subject's consent;
(iv) would not prejudice the Data Subject;
(v) is necessary to maintain, comply with or exercise any law or legal right; and
(vi) collection from the Data Subject is not reasonably practicable.

8.2.4 All Data Subjects have the right to refuse or withdraw their consent to the processing of their Personal Information. A Data Subject may object, at any time, to the processing of their Personal Information on any of the above grounds, unless legislation provides for such processing. If the Data Subject withdraws consent or objects to processing, then AGL may refrain from processing the Personal Information and de-identify it.

8.2.5 AGL shall not distribute any personal information between its associated legal entities, subsidiaries and associated businesses. Personal information is collected from the Data Subject only for the purposes for which it was intended, and it may not

be viewed or processed by any person other than the person to which it was supplied for an identified purpose. The Data Subject may consent to the use of Personal Information via the completion of Annexure "C" to this policy being the Consent Form – Personal Information Usage and Data Sharing.

8.3. **Purpose Specification**

AGL shall only process Personal Information for the specific, explicitly defined and legitimate reasons. AGL shall inform Data Subjects of these reasons prior to collecting or recording the Data Subjects Personal Information.

8.4. **Further Processing**

New processing activity must be compatible with original purpose of processing. Further processing will be regarded as compatible with the purpose of collection if the Data Subject has consented to the further processing, in writing.

8.5. **Information Quality**

AGL shall take reasonable steps to ensure that Personal Information is complete, accurate, not misleading and updated regularly. AGL shall undertake a periodic review Data Subject records to ensure that the Personal Information is still valid and correct.

8.6. **Openness**

Where required to do so, AGL shall take reasonable steps to ensure that the Data Subject is made aware of the reasons why the Personal Information is collected, what personal information is collected, the source of information, which it will be shared with and processing is a legal requirement.

AGL shall further, if required, inform the Data Subject of the consequences of a failure to provide such information. (Example: without disclosure of Personal Information AGL may not be able to offer a customer a credit facility OR a prospective Employee employment)

8.7. **Data Subject Participation**

Data Subjects have the right to request access to, amendment, or deletion of their Personal Information. All such requests must be submitted in writing to the Information Officer for consideration. AGL shall not disclose any Personal Information to any party unless the identity of the requester has been verified.

8.8 **Security Safeguards**

AGL will manage the security of its filing system (automated and manual), to ensure that personal information is protected adequately. Steps to be taken include but are not limited to: -

8.8.1 Security controls will be implemented in order to minimize the risk of loss, unauthorized access, disclosure, interference modification and/or destruction;

8.8.2 AGL will continuously review its security controls which will include regular testing of protocols and measures put in place to combat cyberattacks, hacking and other infringements on AGL's IT network.

8.8.3 The organization will ensure that all paper and electronic records comprising of personal information are securely stored and made accessible only to the authorized individuals making use of them.

8.8.4 All new employees will be required to sign employment contracts containing the necessary contractual provisions directing them as to the use and storage of Employee information and any information relative to a Data Subject, whose information they might process in the course and scope of rendering services to AGL.

8.8.5 Confidentiality clauses are also included to reduce the risk of unauthorized disclosures of personal information for which AGL is responsible.

8.8.6 All existing employees will be furnished with a copy of this policy, and after required consultation has been followed, will be required to sign an addendum to their employment contracts containing the relevant consent and confidentiality clauses.

8.8.7 The organizations operators and 3rd party service providers will be required to enter into Service Level Agreements with AGL, where both parties pledged their mutual commitment to POPI and the lawful processing of personal information as per this policy and POPI.

8.8.8 Written records containing the personal information of Data Subjects in hard copy form will be kept in locked cabinets or safes. These records when being used will not be left unattended in areas where other members of staff may access them. AGL shall implement and maintain a **"Clean Desk Policy"** where all employees will be required to clear their desks of personal information when leaving for any length of time or at the end of the day. Personal information which is no longer required should be de-identified and disposed of.

8.8.9 All electronically held personal information must be saved to a secure database and as far as possible no personal information should be saved on individuals computers laptops or handheld devices. All company computers laptops and handheld devices should be access protected with a password. Electronic Personal Information which is no longer required must be deleted from the individual laptop or computer and the relevant database. The Employee must ensure that the information has been completely deleted and is not recoverable. AGL shall implement and maintain a **"Clean Screen Policy"** where all employees will be required to lock their computers or laptops when leaving their desks for any length of time or log off at the end of the day.

8.8.10 Any loss or theft of, or unauthorized access to, Personal Information (suspected or actual) must be immediately reported to the Information Officer. Any loss or theft of computers, laptops or other devices which may contain Personal Information must be immediately reported to the Information Officer, who shall notify the IT department, who shall take all necessary steps to remotely delete the information, if possible.

8.9 Cross Border Transfer of Personal Information

8.9.1 AGL may not transfer Personal Information to another party who is situated outside South Africa, unless:

8.9.1.1 the Data Subject Consents (POPIA) to such Processing; or

8.9.1.2 the transfer is necessary in order to perform a contract between AGL and a Data Subject, or for reasons of public interest, or to establish, exercise or defend legal claims or to protect the vital or legitimate interests of the Data Subject in circumstances where the Data Subject is incapable of giving Consent;

8.9.1.3 the country where the Personal Information is being transferred to providers with the same level of protection for the Data Subject (s) as housed under the data processing laws applicable in South Africa or alternatively,

8.9.1.4 AGL has concluded an agreement with the recipient of the Personal Information, either in the form of a standard binding corporate rule, or an Operator agreement or a Personal Information transfer agreement, which sets out the rules which apply to the receipt and subsequent Processing of that Persona Information. It is the Data Subject(s) duty to verify compliance of AGL in this regard.

8.9.2 In order to ensure that the above is followed, Personnel may not transfer Personal Information to areas outside South Africa, unless one of the following controls and safeguards are in place:

8.9.2.1 The Information Regulator, or other such territorial appointed authority has issued an "adequacy decision" confirming that the territory or country where AGL proposes transferring the Personal Information to, has adequate Data Protection laws in place which will afford the Data Subject with the same level of protection as that under POPI;

8.9.2.2 a standard binding corporate rule is in place, which covers the recipient of the Personal Information;

8.9.2.3 The Operators or recipient of the Personal Information has agreed that it will afford the Data Subject with the same level of protection as that under POPI;

8.9.2.4 the Data Subject has given Consent to the proposed transfer, having been fully informed of any potential risks;

8.9.2.5 the transfer is necessary in order to perform a contract between AGL and a Data Subject, for reasons of public interest, to establish, exercise or defend legal claims or to protect the vital interests of the Data Subject in circumstances where the Data Subject is incapable of giving Consent (POPIA).

8.10 Direct Marketing

The scope of this aspect of the policy is defined by the provisions of the POPI Act, Chapter 8, which stipulates that direct marketing, including unsolicited direct electronic marketing is prohibited unless the Data Subject has consented to the receipt of this marketing material.

8.10.1 No direct marketing shall be undertaken, including unsolicited direct electronic marketing unless the Data Subject has consented to the receipt of this marketing material.

8.10.2 Whilst direct marketing is not an activity which is generally undertaken by AGL, should it for whatever reason be undertaken, then AGL undertakes that it is sent out in a lawful manner, all Employees shall ensure that:

8.10.2.1 all AGL customers, when approached or dealt with for the first time, are given the opportunity in an informal manner to agree or disagree to the receipt of any direct marketing material;

8.10.2.2 before direct marketing is sent to a non-customer that such person provides his, her, or its consent thereto, which will be in the form of the prescribed "opt in" notice;

8.10.2.3 when marketing material is sent to Data Subjects, that the material houses an “opt out” form, allowing the Data Subject to opt out of any further marketing material; and

8.10.2.4 when a Data Subject exercises his, her or its right to object to receiving direct marketing, in the form of an opt out, that such opt out is recorded and given effect to, and that no further direct marketing is sent to the opted-out customer.

9. DUTIES OF SPECIFIC PERSONS IN THE COMPANY

9.1 Executive Management

POPI and this Policy direct that Executive Management hold accountability and answerability for the compliance of AGL in meeting its legal obligations, in terms of POPI, which may not be delegated. Some of the administrative responsibilities, in terms of POPI, may be delegated to other responsible individuals in AGL.

The core responsibility of Executive Management, and in particular the Chief Executive Officer is to ensure: -

9.1.1 The appointment of an Information Officer and when necessary, a Deputy Information Officer;

9.1.2 That all persons responsible for the processing of personal information on behalf of AGL are appropriately trained and supervised and also understand that they are contractually obligated to protect personal information that they come into contact with

9.1.3 That willful or negligent breach of this policy and procedure may lead to disciplinary action being taken against them. Executive management also holds the duty to ensure that the necessary auditing procedures are conducted annually in order to review the way in which process is personal information.

9.2 Information Officer

The appointment of AGL's Information Officer is an appointment which is regulated by the rules and regulations of the Information Regulator.

The responsibility of AGL's Information Officer is: -

9.2.1 to ensure compliance with POPI;

9.2.2 report to Executive Management on the protection of AGL's responsibilities under POPI;

9.2.3 Analyze privacy regulations and align this policy with any amendments and developments;

9.2.4 Scheduling and ensuring that POPI Audits are conducted regularly;

9.2.5 Put a process in place to allow AGL and any affected Data Subjects to have access to the relief created by this policy;

9.2.6 any notices and communications received either from a Data Subject or the Information Regulator relative to the contents of this policy and POPI, are efficiently processed.

9.3 Employees and other Persons Acting on behalf of the Organization.

This Policy has been put in place throughout AGL, training on the Policy and POPI will take place with all affected employees. Modifications and updates to Data Protection and Information Sharing Policy, legislation, or guidelines will be brought to the attention of all staff.

9.3.1 **Duties**

The duties of the Employee or any other person's acting on behalf of AGL include but are not limited to, ensuring that:-

a) Personal information is not directly or indirectly utilized, disclosed or made public in any manner, to any person or third party, within AGL or externally;

b) No disclosure of personal information is made, unless that personal information is already officially known, or the disclosure is necessary in order for the Employee or person to perform his or her duties;

c) Employees and other persons acting on behalf of the organization will only process personal information where the Data Subject has either consented to the processing; or the processing is necessary to carry out the actions for the conclusion of performance of a contract where the Data Subject is a counterparty; or the processing of personal information complies with any obligation imposed by law on the responsible party; or the processing of personal information complies with any obligation imposed by law on the responsible party; or the processing of personal information is done in a manner that protects the legitimate interest of that Data Subject; or the processing of personal information is necessary for pursuing the legitimate interests of the organization or of a third party to whom the information is supplied;

h) Employees or other persons acting on behalf of the organization must request assistance from their line manager or the Information Officer, if they are unsure about any aspect relating to the protection of the Data Subject's personal information;

i) Prior to the processing of any personal information that consent and written permission if required has been given by the Data Subject for the processing of their personal information;

k) The Data Subject who must clearly understand the purpose for which his or her personal information is needed and also who it will be shared with;

l) Where consent is required, it must be either given expressly in a written form and this includes any electronic medium which can be printed or implied;

m) If the Data Subject is a juristic person, then consent, if required, to process the Data Subject personal information may only be obtained from the duly authorized representative of the Data Subject, who must confirm that designation;

n) All personal information is securely kept by taking sensible precautions and following the guidelines in this policy;

o) Personal information is held in as few places as possible;

p) No additional records or filing systems or data sets are created that are unnecessary;

q) Personal information is encrypted prior to sending or sharing any personal information electronically. In the event of doubt the Line Manager may assist the employee;

r) All computers, laptops and such devices comply with the "Clear Screen Policy" of AGL;

s) Where personal information is stored on removable devices such as external drives that these are kept locked away when not being used;

u) Where personal information is stored on paper, that such hard copy records are kept in a secure place, where unauthorized persons may not access it like a locked drawer of a filing cabinet. Employees are reminded of the "Clean Desk Policy" of AGL.

v) Reasonable steps are taken to ensure that personal information is kept accurate and up-to-date. Where personal information is found to be out of date authorization must first be obtained from the relevant line manager or Information Officer to update the information accordingly. Once updated, prior records must be de-identified;

w) Reasonable steps are taken to ensure that personal information is stored only for as long as is needed or required in terms of the purpose for which it was originally connected. Where personal information is no longer required authorization must be obtained from the relevant line manager or Information Officer to identify the information delete or dispose of it in the appropriate manner;

x) Should the Employee or person acting on behalf of the organization become aware of suspicious activity or any potential security breach such as unauthorized access, interference, modification, destruction or the unsanctioned disclosure of personal information, he or she must immediately report this event or suspicious or suspicion to the Information Officer or Deputy Information Officer concerned.

9.3.2 **Strictly Prohibited Conduct:**

Employees and persons acting behalf of AGL may **NOT**: -

a) Process personal information where consent has not been given by the Data Subject, if consent is needed;

b) Process personal information where it is not a requirement to perform their work related duties or functions;

c) Save copies of personal information directly to their own private computers, laptops, or other mobile devices or smartphones. All personal information must be accessed and updated from AGL's central database or a dedicated server;

d) Share information informally in particular personal information. Where access to personal information is required, this may be requested from the relevant line manager or the Information Officer, in wiritng.

e) Transfer personal information outside of the Republic of South Africa without the express written permission of the Data Subject or Information Officer.

10 POPI COMPLAINTS PROCEDURE

10.1 Should it come to the attention of a Data Subject that their rights under POPI, have not received adequate protection, alternatively have been infringed upon then the following process, read with any additional obligations may be created by AGL's PAIA Manual, may be followed: -

10.1.1 POPI complaints must be submitted to the organization in writing. Complaints should take the form of communications addressed to the Information Officer by the Data Subject preferably in the complaint from appearing at annexure "B" to this policy.

10.1.2 Where a complaint is received by any other person within the organization other than the Information Officer, that person is under a duty to ensure that the full details of the complaint reach the Information Officer, forthwith;

10.1.3 The Information Officer will provide the complainant with a written acknowledgement of receipt of the complaint within two working days;

10.1.4 The Information Officer will carefully consider the complaint and address the complainant's concerns. The Information Officer will endeavor to resolve the complaint in a fair manner and in accordance with the principles outlined in this policy and POPI;

10.1.5 The Information Officer must also determine whether the complaint relates to an error or breach of confidentiality and whether this complaint may have a wider impact on AGL's Data Subjects.

10.1.6 Where the Information Officer has reason to believe that the personal information of a Data Subject has been accessed or acquired by an unauthorized person, the Information Officer will consult with AGL's Executive Management, whereafter the affected Data Subjects and Information Regulator will be informed of the breach.

10.1.7 The Information Officer will revert to the Complainant with the proposed solution with the option of escalating the complaint to AGL's Executive Management within (7) seven working days of the receipt of any complaint.

10.1.8 In all instances, the organization will provide reasons for any decision taken and communicate any anticipated deviation from the specific timelines.

10.2 The Information Officer's response any complaint of a Data Subject shall comprise of the following: -

10.2.1 suggested remedy for the complaint;

10.2.2 dismissal of the complaint and provide reasons;

10.2.3 send an apology and commence disciplinary action against the Employee involved.

10.3 Where the Data Subject is not satisfied with the Information Officers suggested remedy the Data Subject has the right to complain to the Information Regulator.

10.4 The Information Officer will review the complaints process to assess the effectiveness of the procedure on a periodic basis and improve the procedure where it is found to be lacking. The reasons for any complaints will also be reviewed to ensure the avoidance of occurrences giving rise to POPI related complaints.

11. DISCIPLINARY ACTION

11.1 Where a public complaint or POPI infringement investigation has been finalized and it has been found that an Employee concerned has transgressed the provisions of this policy, then appropriate administrative, legal and or disciplinary action may be taken against any Employee reasonably suspected of being implicated in non-compliant activity as outlined in this policy;

11.2 In the case of ignorance or minor negligence, the organization shall provide further awareness training to the Employee concerned;

11.3 Any gross negligence or the willful mismanagement of personal information, will be considered a serious form of misconduct for which the organization may initiate an enquiry which could

result in the dismissal of the employee. Disciplinary procedures will commence where there is sufficient evidence to support an employee's gross negligence.

11.4 As the consequences for the breach of POPI and this Policy are severe, one can expect that immediate actions that may be taken, subsequent to an investigation, may include, but are not limited to:

11.4.1. A recommendation to commence with disciplinary proceedings;

11.4.2 A referral to appropriate law enforcement agency for criminal investigation;

11.4.3 Recovery of funds or assets in order to limit any prejudice for damages caused.

A copy of this policy shall be appended the company disciplinary code of conduct. All employees are required to read and acknowledge their understanding of the policy.

12. POPI AUDIT

AGL's Information Officer will schedule POPI Audits. The Audit shall assess the following subject matter: -

12.1 identify the process to collect, record, store, disseminate and destroy personal information;

12.2 Determine the flow of personal information throughout AGL. Redefine the purpose for gathering and processing information;

12.3 Ensure the processing parameters are still adequately limited and in compliance with legislation;

12.4 Ensure the new Data Subjects are made aware of the processing of their personal information;

12.5 Verify the quality and security of personal information and the process in place around the handling of personal information by AGL;

12.6 Monitor the extent of compliance with POPI and this Policy. Monitor the effectiveness of internal controls established to manage AGL's compliance and risk.

In performing the POPI Audit Information Officers will interact with line managers to look for shortcomings within AGL's operations and identify areas that are most vulnerable or susceptible to the unlawful processing of personal information. The AGL Information Officer will be permitted to direct access and also have the support of line managers and AGL's Executive Management for the purpose of performing this duty.

13. RELATED POLICIES & PROCEDURES

13.1 This Policy must be read together with necessary interrelated policies such as the Promotion of Access to Information Policy (PAIA Manual) and any other policy, directive or Agreement, which may be from time to time required.

13.2 Where any of the above-mentioned Policies conflict with this Policy, then in so far as the conflicting provision (s) provide for and apply to the Processing of Personal Information, then the provisions housed under this Policy will prevail.

14. SIGNATURE PAGE

Version 1

Approved by:	Date:	Signature:
Mark Kerwan	17/11/2021	

ANNEXURE – A PERSONAL INFORMATION REQUEST FORM

Kindly complete and submit to AGL's Information Officer (email: mark.kerwan@aglubricants.co.za) with a copy to the Deputy Information Officer of AGL (email: tessa.meyer@aglubricants.co.za)	
Name	
Tel Number	
Email Address	

Kindly take note: a) that the Information Officer or his Deputy may require you to present an identification to enable your request to
be processed and; b) you may be required to pay a reasonable change for the copies made in processing this request.

A. PARTICULARS OF THE DATA SUBJECT	
Full Name or Entity	
Identity Number or Registration number	
Postal Address	
Contact Number	
Email address	

B. REQUEST		
I require AGL to:		
i	Advise me if it hold any of my personal information	
ii	Provide me with a record or description of my personal information	
iii	Correct or update my personal information	
iv	Destroy or delete my personal information	

C. INSTRUCTIONS

Should this document be signed on behalf of a juristic person then the signatory hereto warrants that he/she has the request authority to execute this Consent.

D. SIGNATURE	E. Date

Annexure B- POPI COMPLAINT FORM

Kindly complete and submit your complaint to AGL's Information Officer (email: mark.kerwan@aglubricants.co.za) with a copy to the Deputy Information Officer of AGL (email: tessa.meyer@aglubricants.co.za)	
Name	
Tel Number	
Email Address	

If we are unable to resolve your complaint to your satisfaction then you have the right to refer your complaint to the Information Regulator, whose details are as follows: -
The Information Regulator,
Physical Address: JD House, 27 Stiemens Street, Braamfontein, Johannesburg, 2001.
Email Address: **complaints.IR@justice.gov.za**
Website: https://www.justice.gov.za/inforeg/index.html

A. PARTICULARS OF THE COMPLAINANT	
Full Name or Entity	
Identity Number or Registration number	
Postal Address	
Contact Number	
Email address	

B. DETAILS OF THE COMPLAINT

C. DESIRED OUTCOME

Should this document be signed on behalf of a juristic person then the signatory hereto warrants that he/she has the request authority to execute this Consent.

D. SIGNATURE	E. Date

15. ACKNOWLEDGEMENT OF PROCESSING ACTIVITIES BY AFRICAN GROUP LUBRICANTS

15.1 By providing AGL with the Personal Information which we require from you:

- you acknowledge that you understand why your Personal Information needs to be processed;
- you accept the terms which will apply to such processing, including the terms applicable to the transfer of such Personal Information cross border;
- where consent is required for any processing as reflected in this Policy, you agree that AGL may process this particular Personal Information.

15.2 Where you provide us with another person's Personal Information for processing, you confirm that you have obtained the required permission from such person (s) to provide us with their Personal Information for processing.

15.3 Should any of the Personal Information concern or pertain to a legal entity whom you represent, you confirm that you have the necessary authority to act on behalf of such legal entity and that you have the right to provide the Personal Information and/or the required permissions in respect of the processing of that Organization or entities' Personal Information and that the details set out hereunder will apply to, and will be of benefit to, each of your successors in title and/or assigns if and where applicable.