Policy title:	POPI Policy	**Revision date:**	12.05.2021
Responsible Dept:	QMS	**Version No.:**	5
Version compiled by:	S Eksteen	**Version approved by:**	S Hewitt
Applicable to:	All	**Pages:**	12
Purpose:	To comply with the Protection of Personal Information Act (POPIA) - Act 4 of 2013 in respect of the information it holds about any Person/ Entity/ Body/ Individual/ Company		
Last date audited:	NA	**Policy No.:**	LEG_001
Last audited by:	NA	**Level:**	BusCrit 1

Protection of Personal Information Act (POPIA)

EXTERNAL PRIVACY POLICY

1. INDEX

Changes v4 to v5 – proposed changed on 04.05.2021 (input Shane Hewitt & Melanie Coetzee)

2. DEFINITIONS

"**AUP**": means Dole's Technology Acceptable Use Policy (AUP) for IT Systems. It is designed to protect Dole Food Company Inc. a corporation of North Carolina, United States, together with its affiliates and subsidiaries collectively referred herein as Dole of which Dole SA is a subsidiary.
"**binding corporate rules**": means personal information processing policies which are adhered to by Dole SA when transferring personal information to a business;
"**data subject**": means the person to whom personal information relates and for the purposes of Dole SA, this will include - employees, suppliers, customers, external service suppliers, all associates of Dole SA and divisions that form part of the Dole SA group.
"**Dole SA**": for purposes of this Policy document means the entire group of companies within the DOLE AFRICA HOLDINGS GROUP i.e. DOLE AFRICA HOLDINGS (PTY) LTD (Registration number 2019/104800/07) and incompasses its subsidiaries: - Dole Africa (Pty) Ltd (Registration number 2004/032448/07); Dole South Africa (Pty) Ltd (Registration number 1997/020817/07); Rekopane Estates (Pty) Ltd (Registration number 2005/011418/07); Fruitcare Services (Pty) Ltd (Registration number 1999/002892/07).
"**Dole Global IT Policies**": which means the global IT policies applicable to all affiliates and subsidiaries of Dole Food Company Inc and to which Dole SA subscribes and includes: Dole Global IT: Email & IM Policy; Dole Global IT: Mobile device Policy; Dole Global IT: IT Network and Information Transfer Policy; Dole Global IT: Physical Security Policy; Dole Global policy: HR25 - Code of Conduct.
"**Inventory of Document Control**": means an inventory as part of the QMS procedure 00004/TQM of all information and documents collected, processed and the time periods for which these will be retained before disposed and the level of access to such documents and information.
"**direct marketing**": means to approach a data subject, either in person or by mail or electronic communication, for the direct or indirect purpose of – a) Promoting or offering to supply, in the ordinary course of business, any goods or service to the data subject; or b) Requesting the data subject to make a donation of any kind for any reason. "electronic communication": means any text, voice, sound or image message sent over an electronic communications network which is stored in the network or in the recipient's terminal equipment until it is collected by the recipient;
"**filing system**": means any structured set of personal information, whether centralised, decentralised or dispersed on a functional or geographical basis, which is accessible according to specific criteria;
"**GDPR**": means The General Data Protection Regulation 2016/679 which is a regulation in EU law on data protection and privacy in the European Union and the European Economic Area. It also addresses the transfer of personal data outside the EU and EEA areas and it imposes obligations onto organizations anywhere, if they target or collect data related to personal information from individuals in the EU. The regulation was put into effect on May 25, 2018.
"**Information officer**": of, or in relation to, a – a) Public body means an information officer or deputy information officer as contemplated in terms of Section 1 or 17 of this Act; or b) Private body means the head of a private body as contemplated in Section 1 of the Promotion of Access to Information Act.
"**person**": means a natural person or a juristic person;
"**Personal information**": means information relating to an identifiable, living, natural person, and where it is applicable, an identifiable, existing juristic person, including, but not limited to: Information relating to the education or the medical, financial, criminal or employment history of the person; Any identifying number, symbol, e-mail address, telephone number, location information, online identifier or other particular assignment to the person; The biometric information of the person; The personal opinions, views or preferences of the person; Correspondence sent by the person that would reveal the contents of the original correspondence if the message is of a personal or confidential nature; The views or opinions of another individual about the person; and The name of the person if it appears with other personal information relating to the person or if the disclosure of the name itself would reveal information about the person;
"**private body**": means – a) A natural person who carries or has carried on any business or profession, but only in such capacity; b) A partnership which carries or has carried on any trade, business or profession; or c) Any former or existing juristic person, but excludes a public body;
"**processing**": means any operation or activity or any set of operations, whether or not by automatic means, concerning personal information, including – a) The collection, receipt, recording, organisation, collation, storage, updating or modification, retrieval, alteration, consultation or use; b) Dissemination by means of transmission, distribution or making available in any other form; or c) Merging, linking, as well as restriction, degradation, erasure or destruction of information;
"**Promotion of Access to Information Act**": means the Promotion of Access to Information Act (PAIA), 2000 (Act No. 2 of 2000);
"**public body**": means – a) Any department of state or administration in the national or provincial sphere of government or any municipality in the local sphere of government; or b) Any other functionary or institution when – I. Exercising a power or performing a duty in terms of the Constitution or provincial constitution; or II. Exercising a public power or performing a public function in terms of any legislation.

"public record": means a record that is accessible in the public domain and which is in the possession of or under the control of a public body, whether or not it was created by that public body.
"**record**": means any recorded information – a) Regardless of form or medium, including any of the following: I. Writing on any material; II. Information produced, recorded or stored by means of any tape-recorder, computer equipment, whether hardware or software or both, or other device, and any material subsequently derived from information so produced, recorded or stored; III. Label, marking or other writing that identifies or describes anything of which it forms part, or to which it is attached by any means; IV. Book, map, plan, graph, or drawing; V. Photograph, film, negative, tape or other device in which one or more visuals images are embodied so as to be capable, with or without the aid of some other equipment, of being reproduced; b) In the possession or under the control of a responsible party; and c) Regardless of when it came into existence;
"**Regulator**": – means the Information Regulator established in terms of Section 39 of the POPIA;
"**re-identify**": in relation to personal information of a data subject, means to resurrect any information that has been de-identified, that – a) Identifies the data subject; b) Can be used or manipulated by a reasonably foreseeable method to identify the data subject; or c) Can be linked by a reasonably foreseeable method to other information that identifies the data subject, and 're-identified" has a corresponding meaning;
"**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;
"**restriction**": means to withhold from circulation, use or publication any personal information that forms part of a filing system, but not to delete or destroy such information;
"**special personal information**": means personal information as referred to in Section 26 of the POPIA which includes Information relating to the race, gender, sex, pregnancy, marital status, national, ethnic or social origin, colour, sexual orientation, age, physical or mental health, well-being, disability, religion, conscience, belief, culture, language and birth of the person;
"**this Act**": means the Protection of Personal Information Act, No. 4 of 2013.
"**unique identifier**": means any identifier that is assigned to a data subject and is used by a responsible party for the purposes of the operations of that responsible party and that uniquely identifies that data subject in relation to that responsible party.

3. INTRODUCTION

Dole South Africa (Dole SA) is an international exporter, producer and marketer of fresh fruit and acts as an agent between the supplier (grower) and receiver (market). It acknowledges that in its daily business operations, the majority of its communications are conducted electronically via the internet and that personal information is collected and processed electronically in compliance with the Electronic Communications and Transaction Act 25 of 2002. In recognizing the international risk of data breach and also to ensure that lawful conditions exist surrounding its data subject's information, Dole SA accepts that all its South African based data subjects' Constitutional Right to Privacy is of utmost importance. Dole SA further accepts that its data subjects based in other parts of the world are entitled to equal rights to privacy in terms of Regulations applicable to such data subjects in the countries in which they are based. As such, Dole SA is committed to comply with South Africa's POPIA and the European GDPR in as far as data subjects situated in the European Union are concerned. Dole SA is further committed to the education of its data subjects in respect of their rights to privacy and will make all operational amendments necessary.

4. OBJECTIVE

The objective of this Policy is to ensure adherence to the provisions within POPIA together with its Regulations aimed at protecting all Dole SA's data subjects from harm by protecting their personal information, to stop identity fraud and generally to protect privacy. This Policy is the EXTERNAL SET OF PRIVACY RULES and sets out the standard for suitable protection of personal information as required by POPIA.

5. POPIA CORE PRINCIPLES

In its quest to ensure the protection of data subjects' privacy, Dole SA fully commits as follows:

5.1. To continue developing and maintaining reasonable protective measures against the possibility of risks such as loss, unauthorised access, destruction, use, alteration or revelation of personal information.

5.2. To regulate the manner in which personal information may be processed, by establishing conditions, in harmony with international standards, that prescribe the minimum threshold requirements for the lawful processing of personal information;

5.3. To ensure that the requirements of the POPIA legislation are upheld within the organisation. In terms of sections 8, 17 and 18 of POPIA, Dole SA confirms that it adheres to an approach of transparency of operational procedures that controls collection and processing of personal information and subscribe to a process of accountability and openness throughout its operation.

5.4. In terms of the requirements set out within sections 9, 10, 11, 12, 13 14 and 15 of POPIA, Dole SA undertakes to collect personal information in a legal and reasonable way, for a specific reason and only if it is necessary for operations and to process the personal information obtained from data subjects only for the purpose for which it was obtained in the first place. In the event that personal information is collected and shared for purposes not originally intended, Dole SA undertakes to obtain the PRIOR APPROVAL of the Information Regulator, if the data subject's consent is not obtained.

5.5. Processing of personal information obtained from customers will not be undertaken in an insensitive, derogative discriminatory or wrongful way that can intrude on the privacy of the customer.

5.6. In terms of the provisions contained within sections 23 to 25 of POPIA, all data subjects of Dole SA will be allowed to request access to certain personal information and may also request correction or deletion of personal information within the specifications of the POPIA.

5.7. To not request or process information related to race, religion, medical situation, political preference, trade union membership, sexual certitude or criminal record unless this is lawfully required and unless the data subject has expressly consented. Dole SA will also not process information of juveniles.

5.8. In terms of the provisions contained within section 16 of POPIA, Dole SA is committed that data subjects' information is recorded and retained accurately.

5.9. To keep effective record of personal information and undertakes not to retain information for a period longer than specified in the QMS document 00004/TQM. Information will be disposed at the end of the retention period.

5.10. In terms of sections 19 to 22 of POPIA, Dole SA will secure the integrity and confidentiality of personal information in its possession. Dole SA will provide the necessary security of data and keep it in accordance with prescribed legislation.

5.11. To comply with any restrictions and requirements that applies to the transborder Information Flow Policy contained in Dole SA's GDPR Policy Document.

6. CONSENT

If data subjects' information is collected, processed or shared for any other reason than the original reason of it being collected, the specific Consent for such purpose must be obtained from the data subject. If SPECIAL PERSONAL INFORMATION is collected, processed and stored for any reason from any of Dole SA's data subjects, specific Consent for such collection must first be obtained

The prohibition on collection and processing of special personal information does not apply if:-

6.1. Processing is carried out with the consent of the data subject;

6.2. Processing is necessary for the establishment, exercise or defense of a right or obligation in law;

6.3. Processing is for historical, statistical or research purposes.

7. COLLECTION AND PROCESSING OF INFORMATION

Dole SA collects and processes personal information from its data subjects for a variety of reasons and in a variety of ways. The primary way of collection and processing of personal information is electronically.
By submitting personal and special personal information details to Dole SA, all data subjects acknowledge the terms of this Policy.

7.1. Personal information collected by Dole SA will be collected directly from the data subject, unless –

7.1.1. The information is contained or derived from a public record or has deliberately been made public by the data subject;

7.1.2. The data subject or a competent person representing the data subject consents;

7.1.3. Collection of the information from another source would not prejudice a legitimate interest of the data subject;

7.1.4. Collection of the information from another source is necessary -

7.1.4.1. To avoid prejudice to the maintenance of the law by any public body, including the prevention, detection, investigation, prosecution, and punishment of offences;

7.1.4.2. To comply with an obligation imposed by law or to enforce legislation concerning the collection of revenue;

7.1.4.3. For the conduct of proceedings in any court or tribunal that have commenced or are reasonably contemplated;

7.1.4.4. In the interest of national security;

7.1.4.5. To maintain the legitimate interests of Dole SA or of a third party to whom the information is supplied;

7.1.4.6. Compliance would prejudice a lawful purpose of the collection;

7.1.4.7. Compliance is not reasonably practicable in the circumstances of the particular case.

7.1.5. Personal information is collected for a specific, explicitly defined, and lawful purpose related to a function or activity of Dole SA;

7.2. Steps will be taken to ensure that the data subject is aware of the purpose of the collection of the information.

7.3. Dole SA will take reasonably practicable steps to ensure that the personal information is complete, accurate, not misleading and updated where necessary, having regard to the purpose for which the personal information is collected and further processed.

7.4. Where personal information is collected form a data subject directly, Dole SA will take reasonably practicable steps to ensure that the data subject is aware of: -

7.4.1. The nature of the information being collected and where the information is not collected from the data subject, the source from which it is collected;

7.4.2. The name and address of Dole SA;

7.4.3. The purpose for which the information is being collected;

7.4.4. Whether or not the supply of the information by the data subject is voluntary or mandatory;

7.4.5. The consequences of failure to provide the information;

7.4.6. Any particular law authorising or requiring the collection of the information;

8. STORAGE OF INFORMATION

Dole SA acknowledges the risks facing data subjects with the storage of personal and special personal information on the Dole SA software systems and to ensure that its best attempts are made to minimize data subjects from suffering loss of personal information, misuse or unauthorised alteration of information, unauthorized access or disclosure of personal information generally, it will:

8.1. Store personal information in databases that have built-in safeguards and firewalls to ensure the privacy and confidentiality of your information.

8.2. Constantly monitor the latest internet developments to ensure that the systems evolve as required. Dole SA tests its systems regularly to ensure that our security mechanisms are up to date.

8.3. Continue to review its internal policies and third party agreements where necessary to ensure that these are also complying with the POPIA and Regulations in line with Dole SA's Policy rules.

9. DISPOSAL OF DATA SUBJECTS' INFORMATION

Dole SA is responsible for ensuring that the necessary records and documents of their data subjects are adequately protected and maintained to ensure that records that are no longer needed or are of no value and are disposed of at the appropriate time.

These rules apply to all documents which are collected, processed or stored by Dole SA and include but are not limited to documents in paper and electronic format, for example, e-mail, web and text files, PDF documents etc.

Each department in Dole SA has compiled a POPIA Inventory of Document Control as part of the QMS procedure 00004/TQM. By compiling this Inventory, Dole SA's Management illustrates its commitment to sufficiently dispose of data subjects' information when appropriate. The key below illustrates the classification of the different sections within the 00004/TQM summary:

POPIA REQUIREMENTS	00004/TQM DETAILS
What is the reason for collecting the personal information?	Procedure name and number
Usage - How and Why it is processed?	Quality records generated
Identify any personal information?	Personal Information? (Yes/No)
What is the Sensitivity of the information?	Sensitivity? (High/Low)
What is the format of the information?	"Format - (electronic / paper)"
Where is the information stored?	Record location
Who the personal information is shared with?	Access to record?
Who will monitor this information?	"Responsibility (for ensuring accurate record keeping)"
Archiving of the information?	"Retention time (according to Dole record retention policy)"
Disposal of the Information?	Disposal Trigger
	Disposal (Way of disposal)

Dole SA's records of data subjects' personal information will be disposed of securely when no longer required. Secure disposal maintains data security and supports compliance with this Dole SA's policy and the QMS procedure 00004/TQM. Dole SA acknowledges that electronic devices and media can hold vast amounts of information, some of which can linger indefinitely.

9.1. In determining whether records of data subjects' personal information will be disposed, Dole SA will adhere to the rules set out in QMS procedure 00004/TQM

9.2. Under no circumstances will paper documents or removable media (CD's, DVD's, discs, etc.) containing personal or confidential information be simply binned or deposited in refuse tips (see Dole Global policy: HR25 - Code of Conduct).

9.3. Dole SA undertakes to ensure that all electrical waste, electronic equipment and data on disk drives be physically removed and destroyed in such a way that the data will by no means be able to be virtually retrievable.

9.4. Dole SA's employees will ensure that all paper documents that should be disposed of, be shredded locally within the department and then be recycled. Where local shredding is not possible, bulk quantities of restricted paper waste will be held in waste sacks. These will be collected and disposed of by an employee instructed to do so by the Information Officer.

9.5. In the event that a third party is used for data destruction purposes, the Information Officer will ensure that such third party will also comply with this policy and any other applicable legislation.

9.6. Dole SA may suspend the destruction of any record or document due to pending or reasonably foreseeable litigation, audits, government investigations or similar proceedings. Dole SA undertakes to notify employees of applicable documents where the destruction has been suspended to which they have access to.

9.7. The documentation and information listed below may not contain all the records and documents processed and in the possession of Dole SA and should merely be used as a guideline.

9.8. In the event that a document and/or information is no longer required to be stored in accordance with this policy and relevant legislation, it should be deleted and destroyed.

9.9. The Information Officer should be consulted where there is uncertainty regarding the retention and destruction of a document and/or information.

10. INTERNET AND CYBER TECHNOLOGY

(Governed by the internal rules contained in the Dole Global IT Policies)

10.1. Acceptable use of Dole SA's Internet Facilities and standard Anti-Virus rules

(in terms of Dole Global IT: Email & IM Policy and Technology Acceptable Use Policy AUP)

Dole SA adheres to the Global AUP for IT to minimize the risk of Dole SA's data subjects from harm caused by the misuse of its IT systems and its data. Misuse includes both deliberate and inadvertent actions.

The AUP describes the technology acceptable use of the Dole IT Systems, computer equipment, network and storage equipment and consolidates all global and local requirements and guidelines for the usage of IT equipment and networks and supersedes the local IT Policies in the business units about the usage of IT equipment.

The repercussions of misuse of Dole IT systems can be severe. Potential damage includes, but is not limited to, malware infection (e.g. computer viruses), legal and financial penalties for data leakage and lost productivity resulting from network downtime.

In order to ensure that Dole IT systems are not misused, everyone who uses Dole IT systems must meet the following five high-level IT Security requirements:

10.1.1. Information must be protected against any unauthorized access
10.1.2. Confidentiality of information must be assured
10.1.3. Integrity of information must be preserved
10.1.4. Availability of information for business processes must be maintained
10.1.5. Compliance with applicable laws and regulations to which Dole is subject must be ensured

Executive management is accountable for providing overall guidance and for setting the "tone at the top".

Business Unit management throughout the company are accountable for ensuring that their staff understand and comply with IT Governance documentation including policies, procedures, standards and guidelines.

All personnel with access to Dole information assets are accountable for understanding and complying with IT Governance documentation including policies, procedures, standards and guidelines. Every user is responsible for exercising good judgment regarding reasonable personal use. Should a user be unclear regarding any information security requirement he/she should speak to his/her manager or a Dole IT Security representative.

10.2. Dole SA's Ownership of Electronic files created

(in terms of Dole Global IT: IT Network and Information Transfer Policy)

The Dole IT Network and Information Transfer Policy set out the direction and use of personnel engaged in the implementation and support of information communication systems and the services delivered. It is intended to establish best practices to secure systems and services and to ensure the protection of information in all networks.

10.3. IT Access Control

(in terms of Dole Global IT: Email & IM Policy and Technology Acceptable Use Policy AUP)

The Access Control Policy is aimed to prevent unauthorized access to systems, services and information.

10.4. Dole SA's Email Rules

(in terms of Dole Global IT: Email & IM Policy)

Email and Instant Messaging (IM) systems are provided by Dole to employees and other authorized users to assist them in carrying out Dole's business. Email and IM allow users to communicate with one another internally as well as with outside individuals and companies via the Internet. Given that email and IM may contain extremely sensitive and confidential Dole information, the information involved must be appropriately protected. In addition, email and IM are potentially sources of spam, social engineering attacks and malware, so Dole must be protected as completely as possible from these threats.

Finally, the misuse of email and IM can post many legal, privacy and security risks, so it is important for users to be aware of the appropriate use of electronic communications.

The purpose of this Email and IM policy is to ensure that information sent or received via these Dole IT systems is appropriately protected, that these systems do not introduce undue security risks to Dole and that users are made aware of what Dole deems as acceptable and unacceptable use of its email and IM.

10.5. Dole SA's Rules related to handheld devices

(in terms of Dole Global IT: Mobile device Policy)

Many users do not recognize that mobile devices represent a threat to IT and data security. As a result, they often do not apply the same level of security and data protection as they would on other devices such as desktop or laptop computers.

This policy outlines Dole's requirements for safeguarding the physical and data security of mobile devices such as smartphones, tablets, and other mobile devices that PC's and Notebooks.

10.6. Physical access control

(in terms of Dole Global IT: Physical Security)

Many of Dole's applications are hosted on equipment located in data centers on Dole premises. This policy is intended to specify the requirements which must be met in order to prevent unauthorized physical access, damage, theft, compromise, interruption or interference to Dole's information and information processing assets.

11. INFORMATION OFFICER

11.1. Appointed Information Officer:

CONTACT DETAILS	Information Officer
Email:	sias.fouche@dole.com
Postal Address:	P O Box 4220, Old Oak, Cape Town, 7537, South Africa
Street Address:	26 Bella Rosa Street; D'Urban Square, Rosenpark, Bellville, 7530, South Africa
Telephone Number:	+27 21 983 3600
Fax Number:	+27 21 983 3666

11.2. The general responsibilities of Dole SA's Information Officer will include the following:

11.2.1. The encouragement of compliance, by Dole SA, with the conditions for the lawful processing of personal information;

11.2.2. Managing requests made to Dole SA pursuant to POPIA;

11.2.3. Working with the Regulator in relation to investigations conducted pursuant to prior authorisation required to process certain information of POPIA in relation to the business.

11.2.4. Ensuring compliance by Dole SA with the provisions of POPIA. This is an ongoing responsibility that will include training of new staff and to update internal policies.

11.2.5. Continuously perform data backups, store at least weekly backup offsite, and test those backups regularly for data integrity and reliability.
11.2.6. Review policy rules at least every 3 years, document the results, and update the policy as needed.
11.2.7. Provide security awareness and disaster recovery education for employees involved.
11.2.8. Continuously update information security policies and network diagrams.
11.2.9. Secure critical applications and data by patching known vulnerabilities with the latest fixes or software updates.
11.2.10. Perform continuous computer vulnerability assessments and audits

11.3. **The data breach responsibilities of Dole SA's Information Officer will include the following:**
11.3.1. Ascertain whether personal data was breached
11.3.2. Assess the scope and impact by referring to the following:
11.3.2.1. Estimated number of data subjects whose personal data was possibly breached
11.3.2.2. Determine the possible types of personal data that were breached
11.3.2.3. List security measures that were already in place to prevent the breach from happening.
11.3.3. Once the risk of the breach is determined, the following parties need to be notified within 72 hours after being discovered:
11.3.3.1. The Information Regulator
11.3.3.2. If the risk to the rights and freedoms of data subjects is high only, the Communications Manager should be involved in all communication to inform the data subjects
11.3.3.3. Communication should include the following:
- Contact details of Information Officer
- Details of the breach,
- Likely impact,
- Actions already in place, and those being initiated to minimise the impact of the data breach.
- Any further impact is being investigated (if required), and necessary actions to mitigate the impact are being taken.

11.3.4. Review and monitor
11.3.4.1. Once the personal data breach has been contained, Dole SA will conduct a review of existing measures in place, and explore the possible ways in which these measures can be strengthened to prevent a similar breach from reoccurring.
11.3.4.2. All such identified measures should be monitored to ensure that the measures are satisfactorily implemented.
11.3.4.3. The Information Officer need to log all actions and keep a Data Breach Register and to be reported to the Social & Ethics Committee.

12. AVAILABILITY AND REVISION

A link to this Policy is available on the Dole SA company website http://www.dolesa.co.za. A copy of this policy, the GDPR Policy, QMS procedure 00004/TQM and all Dole Global IT Policies are available on request from Information Officer or Communications Manager and saved on the Dole SA's Quality Management System.

CONTACT DETAILS	Communications Manager	Information Officer
Email:	dolecpt@dole.com	sias.fouche@dole.com
Postal Address:	P O Box 4220, Old Oak, Cape Town, 7537, South Africa	
Street Address:	26 Bella Rosa Street; D'Urban Square, Rosenpark, Bellville, 7530, South Africa	
Telephone Number:	+27 21 983 3600	
Fax Number:	+27 21 983 3666	

This policy will be updated regularly to comply with legislation, thereby ensuring that personal information will be secure.

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]

Note:

1. *Affidavits or other documentary evidence as applicable in support of the objection may be attached.*
2. *If the space provided for in this Form is inadequate, submit information as an Annexure to this Form and sign each page.*
3. *Complete as is applicable.*

A - DETAILS OF DATA SUBJECT	
Name(s) and surname/ registered name of data subject:	
Unique Identifier/ Identity Number	
Residential, postal or business address:	
	Code ( )
Contact number(s):	
Fax number / E-mail address:	
B - DETAILS OF RESPONSIBLE PARTY	
Name(s) and surname/ Registered name of responsible party:	
Residential, postal or business address:	
	Code ( )
Contact number(s):	
Fax number/ E-mail address:	
C - REASONS FOR OBJECTION IN TERMS OF SECTION 11(1)(d) to (f) (Please provide detailed reasons for the objection)	

Signed at ..... this ..... day of .....20.....

..... *Signature of data subject/designated person*

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]

Note:

1. *Affidavits or other documentary evidence as applicable in support of the request may be attached.*
2. *If the space provided for in this Form is inadequate, submit information as an Annexure to this Form and sign each page.*
3. *Complete as is applicable.*

Mark the appropriate box with an "x".

Request for:

☐ Correction or deletion of the personal information about the data subject which is in possession or under the control of the responsible party.

☐ Destroying or deletion of a record of personal information about the data subject which is in possession or under the control of the responsible party and who is no longer authorised to retain the record of information.

A - DETAILS OF THE DATA SUBJECT	
Name(s) and surname / registered name of data subject:	
Unique identifier/ Identity Number:	
Residential, postal or business address:	
	Code ( )
Contact number(s):	
Fax number/E-mail address:	
B - DETAILS OF RESPONSIBLE PARTY	
Name(s) and surname / registered name of responsible party:	
Residential, postal or business address:	
	Code ( )
Contact number(s):	
Fax number/ E-mail address:	
C - INFORMATION TO BE CORRECTED/DELETED/ DESTRUCTED/ DESTROYED	
D - REASONS FOR *CORRECTION OR DELETION OF THE PERSONAL INFORMATION ABOUT THE DATA SUBJECT IN TERMS OF SECTION 24(1)(a) WHICH IS IN POSSESSION OR UNDER THE CONTROL OF THE RESPONSIBLE PARTY ; and or REASONS FOR *DESTRUCTION OR DELETION OF A RECORD OF PERSONAL INFORMATION ABOUT THE DATA SUBJECT IN TERMS OF SECTION 24(1)(b) WHICH THE RESPONSIBLE PARTY IS NO LONGER AUTHORISED TO RETAIN. (Please provide detailed reasons for the request)	

Signed at ..... this ..... day of .....20.....

..... *Signature of data subject/designated person*

FORM 3

APPLICATION FOR THE ISSUE OF A CODE OF CONDUCT IN TERMS OF SECTION 61(1)(B) OF THE PROTECTION OF PERSONAL INFORMATION ACT, 2013 (ACT NO. 4 OF 2013)

NOT APPLICABLE TO THIS POLICY

FORM 4

APPLICATION FOR THE CONSENT OF A DATA SUBJECT FOR THE PROCESSING OF PERSONAL INFORMATION FOR THE PURPOSE OF DIRECT MARKETING IN TERMS OF SECTION 69(2) OF THE PROTECTION OF PERSONAL INFORMATION ACT, 2013 (ACT NO. 4 OF 2013)

REGULATIONS RELATING TO THE PROTECTION OF PERSONAL INFORMATION, 2018
[Regulation 6]

PART A

TO: _____

_____

_____

(Name of data subject)

FROM: _____

_____

Contact number(s): _____

Fax number: _____

E-mail address: _____

(Name, address and contact details of responsible party)

Full names and designation of person signing on behalf of responsible party:

_____

.....

Signature of designated person

Date: _____

PART B

I, _____ (full names of data subject) hereby:

☐ Consent to

Receive direct marketing of goods or services to be marketed by means of electronic communication.

SPECIFY GOODS or SERVICES: _____

SPECIFY METHOD OF COMMUNICATION:

FAX:

E - MAIL:

SMS:

OTHERS – SPECIFY:

Signed at ..... this ..... day of .....20.....

.....

Signature of data subject