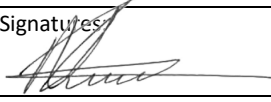


POLICY APPROVED BY (COMMITTEE/...)	M. Lucas	Signatures: 
DATE APPROVED:	1 July 2021	
POLICY VERSION:	1	
UPDATES / AMENDMENTS	Version: Approved by:	Signatures:
UPDATES / AMENDMENTS	Version: Approved by:	

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

Werkomed is a medical supply organization supplying medical goods and services to the medical industry in South Africa and into the African continent.

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.

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.

3. DEFINITIONS

Head Office

Unit A1, 5 Galaxy Avenue,
Linbro Business Park,
Linbro, Johannesburg
South Africa

P.O. Box 5922
Rivonia
2128

Tel: + 27 11 608 4224
Fax: + 27 11 608 4227

www.werkomed.com

- 3.1. **“Applicable Legislation”** means all legislation and data protection legislation applicable to the Company including the POPIA and Promotion of Access to Information Act 02 of 2002, (“PAIA”), 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 clause 7 of 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), temporarily, or on a fixed-term contract, and include contractors that may come into contact with, use, process or otherwise deal with Personal Information.
- 3.4. **“Office-bearer”** means the members of the Board, the General Manager, members of Committees of the Board.
- 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
 - 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 Act and Regulations thereto.
- 3.8. **“Processing”** means any operation or activity or any set of operations, whether or not by automatic means,

Head Office concerning personal information, including:

- 3.8.1. the collection, receipt, recording, organisation, collation, storage, updating or modification, retrieval, alteration, consultation or use;
 - 3.8.2. dissemination by means of transmission, distribution or making available in ⁽¹¹⁾_(SEP) any other form; or
 - 3.8.3. merging, linking, as well as restriction, degradation, erasure or destruction of ⁽¹¹⁾_(SEP) information.
- 3.9. **“Purpose”** means The Company’s purpose to processing of Personal Information as set out under The Company’s PAIA Manual.
- 3.10. **“Responsible Party”** means, for the purpose of this Policy, the Company, 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.
- 3.11. **“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. **THE COMPANY REQUIREMENTS FOR PROCESSING PERSONAL INFORMATION: CONSENT OR NOTIFICATION**

All Processing of Personal Information must be done:

- 4.1. After a written and signed consent in a form developed and approved form by the Company, has been received from the Data Subject.
- 4.2. Where there is a legal requirement to disclose Personal Information for example to authorities, operators, etc., the Data Subject must still be notified of such disclosure, unless the Applicable Law provides otherwise.

5. **NOTIFICATIONS**

- 5.1. The Company will inform all persons whose information is being processed, of that fact.
- 5.2. 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.
- 5.3. The rights of Data Subjects are as follows:
 - 5.3.1. 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;
 - 5.3.2. Notified if there has been unlawful access or acquisition of his/her/its personal information;
 - 5.3.3. Request a record of your Personal Information;
 - 5.3.4. Request the correction, deletion and/or destruction of your Personal Information;
 - 5.3.5. Object to the processing of your Personal Information;
 - 5.3.6. Exercise the right to withdraw the consent to processing, if voluntarily given;
 - 5.3.7. 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;
 - 5.3.8. Not to be subjected to automated decision-making based on the personal information in contravention of section

71, POPI Act;

Head Office

Unit A1, 5 Galaxy Avenue,
Linbro Business Park,
Linbro, Johannesburg
South Africa

P.O. Box 5922
Rivonia
2128

Tel: + 27 11 608 4224
Fax: + 27 11 608 4227

www.werkomed.com

- 5.3.9. Submit a complaint to the Information Regulator at <http://www.justice.gov.za/infoereg/index.html>; and
- 5.3.10. Institute civil proceedings regarding an alleged interference with his/her/its personal information in terms of section 99, POPI Act.
- 5.4. The details of the Information Officer, or the responsible Deputy Information Officer will also be included in all Notifications, and also appear on the Company's PAIA Manual / PAIA Guide.

6. **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:

- 6.1. 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.
- 6.2. 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).
- 6.3. 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.
- 6.4. 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.
- 6.5. Personal Information must be **collected directly from the Data Subject**, should there be a need to collect the information from another source, the consent of the Data Subject must be obtained prior thereto. Where databases are bought or provided by a third party, a **warranty** must be included in the contract that such database have been compiled and is sold in compliance with POPIA.
- 6.6. Only up to date and correct Personal Information can be processed, and Data Subjects must 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.

Head Office

Unit A1, 5 Galaxy Avenue,
Linbro Business Park,
Linbro, Johannesburg
South Africa

P.O. Box 5922
Rivonia
2128

Tel: + 27 11 608 4224
Fax: + 27 11 608 4227

www.werkomed.com

6.7. 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:

6.7.1. **Unauthorised access**, which means that access privileges must be stipulated, and where applicable, indicated in documents, minutes, etc. as follows (just add applicable row or rows in a header or footer of a document):

Accessible by: Public
Board / ... and administrative staff authorized to work with such structure(s)
Committee [insert] & administrative staff authorized to work with such structure(s)
All Company stakeholders
Top management & administrative staff authorized to work with such structure(s)
Designated employees
All employees
Consultant / contractor / vendor / supplier
Other:

6.7.2. **Loss and/or damage of personal information**, through regular back-ups maintained remotely, all company devices which have access to data are appropriately labelled. All electronic goods have IT security systems in place to limit document corruptions.

6.7.3. **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 on site at the company premises.

6.8. 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 Deputy will be sought. Even casual provision of contact details to a third party could constitute a breach of the POPI Act.

6.9. Only relevant Personal Information required for the specified purpose should be collected - nothing in excess of that. The data fields (see definition of "personal information" and "special personal 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:

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

6.9.2. Relevant for that purpose.

Red flag data fields are titles (relevant for communication, but not necessarily for the exercising rights), family relation (not relevant 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 what the Data Subject has consented to and what is relevant for that database should be kept), etc. The physical address of a director is necessary, but the address of a payments clerk at a customer or vendor is not required.

Head Office

Unit A1, 5 Galaxy Avenue,
Linbro Business Park,
Linbro, Johannesburg
South Africa

P.O. Box 5922
Rivonia
2128

Tel: + 27 11 608 4224
Fax: + 27 11 608 4227

www.werkomed.com

- 6.10. 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.
- 6.11. 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.
- 6.12. The Data Subject must be provided access to their Personal Information related upon written request and other request 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.
- 6.13. 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 or contract obliged to continue with such processing. Such requests must be made to the Company on **Form 1** of the POPI Regulations.
- 6.14. Personal Information must be corrected or deleted upon request contained in **Form 2** by the Data Subject to do so. The Company must take measures to also verify the correctness and accuracy of Personal Information in order to ensure that it is not misleading.

7. SECURITY AND ACCESS

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

Electronic records are kept on Shared Drives and Cloud Storage Systems as well as Office Computers which are Password Protected and Regularly Updated. Office Computers are also encrypted using industry recognised encryption software. The Storage of information is in line with international Data storage standards and Practices. Data Stored on the server is Backed up to a Cloud Backup system and Protected with 256bit encryption to protect both private and financial data. Records are secured by an industry recognized Firewall which prevents direct access to the network and data.

- 7.1. Electronic information on shared drives operates on access control and permissions, accidental access must be reported to the Information Officer and IT immediately. The company uses servers and systems that are not based on South Africa for some of the personal information we process, such as Microsoft OneDrive and SharePoint.

- 7.2. No information, including personal information, may be downloaded from shared drives onto device hard drives or any external device.

Head Office

- 7.3. Physical records are kept as follows:
- 7.3.1. Any/All physical records files are kept in locked filing cabinets, in a locked office. The office has 24 hour security, an alarm system, and security cameras.
- 7.4. There are security cameras installed at the premises, 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.
- 7.5. The office building is accessed through a sign-in system with security personnel and a boom gate which is locked at night. The security company act as an Operator and an Operator agreement is in place, ensuring that no personal information provided is stored for longer than necessary and are 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 landlord* to the managing agent.
- 7.6. Regular verification that the safeguards in place are effectively implemented and continually updated in response to any new risks or deficiencies;
- 7.7. The Company has an obligation to notify the Information Regulator and affected Data Subjects in writing, should the Personal Information relating to the Data Subject be compromised or should there be a suspicion that the Personal Information is compromised. All security and access breaches or suspected or potential breaches of Personal Information, including loss of Company devices or devices used for work purposes, must be reported to the Information Officer or hi/her designated Deputy immediately after such breach or potential breach becomes known.
8. **TRANSBORDER DATA TRANSFER**
- 8.1. We use servers and systems such as such as Microsoft OneDrive and SharePoint that are not based on South Africa for some of the personal information we process, such as business service contracts, and consultant services if required.
- 8.2. In these circumstances, we have the following in place, as is required by the POPI Act:
- 8.2.1. An agreement between the South African entity and the overseas entity that the personal information of South African citizens will be handled in line with the POPI Act;
- 8.2.2. Notifications to third parties whose information are stored on overseas services, but only used for purposes to effect business transactions in South Africa, such as payment of invoices;
- 8.2.3. Consents for third parties whose information will be used by an overseas entity who form part of our group, such as that of Key Opinion Leaders or patient support programmes;

Head Office

Unit A1, 5 Galaxy Avenue,
Linbro Business Park,
Linbro, Johannesburg
South Africa

P.O. Box 5922
Rivonia
2128

Tel: + 27 11 608 4224
Fax: + 27 11 608 4227

www.werkomed.com

- 8.2.4. Our email- and financial systems are centrally (globally) hosted and are subject to the company's global policies in relation to privacy / confidentiality and security;

9. RETENTION, STORAGE AND DESTRUCTION

- 9.1. 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.
- 9.2. 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.
- 9.3. Once the purpose for Processing or the retention period has lapsed, or provided under Applicable Legislation expires, the Personal Information must be destroyed 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.
- 9.4. Retention periods, and the destruction of personal information, must be specified in consents and notifications.

10. COLLECTION OF PERSONAL INFORMATION

The Company collects Personal Information from various Data Subjects for varying purposes, but only from its customers, its contractors and industry associates / stakeholders. Such information must be collected in accordance with the provisions of the Act and this policy.

11. PURPOSE AND USE OF PERSONAL INFORMATION

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

- 11.1. 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.
- 11.2. Identify and record the **types of processing** that take place (e.g., collection, collation, manipulation, dissemination and destruction, or collection, recording and storage, etc.).
- 11.3. 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).
- 11.4. 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:
- 11.4.1. the purpose of the Processing or further processing of the Personal Information;
 - 11.4.2. the type of Processing of the Personal Information;
 - 11.4.3. timelines related to the Processing;
 - 11.4.4. the destruction or storage of the personal information; and
 - 11.4.5. the security assurances and measures undertaken by The Company to protect the data and Personal Information.
- 11.5. If processing is mandated by law, describe in a notification what that specific law says, and how processing will take place.

Head Office

11.6. Personal Information about children and special personal information

11.6.1. The Company does hold the personal information of children (persons up till the age of 18) as it relates to surgical procedures as required.

11.6.2. The information of children under the age of 12, or 12 and under 18 years of age, must be processed in terms of the Children's Act, 2005, and the healthcare information according to the HPCSA Ethical Rules and the Medicines and Related Substances Act, 1965.

11.6.3. 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 POPIA.

12. REVIEW AND AMENDMENT

This policy shall be reviewed every 2 (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.

13. TRAINING AND COMMUNICATION

At least 1 (one) a year, training on this Policy, the POPIA, PAIA and how to Process Personal Information in a lawful manner.

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.

14. COMPLIANCE

14.1. The Information Officer, shall maintain a report in relation to POPI and PAIA regarding:

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

- 14.2.1. Reworking of consents, standard clauses and notifications.
- 14.2.2. Reporting loss, breach and/or unauthorized access of Personal Information to relevant authorities, recommending disciplinary action, etc.
- 14.2.3. The destruction of personal information.
- 14.2.4. The de-identification of personal information.
- 14.2.5. The implementation of specific security measures.
- 14.2.6. The implementation of (additional or new) access control measures.
- 14.2.7. The implementation of consents or notifications *ab initio*.
- 14.2.8. Research and verification of legislative mandates.

Head Office

Unit A1, 5 Galaxy Avenue,
Linbro Business Park,
Linbro, Johannesburg
South Africa

P.O. Box 5922
Rivonia
2128

Tel: + 27 11 608 4224
Fax: + 27 11 608 4227

www.werkomed.com

- 14.2.9. Addenda to contracts and service level agreements within business activities and/or with third parties and contractors.
- 14.2.10. Amendments to contract templates.
- 14.2.11. Disciplinary action against employees violating this policy.
- 14.2.12. Action against office bearers violating this policy, in conjunction with the Board of Trustees.
- 14.2.13. Requirements on the submission of (regular) progress reports.
- 14.2.14. Obtaining expert assistance, where required.
- 14.2.15. Undergoing additional or further training on POPI and PAIA.

15. INFORMATION OFFICE

- 15.1. This office houses the Information Officer and his/her deputies: *Unit A1, 5 Galaxy Avenue, Linbro Business Park, Johannesburg*
- 15.2. The following may be directed to the Information Officer in writing to monica@werkomed.com.

16. COMPLAINTS

Any complaints by any person including, 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 Information Officer], 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 Company, when doing so.

The Information Office comprises a Data Governance Council to investigate the matter, and to make findings on the complaint, and recommend action by the relevant departments, units or structures of the Company.

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

- 17.1. Any person can object to processing of Personal Information, withdraw a consent to processing, requests amend or deletion of personal Information.
- 17.2. Anyone who wished to object to, 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.

18. Non-Compliance

- 18.1. Employees who fail to comply with this policy will be considered in violation of the relevant Company codes of conduct and may be subject to disciplinary action or to legal action if laws have been violated. In less serious cases, failure to comply with this policy could result in denial of access to data.

19. INSPECTIONS BY THE REGULATOR

Head Office

Unit A1, 5 Galaxy Avenue,
Linbro Business Park,
Linbro, Johannesburg
South Africa

P.O. Box 5922
Rivonia
2128

Tel: + 27 11 608 4224
Fax: + 27 11 608 4227

www.werkomed.com

19.1. 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.

20. **EFFECTIVE DATE**

20.1. This Policy is in effect from [insert date], with consideration of the fact that the POPIA will be in full force and effect from 1 July 2021.

... Forms follow on next page

Head Office

Unit A1, 5 Galaxy Avenue,
Linbro Business Park,
Linbro, Johannesburg
South Africa

P.O. Box 5922
Rivonia
2128

Tel: + 27 11 608 4224
Fax: + 27 11 608 4227

www.werkomed.com

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 ()

Head Office

Unit A1, 5 Galaxy Avenue,
Linbro Business Park,
Linbro, Johannesburg
South Africa

P.O. Box 5922
Rivonia
2128

Tel: + 27 11 608 4224
Fax: + 27 11 608 4227

www.werkomed.com

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 _____ 2 .

SIGNATURE OF DATA SUBJECT/DESIGNATED PERSON

Head Office

Unit A1, 5 Galaxy Avenue,
 Linbro Business Park,
 Linbro, Johannesburg
 South Africa

P.O. Box 5922
 Rivonia
 2128

Tel: + 27 11 608 4224
 Fax: + 27 11 608 4227

www.werkomed.com

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.]

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**

37.1

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 ()

Head Office

Unit A1, 5 Galaxy Avenue,
Linbro Business Park,
Linbro, Johannesburg
South Africa

P.O. Box 5922
Rivonia
2128

Tel: + 27 11 608 4224
Fax: + 27 11 608 4227

www.werkomed.com

CONTACT NUMBER(S):	
FAX NUMBER/ E-MAIL ADDRESS:	
C	INFORMATION TO BE CORRECTED/DELETED/ DESTROYED/ 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)

Head Office

Unit A1, 5 Galaxy Avenue,
 Linbro Business Park,
 Linbro, Johannesburg
 South Africa

P.O. Box 5922
 Rivonia
 2128

Tel: + 27 11 608 4224
 Fax: + 27 11 608 4227

www.werkomed.com

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.]

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:

Give my 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 _____ on this _____ day of _____ 20____ .

Head Office

Unit A1, 5 Galaxy Avenue,
Linbro Business Park,
Linbro, Johannesburg
South Africa

P.O. Box 5922
Rivonia
2128

Tel: + 27 11 608 4224
Fax: + 27 11 608 4227

www.werkomed.com

Signature of data subject/designated person

Head Office

Unit A1, 5 Galaxy Avenue,
Linbro Business Park,
Linbro, Johannesburg
South Africa

P.O. Box 5922
Rivonia
2128

Tel: + 27 11 608 4224
Fax: + 27 11 608 4227

www.werkomed.com