Procedural Document number:	***Version number:*** V1.0
Title of Policy: Data Protection Policy	***Previous reference number:*** N/A
Author: Liza Strydom	***Title:*** *Compliance and Operations Manager Information Officer*
Reviewed by: Liza Strydom: Information Officer	***Approval date:*** 2021-06-01
	Effective date: 2021-06-01
Approved by: Prof. Oppel Greeff: CEO	Page 1 of 15

1. Purpose

The Data Protection Policy describes and outlines the commitment and methods that Medwell SA (Pty) Ltd and its affiliates will use to meet its legal obligations and requirements to ensure it complies with the **Protection of Personal Information Act, No. 4 of 2013**, *(referred to hereafter as the Act)* and the **Promotion of Access to Information Act, 2000 (Act No. 2 of 2000)** as amended by the Act.

2. Scope and responsibilities

This document applies to all Medwell directors, employees, sub-contractors, agents, and appointees in the Medwell group. The policy provisions are applicable to all functions where processing of personal information is necessary, whether at a Medwell office or off-site.

3. Policy Statement

Medwell SA commits itself to comply with legislation and to follow good practice when processing personal information and respect our client's rights in terms of the Act. We commit to train and enable our employees on how to correctly process personal data so that it supports our company vision of being the leader in providing high-quality, holistic, home healthcare and wellness solutions.

4. Key definitions and clarifications

- Act – the **Protections of Personal Information Act, No. 4 2013** and any regulations or applicable industry code of conduct under the Act.
- Consent – the voluntary, specific and informed expression of will.
- Data subject – the natural or juristic person to whom personal information relates, hereinafter called the 'Client'. Data subject includes employees of the Group.
- Direct marketing – approaching a data subject, in person or by any other form of communication by direct or indirect means to promote, offer to supply goods and services or requesting a donation.
- Group – Medwell SA (Pty) Ltd, Edna Medical Distributors, SGE Recruitment.

- Information Officer – as appointed by the Board in terms of Chapter 5, part B of the Act.
- Medwell employee – any member of staff, employed either in a permanent or temporary capacity.
- PAIA – the **Promotion of Access to Information Act, 2000 (Act No. 2 of 2000)**
- Personal information – information relating to an identifiable, living, natural person and an identifiable juristic person.
- Premises – any premises owned and/or rented and occupied and managed by Medwell and where business is conducted and/or services are delivered. Refers to an entire site, building or occupied floor in a building.
- Processing – any operation or activity or any set of operations, whether by automatic means or not, concerning personal information.
- Record – any recorded information regardless of form or medium.
- Regulator – the Information Regulator.
- Responsible party – Medwell SA and all entities in its group.
- Special Personal Information – religious or philosophical beliefs, race and ethnic origins, trade union membership, political persuasions, health and sex life, criminal behaviour, biometric information.

5. Related policies and protocols

5.1 Access to Information Policy (PAIA manual)
5.2 Electronic Data Security Policy
5.3 Retention and Confidentiality of Documents, Information and Electronic Transactions
5.4 Record Storage and Destruction Procedural Manual
5.5 Risk Management Policy
5.6 Incident Management Policy
5.7 Website Privacy Policy

6. Processing of Personal Information

6.1 <u>Rights of data subjects</u>

The Group commits to abide by section 5 of the Act by aligning its policies and procedures to reflect this commitment. In terms of the Act, our clients have the right to have his/her personal information processed in accordance with the conditions of lawful processing, including having the right to;

- be notified that personal information about him/her is being collected or
- accessed by unauthorised person/s,
- to establish whether the Group is holding personal information and to request access to it to correct, delete or destroy such information,

- to object on reasonable grounds to the processing of such information,
- to object to the processing of his/her personal information for direct marketing purposes,
- not to be subject to automated processing of his/her personal information intended to provide a profile,
- to submit a complaint to the Regulator,
- to institute civil proceedings.

6.2 Purpose of Processing

The Group will only collect and process information that is relevant, necessary, and adequate to enable it to render a service, process an enquiry or for any other need that may arise out of the natural course of conducting business and will be processed for that purpose only. The client will be informed as to the necessary information required and, on any information, deemed optional.

Additional processing purposes may include the following:

- Providing products and services and to carry out related transaction to fulfil the request;
- Processing accounts;
- Conduct credit reference searches or verification;
- Confirming, verifying and updating client details;
- Conducting market or client satisfaction research;
- Audit and record keeping purposes;
- Pertaining to legal proceedings;
- Provide communication in respect of healthcare legislation and/or requirements that may affect a product or service provided by us;
- To comply with any legal and regulatory requirements or when it is required by law.

6.3 Consent

In terms of Section 32(1)(a) of the Act, the Group is permitted to process special personal information relating to the client's health and sex life, as such processing is necessary for the proper treatment and care and for the administration of such care. This extends to the processing of personal information of children relating to their health and sex life.

Consent to process is obtained at introductory and contractual stage and the Group subjects to the prescribes of the National Health Act, Act 61 of 2003 and the guidelines of the Health Professions Council of South Africa.

In terms of section 33(2), the Group is permitted to process special personal information relating to the data subject's (employee) criminal behaviour and biometrical information, provided that such processing will be done in accordance with the rules established in compliance with labour legislation.

For the further processing of any other personal information and special personal information, the Group will attain voluntary, specific and informed consent from our clients for the lawful processing of personal information.

The Group will inform the client on the following:

- the type of information required,
- the purpose for which it is collected,
- whether the client is obliged to supply the information as prescribed by any law, or whether it is voluntary.
- the consequences of failure to provide information,
- whether it intends to transfer the information trans-border and the level of protection afforded by the recipient of the information.

The Group collects the following personal information:

Entity Type	**Personal Information | Special Personal Information Process**
Clients: Natural Persons	Names, contact details, physical and postal addresses, ID number, date of birth, nationality, gender, race, current and medical history information, banking details, electronic communication
Clients: Juristic Persons / Entities	Name of legal entity, physical and postal addresses, contact details, contact persons, financial information, banking details, registration number/s, trade references, shareholding information, authorised signatories, electronic communication
Contracted Service Providers and 3rd party Operators	Name of legal entity, physical and postal addresses, contact details, contact persons, financial information, registration number/s, trade references, shareholding information, authorised signatories, electronic communication
Directors / Employees	Names, contact details, physical and postal addresses, ID number, date of birth, nationality, gender, race, account details, employment history, education information, opinions, criminal records, well-being. Electronic communication
Website visitors	Technical information; data supplied through the use of cookies and activity data. Information supplied on electronic submission forms, subscription to online newsletter, survey, etc. Information from the data subject's visits to the Group's websites, including type of browser and operating system that the data subject uses, access times, pages viewed, URLs clicked on, IP address and pages visited before and after navigating the Group's websites.

6.4 Eight Lawful Processing Conditions

i. Accountability

The Group shall ensure that all the processing conditions are complied with when processing personal information. The Group accepts its responsibility for processing personal information from the time of the determination of the purpose and means of the processing and during the processing itself.

ii. Processing Limitation

In accordance with section 10 of the Act, personal information will be lawfully processed, is adequate, relevant and not excessive and meet the following conditions:

- the client's consent was obtained to collect and process at enquiry, introductory, appointment and needs analysis stage of the relationship,
- the client's consent was obtained to share personal information with a third party where such sharing of information is for the pursuit of conducting legitimate business with the client and/or for the conclusion or performance of a contract to which the client is party to,
- in terms of healthcare services and products, processing the necessary personal information to protect the legitimate interest of the potential and existing client and their representatives in order to provide applicable and beneficial products and services,
- processing the necessary personal information for pursuing the legitimate interests of the Group,
- or an Operator to whom information is supplied of which Operator needs certain personal information for conducting, criminal checks, credit checks or any due diligence checks on behalf of the Group.

iii. Purpose Specific

The Group shall only process personal information as set out in the conditions of point 6.2. Personal information shall not be retained any longer than is necessary for achieving the purpose for which the information was collected. Full details regarding retention and restrictions of records are outlined in the Group's *Record Storage and Destruction Procedural Manual* and *Retention and Confidentiality of Documents, Information and Electronic Transactions*.

iv. Further Processing Limitation.

Any further processing will be compatible and in accordance with the purpose for which it was collected. The Group will further process personal information given the following circumstances:

- the client has consented to further processing,
- personal information is within the public domain,
- personal information has been deliberately made public by the client,
- further processing is required and necessary to comply with any applicable law or to exercise a legal right,
- further processing is necessary to prevent or mitigate a threat to public health and safety, or the life or death of the client,
- the information is used for historical, statistical or research purposes only after de-identifying the data.

v. Information Quality

Reasonable steps will be taken to ensure client information is complete, accurate, not misleading and updated, where necessary. Periodic review of client information will be undertaken to ensure personal information is still valid and correct.

The relevant business function will ensure that personal information is dated when received, dated when changed and that irrelevant and outdated information is deleted or destroyed as per the *Record Storage and Destruction Procedural Manual*.

vi. Openness

In accordance with section 14 or 51 of the **Promotion of Access to Information Act**, and further to points 6.1, 6.3, 6.4(iv) and 6.5, the Group will take reasonable steps to ensure our clients are made aware of and notified when collecting personal information that:

- the information being collected from the client directly and if not directly, from which source,
- the names and addresses of the Group,
- the purpose for which the information is collected,
- the category or nature of the information being collected.

vii. Security Safeguarding

The Group will take appropriate, reasonable security measures to safeguard the integrity and confidentiality of personal information. The guidelines of the *Record Storage and Destruction Procedural Manual* and *Retention and Confidentiality of Documents, Information and Electronic Transactions Policies* must be adhered to. If a breach of data security event has occurred, the Information Officer will report the incident to the Regulator. The client will be notified by the Information Officer as soon as reasonably possible and in writing as per the prescribes of the Act.

- Written Records

Risks	**loss/damage of files, unlawful access**
Practical measures to ensure data security	clean desk policy and routine filing locked filing cabinets access control filing and archiving stores/rooms/cabinets delete/destroy information no longer required
Managing security measures	Report any breach to the Information Officer.

- Electronic Records

Risks	**loss/damage of laptops, cell phones, unlawful access, phishing**
Practical measures to ensure data security	PI to be saved on secure database no storage of PI on personal devices, laptops, electronic devices access protection (passwords, firewalls) Clean Screen Policy (screen lock, full shutdown) delete PI no longer required
Managing security measures	Report any breach to the Information Officer. If a device has been stolen, notify IO and HR department immediately. The IO will inform the IT department who will remotely mitigate the loss through deletion of the information, if possible.

viii. Data Subject Participation

The client has the right to access, amend, or delete their personal information and any requests will be handled by the Information Officer or any Deputy duly appointed with such a responsibility.

All such requests must comply to section 23 to 25 of the Act;

- the request must be in writing with proof of identification,
- processed within a reasonable time and on receipt of the prescribed fee, if any,
- given in a reasonable manner and format,
- informed that personal information may be corrected.

If the client requests that any part or all of the information must be deleted or destroyed, it must be submitted in writing to the Information Officer or any Deputy duly appointed with such a responsibility. The Group will then proceed to correct, destroy or delete the information within a reasonable time and will provide the client with credible evidence in support of this.

Grounds for refusal will be as per applicable sections of Chapter 4 of Part 2 and Chapter 4 of Part 3 of the **Promotion of Access to Information Act**, of which is further explained in the *Access to Information Policy (PAIA manual).*

6.5 Special Personal Information

The nature of some of the Group's business activities does require it to process certain categories of special personal information. Although some of the functional departments in the Group is permitted under Chapter 3, Part B, section 32(1)(b) and 32(3) of the Act to process special personal information, specifically concerning health and sex life, consent will be obtained in writing to process such information to the benefit of the client and to conclude the legal agreement and as per point 6.4(ii) and in line with the **National Health Act, Act no. 61 of 2003**.

The Group undertakes to treat the information as confidential and will not share the information with any third party unless consent was obtained from the client and the third party is also subject to the above-mentioned sections of the Act.

The Group will also only process special personal information, specifically, criminal behaviour and/or biometric information subject to section 33(2), and in accordance with labour legislation.

Any processing of special personal information not mentioned above, will be in accordance with the applicable legislation, if it should be necessary to process such information and as per the following conditions;

- the consent of the client was obtained;
- processing is necessary for the establishment, exercise or defence of a right or obligation in law;
- processing is for historical, statistical or research purposes.

6.6 Trans-border flow of Information

The Group does not, during the normal course of conducting business, transfer personal information to third parties in foreign countries. However, if it is required and necessary to conclude legitimate business or in the interest of the client, the following conditions will be adhered to as per Chapter 9 of the Act.

- With the client's consent.
- When it can be reasonably established that the third party is subject to a similar, law as the Act, subject to binding corporate rules or agreements that provide adequate levels of protection of personal information.
- When the transfer is to the benefit of the client.
- When the transfer is necessary for the performance and/or conclusion of a contract of which the client is party to.

7. Direct Marketing

The Group does not practice direct marketing in an electronic form such as automated messaging, sending unsolicited emails or faxes or through any other similar electronic means.

The Group does, however, from time to time, do direct marketing to existing clients. The Group will only market similar products and services to existing clients. Any information collected from our clients at first contact might be used for marketing purposes, which purpose will be made clear, and the client will have the opportunity to opt in by giving specific consent. We will also ensure the client has the option to withdraw consent at any time if they so wish.

8. Access to Information

Clients, (natural and juristic persons), may request access to their personal information kept by the Group. They may further request the amendment, correction, deletion, or destruction of such information and will be advised as such.

Access will be granted to a client if due process is followed as per the prescribes of the Act, Section 23 and the Guidelines of the Information Regulator. The Group will ensure such requests are handled timeously and provided in a reasonable manner and format. The Group reserves the right to levy a fee and/or charge a deposit of which a written quotation will be provided for the service.

Any individual, juristic person, entity, not being a client of the Group, may also request access to information. Due process will be followed to process such requests as per the guidelines mentioned above.

8.1 Grounds for refusal

The Group may or must refuse access to information requests to which the grounds of refusal of access to records are set out in the applicable sections of Chapter 4 of Part 2 and Chapter 4 of Part 3 of the **Promotion of Access to Information Act**, whichever should apply.

Specific and exact conditions under which access to information may be requested and the grounds for refusal as well as remedies available to the enquirer, may be viewed in the Group's *Access to Information Policy (PAIA Manual).*

9. Record Retention, Storage and Destruction

The Group is bound by applicable legislation to retain documentation for a prescribed period.

Legislation	Period
Companies Act	From 7 years to indefinitely depending on type of document
Consumer Protection Act	3 years
Financial Intelligence Centre Act (FICA)	5 years
Tax – related Acts	5 years
Occupational Health & Safety Act	3 years
Compensation for Occupational Diseases Act	3 - 4 years Certain regulated information which could/does cause long term ill health 30 – 40 years
Basic Conditions of Employment Act	3 yeas
Employment Equity Act	3 years
Labour Relations Act	3 years to Indefinite depending on type of document
Unemployment Insurance Act	5 years

Documents that are no longer required to be retained and stored, will be destroyed by the Group.

The Group, due to its national offices, will use various storage companies (third parties) to safely store records off-site where it is not feasible and practical to store it at any of its offices.

The retention, storage and destruction of electronic documents will be done after the prescribed legislative period has expired and will be done in such a way as to ensure it is not possible to recover or reconstruct information.

Each department will take responsibility for this process in accordance with the Group's *Record Storage and Destruction Procedural Manual.*

10. Managing Operators and 3rd Parties

The Group has the necessary agreements in place with third party service providers to ensure there is always a mutual understanding with regards to the protection of our clients' personal information.

The Group will ensure that Operators and third-party service providers are vetted according to their Privacy Policies in terms of the Act and **Promotion to Access to Information Act, Act 2 of 2000**, before conducting business with them, to ensure that risks are minimised that may potentially lead to a data security breaches.

It is the Group's undertaking that only relevant and applicable information will be shared with Operators and third-party service providers to conclude legitimate business transactions and in the interest of the client.

11. Risk Management / Incident Management

The Group endeavours to ensure that the correct and appropriate technical and organizational security measures are put in place to prevent data loss, damage to data or unlawful destruction or access to personal information, kept by the Group.

A Risk Assessment will be undertaken at least every six months to ensure risks are identified and managed to prevent non-compliance and possible data breach conditions.

To manage and remediate any reasonable and foreseeable risks and incidents, the Group will implement a *Risk Management Policy* and *Incident Management Policy* on which all employees will be trained.

Further to point 6.4(vii), and in line with the Act, reasonable steps will be taken to ensure the client is aware of any breaches, which will also be reported to the Information Regulator using the prescribed process as per the Act.

12. Implementation and Training

All employees of the Group who process or have access to any kind of personal information will receive awareness training to equip them to comply with the prescribes of the Act. The scope of the awareness training will depend on the job function and level of responsibility, which will be made clear and will be fully outlined in the respective annexures to employment contracts.

The Group will provide opportunities for all employees to explore the Act and issues pertaining to their function through training, awareness campaigns and team meetings.

All new employees will be orientated on all applicable and relevant policies and protocols which supports their responsibilities in terms of data security and the processing of personal information. Employees will also be required to sign acceptance of this policy and any other related policies after training and orientation.

As per the prescribe of section 55(a), the Information Officer will regularly conduct awareness audits to uplift and enhance the culture of compliance with the conditions of lawful processing of personal information.

13. Information Officer

The Group CEO will appoint and duly authorise the Information Officer in writing and ensure he/she is registered with the Information Regulator.

As per section 55(a) of the Act and section 4 of the Regulations, the duties of the Information Officer will include the following duties, of which duties may be added to as to ensure the Group will remain in compliance of the prescribes of the Act and Regulations;

- encourage compliance with conditions of lawful processing,
- deal with requests made to the Group pursuant to the Act,
- work with the Regulator in relation to investigations,
- ensure compliance of the Group with the provisions of the Act,
- develop, implement, monitor and maintain a compliance framework,
- do personal information impact assessments to ensure adequate measures and standards are in place,
- develop, monitor, maintain and make available a manual as prescribed in sections 14 and 51 of the Promotion of Access to Information Act, 2000 (Act no. 2 of 2000),
- regulate access to information in terms of the above Act,
- develop internal measures together with adequate systems to process requests for information or access thereto,
- conduct internal awareness sessions regarding the provisions of the Act and Regulations, codes of conduct or any information given by the Regulator.
- submit annually to the Regulator a report detailing the number of requests for access to information and all activities relating to such requests.

The Information Officer may appoint a Deputy Information Officer or Officers, depending on the size and nature of the Group's activities and complexity of operations for it to remain compliant to the prescribes of the Act and the Promotion to Access to Information Act (Act no. 2 of 2000). This designation must be in writing and registered with the Information Officer.

The Information Officer may delegate any power and duty conferred or imposed on him/her to a DIO of which should be performed subject to such conditions as the Information Officer may consider necessary. The Information Officer reserves his/her rights to exercise the powers or to perform the duties and responsibilities concerned himself/herself and may withdraw or amend any delegation to a DIO at any time.

To ensure a level of accountability by a delegated DIO, the duties and responsibilities will be part of his/her job description.

The Information Officer retains accountability and responsibility for functions delegated to the DIO.

14. Information Regulator

The powers and duties of the Regulator, as per Chapter 10 of the Act, are to provide education, monitor and enforce compliance, consult with interested parties, handle complaints, conduct research, issue and amend Codes of Conduct, facilitate cross-border cooperation and general duties such as exercise and perform such other functions, powers, and duties as are conferred or imposed on the Regulator by or under the Act or any other legislation.

14.1 Complaints

Any person may submit a complaint to the Regulator if they feel that the Group has contravened any of the prescribes of the Act. The Group, as the responsible party, may also submit a complaint to the regulator. Complaints must be submitted in writing.

Depending on the complaint, the Regulator may decide to take the following actions;

- action the complaint by doing a pre-investigation and/or a full investigation
- decide not to take any action,
- refer the complaint to another regulatory body,
- settle complaints on behalf of the complainant,
- refer the complaint to the Enforcement Committee.

The Regulator may follow a legal process to apply for a warrant, execute a warrant and seize property in pursuance of a warrant. The Regulator may also institute civil action on behalf of the data subject.

14.2 Assessment and Information Notices

The Regulator may, on its own initiative or at the request of the responsible party and/or data subject, conduct an assessment to determine if processing of personal information complies with the provisions of the Act.

When an Information Notice is served, the Group will provide the Regulator with a report to indicate how the processing of information is taking place or relating to such information concerning a complaint.

The Group, may appeal an Information or Enforcement Notice.

14.3 Offences, Penalties and Administrative Fines

The Regulator may impose penalties and/or administrative fines or institute legal action if any of the prescribes of the Act is contravened.

Such offences include but are not limited to;

- breaches of confidentiality,
- the hindrance, obstruction or unlawful influence of the Regulator,
- obstruction of execution of a warrant,
- failure to comply with enforcement or information notices,
- any offences committed by a witness summoned in terms of section 81,
- unlawful acts by a responsible party in connection with account numbers of a data subject,
- unlawful acts by a third party in connection with account numbers of a data subject.

Any person convicted of an offence, is liable to a fine or to imprisonment for a period of twelve months to ten years and/or a fine of ten thousand rand to ten million rand, depending on the conviction.

The Act provides for civil remedies where a court of law may award compensation for damages to a data subject as well as award aggravated damages, interest and the cost of any legal fees.

15. Amendments to this Policy and subsequent policies relating to this Policy

This policy encompasses the views and statements of the Group and describes all other policies and processes that must be put in place to achieve overall compliance. The Information Officer will review this policy yearly and will consult with the governance body of the Group and any other divisional managers as part of the review process.

This policy will be reviewed prior to its anniversary if any of the following events should occur or if the Group governing body feels that it would be in the best interest of the company to do so.

- Expansion of product and/or service offering
- Expansion of core business functions into related fields
- Cross-border projects
- Data security breach events and incidents
- Information Regulator notices and investigations
- An amendment in the Act, Regulations or any other Acts and Regulations relating to this Policy.

16. References and Regulatory Documents

16.1 Protection of Personal Information Act, No.4 2003

16.2 Promotion of Access to Information Act, 2000 (Act No. 2 of 2000)

16.3 Information Regulator (Regulations and Guidelines)

16.4 Electronic Communications and Transactions Act

16.5 Financial Intelligence Centre Act, Act 38 of 2001

16.6 National Health Act, Act No. 61 of 2003

16.8 Health Professions Council of South Africa Guidelines

16.9 Constitution of South Africa, section 14

Date	Version	Description	Author
01 June 2021	V1.0	Promotion to Access to Information Manual	Information Officer

This information manual has been prepared in accordance with Section 51(1) of the Promotion of Access to Information Act, No.2 of 2000 and is hereby approved:

Signed at Centurion on this 30th day of June 2021.

Liza Strydom
Information Officer

Prof. Oppel Greeff
CEO