Data Processing Agreement “DPA”

Responsible Party: The Pharmacy

Operator: 180 Degrees Marketing PTY LTD

1. Subject matter of this DPA

1.1. In this DPA the terms "data subject," "information officer," "operator," "personal information," "processing," "responsible party," "de-identify," and "Promotion of Access to Information Act (PAIA)" will have the same meanings as they are given in the Protection of Personal Information Act (POPIA).

1.2. The Responsible Party grants the Operator a mandate to process certain Personal Information, set out in **Schedule A**, on its behalf for the purpose and period set out under **Schedule A**.

1.3. In the event of a conflict or inconsistency between any provisions of other contractual agreements between the parties, the provisions of this DPA will prevail where the Processing of Personal Information is concerned.

2. The Responsible Party and the Operator

2.1. The Operator will Process the Personal Information strictly in accordance with the mandate in **Schedule A** and any specific instructions of the Responsible Party and no Personal Information will be Processed unless explicitly instructed by the Responsible Party.

2.2. Should the Operator reasonably believe that a specific Processing activity, beyond the scope of the Responsible Party’s instructions or the mandate in **Schedule A**, is required to comply with a legal obligation to which the Operator is subject, the Operator will inform the Responsible Party of that legal obligation and seek explicit authorization from the Responsible Party before undertaking such Processing. The Operator will never Process Personal Information in a manner inconsistent with the Responsible Party’s documented instructions.

2.3. The Responsible Party warrants that it has all necessary rights to provide the Personal Information to the Operator for the Processing to be performed in relation to the services, and that one or more justification grounds set forth in POPIA support the lawfulness of the Processing. To the extent required by the POPIA, the Responsible Party is responsible for ensuring that all necessary privacy notices are provided to Data Subjects, and unless another justification ground is set forth in POPIA supports the lawfulness of the Processing, that any necessary Data Subject consent to the Processing is obtained, and for ensuring that a record of such consent is maintained. Should such a consent be revoked by a Data Subject, the Responsible Party is responsible for communicating the fact of such revocation to the Operator, and the Operator remains responsible for implementing the Responsible Party's instruction with respect to the Processing of that Personal Information.

3. Confidentiality

Without prejudice to any existing contractual arrangements between the parties, the Operator will treat all Personal Information as confidential and it will inform all its employees, agents and/or approved sub-operators engaged in Processing the Personal Information of the confidential nature of the Personal Information. The Operator will ensure that all such persons or parties have signed an appropriate confidentiality agreement, are otherwise bound to a duty of confidentiality, or are under an appropriate statutory obligation of confidentiality.

4. Security

4.1. Taking into account the industry norm, the costs of implementation, the nature, scope, context and purposes of Processing as well as the risk of varying likelihood and severity for the rights and freedoms of Data Subjects, the Responsible Party and Operator will implement appropriate, reasonable technical and organisational measures to ensure a level of security of the Processing of Personal Information appropriate to the risk. These measures will include, at a minimum, the security measures agreed upon by the parties in **Schedule B**.

4.2. Both the Responsible Party and the Operator will maintain written security policies that are fully implemented and applicable to the Processing of Personal Information. At a minimum, such policies should:

4.2.1. include assignment of internal responsibility for information security management;

4.2.2. devote adequate personnel resources to information security;

4.2.3. provide for the carrying out of verification checks on permanent staff who will have access to the Personal Information;

4.2.4. require employees, vendors and others with access to Personal Information to enter into written confidentiality agreements; and

4.2.5. provide for training to make employees and others with access to the Personal Information aware of information security risks presented by the Processing.

4.3. The Operator's adherence to either an approved code of conduct or to an approved recognised security certification standard, may be used as an element by which the Operator may demonstrate compliance with the requirements set out, provided that the requirements contained in **Schedule B** are also addressed by such code of conduct or recognised security certification standard.

5. Improvements to Security

The parties acknowledge that security requirements are constantly changing and that effective security requires frequent evaluation and regular improvements of outdated security measures. The Operator will therefore evaluate the measures as implemented on an on-going basis in order to maintain compliance with the requirements set out in POPIA.

6. Information Transfers

The Operator will promptly notify the Responsible Party of any planned permanent or temporary transfers of Personal Information to any country outside the borders of the Republic of South Africa. Furthermore the Operator will promptly notify the Responsible Party of any planned transfer of Personal Information to any country without an adequate level of protection, and will only perform such a transfer after obtaining written authorisation from the Responsible Party, which may be refused at its own discretion.

7. Information Obligations and Incident Management

7.1. When the Operator becomes aware of an incident that has an impact on the Processing of the Personal Information that is the subject of this DPA, it will notify the Responsible Party as soon as reasonably possible about the incident and will cooperate with the Responsible Party's reasonable requests in order to enable the Responsible Party to comply with their obligations. Where appropriate, the Operator may charge for these services.

7.2. The term "incident" used in clause 7.1 means:

7.2.1. a complaint or a request with respect to the exercise of a Data Subject's rights in terms of POPIA;

7.2.2. any unauthorized or accidental access, processing, deletion, loss or any form of unlawful Processing of the Personal Information;

7.2.3. any breach of the security and/or confidentiality as set out in this DPA leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, the Personal Information, or any indication of such breach having taken place or being about to take place;

7.2.4. where, in the opinion of the Operator, implementing an instruction received from the Responsible Party would violate applicable laws to which the Responsible Party or the Operator are subject.

7.3. The Operator will at all times have in place written procedures which enable it to promptly respond to the Responsible Party about an incident.

7.4. Any notifications made to the Responsible Party will be addressed to the employee of the Responsible Party whose contact details are provided on the Order.

8. Contracting with Sub-Operators

8.1. A sub-operator means a person who has been mandated by the Operator to Process Personal Information in terms of this DPA, with the Responsible Party's prior approval.

8.2. The Operator will not subcontract any of its activities consisting of the Processing of the Personal Information or requiring Personal Information to be Processed by any third party without the prior written authorisation of the Responsible Party.

8.3. Notwithstanding any authorisation by the Responsible Party, the Operator will remain fully liable to the Responsible Party for the performance of any such sub-operator that fails to fulfil its information protection obligations.

8.4. The Operator will ensure that the sub-operator concludes a Sub-Operator Agreement with it and the Responsible Party in terms of which the sub-operator is bound by data protection obligations compatible with those set out in this DPA including reasonable technical and organizational measures which meet the requirements of the POPIA.

9. Return or Deletion of Personal Information

9.1. Upon termination of this DPA, and upon the Responsible Party's written request, or upon fulfilment of all purposes agreed in the context of the services whereby no further Processing is required, the Operator will, at the discretion of the Responsible Party, either delete, destroy or return all Personal Information to the Responsible Party and delete or return any existing copies. The Operator will be required to provide a certificate of deletion if instructed by the Responsible Party to delete the Personal Information.

9.2. The Operator will notify all third parties supporting its own Processing of the Personal Information of the termination of the DPA and will ensure that all such third parties will either destroy or delete the Personal Information or return the Personal Information to the Responsible Party, at the discretion of the Responsible Party.

9.3. Where appropriate, the Operator may charge the Responsible Party for these requests.

10. Assistance to the Responsible Party

10.1. The Operator will assist the Responsible Party by appropriate technical and organisational measures, insofar as this is possible, for the fulfilment of the Responsible Party's obligation to respond to requests for exercising the Data Subject's rights in terms of the POPIA.

10.2. The Operator will assist the Responsible Party in compliance with obligations pursuant to clause 4 (Security), as well as other Responsible Party obligations in terms of POPIA that are relevant to the information Processing described in **Schedule B**, including notifications to the Information Regulator or to Data Subjects.

10.3. The Operator will provide reasonable assistance to the Responsible Party with any data protection impact assessments.

10.4. The Operator will make available to the Responsible Party all information necessary to demonstrate compliance with the Operator's obligations in terms of this DPA and to respond to reasonable requests for and to contribute to audits, including inspections, conducted by the Responsible Party.

10.5. Where appropriate, the Operator may charge the Responsible Party for these requests.

11. Duration and Termination

11.1. This DPA will come into effect on the date of placing an Order, will endure for duration of the services provided by the Operator as set out in **Schedule A** and will terminate on the completion of use of the services provided by the Operator.

11.2. The Operator will Process Personal Information until the date of expiration or termination of the DPA.

12. Liability

12.1. Where the Responsible Party, its employees or agents breach any of the warranties in this DPA, or fails to comply with any of the provisions of POPIA, then in such an event, the Responsible Party will be liable for all damages it may have caused in consequence of the breach or non-compliance, including patrimonial or non-patrimonial damages suffered by the Operator and holds the Operator and its directors and employees harmless against any such loss, regulatory fine, damage, action or claim which may be brought by anyone against the Operator or any of its directors or employees or against any of its affiliated companies, or their directors or employees, and agrees to pay all and any such amounts on demand.

12.2. In the event of an action or claim referred to in 12.1, the Operator shall provide all assistance reasonably required to defend the claim.

13. Miscellaneous

13.1. This DPA is governed by the laws of the Republic of South Africa. Any disputes arising from or in connection with this DPA will be brought exclusively before the competent court of the Republic of South Africa.

13.2. The relationship between the Operator and Responsible Party is that of an independent contractor and this DPA does not create any agency, partnership, employment and/or right of representation by either party on behalf of the other. No employee or representative of a party will have any authority to bind or obligate the other party to this DPA and neither party will hold itself out as the agent or representative of the other.

13.3. The Parties undertake to do all such things, perform all such acts and take all steps to procure the doing of all such things and the performance of all such acts, as may be necessary or incidental to give or be conducive to the giving of effect to the terms, conditions and import of this DPA.

13.4. This DPA constitutes the whole agreement between the Parties as to the subject matter hereof and no agreement, representations or warranties between the Parties other than those set out herein are binding on the Parties.

13.5. No addition to or variation, consensual cancellation or novation of this DPA and no waiver of any right arising from this DPA or its breach or termination will be of any force or effect unless reduced to writing and signed by both of the Parties or their duly authorised representatives.

13.6. All notices to be provided in terms of the DPA, must be sent to the other party's Information Officer or Deputy Information Officer by email -

13.6.1. Information Officer details for the Responsible Party:
As per an Order

13.6.2. Information Officer details for the Operator:
popia@clicksgroup.co.za

SCHEDULE A: MANDATE TO PROCESS PERSONAL INFORMATION

Nature: Special Personal Information and Personal Information.

Purpose: To enable the carrying on of the business conducted by the Responsible Party as a retail pharmacy.

Duration: For the duration of the Order

Categories of Data Subjects: Pharmacy patients of the customers of the Responsible Party.

Types of Personal Information processed on Data Subjects:

1. unique system identifier;
2. gender;
3. language;
4. title;
5. first name;
6. surname;
7. date of birth;
8. identity number/passport number;
9. VAT number/status;
10. postal, physical and delivery addresses;
11. telephone contact number;
12. email address;
13. medical aid identifying number and details (scheme and plan);
14. where the data subject is a dependent on a medical aid, the identity number and date of birth of main member of their medical aid;
15. where the data subject is a minor, or has a relationship of dependency on another data subject, the identity of the related data subject, including names, identity numbers and date of birth;
16. health data, including details relating to medicine dispensed to the data subject, such as the name and quantity of medicine dispensed; the date on which and location at which the medicine was dispensed; the details of healthcare practitioners who prescribed and dispensed medicine for the data subject; and the data subject's medical conditions such as allergies;
17. notes on the data subject made by the dispensing pharmacist, which may be sensitive in nature;
18. identity of prescribing doctor(s) – name, contact details and practice number;
19. marketing consent indicator.

SCHEDULE B: OPERATOR’S TECHNICAL AND ORGANISATIONAL MEASURES

1. DATA SECURITY GOVERNANCE

The Operator maintains internal organisational and governance procedures to appropriately manage information throughout its lifecycle. The Operator regularly tests, assesses and evaluates the effectiveness of its technical and organisational measures.

The Operator will engage, at its own expense once per year or after any major system or application/code changes on the Operator’s systems, a third party vendor ("Testing Company") to perform penetration and vulnerability testing ("Security Tests") with respect to Operator’s systems containing and/or storing personal information.

On the Responsible Party’s request, and at the Responsible Party’s cost, the Operator will undergo additional Security Tests.

2. PHYSICAL ACCESS CONTROL

The Operator uses a variety of measures appropriate to the function of the location to prevent unauthorised access to the physical premises where Personal Information is Processed. Those measures include:

- Centralised key and code management, card-key procedures
- Batch card systems including appropriate logging and alerting mechanisms
- Surveillance systems including alarms and, as appropriate, CCTV monitoring
- Receptionists and visitor policies
- Locking of server racks and secured equipment rooms within data centres

3. VIRTUAL ACCESS CONTROL

The Operator implements appropriate measures to prevent its systems from being used by unauthorised persons. This is accomplished by:

- Individual, identifiable and role-based user account assignment, role-based and password protected access and authorisation procedures
- Centralised, standardised password management and password policies (minimum length/characters, change of passwords)
- User accounts are disabled after excessive failed log-on attempts
- Automatic log-off in case of inactivity
- Anti-virus management

4. DATA ACCESS CONTROL

Individuals that are granted use of the Operator’s systems are only able to access the data that are required to be accessed by them within the scope of their responsibilities and to the extent covered by their respective access permission (authorisation) and such data cannot be read, copied, modified or removed without specific authorisation. This is accomplished by:

- Authentication at operating system level
- Separate authentication at application level
- Authentication against centrally managed authentication system
- Change control procedures that govern the handling of changes (application or OS) within the environment
- Remote access has appropriate authorisation and authentication
- Logging of system and network activities to produce an audit-trail in the event of system misuse
- Implementation of appropriate protection measures for stored data commensurate to risk, including encryption, De-identified password controls.

5. DISCLOSURE CONTROL

The Operator implements appropriate measures to prevent data from being read, copied, altered or deleted by unauthorised persons during electronic transmission and during the transport of data storage media. The Operator also implements appropriate measures to verify to which entities' data are transferred. This is accomplished by:

- Data transfer protocols including encryption for data carrier/media
- Profile set-up data transfer via secure file transfer methods
- Encrypted VPN
- No physical transfers of backup media

6. DATA ENTRY CONTROL

The Operator implements appropriate measures to monitor whether data have been entered, changed or removed (deleted), and by whom. This is accomplished by:

- Documentation of administration activities (user account setup, change management, access and authorisation procedures)
- Archiving of password-reset and access requests
- System log-files enabled by default
- Storage of audit logs for audit trail analysis

7. INSTRUCTIONAL CONTROL

The Operator implements appropriate measures to ensure that data may only be Processed in accordance with relevant instructions. Those measures include:

- Binding policies and procedures on the Operator's employees
- Where sub-operators are engaged in the Processing of data, including appropriate contractual provisions to the agreements with sub-operators to maintain instructional control rights

8. AVAILABILITY CONTROL

The Operator maintains appropriate levels of redundancy and fault tolerance for accidental destruction or loss of data, including:

- Extensive and comprehensive backup and recovery management systems
- Documented disaster recovery and business continuity plans and systems
- Storage and archive policies
- Anti-virus, anti-spam and firewall systems and management including policies
- Data centres are appropriately equipped according to risk, including physically separated back up data centres, uninterruptible power supplies (including backup generators), fail redundant hardware and network systems and alarm and security systems (smoke, fire, water)
- Appropriate redundant technology on data storage systems
- All critical systems have backup and redundancy built into the environment.

9. SEPARATION CONTROL

The Operator implements appropriate measures to ensure that data that are intended for different purposes are Processed separately. This is accomplished by:

- Access request and authorisation processes provide logical data separation
- Separation of functions (production / testing)
- Segregation of duties and authorisations between users, administrators and system developer.