GoMobile (Pty) Ltd

Data Processing Agreement

March 2021 | Version 1.0

In alignment with the GoMobile Data Protection Policy [https://bit.ly/3sDtmpX]; in this document reference is made in the majority to the GDPR as the guiding law and less so to the POPIA.

Note the following interchangeable role definitions:

POPIA: responsible party = **GDPR:** controller

POPIA: operator = **GDPR:** processor

Agreement

1. Introduction

This is the agreement between:

- **controller** – a company incorporated in South African law; and
- **processor** – a company incorporated in South African law;

each having their registered offices and principal business places at the physical addresses and with the registration or identification numbers specified in the Subscriber Agreement, to fulfil controller’s obligation as a controller to enter into a contract with processor as controller’s processor and vice versa.

2. Definitions, parties, principal agreement and interpretation

2.1. ***Definitions***. In this agreement:

applicable data protection laws means relevant data protection laws, including:

- the South African Protection of Personal Information Act 4 of 2013; and
- Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation);

together with any other related laws that are specifically agreed between the parties in writing;

appropriate technical and organisational measures means regarding a given goal, the technical and organisational efforts that a reasonable person in processor’s position would use to achieve that goal as quickly, effectively, and efficiently as possible;

personal data means any information about a living human being or existing organisation (as applicable data protection laws require), provided that someone is capable of identifying them from that information;

personnel means any:

- director, employee, or other person who works (permanently or temporarily) under either party’s supervision; or
- person who renders services to either party for the purpose of their obligations under this agreement as their agent, consultant, contractor, or other representative;

processing means doing anything with personal data, including gathering it, disclosing it, or combining it with other information; and

sub-processor means any downstream processor that the processor engages to process personal data in accordance with the principal agreement and this agreement, as those documents permit.

2.2. ***Parties***. In this agreement:

controller is the Subscriber, and means the person who determines the purpose (’why’) and means (’how’) of processing the personal data alone or in conjunction with others [although it is more important that they determine why to process the personal data than how, and those related to it [Controller definition - Article 4.7 GDPR]]; and

processor is GoMobile, and means the person who:

- processes personal data on controller's behalf in terms of a contract; and
- enters into this agreement with controller; and

those related to them [Processor definition - Article 4.8 GDPR].

2.3. ***Principal agreement meaning***. In this agreement, **principal agreement** means the Subscription Agreement between controller and processor in terms of which processor processes data on controller's behalf.

2.4. ***Principal agreement terms***. The principal agreement's terms remain in full force and effect except as modified in this agreement.

2.5. **Controller's documented instructions**. In this agreement, **controller's documented instructions** means the principal agreement and any other relevant written agreements between the parties, unless the parties agree otherwise in writing.

2.6. ***Undefined terms***. Any terms not otherwise defined in this agreement have the meaning the principal agreement gives to them.

2.7. ***Data protection law terms***. Terms used in this agreement that have meanings ascribed to them in applicable data protection laws, including 'data subject', 'processing', 'personal data', 'controller' and 'processor', carry the meanings set out under those laws to the extent that this principal agreement does not define them.

2.8. ***Agreement terms prevail***. This agreement's provisions will prevail in the event of a conflict between any of the principal agreement's provisions and this agreement's provisions.

3. Purpose

This agreement adds supplementary requirements to controller's principal agreement with processor and clarifies the relationship between controller and processor in terms of applicable data protection laws.

4. Application

This agreement applies when processor processing personal data on controller's behalf for specific activities subject to applicable data protection laws to achieve controller's purposes as set out in the principal agreement between controller and processor. It does not apply to any of processor's:

- processing on controller's behalf in terms of any other activity not set out in the principal agreement between controller and processor; or
- other processing, such as on processor's own behalf.

5. Requirements

5.1. ***Measure guarantees***. Processor guarantees best effort to implement appropriate technical and organisational measures in order to:

- meet applicable data protection laws' requirements; and
- protect the data subject's rights [Measure guarantees - Article 28.1 GDPR].

5.2. ***Required details***. Annexure 2 provides an overview of the following details related to the processing:

- the processing's subject-matter [Processing subject-matter - Article 28.3 GDPR];
- the processing's duration [Processing duration - Article 28.3 GDPR];
- the processing's nature [Processing nature - Article 28.3 GDPR];
- the processing's purpose [Processing purpose - Article 28.3 GDPR];
- the personal data type [Personal information type - Article 28.3 GDPR];
- the data subject categories [Data subject categories - Article 28.3 GDPR]; and
- the controller rights [Controller rights - Article 28.3 GDPR];

to the extent that the principal agreement does not specify those details.

5.3. ***Purpose pursuit***. The parties have entered into a principal agreement for the purposes set out in Annexure 2 and processor may choose the means they consider necessary to pursue those purposes in their own discretion, provided that their choices are compatible with:

- this agreement's requirements; and
- particularly controller's written instructions [Instructions steps - Article 32.4 GDPR].

5.4. ***Downstream processor contracts***. Processor must respect the conditions for downstream processor contracts in terms of applicable data protection laws [Downstream processor contracts - Article 28.3(d) GDPR].

5.5. ***Downstream contract***. Processor must enter into a contract or other written agreement with any sub-processor to govern processing by a sub-processor in the same way as the contract or other agreement between controller and processor, particularly when it comes to appropriate technical and organisational measures. [Downstream contract - Article 28.4 GDPR]

6. Controller and processor

6.1. ***Determination by controller***. Controller will determine the scope, purposes and manner by which processor may access or process the personal data, to the extent that the principal agreement does not adequately describe processor's data processing activities.

6.2. ***Processing instructions***. Processor may only process the personal data:

- on controller's documented instructions (principal agreement) [Processing instructions - Article 28.3(a) GDPR];
- to the extent that providing the services related to the processing activities requires them to; and

may not process the personal data:

- in a manner inconsistent with controller's documented instructions.

6.3. ***Infringing instructions notification***. Processor will immediately tell controller if they believe that any instruction infringes applicable data protection laws, provided that this:

- is not an obligation to monitor or interpret the laws that apply to controller; and
- does not constitute legal advice to controller.

6.4. ***Controller's warranties***. Controller warrants that:

- they have all necessary rights to provide the personal data to processor for the processing to be performed in relation to the services related to the processing activities; and
- one or more lawful grounds set out in applicable data protection laws support the lawfulness of the processing.

6.5. ***Controller's responsibilities***. Controller is responsible for making sure that certain designated personnel within their organisation:

- provide all necessary privacy notices to data subjects;
- obtain any necessary data subject consent to the processing;
- maintain a record of such consent;
- communicate the fact that a data subject has revoked consent to processor where a data subject does so;

to the extent that applicable data protection laws require.

7. Data sharing

7.1. ***Responsibility for secure data transfer***. Each party is responsible for the secure transfer of any data they share with the other party.

7.2. ***Technical and organizational safeguards for secure data transfer***. Each party must take appropriate technical and organisational measures to make sure that they transfer data securely to the other party. Technical measures may include the use of:

- a virtual private network (VPN);
- secure file transfer protocol (SFTP);
- a web portal or an application with an encrypted connection; or
- any other means that will sufficiently secure the data stream from any incident that may compromise the integrity of the data concerned.

Organisational measures may include any methods that make sure personnel implement these technical measures, such as:

- written policies;
- documented procedures; and
- necessary training.

8. Confidentiality

8.1. ***Authorised persons confidentiality***. Processor must make sure that their personnel authorised to process the personal data have committed themselves to confidentiality, such as by:

- signing an appropriate confidentiality agreement; or
- being otherwise bound to a duty of confidentiality;

or are under an appropriate statutory obligation of confidentiality [Authorised persons confidentiality - Article 28.3(b) GDPR].

9. Security

9.1. ***Data security***. Controller and processor will implement appropriate technical and organisational security measures to make sure that the level of security is appropriate to the risks to the personal data in terms of applicable data protection laws, taking into account the:

- state of the art (being the most recent level of development of technology of security measures at that particular time);
- implementation costs;
- processing nature, scope, context and purposes; and
- varying risks to people's rights and freedoms in terms of likelihood and severity [Data security - Article 28.3(c) GDPR; Section 19 read with section 21(1) of POPIA] [Appropriate measures requirement - Article 32.1 GDPR].

9.2. ***Security policies***. Controller and processor will each maintain and fully implement written security policies that apply to personal data processing.

9.3. ***Audits***. Processor will allow for audits by the controller or another auditor that they mandate. Processor must immediately tell controller if they think the instruction to allow for and contribute to audits breaks the law. [Audits - Article 28.3(h) GDPR]

9.4. **Evidence of compliance**. Processor may use their adherence to either a:

- code of conduct; or
- a written policy;

recognized under applicable data protection laws as an element to show compliance with the requirements set out in relevant data protection laws [Code of conduct or certification mechanism - Article 32.3 GDPR].

10. Improvements to security

10.1. ***Cost negotiations***. The parties will negotiate the cost to implement material changes required by specific updated security requirements set out in applicable data protection laws or by data protection authorities of competent jurisdiction in good faith.

10.2. ***Amendment negotiations***. The parties will negotiate an amendment to the principal agreement in good faith where one is necessary to execute a controller instruction to processor to improve security measures as may be required by changes in applicable data protection laws from time to time.

11. Data transfers

11.1. ***Timeous notification***. Processor will inform controller timeously of any plans to transfer personal data to a third country, whether permanently or temporarily.

11.2. ***Transferring instructions***. Processor may only transfer personal data to a third country or international organisation on controller's documented instructions, unless required to do so by applicable law.

11.3. ***Statutory mechanism cooperation***. The parties agree to cooperate in good faith if they are relying on a specific statutory mechanism to standardize international data transfers and:

- the relevant authority subsequently modifies or revokes that mechanism; or
- a court of competent jurisdiction holds it to be invalid;

by:

- promptly suspending that transfer; or
- pursuing a suitable alternate mechanism that can lawfully support the transfer.

12. Information obligations and incident management

12.1. ***Processor incident notification***. Processor must notify controller after becoming aware of a personal data incident without undue delay [Processor breach notification - Article 33.2 GDPR], provided that:

- the incident has a material impact on personal data processing that is the subject of the principal agreement.

12.2. ***Incident scope***. A personal data incident means:

- a complaint or a request regarding the exercise of a data subject's rights under applicable data protection laws;
- an investigation into or personal data seizure by government officials, or a specific indication that such an investigation or seizure is imminent;
- any unauthorized, accidental or otherwise unlawful personal data processing;
- any breach of security or confidentiality in terms of this agreement leading to confirmed or possible risks to the personal data; or
- where implementing an instruction received from controller would violate applicable laws to which controller or processor are subject, in the opinion of processor.

12.3. ***Incident notification requirements***. Processor will address any incident notifications to the controller's employee whose contact details are set out in the principal agreement and to contain the following information to assist controller in fulfilling its obligations under applicable data protection laws:

- a description of the nature of the incident, including where possible the categories and approximate number of data subjects and personal data records concerned;
- the name and contact details of processor's data protection officer or another contact point where controller can obtain more information;
- a description of the likely consequences of the incident; and
- a description of the measures processor has taken or proposes to take to address the incident.

13. Contracting with sub-processors

13.1. ***Downstream processor restriction***. Processor may not subcontract any of their services related to the processing activities consisting of the processing of the personal data or assign their obligations to another processor without controller's:

- general written authorisation (provided that the processor tells the controller the details of any processor that they intend to subcontract or assign their obligations to and gives the controller an opportunity to object); or
- prior specific authorisation [Downstream processor restriction - Article 28.2 GDPR].

13.2. ***Prior specific authorisation***. Controller authorises processor to engage the sub-processors listed in Annexure 4 for the data processing activities related to the services described in Annexure 2.

13.3. ***Sub-processor changes***. Processor will inform controller of any addition or replacement of sub-processors and give controller an opportunity to object to such changes, provided that:

- the parties will make a good-faith effort to resolve controller's objection if controller timeously sends processor a written objection notice, setting forth a reasonable basis for objection; and
- each party may terminate the portion of the service which cannot be provided without the sub-processor if processor's efforts are not successful within a reasonable time.

13.4. ***Processor remains liable***. Processor remains liable to controller for any sub-processor's failure to perform their data protection obligations despite controller's authorisation. [Processor remains liable - Article 28.4 GDPR]

13.5. ***Processor's sub-processor obligations***. Processor will:

- make sure that the sub-processor is bound by data protection obligations compatible with those of processor under this agreement; and
- impose on its sub-processors the obligation to implement appropriate technical and organizational measures in such a manner that the processing will meet the requirements of applicable data protection laws.

14. Return or destruction of personal data

14.1. ***Deletion or return obligations***. Processor must:

- delete or return all the personal data to controller, at the controller's choice; and
- delete all existing copies unless the law requires them to continue to store those copies;

when:

- processor has finished providing processor with the services related to the processing;
- this agreement terminates;
- controller requests processor to do so in writing; or
- processor has otherwise fulfilled all purposes agreed in the context of the services related to the processing activities where controller does not require them to do any further processing [Deletion or return when the services end - Article 28.3(g) GDPR].

15. Assistance to controller

15.1. ***Help controller respond***. Processor must help controller with appropriate technical and organisational measures to fulfil their obligation to respond to requests by data subjects exercising their rights [Help controller respond - Article 28.3(e) GDPR], provided that:

- processor will assist controller with appropriate technical and organisational measures insofar as possible to respond to requests by data subjects exercising their rights; and
- controller will be responsible for reasonable costs processor incurs in providing this assistance.

15.2. ***Other help to controller***. Processor must help controller with:

- their obligations regarding security of processing [Help controller with security of processing - Article 28.3(f) GDPR]; and
- their prior consultation obligations in terms of applicable data protection laws [Help controller with prior consultation - Article 28.3(f) GDPR];

considering the nature of the processing and the information available to processor.

15.3. ***Make compliance information available***. Processor must make all information necessary to show compliance with the legal rules that apply to processors available to controller on request [Make compliance information available - Article 28.3(h) GDPR].

16. Liability and indemnity

Each party indemnifies the other and holds them harmless against all claims, actions, third party claims, losses, damages and expenses that the other party incurs arising out of a breach of this agreement or applicable data protection laws by the indemnifying party, provided that:

- each party provides the other with a notice of the claim promptly after receiving it;
- the indemnified party gives the indemnifying party the right to control the defence;
- the indemnified party will provide the indemnifying party with reasonable assistance as necessary; and
- the indemnified party will avoid admission of liability.

17. Duration and termination

17.1. ***Commencement***. This agreement will come into effect on the effective date of the principal agreement.

17.2. ***Duration***. Processor will process personal data until the principal agreement expires or terminates, unless:

- controller instructs them to do otherwise; or
- they or their sub-processor (as the case may be) returns or destroys the personal data (at controller’s choice).

18. General

18.1. ***Governing law***. This agreement is governed by the laws of country specified in the relevant provisions of the principal agreement.

18.2. ***Dispute resolution***. Any disputes arising from or in connection with this agreement will be brought exclusively before the competent court of the jurisdiction specified in the relevant provisions of the principal agreement.

Annexure 1: Officer Contact Information

1. Processor’s information officer or contact point

Contact information of processor’s information officer or other appropriate contact point:

Name:	Paul Marcellin
Phone number:	010 447 1058
Email address:	**paul@magnitudde4u.com**

Annexure 2: Requirement Details

1. **Processing subject-matter**
   Processing duration
   Processing nature
   Processing purpose
   Personal data types

   [Article 28.3 GDPR]

   As per the principal agreement

2. **Data subject categories**

   [Article 28.3 GDPR]

   The data subject categories may include: Consultants, Contractors, Customers, Employees, Job applicants, Prospects, Suppliers, Visitors.

3. **Controller rights**

   [Controller rights - Article 28.3 GDPR]

   The controller rights:

   Under **Article 28 of the General Data Protection Regulation** ("GDPR"), controllers must only appoint processors who can provide "sufficient guarantees" to meet the requirements of the GDPR. Processors must only act on the documented instructions of the controller and they can be held directly responsible for non-compliance with the GDPR obligations, or the instructions provided by the controller, and may be subject to administrative fines or other sanctions and liable to pay compensation to data subjects.

Annexure 3: Security Measures

Processor will develop and continue to develop an information security program to:

- help controller secure personal data against data breaches, leaks or other incidents where an unauthorised party could gain access to it;
- identify risks to the security of processor's equipment, premises, systems, networks and other means of processing personal data; and
- minimise security risks, including through risk assessments and regular testing.

Processor will designate personnel to coordinate and be accountable for the information security program and the program will include at least the physical, technical, operational and administrative controls described below.

1. Physical controls

Physical controls are measures that you can see or touch which protect data on equipment and premises from unauthorised physical interaction and include:

- **physical access** measures, such as locking filing cabinets or office doors and physical access controls (such as key cards, biometrics, or other identification methods to ensure that personnel have the correct access);
- **physical monitoring** measures, such as video surveillance (including CCTV systems) and security personnel (including security guards);
- **hard copy records management** measures, such as shredding paper records and enforcing a clean desk policy (where appropriate);
- **physical privacy** measures, such as having private consulting and storage areas (where appropriate); and
- any other measures that physically limit or prevent access to data, be it on IT equipment, systems or infrastructure or in hard copy records.

2. Technical controls

Technical controls are electronic and digital measures which protect data on systems and networks from unauthorised electronic interaction and include:

- **data security** measures, such as file encryption and password protection, unstructured data discovery and export control and data classification;
- **equipment and systems security** measures, such as device and removable storage media encryption, user access management, mobile device management and secure disposal or re-use of equipment;
- **networking and communications security** measures, such as firewalls, end-to-end encryption, digital access control, penetration testing and endpoint protection;
- **software security** measures, such as having antivirus software and keeping software up to date; and
- other measures related to hardware or software that is supposed to protect systems and resources.

Technical controls differ from physical controls in that they prevent access to the contents of a system, but not the physical systems themselves.

3. Operational controls

Operational controls are measures that relate to routine functions and operations which protect personal data from operational risks and include:

- **operational awareness** measures, such as fostering a culture of data protection through an employee awareness campaign;
- **training** measures, such as providing in-house and external personnel training to operationalise policies (particularly to people in data protection roles);
- **operational monitoring** measures, such as monitoring workstations and providing a way of reporting data protection incidents;
- **procedures**, such as employee on-boarding and exit and security procedures; and
- other measures that involve the ordinary members of the organisation.

4. Administrative controls

Administrative controls are measures that originate from key decision makers or formal structures which protect personal data from business risks and include:

- **administrative awareness** measures, such as director awareness and impressing management responsibility;
- **security planning** measures, such as planning around data protection, business continuity arrangements and considering acceptable standards;
- **security documentation** measures, such as drafting and updating privacy, cybersecurity, incident response and bring-your-own-device (BYOD) policies;
- **security assurances**, such as maintaining cyber insurance, doing due diligence of prospective employees or subcontractors and implementing audit controls (where appropriate); and
- other measures that involve decisions by the leadership of the organisation.

5. Continued review

Processor will continually review the:

- security of their equipment, premises, systems, networks and other means of processing personal data; and
- adequacy of their information security program;

against industry security standards and their policies and procedures to determine whether they require additional or different security measures to respond to new or emerging security risks.

Annexure 4: Sub processors

GoMobile engages the services of the following companies in a capacity that may be defined as sub-processor.

MS Azure

- Is our hosting-infrastructure service provider and is GDPR compliance-ready
- Further information and resources at:
  https://www.microsoft.com/en-ww/trust-center/privacy/gdpr-overview
  https://docs.microsoft.com/en-us/compliance/regulatory/gdpr-arc?view=o365-worldwide

KCS (Pty) Ltd

- Is our principle software development partner: **https://www.kcsitglobal.com/**
- Formal data-security governance is managed between our two companies via:
  - Comprehensive NDA document per team member
  - DPA at company level