

MCI's DATA PROCESSING AGREEMENT

1. INTRODUCTION

1.1 To the extent **MCI** may be required to process **Personal Information** on behalf of **the Client** under the **Agreement**, **MCI** will do so in accordance with the terms set out in this **Data Processing Agreement ('DPA')**.

2. DEFINITIONS

2.1. **MCI Consultants (Pty) Ltd**, will be referred to as **MCI**.

2.2. **"The Client"** means the organization that has entered into this **Agreement** with **MCI**.

2.3. **"Parties"** means **the Client** and **MCI**, and **Party** means any one of them as the context requires.

2.6 **'Data Protection Laws'** means any law relating to data protection privacy, and security applicable to a party in connection with the processing of **Personal Information** under **the Agreement** including but not limited to (each as amended or replaced from time to time) (a) **POPIA**, and (b) **any applicable laws worldwide** relevant to **MCI** or **the Client** (where applicable and as recipient of **Services** provided by **MCI**) relating to **Data Protection**.

2.7 **'Personal information'** means all personal information provided to **MCI** by, or on behalf of, **the Client** through **MCI's** provision of the **Services**.

2.8 **'Data Privacy and Protection Agreement'** means the then-current **Data Privacy and Protection Agreement** describing **MCI's** treatment of **Personal Information** in its general business administration, management, and operations.

2.9 **'POPIA'** means the Protection of Personal Information Act 4 of 2013.

2.10 **Lower case terms:** The following lower-case terms used but not defined in this DPA, such as **'data subject'**, **information regulator**, **'operator'**, **'personal information'**, **'responsible party'** and **'processing'** will have the same meaning as terms defined in those **Data Protection Laws**.

3. APPLICABLE LAW

3.1 **MCI** may be required to process **Personal Information** on behalf of **the Client** under any applicable **Data Protection Laws**.

3.2 Unless expressly stated otherwise, in the event of any conflict between the main body of this **DPA** and **Data Protection Laws**, the applicable **Data Protection Laws** will prevail.

4. DURATION AND TERMINATION

4.1 This **DPA** will commence on the date as the **Agreement** is signed by **the Client** who signs it last and will remain in force so long as the **Agreement** remains in effect or **MCI** retains any **Personal Information** related to the **Agreement** in its possession or control.

4.2 **MCI** will process **Personal Information** until the date of expiration or termination of the **Agreement**, unless instructed otherwise by **the Client** in writing, or until such **Personal Information** is returned or destroyed on the written instructions of **the Client** or to the extent that **MCI** is required to retain such **Personal Information** to comply with applicable laws.

5. PERSONAL INFORMATION TYPES AND PROCESSING PURPOSES

5.1 **The Client** and **MCI** acknowledge that **the Client** is the responsible party and **MCI** is the operator or sub-operator of **Personal Information**.

5.2 The details of the processing operations, in particular the categories of **Personal Information** and the purposes of processing for which the **Personal Information** is processed on behalf of the responsible party concerning the **Services** described in the **Agreement**, are specified in **Clause 18**.

5.3 **The Client** remains responsible for its compliance obligations under applicable **Data Protection Laws**, including providing any required notices, obtaining any required consents, and for the processing instructions it gives to **MCI**.

6. MCI's OBLIGATIONS

- 6.1 **Client Knowledge, Authorisation and Documented Instructions.** When MCI acts as the operator of Personal Information, it will only process the Personal Information with the Client's knowledge, authorisation, and on the Client's documented instructions as identified in Clause 18, and to the extent that this is required to fulfil the Services as per the Agreement. MCI will not process the Personal Information for any other purpose or in a way that does not comply with this DPA or applicable Data Protection Laws.
- 6.2 **Processing Beyond Instructions.** Should MCI reasonably believe that a specific processing activity beyond the scope of the Client's instructions is required to comply with a legal obligation to which MCI is subject, MCI must inform the Client of that legal obligation and seek explicit authorisation from the Client before undertaking such processing. MCI will not process the Personal Information in a manner inconsistent with the Client's documented instructions.
- 6.3 **Independent Responsible Party.** To the extent MCI uses or otherwise processes Personal Information in connection with MCI's legitimate business operations, MCI will be an independent responsible party for such use, will process Personal Information in accordance with its Data Privacy and Protection Agreement, and will be responsible for complying with all applicable laws and responsible party obligations.
- 6.4 **Compliance.** MCI will reasonably assist the Client in complying with the Client's obligations under applicable Data Protection Laws, considering:
- 6.4.1 the nature of MCI's processing,
 - 6.4.2 the information made available to MCI, including in relation to data subject rights,
 - 6.4.3 data protection impact assessments and
 - 6.4.4 reporting to and consulting with the Information Regulator.
- 6.5 **Notification.** MCI will immediately notify the Client if, in its opinion, any instruction infringes applicable Data Protection Laws. This notification will neither constitute a general obligation on the part of MCI to monitor or interpret the laws applicable to the Client, nor constitute legal advice to the Client.
- 6.6 **Disclosure.** MCI will not disclose Personal Information except: (a) as the Client directs in writing, (b) as described in this DPA or (c) as MCI will use reasonable endeavors to notify the Client and attempt to redirect the public authority to request the Personal Information directly from the Client.

7. CONTRACTING WITH SUB-OPERATORS

- 7.1 **List of Sub-Operators.** A list of MCI's sub-operators that MCI directly engages for the specific Services as an operator is available on request to the MCI contact mentioned in Clause 17.
- 7.2 **General Authorisation.** The Client provides its general authorisation to MCI's engagement with sub-operators, to provide some of Services e.g. hosting services, on its behalf. To the fullest extent permissible under applicable Data Protection Laws this DPA will constitute the Client's general written authorisation to the sub-contracting by MCI of the Services as disclosed to the Client.
- 7.3 **Changes.** MCI will notify the Client in writing of any intended changes to the agreed outsourced Services.
- 7.4 **Performance.** MCI is responsible for its sub-operator's compliance in relation to MCI's obligations in this DPA.

8. THE CLIENT'S OBLIGATIONS

- 8.1 **Data Subject Requests.** If MCI receives a request from the Client's Data Subject to exercise one or more of its rights under applicable Data Protection Laws, in connection with a Service for which MCI is an operator, MCI will redirect the Data Subject to make its request directly to the Client. The Client will be responsible for responding to any such request. MCI will comply with reasonable requests by the Client to assist with the Client's response to such a Data Subject request. The Client will be responsible for reasonable costs MCI incurs in providing this assistance.
- 8.2 **The Client Requests.** MCI must promptly comply with any Client request (a) requiring MCI to amend, transfer, delete or otherwise process the Personal Information, or to stop, mitigate or remedy any unauthorised processing, (b) relating to the Client's obligations regarding the security of processing and (c) the Client's obligations in terms of applicable Data Protection Laws, considering the nature of the processing and the information available to MCI.

8.3 **Warranty.** **The Client** warrants that: (a) it has all necessary rights to provide the **Personal Information** to **MCI** for the processing to be performed in relation to **the Services**, and (b) **MCI's** expected use of the **Personal Information** for **the Services** as specifically instructed by **the Client**, will comply with all applicable **Data Protection Laws**.

8.4 **Privacy Notices.** To the extent required by applicable **Data Protection Laws**, **the Client** is responsible for ensuring that all necessary privacy notices are provided to **Data Subjects**, and unless another legal basis set forth in applicable **Data Protection Laws** supports the lawfulness of the processing, any necessary **Data Subject** consents to the processing are obtained and a record of such consents is maintained. Should such consent be revoked by a **Data Subject**, **The Client** is responsible for communicating the fact of such revocation to **MCI**, and **MCI** remains responsible for implementing **the Client's** instruction with respect to the processing of that **Personal Information**.

9. SECURITY

9.1 **TOMs.** **MCI** will implement appropriate and reasonable **Technical and Organisational Measures** ('**TOMs**') to ensure the security of the **Personal Information** in terms of applicable **Data Protection Laws**, including the security measures set out in **Clause 19**. This includes protecting the **Personal Information** against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access to the **Personal Information**.

9.2 **Access to Personal Information.** **MCI** will grant access to the **Personal Information** undergoing processing to members of its personnel only to the extent strictly necessary for implementing, managing and monitoring the **Agreement**. **MCI** will ensure that people authorised to process the **Personal Information** received have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

10. AUDITS

10.1 **Certifications.** **MCI** will maintain any certifications that it is contractually obligated to maintain and comply with as expressly stated in the **Agreement**. **MCI** will re-certify against those certifications as reasonably required.

10.2 **Provision of Evidence.** At **the Client's** written request, **MCI** will provide **the Client** with evidence of those certifications relating to the processing of **Personal Information**, including applicable certifications or audit reports of its computing environment and physical data centers that it uses in processing **Personal Information** to provide **the Services** so that **the Client** can reasonably verify **MCI's** compliance with its obligations under this **DPA**.

10.3 **Compliance with TOMs.** **MCI** may also rely on those certifications to demonstrate compliance with the requirements set out in **Clause 9.1**.

10.4 **Confidential Information.** Any evidence provided by **MCI** is confidential information and is subject to non-disclosure and distribution limitations of **MCI** and/or any **MCI** sub-operator.

10.5 The Client Audits

10.5.1 **The Client** or its agent shall have the right to audit **MCI** at any time, with reasonable notice, if:

10.5.1.1 there is a reasonable suspicion that **MCI** is not complying with the provisions of this **Agreement**; or

10.5.1.2 There is a suspicion that the confidentiality, integrity and accessibility of **Personal Information** is likely to be compromised; or

10.5.1.3 **MCI** has not provided sufficient evidence of the measures taken under **Clause 9**; or

10.5.1.4 An audit is formally required by the **Information Regulator**.

10.5.2 Applicable **Data Protection Laws** provide **the Client** with a direct audit right (and as long as **the Client** only conducts an audit once in any twelve-month period unless mandatory applicable **Data Protection Laws** require more frequent audits).

10.5.3 Such audit rights shall include the right of access to systems, procedures and software, and inspection of the physical security of **MCI's** premises.

10.6 The Client Audit Process.

- 10.6.1 **The Client** audit may be carried out by a third party (but must not be a competitor of **MCI** or not suitably qualified or independent) who must first enter into a **Confidentiality Agreement** with **MCI**.
- 10.6.2 **The Client** must provide at least 60 days' advance notice of any audit unless mandatory applicable **Data Protection Laws** or a data protection authority of competent jurisdiction requires shorter notice.
- 10.6.3 **MCI** will cooperate with such audits carried out and will grant **the Client's** auditors' reasonable access to any premises and devices involved with the processing of **the Client's Personal Information**.
- 10.6.4 **The Client** audits will be limited in time to a maximum of three business days. Beyond such restrictions, the parties will use current certifications or other audit reports to avoid or minimise repetitive audits.
- 10.6.5 **The Client** must bear the costs of any **Client** audit unless the audit reveals a material breach by **MCI** of this **DPA** in which case **MCI** will bear the costs of the audit. If the audit determines that **MCI** has breached its obligations under the **DPA**, **MCI** will promptly remedy the breach at its own cost.
- 10.6.6 To the extent that **MCI** engages an independent auditor in relation to the provisions of applicable data privacy and protection legislation to carry out an audit of its operations, **MCI** agrees to provide **the Client** with copies of the audit reports of all such audit exercises.
- 10.6.7 Nothing in this clause 10.6 should be read as providing **the Client** with unlimited access to audit **MCI** without just cause.

11. INCIDENT MANAGEMENT

- 11.1 **Security Incidents.** If **MCI** becomes aware of a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to **Personal Information** while processed by **MCI** (each a '**Security Incident**'), **MCI** will promptly and without undue delay:
 - 11.1.1 notify **the Client** of the **Security Incident**.
 - 11.1.2 investigate the **Security Incident** and provide **the Client** with sufficient information about the **Security Incident**, including whether the **Security Incident** involves **Personal Information** of **the Client**.
 - 11.1.3 take reasonable steps to mitigate the effects and minimise any damage resulting from the **Security Incident**.
- 11.2 **Security Incident Notification.** Notification(s) of **Security Incidents** will take place in accordance with clause 11.1. Where the **Security Incident** involves **Personal Information** of **the Client**, **MCI** will make reasonable efforts to enable **the Client** to perform a thorough investigation into the **Security Incident**, formulate a correct response, and take suitable further steps in respect of the **Security Incident**. **MCI** will make reasonable efforts to assist **the Client** in fulfilling **the Client's** obligation under **Section 22 of POPIA** or other applicable **Data Protection Laws** to notify the relevant **Data Protection Authority** and **Data Subjects** about such **Security Incident**. **MCI's** notification of or response to a **Security Incident** under this clause is not an acknowledgement by **MCI** of any fault or liability for the **Security Incident**.
- 11.3 **Other incidents.** **MCI** will notify **the Client** promptly if **MCI** becomes aware of:
 - 11.3.1 a complaint or a request concerning the exercise of a **Data Subject's** rights under any applicable **Data Protection Laws** about **Personal Information** **MCI** processes on behalf of **the Client** and its **Data Subjects**; or
 - 11.3.2 an investigation into or seizure of the **Personal Information** of **the Client** by government officials, or a specific indication that such an investigation or seizure is imminent; or
 - 11.3.3 where, in the opinion of **MCI**, implementing instruction received from **the Client** about the processing of **Personal Information** would violate applicable laws to which **the Client** or **MCI** are subject.
- 11.4 **The Client Notifications.** Any notifications made to **the Client** under clause 11 will be addressed to **the Client** as per the **Agreement**.

12. CROSS BORDER TRANSFERS OF PERSONAL INFORMATION

- 12.1 **General.** Except as described elsewhere in the **DPA**, **Personal Information** that **MCI** processes on **the Client's** behalf may be transferred to and stored and processed in any country in which **MCI** or its sub-operators may operate.

- 12.2 **Adequate Safeguards.** MCI will identify in **Clause 18** the transfer mechanism that provides an appropriate level of protection to the third party who receives the **Personal Information** either by way of a law, binding corporate rules or binding agreement under **Section 72(1)(a) of POPIA.**

13. RETURN OR DESTRUCTION OF PERSONAL INFORMATION

- 13.1 **The Client Deletion.** For certain **Services**, MCI is responsible for installing, hosting, and processing **Personal Information**. Here only MCI can access, extract and delete **Personal Information** stored in that **Service**. Where the **Service** does not support access, retention or extraction of **Software** provided by **the Client**, MCI has no liability for the deletion of **Personal Information** as described in this **Clause 13.1**
- 13.2 **Delete or Return.** Where the **Agreement** requires MCI to retain **Personal Information**, MCI will delete that **Personal Information** within the period agreed to in the **Agreement**, unless MCI is permitted or required by applicable law to retain such **Personal Information**. Where the retention of **Personal Information** has not been addressed in the **Agreement**, MCI will either delete, destroy, or return all **Personal Information to the Client** and destroy or return any existing copies when MCI has finished providing **Services**:
- 13.2.1 related to the processing.
 - 13.2.2 when this **DPA** terminates.
 - 13.2.3 **The Client** requests MCI to do so in writing; or
 - 13.2.4 MCI has otherwise fulfilled all purposes agreed in the context of the **Services** related to the processing activities where **the Client** does not require MCI to do any further processing.
- 13.3 **Certificate of Destruction.** MCI will provide **the Client** with a destruction certificate at **the Client's** request. Where the deletion or return of the **Personal Information** is impossible for any reason, or where backups and/or archived copies have been made of the **Personal Information**, MCI will retain such **Personal Information** in compliance with applicable **Data Protection Laws**.
- 13.4 **Third Parties.** On termination of this **DPA**, MCI will notify all sub-operators supporting its processing and make sure that they either destroy the **Personal Information** or return the **Personal Information to the Client**, at the discretion of **the Client**.

14. LIABILITY AND WARRANTY

- 14.1 Any limitation of liability in the **Agreement** will apply to this **DPA**, other than to the extent such limitation (a) limits the liability of the parties to data subjects or (b) is not permitted by applicable law.

15. NOTICE

- 15.1 Any notice or other communication given to a party under or in connection with this **DPA** must be in writing and delivered to the other party by email.
- 15.2 **Clause 15.1** does not apply to the service of any proceedings or other documents in any legal action or, where applicable, any arbitration or other method of dispute resolution.
- 15.3 Any notice or other communication will be deemed given when:
- 15.3.1 delivered in person.
 - 15.3.2 received by email; or
 - 15.3.3 received by an internationally recognized courier service (proof of delivery received by the noticing party) at the physical notice address (as identified above), with an electronic copy sent to the electronic notice address (as identified in the table above).

16. MISCELLANEOUS

- 16.1 **Conflict of Terms.** The **Agreement** terms remain in full force and effect except as modified in this **DPA**. Insofar as MCI will be processing **Personal Information** subject to applicable **Data Protection Laws** on behalf of **the Client** during the performance of the **Agreement**, the terms of this **DPA** will apply. If the terms of this **DPA** conflict with the terms of the **Agreement**, the terms of this **DPA** will take precedence over the terms of the **Agreement**.
- 16.2 **Governing Law.** This **DPA** is governed by South African law.
- 16.3 Subject to **Clause 16.7** (Dispute Resolution):

16.3.1 **The Client** irrevocably submits to the exclusive jurisdiction of the courts of the Republic of South Africa; and

16.3.2 **Either Party** may bring proceedings in any court of competent jurisdiction,

16.3.3 In respect of any action, claim or matter arising under or in connection with this **DPA**.

16.4 **Dispute Resolution.** Any disputes arising from or in connection with this **DPA** will be brought exclusively before the competent court of jurisdiction specified in **Clause 16.2** above.

16.5 **Counterparts:** This **DPA** may be executed in any number of counterparts, each of which will constitute an original, but which will together constitute one agreement. Where one or both of the parties chooses to execute this **DPA** by electronic signature, each electronic signature will have the same validity and legal effect as the use of a signature affixed by hand and is made to authenticate this **DPA** and evidence the intention of that party to be bound by this **DPA**.

17. **MCI CONTACT POINT**

17.1 Contact information of **MCI's Information Officer:**

Name: Aliko Droussiotis

Email: aliki@mci.co.za

18. **PARTICULARS OF PROCESSING**

18.1 **Categories of Data Subjects whose Personal Information is Processed:**

18.1.1 **MCI** acknowledges that, depending on **the Client's** use of the **Services**, **MCI** may process the **Personal Information** of any of the following types of **Data Subjects**:

- The Client employees, contractors, temporary workers, agents and representatives
- The Client's Clients
- Applicant and/or candidate information
- Categories of Personal Information

18.1.2 **MCI** acknowledges that, depending on **the Client's** use of the **Services**, the types of **Personal Information** processed by **MCI** may include, but are not limited to the following:

- Basic personal information (for example first name, last name, email address and work address).
- Bank account information.
- Contact information (for example work email and phone number).
- Professional or employment-related information (for example, employer name and job title).
- Location information (for example, geo-location network data).

18.2 **Duration and Object of Processing:**

18.2.1 The duration of processing will be for the duration of the **Agreement** between **the Client** and **MCI**.

18.2.2 The objective of the data processing is the provision of **Services**.

18.2.3 **Personal information** may be processed on a continuous basis in order to provide the **Services** under the existing **Agreement**.

18.3 **Nature of the Processing:**

The **Personal Information** processed will be subject to the following basic processing activities:

- 18.3.1 Receiving information, including collection, accessing, retrieval, recording, and data entry.
- 18.3.2 Holding information, including storage, organisation and structuring.
- 18.3.3 Using information, including analysing, consultation, testing, automated decision making and profiling.
- 18.3.4 Updating information, including correcting, adaptation, alteration, alignment and combination.
- 18.3.5 Protecting information, including restricting, encrypting, and security testing.
- 18.3.6 Sharing information, including disclosure, dissemination, allowing access or otherwise making available.
- 18.3.7 Returning information to **the Client** or **Data Subject**.
- 18.3.8 Erasing information, including destruction and deletion.

18.4 **Purpose(s) of the Processing and Further Processing:**

The purpose of processing **Personal Information** is for **MCI** to provide the **Services** under the existing **Agreement**.

18.5 **The Retention Period:**

See **Clause 13** of the **DPA**.

18.6 **Data Transfers to (sub-) Processors:**

In accordance with the **DPA**, **MCI** may engage sub-operators to provide **Services** on **MCI's** behalf. Any such sub-processors will be permitted to obtain **Personal Information** only to provide **the Services MCI** has engaged them to provide, and they are prohibited from using **Personal Information** for any other purpose.

19. TECHNICAL AND ORGANISATIONAL MEASURES

19.1 **Information Security Policy**

19.1.1 **MCI** shall develop, implement, maintain, and monitor a written **Information Security Policy** that contains appropriate technical and organisational measures (ensuring a level of security appropriate to the risk presented by the Processing) to protect **Personal Data** against **Security Breach** and against all other unauthorised forms of Processing ("**Information Security Policy**").

19.1.2 **MCI** shall ensure that the **Information Security Policy** contains appropriate procedures to respond to a **Security Breach**.

19.1.3 **MCI** shall develop, implement and maintain a process for regularly testing, assessing, and evaluating the effectiveness of its **Information Security Policy**.

19.1.4 **MCI** shall update its **Information Security Policy** as required to effectively maintain the security of **Personal Data**.

19.1.5 **MCI** shall keep **Personal Data** logically separate to **Data Processed** on behalf of any other third party.

19.1.6 **MCI** shall safeguard the security and confidentiality of all encryption keys associated with encrypted **Personal Data**.

19.1.7 **MCI** shall ensure that any person Processing **Personal Data** on the Operator's behalf will do so in compliance with this **Clause 19**.

19.2 **Organisational Security Measures**

19.2.1 **MCI** will maintain the following controls and safeguards applied to its employees:

- All employees undergo **POPIA** and **Information Security Awareness Training** annually.
- Employees can only access any dashboards and/or files containing **Personal Data** with Authentication and MFA (Multifactor Authentication) completed on access devices.
- All company provided access devices run centrally managed antivirus, firewall, threat control and anti-exploit software, which software is updated automatically.
- All company devices must be locked at all times when not in use with a 15-minute lockout window.
- Employees have access to document shredders and secure disposal bins.

19.3 **Physical Security Measures on Premises and Access Controls**

19.3.1 **MCI** will maintain the following access controls to the premises:

- Physical access controlled by locks and electronic tags.
- All employees are assigned unique access tags.
- All employee access is logged by entry point, date stamp and access tag identifier.
- Access control is limited to the employees' required level of access (i.e. the principle of least privilege is adhered to).
- Authorised access to systems by employees is reviewed on a regular basis.
- All doors to the premises are locked outside of working hours.
- Alarms at all entry locations.

19.4 **Network Security Controls**

19.4.1 **MCI** shall apply the following network security measures:

- Separate 'Guest' Wi-Fi from "Company" Wi-Fi network access, where the former is limited to pure internet breakout only and the latter includes access to company network resources.
- User access to Wi-Fi networks is secured via a password.

- User access to the company LAN is secured via a domain authenticated profile (username and password).
- Firewalls are deployed to separate internal network zones and between these zones and public networks (i.e. the internet).
- Access to company shared files is secured via domain authenticated profiles and only accessible from company LAN or VPN.
- Remote user access to the company LAN is provided only via VPN secured via password and MFA.