



MANDALA CONSULTING
INTEGRATION FOR SUSTAINABILITY

Cookie Policy

1) Introduction:

- The purpose of this cookie policy is to describe what cookies are, what we use them for and how you can manage them during your visit to or use of our website or any of our platforms (hereinafter collectively referred to as our “**Site/s**”). This cookie policy works alongside our privacy policy.

2) What are cookies?

- A cookie is a small piece of data (text file) that a website / when visited by a user – asks your browser to store on your device in order to remember information about you, such as your language preference or log in information. Those cookies are set by us and called first party cookies. We also use third party cookies – which are cookies from a domain different than the domain of the website you are visiting – for our advertising and marketing efforts.

3) Why do we use cookies?

- We use cookies and other tracking technologies for the following purposes:
 - Assisting you in navigations;
 - Assisting in registration to our events, login, and your ability to provide feedback (where applicable);
 - Analysing your use of our products, services, applications and/or Sites;
 - Assisting with our promotional and marketing efforts (including behavioural advertising);
 - Granting you access to restricted content;
 - Tailoring our Sites’ functionality to you personally by letting us remember your preferences, location or device type;
 - Improving how our website performs;
 - Understanding who our audience is so that we can provide content most relevant to you;
 - Allowing third parties to provide services to our website; and
 - Helping us deliver interest – based advertising where appropriate in compliance with the applicable laws.

4) The types of cookies that we use:

- We make use of different types of cookies on our Sites. Some of these cookies are placed by us and others are placed by our third-party plug-ins, suppliers or advertisers. These cookies may be deleted from your device at different times, such as the end of your browsing session (when you leave the Site) or after a pre-set amount of time, or they may exist and function on your device until such time that you proceed to delete them.
- We use the following types of cookies on our Sites:
 - **Strictly necessary cookies / essential cookies:**
These cookies are necessary for the Site to function and cannot be switched off in our systems. They are

usually only set in response to actions made by you which amount to request for services, such as setting your privacy preference, logging in or filling in forms. You can set your browser to block or alert you about these cookies, but some parts of the Site may then not work. These cookies do not store any personally identifiable information.

▪ **Performance cookies / Site analytics cookies:**

These cookies allow us to count visits and traffic sources, so we can measure and improve the performance of our Site. They help us know which pages are the most and least popular and see how visitors move around the Site. All information these cookies collect is aggregated and therefore anonymous. If you do not allow these cookies, we will not know when you have visited our Site.

▪ **Functional cookies:**

These cookies enable the Site to provide enhanced functionality and personalisation. They may be set by us or by third party providers whose services we have added to our pages. If you do not allow these cookies, then some or all of these services may not functional properly. These cookies remember who you are as a user to our Site. We use them to remember any preferences you may have selected on our Site, like saving your username and password or settings.

▪ **Targeting cookies:**

These cookies may be sent through our Site by our advertising partners, if any. They may be used by those companies to build a profile of your interests and show you relevant adverts on other Sites. They do not store personal information directly but are based on uniquely identifying your browser and internet device. If you do not allow these cookies, you will experience less targeted advertising.

5) Deleting cookies:

- Your internet browser generally accepts cookies automatically, but you can often change the setting to stop accepting them. You can also delete cookies manually. You will be able to delete and control your cookie preferences by following the prompt settings on your preferred internet browser.
- Deleting or no longer accepting cookies may prevent you from accessing certain aspects of our Site where cookies are necessary or because the website forgot your preferences.

6) Updates to this cookie policy:

- We reserve the right to vary the terms of this cookie policy. We will notify you of any change and give you an opportunity to review, the revised cookie policy before you choose to continue to make use of our Sites. It is your responsibility to familiarise yourself with the most recent version of this cookie policy each time you access our Sites and before you elect to continue to make use of our Sites.



MANDALA CONSULTING

INTEGRATION FOR SUSTAINABILITY



MANDALA CONSULTING
INTEGRATION FOR SUSTAINABILITY

Data Breach Management Policy

1) Policy Statement:

- As an organisation which processes personal data, every care is taken to protect personal data and to avoid a data protection breach. This policy outlines the measures we take against unauthorised or unlawful processing or disclosure and against accidental loss, destruction of or damage to personal data.
- In the event of data being lost or shared inappropriately, we will take appropriate action to minimise any associated risk as soon as possible. This procedure applies to all personal and sensitive data held by us and our staff, employees, affiliates and contractors, referred to herein after as “**staff**”.
- This Policy forms part of our Data Protection Procedure and Protocol and all staff are made aware of these procedures through induction, supervision and ongoing training.

2) Purpose:

- It is a regulatory requirement under the Protection of Personal Information Act 4 of 2013 (“**POPIA**”) for responsible parties to have consistent and effective governance and control arrangements to protect the personal data that it processes. This Policy therefore sets out the course of action to be followed by all staff in the event of a real or potential data protection breach.

3) Personal Data:

- Personal data means any information relating to an identified or identifiable natural person (i.e. human being) or juristic person (i.e. legal entity for e.g. a company). An identifiable natural person or juristic person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, identification number, registration number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.



- As examples, this might include personnel data such as name, address information, telephone number, date of birth, marital status, bank account, identity number, registration number and social security numbers, medical records and testimonials, for employees, customers or third parties.
- It also might include data about persons who are our suppliers or customers or work for or are customers of our corporate customers or suppliers, such as name, address information, telephone number, order history, payment details, photos and medical data.

4) Definition of Personal Data Breach:

- A personal data breach means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. This includes breaches that are the result of both accidental and deliberate causes and/or any other type of breach of personal information as recognised under POPIA.
- A personal data breach can be broadly defined as a security incident that has affected the confidentiality, integrity or availability of personal data. In summary, there will be a personal data breach whenever any personal data is lost, destroyed, corrupted or disclosed; if someone accesses the data or passes it on without proper authorisation; or if the data is made unavailable, for example, when it has been encrypted by ransomware, or accidentally lost or destroyed.
- Personal data breaches can include:
 - Loss or theft of personal data and/or equipment on which data is stored
 - Access by an unauthorised third party
 - Deliberate or accidental action (or inaction) by a controller or processor
 - Sending personal data to an incorrect recipient
 - Computing devices containing personal data being lost or stolen
 - Alteration of personal data without permission
 - Loss of availability of personal data
 - Hacking attack



- Cyber attack
- Equipment failure
- Human error
- Unforeseen circumstances such as a fire or flood
- Flawed data destruction procedures.

5) Aim of Data Breach Management Policy:

- The aim of this Policy is to ensure a standardised and consistent approach is followed when responding to data breaches to enable us to:
 - Report data breaches without delay to the Information Officer
 - Identify incidents of data breaches quickly and investigate them properly and in a timely manner
 - Record and document all incidents and report them to the Information Officer and his/her data protection team (“DPT”) responsible for managing data protection and/or data security and/or data breach incidents within the organisation
 - Assess the severity and impact of the data breach and inform the Information Regulator under POPIA and/or any other required law enforcement agencies, supervisory authorities and, subject to the law, effected data subject(s)
 - Take action which is proportionate, consistent and transparent to prevent further damage
 - Regularly monitor and review all data breach incidents and potential situations that may lead to a data breach to identify improvements in policies, procedures and control mechanisms to remove or mitigate risk of further repetition.

6) Managing a Data Breach:

Step 1: Containment and Recovery:

- The Information Officer will ascertain the severity of the breach, whether any personal data is involved and whether the breach is still occurring.
- If the breach is still occurring, the Information Officer will establish what steps need to be taken immediately to minimise the effect of the breach and contain the breach from further data loss (e.g. alert the Company's IT Technical support, restricting access to systems or close down a system etc).
- The Information Officer, together with the DPT, will consider and implement appropriate steps required to recover any data loss where possible and limit damage caused (e.g. use of back-ups to restore data; changing passwords etc.).
- In line with the provisions of Step 4 below, the Information Officer together with the DPT must consider and implement the data breach notification procedure as required by POPIA.
- The Information Officer and DPT shall, based on the severity and likely impact of the breach, inform the board of the Company. At the same time, depending on the nature and extent of the breach, the Information Officer may seek expert or legal advice and/or a public body responsible for the prevention, detection or investigation of offences if it is believed that illegal activity has occurred or likely to occur.
- Where a significant breach is occurred, the Information Officer will inform the Information Regulator within 72 (seventy two) hours of the discovery of the breach (refer to data breach notification procedure at Step 4 below).
- Any decisions taken and reasons therefore in relation to a data breach must be documented by the Information Officer. In this regard all the key actions and the decisions are required to be fully documented and logged in the Company's data security breach log.



Step 2: Preliminary Assessment of Risk

- Further actions may be needed beyond immediate containment of the data breach. To help the Company determine the next course of action, an assessment of the risks associated with the breach is undertaken to identify whether any potential adverse consequences for persons are likely to occur and the seriousness of these consequences. The information officer will consider the points arising from the following questions:
 - What type and volume of data is involved?
 - How sensitive is the data? Could the data breach lead to distress, financial or even physical harm?
 - What events have led to the data breach? What has happened to the data?
 - Has the data been unofficially disclosed, lost or stolen? Were preventions in place to prevent access/misuse? (e.g. encryption)
 - How many persons are affected by the data breach?
 - Who are the persons whose data has been compromised?
 - What could the data tell a third party about the persons? Could it be misused regardless of what has happened to the data?
 - What actual/potential harm could come to those persons? E.g. physical safety; emotional wellbeing; reputation; finances; identity theft; one or more of these and other private aspects to their life
 - Are there wider consequences to consider?
 - Are there others that might advise on risks/courses of action (such as banks if person's banking details have been affected by the breach)?

Step 3: Data Breach Notification

Company acting as a Responsible party:

- In the event of a personal data breach, if the Company is the responsible party in respect of the personal data in question, it shall without undue delay and, where feasible, not later than 72 (seventy two) hours after having becoming aware of it, notify the Information Regulator under POPIA in accordance with Section 22 of



POPIA and where required to do so, the effected data subject(s) unless the personal data breach notification to the data subject shall, according to a public body responsible for the prevention, detection or investigation of offences or the Information Regulator, determines that same would impede a criminal investigation by the public body concerned. Where the notification to the Information Regulator is not made within 72 (seventy two) hours, it shall be accompanied by reasons for the delay.

- The notification shall at least:
 - Describe the nature of the personal data breach including where possible, the categories and approximate number of Data subjects concerned and the categories and approximate number of personal data records concerned
 - Communicate the name and contact details of the data protection officer or other contact point where more information can be obtained
 - Describe the likely consequences of the personal data breach
 - Describe the measures taken or proposed to be taken by the Company as the Responsible party to address the personal data breach, including, where appropriate, measures to mitigation its possible adverse effects
 - A recommendation with regard to the measures to be taken by the Data subject to mitigate the possible adverse effects of the security compromise
 - If known to the Responsible party, the identity of the unauthorised personal who may have access or acquire the personal data.
- Where, and insofar as, it is not possible to provide the information at the same time, the information may be provided in phases without further undue delay.

The Responsible party shall document any personal data breaches, comprising the facts relating to the personal data breach, its affects and the remedial action taken. That documentation shall enable the Information Regulator to verify compliance with the provisions of POPIA.

Company acting as an Operator:

- Where the Company is acting as the operator, it shall notify the responsible party without undue delay after becoming aware of a personal data breach and provide information about the breach only to the Responsible party. The Responsible party is then responsible for notifying the data breach to the Information Regulator. Under no circumstances should the Company, when it is acting as an operator for a Responsible party notify a personal data breach directly to the Information Regulator or a data subject, unless otherwise advised by such Responsible party in writing.
- As soon as any member of staff discovers or receives a report of a data breach, they must inform the Information Officer as soon as possible and without delay. If the breach occurs or is discovered outside normal working hours, then notification should be sent as soon as is practicable.
- An emailed report can be submitted to the Information Officer at stefan@mandalaconsulting.co.za in the first instance and should include accurate details of the incident. The Information Officer can be contacted telephonically at 0769073277.
- An initial assessment of the data breach by the Information Officer will include a written collection and report of as much information as possible about the incident in order to fully assess the impact of the data breach and determine actions required.

Step 4: Evaluation and Response:

- When the Company's response to a data breach has reached a conclusion, the Information Officer together with DPT, will undertake a full review of both the causes of the breach and the effectiveness of the response. The full review is reported to the Company board for information and discussion as soon as possible after the data breach has been identified.

- If through the review, systematic or ongoing problems associated with weaknesses in internal processes or security measures have been identified as a cause of the data breach, then appropriate action plans will be drafted, actioned and monitored to rectify any issues and implement recommendations for improvements. Where the Information Officer deems necessary and as required by the Company's procedure, the board will be party to discussions regarding action plans and be able to monitor progress against the actions appropriately.
- If a breach warrants a disciplinary investigation, legal advice will be sought through Human Resources channels.

7) Implementation of these Procedures:

- The Information Officer will be responsible for ensuring that staff are aware of these procedures for reporting and managing data breaches. Data protection training for all staff is mandatory, including new employees and all staff will undertake refresher training annually.
- If staff have any queries or questions relating to these procedures, they should discuss this with their Department Head/line manager and/or the Information Officer.

8) Complaints about our Data Breach Management Procedure:

- If any person believes that a data breach has not been dealt with properly, a complaint should be made to the Company through our normal complaints procedure. This does not affect any right a person may have in terms of POPIA to lodge a complaint directly with the Information Regulator.

Last updated: _____ July 2021



MANDALA CONSULTING

INTEGRATION FOR SUSTAINABILITY



MANDALA CONSULTING
INTEGRATION FOR SUSTAINABILITY

Employee Privacy Notice

Purpose of this Employee Privacy Notice

This Employee Privacy Notice explains our practices as the responsible party regarding the processing of personal information relating to our employees in connection with their employment at *Mandala Consulting* (hereinafter the “**Company**”). This document is not part of the employment contract, and we may update it from time to time, e.g. in accordance with the Protection of Personal Information Act 4 of 2013 (“**POPIA**”) or other applicable law, or if we implement new systems or processes that involve the use of personal information.

What Personal Information is collected?

The Company collects and processes the following categories of personal information about you (hereinafter the “**Personal Data**”):

- **identification data**, such as your name, employee/staff ID, citizenship, date of birth, personal identification number/social security number and tax reference;
- **contact details**, such as your work and home addresses, telephone numbers, email addresses, and emergency contact details;
- **information about your job**, such as job title and code, work location, division, department, position level, employment contract, assigned tasks and projects, use of Company devices and IT tools, reporting derived from Company IT tools, registration of working hours, flexitime and holiday registration, manager's name, business travel data, ethics and compliance training data, start and end date;
- **information about your salary and benefits**, such as your basic salary, bonus and commission entitlements, insurance benefits (including information about you and your dependents that we provide to the insurer), tax code, accrued salary information, and information relating to your pension;
- **communication data/IT information**, such as IP address and user login name, emails, telephone connections; and
- **performance and disciplinary information**, such as performance reviews, evaluations and ratings, information about disciplinary allegations, the disciplinary process and any disciplinary warnings, details of grievances, and any outcome.

In addition, the Company processes the following special categories of personal information about you (collectively, "**Sensitive Personal Data**"):

- **number of sick days** for purposes of administering and providing compensation, administering the workforce (e.g., workforce planning), and compliance with applicable laws and employment-related requirements (e.g., statutory wage tracking);
- **information on work-related accidents** for purposes of administering and providing compensation (e.g., insurance compensation), and compliance with applicable laws and employment-related requirements (e.g., work safety, reporting obligations);
- **information on disability** (if provided voluntarily) for purposes of administering the workforce (e.g., accommodating the work place) and compliance with applicable laws and employment-related requirements; and
- **information on maternity leave** for purposes of administering the workforce (e.g., workforce planning), and compliance with applicable laws and employment-related requirements.

The Company stores and processes such Personal Data and Sensitive Personal Data that the Company receives from you in connection with the employment relationship. To the extent necessary, the Company also processes such Personal Data and Sensitive Personal Data that the Company lawfully received from public sources, other group companies and/or other authorised third parties (e.g. public authorities).

You are obliged to provide the Personal Data and, where applicable, Sensitive Personal Data, as part of your employment. If you do not provide the (Sensitive) Personal Data you may not be able to perform your job or receive your salary, and the Company may be required to terminate your employment.

The purpose of collecting Personal Data and Sensitive Personal Data

Sensitive Personal Data is collected, processed and used for the purposes mentioned above.

Personal Data is collected, processed and used for the following purposes:



Purpose	Categories of Personal Data Involved
administering and providing compensation, benefits and other work-related allowances , including reporting of benefit entitlements and use, such as discount agreements and Company share programme entitlements, if applicable	identification data, contact details, information about your job, information about your salary and benefits, and performance and disciplinary information
administering the workforce , including managing work activities, providing promotions, producing and maintaining corporate organisation charts, matrix management, entity and intra-entity staffing and team management, managing and monitoring business travel, carrying out workforce analysis, conducting talent management and career development, providing references as requested, and administering ethics and compliance trainings, where applicable	identification data, contact details, information about your job, information about your salary and benefits, and performance and disciplinary information
complying with applicable laws and employment-related requirements along with the administration of those requirements, such as income tax and employment and immigration laws	identification data, contact details, information about your job, information about your salary and benefits, and performance and disciplinary information
ensuring compliance with applicable the Company rules, guidelines and procedures , including without limitation avoiding the use of unauthorised file share programs and the use of the Company email accounts for illegal or inappropriate purposes	identification data, contact details, information about your job, information about your salary and benefits, communication data/IT information, and performance and disciplinary information

communicating with your designated contacts in case of an emergency	identification data and contact details
responding to and complying with requests and legal demands from regulators or other authorities in or outside of your home country	identification data, contact details, information about your job, information about your salary and benefits, communication data/IT information, and performance and disciplinary information

The legal basis for collecting Personal Data

The processing of your Personal Data is necessary for the performance of your employment contract.

Moreover, the processing of your Personal Data is necessary to comply with a legal obligation, in particular in the area of labour and employment law, social security and protection law, data protection law, tax law, and corporate compliance laws.

Finally, in certain cases, the processing of your Personal Data is necessary to fulfil or protect the legitimate interest of the Company. The legitimate interests and objectives of the Company could be in particular:

- measures to maintain operational activity (e.g. succession planning),
- measures for personnel development planning (e.g. evaluation),
- prevention of fraud, misuse of company IT systems, or money laundering,
- physical security, IT and network security,
- measures due to organizational changes, e.g. mergers and acquisitions and
- offer employee benefits such as discount agreements or share programme entitlements,
- implementation and operation of a group-wide matrix structure and group-wide information sharing, measures to maintain operational activity (e.g. succession planning), where applicable.

The Company has deemed that these interests override any interests or fundamental

rights and freedoms you may have which require the protection of personal data unless otherwise prescribed by law. Special regard is given to the reasonable expectations of you as an employee in the employment relationship, and the fact that the processing is ultimately also in your interest.

The legal basis for collecting Sensitive Personal Data

The processing of your Sensitive Personal Data is necessary for the purposes of carrying out the obligations and exercising the specific rights of the Company or you in the field of employment law and labour law and as permitted by POPIA.

Moreover, the processing of your Sensitive Personal Data is necessary for the purposes of establishing, exercising, or defending legal claims.

Your Personal Data and Sensitive Personal Data may only be processed for different purposes if this is necessary to comply with legal or regulatory obligations (e.g. transfer to courts or criminal prosecution authorities), if you have consented to the respective processing, or if the processing is otherwise lawful under applicable law. If processing for a different purpose takes place we may provide you with additional information.

Details of the Responsible Party and recipients of the Personal Data and Sensitive Personal Data

Within the Company, access to Personal Data and Sensitive Personal Data will be granted to departments and persons, e.g. superiors, HR department, works councils and other control functions on a need to know basis and to the extent required to comply with a contractual or statutory obligation.

The Company's subsidiaries and/or affiliates may receive your personal data as necessary for the purposes mentioned above, in particular in order to administer the workforce, to operate in the matrix structure, monitor and ensure compliance with applicable Company procedures, and respond to and comply with requests and legal demands. The transfer to these persons is based on our legitimate interests, such as personnel management, or for

IT support purposes.

The Company can share your Personal Data and Sensitive Personal Data with third parties acting as the Company's operators for processing your Personal Data and Sensitive Personal Data according to the purposes mentioned above. The following types of operators are used:

- Business partners who assist the Company in payroll matters, including providing systems for the processing
- Business partners who assist the Company in IT administration matters, including providing systems for the processing
- Business partners who assist the Company in employee administration matters, including providing systems for the processing
- Business partners who assist the Company in travel management matters, where applicable.
- Other recipients, typically consultants, that will assist with IT support for the above systems and assist with the processing of your Personal Data and Sensitive Personal Data on behalf of the Company.

Other authorised third parties may need to access or store Personal Data and Sensitive Personal Data if required or permitted by applicable law (e.g. governmental authorities, courts, external advisers and similar third parties that are public bodies).

Transfer of the Personal Data and Sensitive Personal Data

In certain cases, your Personal Data and Sensitive Personal Data may be transferred to outside of the Republic of South Africa ("**RSA**"). The Company ensures that such transfer will be carried out in accordance with POPIA and/or other relevant law. This entails that any party outside of RSA which comes into possession of your Personal Data and Sensitive Personal Data must ensure an adequate level of protection, for example by entering into the standard contractual clauses, or implement and comply with binding corporate rules, where applicable. If you have any inquiries in relation hereto, you are welcome to contact the Company – please see the contact information below in the '*How*

can you access your Personal Data and Sensitive Data?/Further rights' section.

Retention period

Your Personal Data is stored by the Company and/or our service providers/operators, to the extent necessary for the performance of our obligations and strictly for the time necessary to achieve the purposes for which the information is collected, in accordance with POPIA. Please note that the employment relationship is a continuing obligation existing for a longer period. When the Company no longer needs to use your personal data to comply with contractual or statutory obligations, we will remove it from our systems and records and/or take steps to properly anonymise it so that you can no longer be identified from it, unless we need to keep your information, including personal data, to comply with legal or regulatory obligations to which the Company is subject, e.g. statutory retention periods, or if we need it to preserve evidence within the statutes of limitation.

How can you access your Personal Data and Sensitive Personal Data?/Further rights

Under POPIA and any other applicable law, you may have various rights (under the conditions set out in such applicable law).

Withdrawal of consent: If you have declared your consent for any Personal Data processing activities you can withdraw this consent at any time with future effect. Such a withdrawal will not affect the lawfulness of the processing prior to the consent, or the continued processing if the law so requires.

Right of access: You may have the right to obtain from us confirmation as to whether or not (Sensitive) Personal Data concerning you is processed, and, where that is the case, to request access to this (Sensitive) Personal Data. The access information includes – inter alia – the purposes of the processing, the categories of (Sensitive) Personal Data concerned, and the recipients or categories of recipients to whom the (Sensitive) Personal Data has been or will be disclosed. However, this is not an absolute right and the interests of other persons may restrict your right of access.

You may have the right to obtain a copy of the (Sensitive) Personal Data undergoing processing. For further copies requested by you, we may charge a reasonable fee based on administrative costs.

Right to rectification: You may have the right to obtain from us the rectification of inaccurate (Sensitive) Personal Data concerning you. Depending on the purposes of the processing, you may have the right to have incomplete (Sensitive) Personal Data completed, including by means of providing a supplementary statement.

Right to erasure ("right to be forgotten"): Under certain circumstances, you may have the right to obtain from us the erasure of (Sensitive) Personal Data concerning you and we may be obliged to erase such (Sensitive) Personal Data.

Right to restriction of processing: Under certain circumstances, you may have the right to obtain from us restriction of processing your (Sensitive) Personal Data. In this case, the respective data will be marked and may only be processed by us for certain purposes.

Right to object: Under certain circumstances, you may have the right to object the processing of your (Sensitive) Personal Data by Company, on grounds relating to your particular situation, at any time. Company may be required to cease processing your personal data.

Right to data portability: Under certain circumstances, you may have the right to receive the (Sensitive) Personal Data concerning you, which you have provided to us, in a structured, commonly used and machine-readable format and you may have the right to transmit that data to another entity without hindrance from us.

If you would like to know more or wish to exercise one or more of the rights listed above, you are welcome to contact the Company through the Company's HR channel or applicable Company communication channel in accordance with the Company's internal policies and procedures.

Alternatively you may contact the Company's Information Officer at:

Mr Stefan Viljoen

Contact Number: 076 907 3277

Email address: Stefan@mandalaconsulting.co.za

Filing of complaints

In case of complaints, you also have the right to lodge a complaint with the Information Regulator regarding the processing of your Personal Data and/or Sensitive Personal Data.



Changes to the Privacy Notice

We reserve the right to change or supplement this Employee Privacy Notice at any time. To the extent the changes of Employee Privacy Notice are regarded as material and significant, you will be informed hereof, for example via email on Insite.

Last updated: July 2021



MANDALA CONSULTING
INTEGRATION FOR SUSTAINABILITY



MANDALA CONSULTING
INTEGRATION FOR SUSTAINABILITY

Operator Agreement



Table of Contents

1. Recordal3	
2. Definitions & Interpretation	3
3. Scope of Processing	4
4. Processing of Personal Data	5
5. Ownership of Personal Data	5
6. Instructions of Responsible Party	5
7. General obligations of Operator	6
8. Technical and organisational measures	7
9. Information Officer	7
10. Obligations regarding personnel	8
11. Sub-Operators	8
12. Data Processing within the RSA	9
13. Control and audit rights	9
14. Term and Termination	9
15. Miscellaneous	10
16. Indemnity	10
Annex 1 – Scope of Processing under Principal Agreement	12
Annex 2 – Technical and Organisational Measures	14
Annex 3 – Information Officer	17
Annex 4 – Approved Sub-Operators	18



MANDALA CONSULTING
INTEGRATION FOR SUSTAINABILITY

1. Recordal

This is an operator agreement entered into between

(1) _____,
(Registration No./ID number: _____) (“**Responsible Party**”).

and

(2) _____,
(Registration No./ID number: _____) (“**Operator**”).

(the Responsible Party and Operator shall hereinafter collectively be referred to as the “**Parties**”)

Preamble

- (A) Responsible Party and Operator have entered into one or more service agreements regarding the supply of certain products and/or services (each a **Principal Agreement**).
- (B) This agreement (**Agreement**) shall ensure that the data protection requirements under the Data Protection Laws are fully complied with.

Now, therefore, the Parties agree as follows:

2. Definitions & Interpretation

2.1 The following expressions shall have the meaning as defined hereunder:

Data Breach means a suspected or actual breach of data protection or security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, Personal Data.

Data Protection Laws means the data protection laws applicable to Responsible Party and/or Operator, and POPIA.

Data Subject shall have the meaning ascribed to it in terms of POPIA.

Good Industry Practice means the exercise of the professional standard of skill, care, diligence, prudence and reasonable foresight as may reasonably be expected from a data Operator for the type of services provided under the Principal Agreement and taking into account the state of the art;

Information Officer shall have the meaning ascribed to it in terms of POPIA;

Personal Data means any information relating to an identified or identifiable person as further defined in the Data Protection Laws and that is provided by Responsible Party or by any affiliate of Responsible Party using the services under the Principal Agreement to Operator or collected by Operator on Responsible Party's

behalf or on behalf of any affiliate of Responsible Party using the services under the Principal Agreement under this Agreement, including the personal data and categories of personal data more specifically described in **Annex 1**.

POPIA means the Protection of Personal Information Act (Act No. 4 of 2013), as amended from time to time.

Processing of Personal Data is the collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction in the meaning of the Data Protection Laws and as further specified in this Agreement. **“Process”**, **“Processes”** and **“Processed”** will be construed accordingly.

Sub-Operator means another Operator engaged by Operator for carrying out specific Processing activities on behalf of Responsible Party.

2.2 This Agreement shall be interpreted according to the following provisions, unless inconsistent with or otherwise indicated by the context –

- 2.2.1 the headings of clauses have been inserted for convenience only and shall not affect the interpretation of this Agreement;
- 2.2.2 any reference to one gender shall include the other gender and the neuter;
- 2.2.3 words in the singular number shall include the plural and vice versa;
- 2.2.4 references to a “person” shall include where the context so requires, an individual, firm, company, corporation, juristic person, local authority, and any trust, organisation, association or partnership, whether or not having separate legal personality;
- 2.2.5 words defined in a specific clause have the same meaning in all other clauses of this Agreement;
- 2.2.6 references to the provisions of any law shall include any such law as amended, varied, replaced, re-enacted, restated or reinterpreted from time to time;
- 2.2.7 if any definition in this clause 2 (*Definitions and Interpretation*) contains a substantive provision conferring rights or imposing obligations on any Party, effect shall be given to such provision as if it was a substantive provision in the body of this Agreement; and
- 2.2.8 the Parties agree that no provision or word used in this Agreement shall be interpreted to the disadvantage of either Party because that Party was responsible for or participated in the preparation or drafting of this Agreement or any part of it;
- 2.2.9 if there is any conflict between the provisions of this Agreement and the provisions of the Principal Agreement, then the provisions of this Agreement shall prevail, unless the provisions of the Principal Agreement provide for more onerous requirements, especially in relation to the Processing of Personal Data, in which event the more onerous requirements will prevail.
- 2.2.10 The Recordal (clause 1) forms part of this Agreement and should be taken into account in the interpretation of this Agreement’s provisions.

3. Scope of Processing

The Parties agree in relation to the Personal Data to be Processed under this Agreement on

- (a) the subject-matter of the Processing services,
- (b) the duration of Processing,
- (c) the nature of Processing,
- (d) the purposes of Processing,
- (e) the types of Personal Data including any special categories of data; and
- (f) the categories of Data Subjects

set out in **Annex 1**.

4. Processing of Personal Data

- 4.1 Between the Parties, Responsible Party solely determines the purposes and manner of the Processing of Personal Data and Operator Processes the Personal Data solely on behalf of and in the interests of Responsible Party.
- 4.2 Responsible Party shall be responsible for the lawfulness of the Processing under the Data Protection Laws applicable to Responsible Party's Processing of Personal Data, including in particular, the lawfulness of the transfer of Personal Data to Operator for the purposes of this Agreement. Responsible Party may require Operator to Process Personal Data of any of its affiliated companies (using the services under the Principal Agreement) under this Agreement, provided that Responsible Party is responsible for obtaining all necessary consents of its affiliates and for being effectively authorized to give instructions on behalf of its affiliated companies.
- 4.3 Operator shall Process the Personal Data only for Responsible Party's purposes and for no other purposes. Operator shall not use any Personal Data for any of its own purposes or for any purposes of a third party, including commercial, analytical or statistical purposes. This shall also apply in relation to any pseudonymised or anonymised data, information, business secrets and know-how derived from the Personal Data. Any such information shall be deemed as confidential information of Responsible Party in the meaning of the Principal Agreement.
- 4.4 Operator shall Process the Personal Data only with the agreed methods, means and facilities set out in this Agreement and in accordance with the terms and conditions of this Agreement and the Principal Agreement.

5. Ownership of Personal Data

- 5.1 Between the Parties, Responsible Party shall be the sole owner of all Personal Data Processed and collected by Operator on Responsible Party's behalf.
- 5.2 Operator shall not acquire any rights or interest in Responsible Party's Personal Data or pseudonymised or anonymised data, information, business secrets or know-how derived from the Personal Data.

6. Instructions of Responsible Party

- 6.1 Operator shall only Process and use the Personal Data in accordance with the documented instructions of Responsible Party and the applicable Data Protection Laws.
- 6.2 Responsible Party may at any time give instructions to Operator regarding the Processing of the Personal Data. Instructions may be changed, amended or replaced by Responsible Party at any

time either generally and/or on a case-by-case basis. Operator shall without undue delay comply with any such instructions.

- 6.3 Any instructions shall generally be given in writing or in electronic format (e.g. by e-mail). In case of imminent danger or urgency, Responsible Party may give instructions orally (e.g. by phone), provided that Responsible Party shall confirm any such instructions in writing or in electronic format as soon as reasonably possible thereafter.
- 6.4 All instructions regarding the Processing of Personal Data shall be given only by the designated personnel of Responsible Party to the designated personnel of Operator. Responsible Party and Operator will inform each other about the authorized personnel for these purposes.
- 6.5 Where Operator believes that compliance with the instructions of Responsible Party would result in a violation of any Data Protection Law, Operator shall immediately inform Responsible Party thereof and request Responsible Party's decision. Operator may suspend the implementation of any instructions until Responsible Party has either confirmed or changed the relevant instructions. Operator shall have no withholding rights or other rights to refuse compliance with Responsible Party's instructions regarding the handling of Personal Data. This applies in particular as regards instructions and requests of Responsible Party regarding correction, alternation, pseudonymisation, anonymization, disclosure, making available, restriction, erasure, destruction or return of Personal Data.

7. General obligations of Operator

- 7.1 Operator shall maintain all Personal Data as strictly confidential and shall not disclose the Personal Data to, or allow access by, any unauthorized third Parties, unless required to do so by mandatory laws applicable to Operator.
- 7.2 Operator shall notify Responsible Party without undue delay in the event of significant disruptions of the services, of suspected or actual infringements of this Agreement and of any other material irregularity in relation to the Processing of Responsible Party's Personal Data arising from Operator, its personnel or other third Parties. Operator will without undue delay investigate and rectify any non-compliance. Upon Responsible Party's request, Operator shall adequately inform Responsible Party with regard to the suspected or actual non-compliance.
- 7.3 Operator shall notify Responsible Party without undue delay after becoming aware of a Data Breach. The notification shall describe the nature of the Data Breach and include where possible, the categories and approximate number of Data Subjects concerned, and the categories and approximate number of personal data records concerned.
- 7.4 Operator shall also describe to Responsible Party without undue delay the measures taken or proposed to be taken to address the Data Breach, including, where appropriate, measures to mitigate its possible adverse effects.
- 7.5 In any event Operator shall take all reasonable measures to secure the Personal Data from any further data breaches of similar nature and limit any adverse effects. Operator shall provide reasonable assistance to Responsible Party to help Responsible Party meet its obligations under the Data Protection Laws to inform Data Subjects and the competent supervisory authorities of a Data Breach.
- 7.6 Operator shall inform Responsible Party without undue delay if and when the Personal Data of Responsible Party held by Operator is or is likely to become subject to any seizures, enforcement, insolvency measures or any other measures of third Parties. Operator shall inform all relevant third Parties that claim access to, or intent to take possession of, Responsible Party's Personal Data that Responsible Party is the sole owner of such Personal Data.

- 7.7 Operator shall inform Responsible Party without undue delay of requests, audits or other enquiries by a supervisory authority or any other authority in relation to Responsible Party's Personal Data or its Processing by Operator. Operator shall make available to Responsible Party any relevant reports, statements or decisions of such authority or correspondence with such authority to the extent they concern Responsible Party's Personal Data or the Processing thereof.
- 7.8 If and to the extent Responsible Party is obliged to provide any Data Subjects with information regarding the Processing of their data by Operator, Operator shall reasonably support Responsible Party in responding to such request and provide all necessary information regarding the Processing by Operator without undue delay. In case Data Subjects address any such requests or enquiries directly to Operator, Operator will forward those to Responsible Party without undue delay. Operator shall not respond to such requests or enquiries of Data Subjects on its own or on behalf of Responsible Party without prior consent of Responsible Party, except as otherwise required by mandatory laws applicable to Operator.
- 7.9 Operator shall reasonably support Responsible Party to fulfil any notification obligations to domestic or foreign supervisory authorities or to comply with other obligations under the Data Protection Laws related to the Processing by Operator. This shall include in particular the provision of all necessary information on Operator and its Sub-Operators, their undertakings, facilities, technical and

organisation measures and other circumstances of Processing the Personal Data of Responsible Party.

- 7.10 Operator shall support Responsible Party appropriately in connection with the defence against any claims against Responsible Party due to any actual or alleged violation of Data Protection Laws by Operator or any of its Sub-Operators.
- 7.11 Operator shall indemnify Responsible Party against any and all loss and or damages that Responsible Party may incur as a result of a failure and/or a breach by Operator of any of its obligations in terms of this Agreement, and especially a failure and/or a breach and/or an infringement of the Data Protection Laws by Operator.

8. Technical and organisational measures

- 8.1 Operator shall during the term of this Agreement implement and maintain appropriate technical and organisational measures such that the Processing will meet the requirements of the Data Protection Laws and at least Good Industry Practice.
- 8.2 More specifically, Operator shall apply at least the technical and organisational measures detailed in **Annex 2** to this Agreement. The Parties shall mutually agree on updates of **Annex 2** from time to time taking into account improvements of technological standards.
- 8.3 Operator shall notify any changes to the technical and organisational measures that might have an adverse impact to the security of the Processing and the Personal Data.

9. Information Officer

The contact details of the Information Officer of both Parties (if applicable) at the date hereof are set out in **Annex 3**. Each Party shall inform the other Party in writing or electronically (e.g. by e-mail) of any change of its Information Officer.

10. Obligations regarding personnel

- 10.1 Operator shall ensure that its personnel authorised to Process the Personal Data will comply with the terms and conditions of this Agreement.
- 10.2 Operator may grant access and access rights to its personnel in relation to Personal Data only on a need-to-know basis to the extent necessary for the relevant person to comply with his/her obligations and in accordance with Operator's technical and organisational measures.
- 10.3 Operator shall ensure and adequately document that all of its personnel involved in the Processing:
 - (a) have committed themselves to confidentiality in connection with their employment agreement or are under an appropriate statutory obligation of confidentiality; and
 - (b) have been duly instructed and trained in relation to compliance with their obligations under Data Protection Laws and Operator's contractual obligations regarding the handling of Personal Data.
- 10.4 Operator shall appropriately monitor the compliance of its personnel with data protection and confidentiality obligations.
- 10.5 Responsible Party may at any time inspect any documentation of Operator regarding the data protection and confidentiality obligations of its personnel and/or may request a written confirmation that Operator has complied with its obligations regarding personnel under this section.

11. Sub-Operators

- 11.1 Operator may only engage any Sub-Operators with the prior written consent of Responsible Party and in accordance with the Principal Agreement. The pre-approved Sub-Operators and the services and tasks for which they are approved are set out in **Annex 4** to this Agreement.
- 11.2 The approved Sub-Operators shall comply with all requirements of this Agreement in all respects, in addition to, and not instead of, their obligations under any EU Standard Contractual Clauses entered into and the Data Protection Laws. Responsible Party shall have in particular the same instruction, control and audit rights vis-à-vis each Sub-Operator as vis-à-vis Operator under this Agreement. Operator ensures that Responsible Party may at any time exercise such rights vis-à-vis the relevant Sub-Operator.
- 11.3 Operator shall regularly monitor and control the compliance of its Sub-Operators with this Agreement. Operator may only transfer any Personal Data to the Sub-Operator after having sufficiently convinced itself that the Sub-Operator provides adequate guarantees that it will comply with the terms and conditions of this Agreement.
- 11.4 Responsible Party shall be entitled to receive information from Operator on the material content of the data processing agreement between Operator and its Sub-Operator. This includes a copy of the relevant data protection provisions agreed between Operator and its Sub-Operator (excluding any commercial terms or pricing information).
- 11.5 The terms and conditions of the Principal Agreement regarding the employment of sub-contractors shall remain unaffected and shall apply in addition to the above provisions.
- 11.6 Operator shall maintain up-to-date records of the name and contact details of approved Sub-Operators, their representatives and Information Officer. Upon Responsible Party's request, Operator will make available such information to Responsible Party.

12. Data Processing within the RSA

- 12.1 Unless otherwise agreed in writing, any Processing by Operator hereunder shall only occur in the Republic of South Africa ("**RSA**") (herein after the "**Territory**"). For the avoidance of doubt, Operator shall, in particular, not allow any remote access from any other country outside the Territory. This shall also apply to any transfer to, or access from, other countries even within the same legal entity or within the same group of undertakings. Operator shall notify to Responsible Party any material changes regarding the Processing locations even within the Territory without undue delay.
- 12.2 Any Processing of Personal Data by an Operator outside the Territory will only be permitted at Responsible Party's sole and free discretion and upon signing such other agreement or terms as the Responsible Party may determine in its sole discretion ("**Global DPA**"), between Responsible Party and Operator. Unless otherwise agreed in writing, this shall apply in relation to any Processing outside the Territory, regardless of the existence of any standard contractual clauses or binding corporate rules that may exist from time to time.
- 12.3 Sub-Processing: Operator warrants and represents that, before the commencement of any sub-Processing of Personal Data outside the Territory, Operator's entry into a Global DPA as agent for and on behalf of that Sub- Processor, will have been duly and effectively authorised, or subsequently ratified, by that Sub-Operator.

13. Control and audit rights

- 13.1 Responsible Party may perform, or have performed by a knowledgeable third party auditor being subject to contractual confidentiality obligations or professional secrecy, regular audits of Operator's compliance with the Data Protection Laws and this Agreement including the agreed technical and organisational measures for the Processing. Any regular audit may not be requested by Responsible

Party more than once per contract year. The third party auditor shall not be a competitor of Operator or the Sub-Operators used. The audit may include an inspection at the relevant Processing locations of Operator upon reasonable advance notice (of five business days) during the usual business hours and without significant disruption of the services and business of Operator. Operator shall support any such audit and cooperate with Responsible Party in exercising such right. This shall include in particular the provision of all necessary information on Operator and its Sub-Operators, their undertakings, facilities, technical and organization measures and other circumstances of Processing Personal Data of Responsible Party.

- 13.2 Responsible Party and Operator may agree in writing that any audit and inspections may be replaced wholly or in part by up-to-date attestations, reports or extracts thereof from independent bodies (e.g. external independent auditors, internal audit, the Information Officer, the IT security department or quality audits) or suitable certification on the basis of IT security or data protection audits.
- 13.3 If the audit reveals that Operator does not comply with the Data Protection Laws or its obligations under this Agreement, Operator shall take, at its own cost, all corrective measures including any temporary work-arounds necessary to achieve compliance.

14. Term and Termination

- 14.1 This Agreement is entered into for the term of the Principal Agreement and shall continue to apply until the completion of all services under the Principal Agreement, including any termination assistance (if any) to be provided by Operator.
- 14.2 Upon expiry or termination of this Agreement, Operator shall, unless otherwise agreed in the Principal Agreement, return the Personal Data to Responsible Party or a third party designated by

Responsible Party or, upon Responsible Party's instruction, securely delete the Personal Data. Upon Responsible Party's request, Operator shall confirm secure deletion of all Personal Data in writing signed by a duly authorized representative within thirty days from the receipt of such request.

- 14.3 Operator's statutory retention obligations shall remain unaffected. If Operator claims any statutory obligations to retain any Personal Data notwithstanding the above provisions, Operator shall notify to Responsible Party upon request the legal basis and the Personal Data concerned without undue delay. For the duration of any such retention, this Agreement shall continue to apply.

15. Miscellaneous

- 15.1 Unless otherwise set out in the Principal Agreement, each Party shall bear its own costs in connection with the performance of this Agreement. All charges payable by Responsible Party are exclusively set out in the Principal Agreement.
- 15.2 Operator shall not be permitted to suspend or withhold performance of any of its obligations under this Agreement.
- 15.3 Neither Party shall assign, transfer or otherwise deal with any of its rights or obligations under this Agreement without the prior written consent of the other Party.
- 15.4 This Agreement and its Annexes set out the entire agreement between the Parties regarding the Processing together with the Principal Agreement. This Agreement supersedes any prior agreement of the Parties on the subject matter of this Agreement.
- 15.5 No amendment, variation or waiver of this Agreement including its Annexes and schedules shall be valid unless in writing and duly executed by or on behalf of all of the Parties to it.
- 15.6 Should individual provisions of this Agreement be or become invalid, the validity of the remaining provisions shall remain unaffected. The statutory provisions shall apply instead of the invalid provisions.
- 15.7 This Agreement shall be governed by, and interpreted in accordance with, the laws of the RSA.
- 15.8 Unless otherwise agreed in the Principal Agreement, venue for all disputes arising out of or in connection with this Agreement shall be the seat of Responsible Party.

16. Indemnity

- 16.1 The Parties agree that if Responsible Party is held liable for a violation of data protection legislation, or incurs any loss and/or damage as a result thereof, then to the extent that this is a result of a failure and/or breach by Operator of the terms and conditions of this Agreement, Operator hereby indemnifies Responsible Party for any cost, charge, damages, expenses or loss Responsible Party has incurred or may incur as a result of such breach and/or failure by the Operator.

* * *



MANDALA CONSULTING
INTEGRATION FOR SUSTAINABILITY

On behalf of Responsible Party

On behalf of Operator

(Place, date)

(Signature)

(Place, date)

(Signature)

Name:

Function:

Name:

Function:

Annex 1 – Scope of Processing under Principal Agreement

Subject-matter of the services and Processing of Personal Data	[•]
Duration of Processing	☐ For the duration of the Principal Agreement ☐ Other (please detail):
Nature of Processing	[•]
Purposes of Processing	[•]
Types of Personal Data	☐ Employee data (please detail): ☐ Customer data (please detail): ☐ Supplier data (please detail): ☐ Consumer data (please detail): ☐ Other (please detail):
Special categories of Personal Data	☐ Data revealing racial or ethnic origin (please detail): ☐ Data revealing political opinions (please detail): ☐ Data revealing religious or philosophical beliefs (please detail): ☐ Data revealing trade union membership (please detail): ☐ Genetic or biometric data (please detail): ☐ Data concerning health (please detail): ☐ Data concerning a person's sex life or sexual orientation (please detail): ☐ Data relating to criminal convictions and offences (please detail): ☐ Other (please detail):
Categories of Data Subjects	☐ Responsible Party Employees (please detail): ☐ Customer employees (please detail): ☐ Supplier employees (please detail):



	☐ Consumers (please detail): ☐ Other (please detail):
--	--

* * *

Annex 2 – Technical and Organisational Measures

A. General Principles

Based on a risk assessment, Responsible Party and Operator agree on the technical and organisational measures that are intended to achieve the following purposes:

1. Prevent access of unauthorized persons to processing facilities (access control),
2. prevent of unauthorized reading, copying, changing or deleting of data carriers (data carrier control),
3. prevent the unauthorized entry of personal data and the unauthorized view, modification and deletion of stored personal data (storage control),
4. prevent the use of automated Processing systems by means of data transmission facilities by unauthorized persons (user control),
5. guarantee that the persons entitled to use an automated Processing system have access only to the personal data covered by their access authorization (access control),
6. ensure that it is possible to check and determine to which places personal data have been transmitted or made available by means of data transmission facilities (transmission control),
7. ensure that it is possible to subsequently verify and ascertain which personal data have been entered or changed at any time and by whom in automated Processing systems (input control),
8. ensure that the confidentiality and integrity of the data are protected in the transfer of personal data and the transport of data carriers (transport control),
9. guarantee that systems used can be restored in case of failure (recoverability),
10. ensure that all functions of the system are available and any malfunctions occurring are reported (reliability),
11. ensure that stored personal data cannot be damaged by system malfunction (data integrity),
12. guarantee that personal data Processed on behalf of a Responsible Party can only be Processed according to the instructions of the Responsible Party (order control),
13. ensure that personal data is protected against destruction or loss (availability control),
14. ensure that personal data collected for different purposes can be Processed separately (separability).

B. Technical and organisational measures

Responsible Party and Operator agree on the following technical and organisational measures that shall be implemented by Operator:

[Please complete or replace by Operator's more specific technical and organisational

measures]

Physical Access Control	
☐ Alarm system ☐ Protection of shaft entry to buildings ☐ Automatic entry control system ☐ Chip card or transponder system ☐ Locking system with code requirements ☐ Manual locking system ☐ Biometric access control ☐ Video surveillance of entrance zone	☐ Light barrier, motion detector ☐ Security locks ☐ Recording of visitors ☐ Careful selection of cleaning staff ☐ Careful selection of security staff ☐ Request to carrying credentials ☐ Recording of visitors
☐ Other/comments (please detail):	
User control, Storage Control	
☐ User authentication ☐ Use of user profiles ☐ Password assignment ☐ Authentication with biometrical systems ☐ Authentication with user name and password ☐ Assignment of user profiles to IT Systems ☐ Locking devices for cases ☐ Use of VPN- technology ☐ Locking of external interfaces	☐ Security locks ☐ Use of Intrusion-Detection Systems ☐ Use of antivirus software ☐ Encryption of data carriers in laptops ☐ Use of hardware firewall ☐ Use of software firewall ☐ Encryption of mobile data carriers ☐ Encryption of smart phone content ☐ Use of central Smartphone Administration Software (e.g. for external deleting of personal data)
☐ Other/comments (please detail):	
Access Control, Input Control	
☐ Maintenance of an adequate authorization concept ☐ Administration of rights by system administrator ☐ As few administrators as necessary ☐ Password policies including rules regarding length of password and change of password	☐ Recording of accesses to applications, specially input, change or deletion of personal data ☐ Traceability of input, change and deletion of personal data by individual user name (not only user groups) ☐ Transparent allocation of rights to input, change or delete personal data in accordance with an authorization concept
☐ Other/comments (please detail):	
Transport Control	
☐ Secure storage of data carriers ☐ Physical deletion of data carriers prior to reuse ☐ Proper destruction of data carriers by certified service provider ☐ Use of shredder or service provider (if possible with privacy seal)	☐ Recording of destruction ☐ Encryption of data carriers ☐ Secure containers and packages ☐ Careful selection of transportation staff and vehicles
☐ Other/comments (please detail):	
Transmission control	
☐ Use of VPN technology ☐ Transfer of personal data anonymously or pseudo anonymously ☐ Email encryption	☐ SSL encryption (e.g. websites) ☐ Creating an overview of regular request and transmission procedures ☐ Documentation of who receives personal data
☐ Other/comments (please detail):	
Order control	
☐ Measures to ensure that personal data Processed on behalf of others are Processed strictly in compliance with the Sub Processor r's instructions ☐ Careful selection of Sub-Operator, in particular in terms of data security ☐ Review of the Sub-Operator's security measures ☐ Obligation of employees to commit to data protection and confidentiality	☐ Appointment of Information Officer ☐ Secured destruction of personal data after termination of the agreement ☐ Agreement of effective control rights towards Sub-Operator ☐ Regular review of Sub-Operator
☐ Other/comments (please detail):	

Data Integrity, Availability Control

- | | |
|--|--|
| ☐ Measures to ensure that personal data are protected against accidental destruction, change or loss.
☐ Uninterruptable power supply (UPS)
☐ Air-condition in server rooms
☐ Devices for monitoring temperature and humidity in server rooms
☐ Secured power outlet strips
☐ Fire and smoke detector
☐ Fire extinguishers in server rooms
☐ Other/comments (please detail): | ☐ Alarm system against unauthorized entrance to server rooms
☐ Maintenance of a backup and recovery concept
☐ Adequate testing of data recovery tools
☐ Maintenance of an emergency plan
☐ Storage of personal data backup on a safe and external place
☐ No server rooms under sanitary facilities
In flood areas: server rooms above the water level |
|--|--|

Separation Control

- | | |
|--|--|
| ☐ Measures to ensure that personal data collected for different purpose can be Processed separately.
☐ Physically isolated storage on separate systems or data carriers
☐ Other/comments (please detail): | ☐ Logical customer separation (software-sided)
☐ Maintenance of an authorization concept
☐ Determination of rights regarding data bases |
|--|--|

[C. Certificates

Responsible Party and Operator agree on the following certificates that Operator shall maintain during the term of the Agreement or replace by comparable certifications:

[•]][OPTIONAL]

* * *



MANDALA CONSULTING
INTEGRATION FOR SUSTAINABILITY

Annex 3 – Information Officer

Information Officer of Responsible Party

Name: [●]
Address: [●]
Tel: [●]
Fax: [●]
E-Mail: [●]

Information Officer / Contact of Operator:

Name: [●]
Address: [●]
Tel: [●]
Fax: [●]
E-Mail: [●]

* * *



Annex 4 – Approved Sub-Operators

Sub-Operator (name and address)	Description of sub-contracted Processing services and tasks
[•]	[•]
[•]	[•]
[•]	[•]

* * *



MANDALA CONSULTING
INTEGRATION FOR SUSTAINABILITY



MANDALA CONSULTING
INTEGRATION FOR SUSTAINABILITY

Private Policy

1) Purpose of this privacy policy:

- The purpose of this privacy policy is to set out the basis upon which we process personal information when making use of our products and/or our services (“Products/Services”) or any of our platforms (herein after collectively referred to as our “Site/s”)
- By utilising our Products/Services or any of our Sites, you are accepting and consenting to the practice described in this privacy policy.

2) Interpretation and definitions:

- Words that are defined in the Protection of Personal Information Act No. 4 of 2013 (“POPIA”) and used in this privacy policy will bear the same meaning as in POPIA unless the context requires otherwise;
- Reference to “consent” shall include any electronic means by which you convey your acceptance and acknowledgement that you agree to us processing your personal information, whether it be by the clicking of a button, or through biometric means, subscribing, submitting or sending of a message, updating your profile or clicking “I Agree” button or pressing the “enter” button, or by any other means, to submit/convey any information to us;
- Any reference to singular shall include plural, and any reference to a certain gender shall include the opposite gender.

3) Introduction:

- We recognise the importance of protecting your privacy in respect of your personal information collected by us.
- In adopting this privacy policy, we wish to balance our legitimate business interests and your reasonable expectation of privacy. Accordingly, we will take appropriate and reasonable technical and organisational steps to prevent unauthorised access



to, or disclosure of your personal information. However, we do not guarantee that your personal information shall be 100% secure.

- Where there are reasonable grounds to believe that your personal information has been accessed or acquired by any unauthorised person, we will notify you and the Information Regulator which is appointed in terms of POPIA.
- We will delay notifying you of the unauthorised access or acquisition of your personal information if a public body responsible for detection, prevention or investigation of offences or the Information Regulator informs us that notifying you will impede a criminal investigation.
- When we notify you of the compromise to the security of your personal information, we will provide you with sufficient information to allow you to take protective measures against the potential consequences of the compromise.

4) Consent:

- By continuing to use our Products/Services and/or our Site:
 - You agree to the terms set out in this privacy policy. If you do not agree with this privacy policy, please do not continue to use our Products/Services and/or our Site and/or the Products/Services provided by any of our partners; and
 - You agree that we may process your personal information for, amongst other things, (i) the purposes of providing you with access to our Products/Services, our Site; and (ii) for any other purposes set out in this privacy policy.

5) Variation of privacy policy:

We reserve the right to vary the terms of this privacy policy. We will notify you of any such change and give you an opportunity to review the revised policy before you choose to continue to make use of our Products/Services and/or our Site. It is your responsibility to familiarize yourself with the most recent version of this privacy policy each time you access our Products/Services and/or our Site and before you elect to continue to make use of our Products/Services and/or our Site.

6) What type of personal information do we process:

The personal information that we may process includes information necessary for us to provide you with the Products/Services and to protect and ensure our legitimate business interests. This may include all of the categories of personal information listed in POPIA, and amongst other, include at least all of the following information: -

- **Information and content you provide.** We collect the consent, communications and other information you provide when you use our Products/Services, including when you sign up for an account, create or share content, and message or communicate with us via our Site or via any other means. Our systems automatically process content and communications you and others provide to analyse context and what's in them for the purposes described below. We specifically process your name and identity number, e-mail and physical addresses, postal address, contact information, information relating to your race, gender, and age, and such other information regarding yourself and/or your views if you choose to share same via our Site;
- **Your usage.** We collect information about how you use our Products/Services and/or our Site, such as the types of content you view or engage with; the features you use; the actions you take; the accounts you interact with; and the time, frequency and duration of your activities. For example, we log when you're using and have last used our Products/Services and/or our Site, and what posts, pages and other content you view on our Site. We also collect information about how you use certain features of our Products/Services and/or our Site;
- **Device Information.** As described below, we collect information from and about the computers, phones, connected TVs and other web-connected devices you use that integrate with our Site, and we combine this information across different devices you use. For example, we use information collected about your use of our Products/Services and/or our Site on your phone to better personalize the content (including ads) or features you see when you use our Products/Services on another device, such as your laptop or tablet, or to measure whether you took an action in

response to an advertisement we showed you on your device. Information we may obtain from these devices include:

- Device attributes: information such as the operating system, hardware and software versions, battery level, signal strength, available storage space, browser type, app and file names and types, and plugins.
- Device operations: information about operations and behaviours performed on the device, such as whether a window is foregrounded or backgrounded, or mouse movements (which can help distinguish humans from bots).
- Identifiers: unique identifiers, device IDs, and other identifiers, such as from services, apps, pages or accounts you use, or other identifiers unique to us or our Products/Services associated with the same device or account.
- Device signals: Bluetooth signals, and information about nearby Wi-Fi access points, beacons, and cell towers.
- Data from device settings: information you allow us to receive through device settings you turn on, such as access to your GPS location, camera or photos.
- Network and connections: information such as the name of your mobile operator or ISP, language, time zone, mobile phone number, IP address, and connection speed and, in some cases, information about other devices that are nearby or on your network, so we can do things like help you stream content to or through all your devices.
- Cookie data: data from cookies stored on your device, including cookie IDs and settings.
- Information from partners. Advertisers, Site developers, and publishers can send us information through, including our social plug-ins, such as our APIs. These partners provide information about your activities on our Site, including information about your device, websites you visit, purchases you make, the advertisements you see, and how you use their services. Whether or not you have an account with us or are logged into our Site. For example, a partner could use our API to tell us what pages you viewed, or a business could tell us about a purchase you made in its store. We also receive information about your online and offline actions and purchases from third-party data providers who have the rights to provide us with your information.



- Partners receive your data when you visit or use their services or through third parties they work with. We require each of these partners to have lawful rights to collect, use and share your data before providing any data to us.
- We will limit the types of personal information processed to only that to which you have given your consent and which is necessary for our legitimate business interests, or as allowed by law.

7) When will we process your personal information:

- Personal information may be processed by us when:
- You visit, browse, register, subscribe and/or apply for and use our Products/Services and/or our Site;
- You register to receive any notifications from us in respect of our email authentication service and/or our text message authentication service;
- We carry out research; and
- When or if required by law; and
- When and if it is in your best interest.
- You acknowledge that all personal information processed by us may be stored by us and used, inter alia, for any of the purposes, but not exclusively, listed in clause 8 below.

8) How do we use your personal information:

- We may use your personal information:
 - to deliver our Products/Services, including to personalise features and content (such as services, products and advertisements) and make suggestions for you (such as pages, services and information you may be interested in or topics you may want to follow) on or about our Products/Services or on our Site. To create personalised content that are unique and relevant to you, we use your connections, preferences, interests and activities based on the data we collect and learn from you and others (including any data with special protections you

choose to provide); how you use and interact with our Site; and the people, places, or things you're connected to and interested in, on and off our Site.

- to develop, test and improve our Products/Services and/or our Site, including by conducting surveys and research, and testing and troubleshooting new products and services and features.
- to select and personalise advertisements, offers and other sponsored content that we show you;
- to provide measurement, analytics, and other business services. We use the information we have (including your activity off our Products/Services, such as the websites you visit and advertisements you see) to help advertisers and other partners measure the effectiveness and distribution of their advertisements and services, and understand the types of people who use their services and how people interact with their websites, apps, and services.
- to promote safety, integrity and security. We use the information we have to verify accounts and activity, combat harmful conduct, detect and prevent spam and other bad experiences, maintain the integrity of our Products/Services, and promote safety and security on and off of our Products/Services. For example, we use data we have to investigate suspicious activity or violations of our terms or policies;
- to communicate with you. We use the information we have to send you marketing communications, communicate with you about our Products/Services, and let you know about our policies and terms. We also use your information to respond to you when you contact us;
- Research and innovate for social good. We use the information we have (including from research partners we collaborate with) to conduct and support research and innovation on topics of general technological advancement of our Products/Services.
- For helping us in any future dealings with you; and
- For any other purpose as legally authorised to do and as is allowed by law.

9) Where we store your personal information

- All of the information you provide to us is stored manually, and/or on our secure cloud-based platform and/or servers operated, maintained and protected in the Republic of South Africa (RSA);
- The information that we collect from you may also be transferred to, and stored at, a destination outside the RSA ("RSA"). It may also be processed by staff operating outside the RSA who work for us or for one of our suppliers, content providers or service providers. Such staff may be engaged in, among other things, the fulfilment of our obligations towards you, the processing of your payment details and the provision of support Products/Services. We will take all steps reasonably necessary to ensure that the information is treated securely and in accordance with this privacy policy, and that said destination's data protection legislation is similar to POPIA, and if such destination's data protection legislation is not similar to POPIA, then we shall only transfer your personal information with your consent, or if we are required by law to do so, or under an agreement with the relevant receipt in such destination whereby we ensure that adequate safeguards are put in place to ensure the protection of your personal information;
- Where we have given you (or where you have chosen) a password which enables you to access certain parts of our Site (login facility), you are responsible for keeping this password confidential. We ask you not to share a password with anyone. Should you share your password with anyone, you indemnify us against any damages or third party claims which resulted from said sharing;
- Records of the personal information will not be retained for longer than is necessary for operational or archiving purposes, unless retention of record is required or authorised by law. Records of the information may be retained for periods in excess of those contemplated for historical, statistical or research purposes. This will be subject to us establishing appropriate safeguards (which can include de-identifying the records) against the records being used for any other purpose;
- Unfortunately, the transmission of information via the internet is not completely secure. We will use appropriate and reasonable technical and organisational measurements to protect the information, we cannot however guarantee the

security of your data transmitted to our Site or to any other location by electronic means. Any transmission is at your own risk. However, once we have received the information, we will use appropriate and reasonable technical organisational measurements to try and prevent unauthorised access.

10) Sharing of your personal information:

- We will not disclose any of your personal information to any person, except when we have your consent and/or permission to do so or where we are required to do so in terms of law or if same is in your best interest;
- You agree that your personal information may be shared: -
 - to our holding companies, subsidiary companies, agents, advisers, partners, service providers and suppliers, or in the event of a change control if the ownership or control of all or a part of our Products/Services changes, we may transfer your information to such new owner.
 - where the law requires that we disclose your personal information to a party, and where we have reason to believe that a disclosure of personal information is necessary to identify, contact or bring legal action against a party who may be in breach of the terms or may be causing injury to or interference with (either intentionally or unintentionally) our rights or property, other users, or anyone else that could be harmed by such activities, or where the disclosure of your personal information would be in your best interest.

11) Your rights:

- **You have the right** to, in accordance with these terms, request that we correct, destroy or delete any of your personal information that we have processed on our Products/Services and/or our Site. The personal information that you may request us to correct, destroy or delete is personal information that has been processed in accordance with these terms that is inaccurate, irrelevant, excessive, out of date,



incomplete, misleading, obtained unlawfully or that we are no longer authorised to retain.

- **You have the right** to withdraw your consent for us to process your personal information at any time. The withdrawal of your consent can only be made by you on the condition that the withdrawal of your consent does not affect the processing of your personal information before the withdrawal of your consent; or that the withdrawal of your consent does not affect the processing of your personal information if the processing is in compliance with an obligation imposed by law on us; or that the withdrawal of your consent does not affect the processing of your personal information where such processing is necessary for the proper performance of a public law duty by a public body; or that the withdrawal of your consent does not affect the processing of your personal information as required by law; or that the withdrawal of your consent does not affect the processing of your personal information as required to finalise the performance of a contract in which you are a party; or that the withdrawal of your consent does not affect the processing of your personal information as required to protect your legitimate interests or our own legitimate interests or the legitimate interests of a third party to whom the information is supplied.
- **You have the right** to object to the processing of your personal information at any time, on reasonable grounds relating to your particular situation, unless the processing is required by law. You can make the objection if the processing of your personal information is not necessary for the proper performance of a public law duty by a public body; or if the processing of your personal information is not necessary to pursue your legitimate interests, our legitimate interests or the legitimate interests of a third party the information is supplied to.
- **You have the right** to object to the processing of your personal information, at any time, if the processing is for purposes of direct marketing other than direct marketing by means of unsolicited electronic communications and you have not given your consent for that processing.
- You have the right to not have your personal information processed for purposes of direct marketing by means of unsolicited electronic communications from third parties unknown to you.

- **You have the right** to submit a complaint to the Information Regulator regarding an alleged interference with the protection of personal information processed in accordance with these terms. The Information Regulator's contact details are published by the government from time to time in terms of POPIA. When they are published POPIA places a duty on us to inform you what those contact details are and we will do so via our Products/Services and/or our Site.
- **You have the right** to institute civil proceedings regarding an alleged interference with the protection of your personal information processed in accordance with these terms.

12) Use of cookies:

- Cookies are pieces of information our Products/Services and/or our Site transfers to a user's hard drive for record-keeping purposes. Cookies make surfing the web easier for you by saving you preferences and, tracking your online habits, traffic patterns, and making sure that you do not see the same advertisement too often. The use of cookies is an industry standard.
- We may place a "cookie" on your browser to store and sometimes track information about you.
- While most browsers are initially set up to accept cookies, you can reset the data's subject's browser to refuse all cookies or indicate when a cookie is being sent. Please note that some parts of our Products/Services and/or our Site will not function properly if you refuse cookies.

13) Links to other Sites:

When you use our Products/Services and/or our Site, you could be directed to other site/s that are beyond our control. These other site/s may send their own cookies to you, collect data, or solicit personal information. We do not control the privacy policies of those third party and we cannot be held liable for the use thereof by you for any reason whatsoever.

14) Director Marketing:

- We may process your personal information for the purposes of providing you with information regarding services that may be of interest to you. You may unsubscribe for free at any time.
- If you currently receive marketing information from us which you would prefer not to receive in the future, please email us at [insert] or alternatively, unsubscribe using the unsubscribe function when receiving marketing communication from us.

15) Passwords and login information:

- You may register your personal information with us via e-mail or via our Site, or manually or as may be otherwise communicated to you from time to time.
- If you register your personal information, you will be able to create your own user name and password.
- You must not provide your username or password to anyone. You are solely responsible for keeping your username or password secret.
- You are solely responsible for any loss you may suffer should any other person use your username or password.

16) Contact Details:

- You may contact us at -
 - The Information Officer:
 - *Mandala Consulting*
 - Attention: Mr/Miss/Mrs – Stefan Viljoen or Marelize de Lange
 - Contact Number: 076 907 3277 or 083 348 4576
 - Email address: stefan@mandalaconsulting.co.za or marelize@mandalaconsulting.co.za



MANDALA CONSULTING
INTEGRATION FOR SUSTAINABILITY



MANDALA CONSULTING
INTEGRATION FOR SUSTAINABILITY

WEBSITE USER AGREEMENT



1. WEBSITE TERMS AND CONDITIONS OF USE

- 1.1 This document sets out the terms and conditions of use of our website, social media site or any other electronic platform owned by us (referred to herein as “**Our Sites**” or the “**Sites**”) and regulates your use thereof.
- 1.2 We shall refer to ourselves in this document as “we”, “us”, “our” or the “Company”.
- 1.3 Our Sites are used for marketing, information and other purposes.
- 1.4 Should any person that accesses the Sites, (herein referred to as “**you**” or “**user**”) disagree with any of the Terms, you must refrain from accessing the Sites and/or using our services.
- 1.5 If you are under the age of 18, you must obtain your parents' or legal guardians' advance authorization, permission and consent to be bound by these Terms before purchasing any products or services.
- 1.6 The Company reserves the right, in its sole discretion, to amend and/or replace any of, or the whole of, the Terms. Such amendments shall supersede and replace any previous Terms and shall be made available on Our Sites.
- 1.7 Each time a user accesses Our Sites and/or uses the services, the user shall be deemed to have consented, by such access and/or use, to the Terms, as amended and/or replaced by the Company from time to time. If you are not satisfied with the amended Terms, you should refrain from using the Sites.
- 1.8 The collection of your personal information is subject to and is regulated by our privacy policy (“**Privacy Policy**”) which can be accessed and/or viewed on our Site from time to time.
- 1.9 The provision of our products and/or services may be subject to separate terms and conditions of sale (“**T’s&C’s**”), which can also be accessed and/or viewed

from our official Sites from time to time or as may be provided to you with our products or services from time to time.

- 1.10 If there is anything in these Terms that you do not understand then please contact us as soon as possible.

2. CONTENT OF THE SITES

- 2.1 The Company reserves the right to make improvements, to change or to discontinue, without notice, any aspect or feature of the Sites and any information or content on the Sites.
- 2.2 The Company reserves the right to change and amend the products, prices and rates quoted on the Sites from time to time without notice.
- 2.3 The Company may use the services of third parties to provide information on the Sites. The Company has no control over this information and makes no representations or warranties of any nature as to its accuracy, appropriateness or correctness. The user agrees that such information is provided "as is" and that the Company and its online partners shall not be liable for any losses or damages that may arise from the user's reliance on it, howsoever these may arise.
- 2.4 the Company makes no representations or warranties, whether express or implied, as to the accuracy, completeness or reliability of any information, data and/or content on the Sites, including without limitation:
- 2.4.1 The Company does not warrant that the Sites or information or downloads shall be error-free or that they shall meet any particular criteria of performance or quality. The Company expressly disclaims all implied warranties, including without limitation, warranties of merchantability, fit-ness for a particular purpose, non-infringement, compatibility, security and accuracy;

- 2.4.2 Whilst the Company has taken reasonable measures to ensure the integrity of the Sites and its contents, no warranty, whether express or implied, is given that any files, downloads or applications available via the Sites are free of viruses, or any other data or code which has the ability to corrupt, damage or affect the operation of the user's system; and
- 2.4.3 The Company disclaims any responsibility for the verification of any claims. Information published on the Sites may be done so in the format in which the Company receives it and statements from external parties are accepted as fact.

3. LINKED THIRD PARTY WEBSITES AND THIRD PARTY CONTENT

- 3.1 The Company may provide links to third party websites on the Sites. These links are provided to the user for convenience purposes only and the Company does not endorse, nor does the inclusion of any link imply the Company's endorsement of, such websites, their owners, licensees or administrators or such websites' content or security practices and operations.
- 3.2 While the Company tries to provide links only to reputable websites or online partners, the Company cannot accept responsibility or liability for the information provided on other websites. Linked websites or pages are not under, nor subject to, the control of the Company. The Company is not responsible for and gives no warranties or makes any representations in respect of the privacy policies or practices of linked or any third party or advertised websites on the Sites.
- 3.3 You agree that the Company shall not be held liable, directly or indirectly, in any way for the content, the use or inability to use or access any linked website or any link(s) contained in a linked website, nor for any loss or damage of any sort incurred as a result of any dealings with, or as the result of the presence of such third party linked websites on Our Sites. Any dealings that you may have with



any linked websites, including advertisers, found on the website, are solely between you and the third party website.

4. USAGE RESTRICTIONS

The user hereby agrees that it shall not itself, nor through a third party:

- 4.1 copy (other than for backup, archival or disaster recovery purposes), reproduce, translate, adapt, vary, modify, lease, licence, sub-licence, encumber or in any other way deal with any part of the Sites for any reason and in any manner, unless it is consistent with the intent and purpose of these Terms;
- 4.2 decompile, disassemble or reverse engineer any portion of the Sites;
- 4.3 write and/or develop any derivative of the Sites or any other software program based on the Sites;
- 4.4 modify or enhance the Sites. In the event of a user effecting any modifications or enhancements to the Sites in breach of this clause, such modifications and enhancements shall be the property of the Company;
- 4.5 without the Company's prior written consent, provide, disclose, divulge or make available to or permit the use of or give access to the Sites by persons other than the user;
- 4.6 remove any identification, trademark, copyright or other notices from the Sites;
- 4.7 post or transmit, by means of reviews, comments, suggestions, ideas, questions or other information through the Sites, any content which is unlawful, harmful, threatening, abusive, harassing, defamatory, vulgar, ob-scene, sexually-explicit, profane or hateful, or racially, ethnically or otherwise objectionable content of any kind; and/or

- 4.8 notwithstanding anything contained to the contrary in these Terms, use the Sites for any purpose other than personal, non-commercial and information purposes.

5. SECURITY

- 5.1 In order to ensure the security and reliable operation of the services to all the Company's users, the Company hereby reserves the right to take whatever action it may deem necessary to preserve the security, integrity and reliability of its network and back-office applications.
- 5.2 You may not utilise the Sites in any manner which may compromise the security of the Company's networks or tamper with the Sites in any manner whatsoever, which shall include without limitation, gaining or attempting to gain unauthorised access to the Sites, or delivering or attempting to deliver any unauthorised, damaging or malicious code to the Sites, all of which is expressly prohibited. Any person or entity which does so, or attempts to do so, shall be held criminally liable. Further, should the Company suffer any damage or loss, civil damages shall be claimed by the Company against the user.
- 5.3 Any user who commits any of the offences detailed in Chapter 13 of the Electronic Communications and Transactions Act 25 of 2002 ("ECTA") (specifically sections 85 to 88 (inclusive)) shall, notwithstanding criminal prosecution, be liable for all resulting liability, loss or damages suffered and/or incurred by the Company and its affiliates, agents and/or partners.

6. INTELLECTUAL PROPERTY RIGHTS

- 6.1 For the purpose of this clause, the following words shall have the following meanings ascribed to them:
- 6.1.1 "Intellectual property rights" means all and any of the rights in and to intellectual property of any nature whatsoever owned and/or controlled



directly or under licence by the Company, now or in the future, including without limitation, the Company's rights, title and interest in and to all technology, source code/s, trade secrets, logos, systems, methods, trademarks, trade names, styles, insignia, designs, patents and copyright, and all similar proprietary rights which may subsist in any part of the world, whether registered or not.

- 6.2 All copyright and other intellectual property rights in all content, trademarks, software, data, material, including logos, databases, text, graphics, icons, hyperlinks, confidential information, designs, agreements, and multimedia works, published on or via the Sites ("proprietary material"), are the property of, or are licensed to, the Company and as such are protected from infringement by local and international legislation and treaties.
- 6.3 By submitting reviews, comments and/or any other content (other than your personal information) to the Company for posting on the Sites, you automatically grant the Company and its affiliates a non-exclusive, royalty-free, perpetual, irrevocable right and licence to use, reproduce, publish, translate, sub-license, copy and distribute such content in whole or in part worldwide, and to incorporate it in other works in any form, media, or technology now known or hereinafter developed, for the full term of any copyright that may exist in such content. Subject to this licence, you retain any and all rights that may exist in such content.
- 6.4 All rights not expressly granted are reserved and no right, title or interest in any proprietary material or information contained in the Sites is granted to you.
- 6.5 Except with the Company's express written permission, no proprietary material from the Sites may be copied or retransmitted.
- 6.6 Irrespective of the existence of copyright, the user acknowledges that the Company is the proprietor of all material on the Sites (except where a third party is indicated as the proprietor), whether it constitutes confidential information or not, and that the user has no right, title or interest in any such material.

- 6.7 The Company authorises you only to view, copy, temporarily download to a local drive and to print the content of the Sites, or any part thereof, provided that such content is used for personal purposes and for information purposes only, and such content is used for non-commercial purposes.

7. RISK, LIMITATION OF LIABILITY AND INDEMNITY

- 7.1 The user's use of Our Sites and the information contained on Our Sites is entirely at the user's own risk and the user assumes full responsibility and risk of loss resulting from the use thereof.
- 7.2 The transmission of information via the internet, including without limitation e-mail, is susceptible to monitoring and interception. The user bears all risk of transmitting information in this manner. Under no circumstances shall the Company be liable for any loss, harm, or damage suffered by the user as a result thereof. The Company reserves the right to request independent verification of any information transmitted via e-mail and the user consents to such verification should the Company deem it necessary.
- 7.3 To the extent permissible by law:
- 7.3.1 Neither the Company, its affiliates, shareholders, agents, consultants or employees shall be liable for any damages whatsoever, including without limitation any direct, indirect, special, incidental, consequential or punitive damages, howsoever arising (whether in an action arising out of contract, statute, delict or otherwise) related to the use of, or the inability to access or use the content of the website or any functionality thereof, or the information contained on the website, or of any linked website, even if the Company knows or should reasonably have known or is expressly advised thereof.
- 7.3.2 The liability of the Company for faulty execution of the website as well as all damages suffered by the user, whether direct or indirect, as a



result of the malfunctioning of the website shall be limited to the Company rectifying the malfunction, within a reasonable time and free of charge, provided that the Company is notified immediately of the damage or faulty execution of the website. This liability shall fall away and be expressly excluded if the user attempts to correct or allows third parties to correct or attempt to correct the website without the prior written approval of the Company. However in no event shall the Company be liable to the user for loss of profits or for special, incidental, consequential or punitive losses or damages arising out of or in connection with Our Sites or its use or the delivery, installation, servicing, performance or use of it in combination with other computer software.

7.3.3 You hereby unconditionally and irrevocably indemnify the Company and agree to hold the Company free from all loss, damages, claims and/or costs, of whatsoever nature suffered or incurred by the Company or instituted against the Company as a direct or indirect result of:

7.3.3.1 your use of the Sites;

7.3.3.2 software, programs and support services supplied by, obtained by or modified by you or any third party without the consent or knowledge of the Company;

7.3.3.3 your failure to comply with any of the Terms or any other requirements which the Company may impose from time to time;

7.3.3.4 the actions or requirements of any telecommunications authority or a supplier of telecommunications services or software; or

7.3.3.5 any unavailability of, or interruption in, the service which is beyond the control of the Company.

7.4 The Company makes no warranty or representation as to the availability, accuracy or completeness of the content of the Sites. You expressly waive and renounce all your rights of whatever nature that you may have against the Company for any loss and/or damage suffered by you, as a result of information supplied by the Company being incorrect, incomplete or inaccurate.

8. THE COMPANY PRIVACY POLICY AND T'S&C'S

8.1 The Company takes your privacy seriously and is committed to protecting your personal information. We use the personal information that we collect from you in accordance with our Privacy Policy, which Privacy Policy can be accessed and/or viewed from our official Sites and forms part of and is incorporated into these Terms as if specifically set out herein.

8.2 Your use of our products and/or services signifies your consent to us collecting and using your personal information as specified in our Privacy Policy, and may furthermore be subject to our T's&C's. Our T's&C's can be accessed and/or viewed from our official Sites from time to time, or may be provided to you when making use of our products or services from time to time.

9. CONFIDENTIALITY

9.1 By subscribing as a user, you agree that you shall hold in the strictest confidence and not disclose to any third party information acquired in connection with any aspect of the products and/or services offered by the Company. You shall notify the Company should you discover any loss or unauthorised disclosure of the information.

9.2 Any information or material sent to the Company will be deemed not to be confidential, unless otherwise agreed in writing by the user and the Company.



10. BREACH OR CANCELLATION BY SERVICE PROVIDER

10.1 the Company is entitled without notice, in addition to any other remedy available to it at law or under these Terms, including obtaining an interdict, to cancel these Terms, limit or deny such user use of the Sites, products and services, or to claim specific performance of any obligation whether or not the due date for performance has arrived, in either event without prejudice to the Company's right to claim damages, should any user:

10.1.1 breach any of these Terms;

10.1.2 in the sole discretion of the Company, use the Sites in an unauthorised manner; or

10.1.3 infringe any statute, regulation, ordinance or law.

10.2 Breach of these Terms entitles the Company to deny you any further access to our Sites, and/or to take legal action as the Company may deem appropriate and/or necessary to protect its rights and interests, without prior notice to the user and the user agrees to reimburse the costs associated with such legal action to the Company on an attorney and own client scale.

11. COMPLIANCE WITH LAWS

You shall comply with all applicable laws, statutes, ordinances and regulations pertaining to your use of and access to Our Sites.

12. NOTICES

Except as explicitly stated otherwise, any notices shall be given by email to our email address or contact details made available on our official website (in the case of the Company) or to the e-mail address you have provided to the Company (in your case), or such other address that has been specified. Notice shall be deemed given 48 (forty eight) hours after an email is sent, unless the sending party is notified that the email address is

invalid. Alternatively, the Company may give you notice by registered mail, postage prepaid and return receipt requested, to the address which you have provided to the Company. In such case, notice shall be deemed given 7 (seven) days after the date of mailing. You acknowledge that all agreements, notices or other communication required to be given in terms of the law or these Terms may be given via electronic means and that such communications shall be "in writing". Notwithstanding anything to the contrary, a written notice or communication actually received by a party shall be an adequate written notice or communication to it, notwithstanding that it was not sent to or delivered at its chosen address(es) for that purpose.

13. GENERAL CLAUSES

- 13.1 These Terms shall be governed in all respects by the laws of the country where our head office is based as shown on Our Sites ("**Our Domicilium**").
- 13.2 Our Sites are controlled, operated and administered by the Company from its head offices. The Company makes no representation that the content of the Sites is appropriate or available for use outside of Our *Domicilium*. Access to the Sites from territories or countries where the content of the Sites is illegal is prohibited. Users may not use the Sites in violation of the laws of Our *Domicilium* or export laws and regulations. If the user accesses the Sites from locations outside of Our *Domicilium*, that user is responsible for compliance with all local laws.
- 13.3 The Company does not guarantee continuous, uninterrupted or secure access to our services, as operation of Our Sites may be interfered with as a result of a number of factors which are outside of our control.
- 13.4 If any provision of these Terms is held to be illegal, invalid or unenforceable for any reason, such provision shall be struck out from these Terms and the remaining provisions shall be enforced to the full extent of the law.



- 13.5 The Company's failure to act with respect to a breach by you or others does not constitute a waiver of our right to act with respect to subsequent or similar breaches.
- 13.6 You shall not be entitled to cede your rights or assign your rights or delegate your obligations in terms of these Terms to any third party without the prior written consent of the Company.
- 13.7 No party shall be bound by any express or implied term, representation, warranty, promise or the like not recorded herein, whether it induced the contract and/or whether it was negligent or not.
- 13.8 The head notes to the paragraphs to these Terms are inserted for reference purposes only and shall not affect the interpretation of any of the provisions to which they relate.
- 13.9 Words importing the singular shall include the plural and vice versa, and words importing the masculine gender shall include females and words importing persons shall include partnerships and corporate and unincorporated entities.
- 13.10 These Terms set forth the entire understanding and agreement between the Company and you with respect to the subject matter hereof.



MANDALA CONSULTING
INTEGRATION FOR SUSTAINABILITY
