MANDALA CONSULTING
INTEGRATION FOR SUSTAINABILITY

Operator Agreement

Table of Contents

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 take 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.

* * *

On behalf of Responsible Party

_____,
_____
(Place, date) (Signature)

_____
Name:
Function:

On behalf of Operator

_____,
_____
(Place, date) (Signature)

_____
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	☐ Light barrier, motion detector
☐ Protection of shaft entry to buildings	☐ Security locks
☐ Automatic entry control system	☐ Recording of visitors
☐ Chip card or transponder system	☐ Careful selection of cleaning staff
☐ Locking system with code requirements	☐ Careful selection of security staff
☐ Manual locking system	☐ Request to carrying credentials
☐ Biometric access control	☐ Recording of visitors
☐ Video surveillance of entrance zone	

☐ Other/comments (please detail):

User control, Storage Control

☐ User authentication	☐ Security locks
☐ Use of user profiles	☐ Use of Intrusion-Detection Systems
☐ Password assignment	☐ Use of antivirus software
☐ Authentication with biometrical systems	☐ Encryption of data carriers in laptops
☐ Authentication with user name and password	☐ Use of hardware firewall
☐ Assignment of user profiles to IT Systems	☐ Use of software firewall
☐ Locking devices for cases	☐ Encryption of mobile data carriers
☐ Use of VPN- technology	☐ Encryption of smart phone content
☐ Locking of external interfaces	☐ 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	☐ Recording of accesses to applications, specially input, change or deletion of personal data
☐ Administration of rights by system administrator	☐ Traceability of input, change and deletion of personal data by individual user name (not only user groups)
☐ As few administrators as necessary	☐ Transparent allocation of rights to input, change or delete personal data in accordance with an authorization concept
☐ Password policies including rules regarding length of password and change of password	

☐ Other/comments (please detail):

Transport Control

☐ Secure storage of data carriers	☐ Recording of destruction
☐ Physical deletion of data carriers prior to reuse	☐ Encryption of data carriers
☐ Proper destruction of data carriers by certified service provider	☐ Secure containers and packages
☐ Use of shredder or service provider (if possible with privacy seal)	☐ Careful selection of transportation staff and vehicles

☐ Other/comments (please detail):

Transmission control

Use of VPN technology	☐ SSL encryption (e.g. websites)
Transfer of personal data anonymously or pseudo anonymously	☐ Creating an overview of regular request and transmission
Email encryption	☐ 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	☐ Appointment of Information Officer
☐ Sub Processor r's instructions	☐ Secured destruction of personal data after termination of the agreement
☐ Careful selection of Sub-Operator, in particular in terms of data security	☐ Agreement of effective control rights towards Sub-Operator
☐ Review of the Sub-Operator's security measures	☐ Regular review of Sub-Operator
☐ Obligation of employees to commit to data protection and confidentiality	

☐ 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	☐ 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
☐ Other/comments (please detail):	
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	☐ Logical customer separation (software-sided) ☐ Maintenance of an authorization concept ☐ Determination of rights regarding data bases
☐ Other/comments (please detail):	

[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]

* * *

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