OPERATOR AGREEMENT / ADDENDUM
***(template*)**

between

.....
Registration no: .....
(Hereinafter referred to as the "**Company**")

and

.....
Registration no: .....
(Hereinafter referred to as the "**Operator**")

---

1. INTRODUCTION

1.1. There are a variety of Personal Information privacy or data laws around the world which regulate the processing of Personal Information. In South Africa, the Protection of Personal Information Act, 4 of 2013 (POPIA), which as its main function and objective, regulates and controls the processing of Personal Information by a Responsible Party.

1.2. The Company in its capacity as Responsible Party, for the purposes of carrying out its business and related objectives, does and will from time to time, process Personal Information belonging to several persons, including legal entities and individuals, who are referred to as Data Subjects under data processing laws, including POPIA.

1.3. The Company is obligated to comply with all data processing laws, including the data protection conditions housed under POPIA with respect to the processing of all and any Personal Information pertaining to Data Subjects.

1.4. The Company may request third parties to process Personal Information obtained from Data Subjects on its behalf.

1.5. In terms of section 20 of POPIA, where the Company makes use of an operator to process Personal Information of Data Subject (s) on its behalf, then the Company is legally obliged to conclude a written agreement with such operator, which written agreement contractually obliges the operator to:

1.5.1. comply with the provisions of POPIA and the POPIA processing conditions when processing such Personal Information on behalf of the Company;

1.5.2. only process the Personal Information received from the Company in accordance with the mandate or written instruction received from the Company;

1.5.3. keep all the Personal Information held by the operator on behalf of the Company and or belonging to the Company Data Subjects, confidential;

1.5.4. put measures in place to keep all such Personal Information held by the operator, and processed on behalf of the Company confidential, safe, and secure from misuse, abuse and or unauthorised use or access.

1.6. The Company is desirous of providing the Operator with certain Personal Information which pertains to certain of its Data Subjects (individuals/legal entities), which the Company would like the Operator to process on its behalf.

1.7. In accordance with section 20 of POPIA, the Operator agrees to process the Personal Information on behalf of the Company, subject to the terms and conditions set out under this Agreement / Addendum.

2. DEFINITIONS

2.1. The parties must note the following definitions, which will be used throughout this Operator Agreement, unless the context indicates a contrary meaning:

2.1.1. **"Agreement"** means in the absence of any other agreements between the parties, this Agreement that will govern the relationship between the parties in relation to the processing of Personal Information;

2.1.2. **"Addendum"** means where there are other agreements between the parties, this Addendum should be read together with the other agreements. This Addendum will govern the relationship between the parties in relation to the processing of Personal Information;

2.1.3. **"Best Industry Practice"** includes, in relation to an obligation, undertaking, activity or a service, the exercise of the degree of skill, speed, care, diligence, judgement, prudence and foresight and the use of practices, controls, systems, technologies and processes, which would be expected from a skilled, experienced and market leading service provider that is an expert in performing the same or similar obligation, undertaking, activity or service and utilising and applying skilled resources with the requisite level of expertise;

2.1.4. **"Data Protection Legislation**" means any data protection or data privacy laws applicable, including but not limited to the Protection of Personal Information Act 4 of 2013, the Electronic Communications and Transactions Act 26 of 2005, the Consumer Protection Act 68 of 2008, the General Data Protection Act (GDPR), the UK Data Privacy Act (UKDPA) and the California Privacy Act;

2.1.5. **"Data Subject (s)"** means the person (s) who own (s) the Personal Information, which is to be processed by the Operator, on behalf of the Company, in terms of this Agreement/ Addendum;

2.1.6. "**parties"** means the parties to this Agreement/Addendum;

2.1.7. **"Person"** means an identifiable, living, natural person, or an identifiable, existing juristic person;

2.1.8. **"Personal Information"** means personal information relating to any identifiable, living, natural person, and an identifiable, existing juristic person, including, but not limited to:

- **in the case of an individual:**
  - name, address, contact details, date of birth, place of birth, identity number, passport number, bank details, details about your employment, tax number and financial information;
  - vehicle registration;
  - dietary preferences;
  - financial history;
  - information about next of kin and or dependants;
  - information relating to education or employment history; and
  - **Special Personal Information** including race, gender, pregnancy, national, ethnic, or social origin, colour, physical or mental health, disability, criminal history, including offences committed or alleged to have been committed, membership of a trade union and biometric information, such as images, fingerprints and voiceprints, blood typing, fingerprinting, DNA analysis, retinal scanning and voice recognition;
- **in the case of a juristic person:**
  - name, address, contact details, registration details, financials and related history, B-BBEE score card, registered address, description of operations, bank details, details about employees, business partners, customers, tax number, VAT number and other financial information; and
  - correspondence sent by the person that is implicitly or explicitly of a private or confidential nature or further correspondence that would reveal the contents of the original correspondence;
  - the views or opinions of another individual about the person; and
  - the name of the person if it appears with other Personal Information relating to the person or if the disclosure of the name itself would reveal information about the person.

2.1.9. **"Personal Information Breach"** means any act or omission that compromises the security, confidentiality, integrity or availability of Personal Information or the physical, technical, administrative or organisational safeguards that are put in place to protect it including, without limitation, the loss or unauthorised access, disclosure or acquisition of Personal Information;

2.1.10. "**POPIA"** means the Protection of Personal Information Act 4 of 2013;

2.1.11. **"process or processing"** means any operation or activity or any set of operations, whether by automatic means, performed by the Operator concerning a Data Subject's Personal Information, including—

(a) the collection, receipt, recording, organization, collation, storage, updating or

modification, retrieval, alteration, consultation, or use;

(b) dissemination by means of transmission, distribution or making available in any other form; or

(c) merging, linking, as well as restriction, degradation, erasure, or destruction of information;

2.1.12. **"record"** means any recorded information—

(a) regardless of form or medium, including any of the following:

(i) writing on any material;

(ii) information produced, recorded, or stored by means of any tape-recorder, computer equipment, whether hardware or software or both, or other device, and any material subsequently derived from information so produced, recorded or stored;

(iii) label, marking or other writing that identifies or describes anything of which it forms part, or to which it is attached by any means;

(iv) book, map, plan, graph, or drawing;

(v) photograph, film, negative, tape or other device in which one or more visual images are embodied to be capable, with or without the aid of some other equipment, of being reproduced;

(b) in the possession or under the control of a Responsible Party;

(c) whether or not it was created by a Responsible Party; and

(d) regardless of when it came into existence.

2.1.13. "**Responsible Party**" shall have the meaning given to it in any Data Protection Legislation;

2.1.14. **"Sub Operator"** means the person who has been mandated by the Operator, with prior approval by the Company, in terms of the Agreement/Addendum to process Personal Information belonging to certain Data Subjects(s) on the Company and the Operators behalf;

3. MANDATE TO PROCESS

The Company hereby grants to the Operator a mandate to process certain Personal Information, belonging to Data Subjects, on its behalf and in accordance with the terms of this Agreement/Addendum and where applicable any specific terms as contained in **Annexure A**.

(Optional: Per the terms of Annexure A)

4. OBLIGATIONS OF THE OPERATOR

4.1. The Operator expressly warrants and undertakes that it will:

4.1.1. process the Personal Information strictly in accordance with:

- this Agreement/Addendum mandate,
- read together with **Annexure A,**
- any agreement concluded between the Operator and the Company, and
- any specific written instructions provided to it by the Company from time to time*;*

4.1.2. process Personal Information strictly in accordance with POPIA and the POPIA processing conditions and further comply with all reasonable directions and instructions that may be given by the Company regarding the processing of the Personal Information in terms of the Agreement/Addendum. The parties agree that any directions or instructions required for purposes of ensuring compliance with any applicable laws, including Data Protection Legislation shall be deemed reasonable;

4.1.3. not use the Personal Information for any other purpose, save for the purpose of processing Personal Information as per the Agreement/Addendum*;*

4.1.4. treat the Personal Information as confidential and only disclose, transfer and or hand over the Personal Information to those persons(s) employed by it and who need to process the Personal Information in accordance with the mandate to process as an Operator and /or in terms of the Agreement/Addendum under strict undertakings of confidentiality;

4.1.5. in addition to clause 4.1.4, treat the Personal Information as confidential and not disclose the Personal Information to any other third parties unless required by law and only once it has provided the Company with adequate warning of this requirement to disclose and the related details thereof. Details provided to the Company should include the identity of the person/legal entity who is to receive the Personal Information; the reason for the disclosure; and confirmation that the person/legal entity to whom the Personal Information is to be disclosed to, has signed the POPIA onwards transmission notice attached hereto, marked **Annexure B;**

4.1.6. ensure that it has and will continue to have in place, appropriate technical and organisational measures to protect and safeguard the Personal Information against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access. This should be in accordance with Best Industry Practice that provides a level of security appropriate to the risk represented by the processing and the nature of the Personal Information to be protected. The safeguards must comply with the requirements set out under POPIA and be in line with the requirements described under the attached **Annexure C;**

4.1.7. promptly and without undue delay notify the Company if any Personal Information is

lost or destroyed or becomes damaged, corrupted, or unusable. The Operator will restore such Personal Information at its own expense;

4.1.8. without undue delay notify the Company if it becomes aware of any reason to believe that there was an occurrence of any accidental, unauthorised or unlawful processing of the Personal Information; or any Personal Information Breach and in such case without undue delay, also provide the Company with the following information:

(a) description of the nature of any accidental, unauthorised or unlawful processing of the Personal Information; or

(b) any Personal Information Breach (including the categories and approximate number of both Data Subjects and Personal Information records concerned the likely consequences; and

(c) description of the measures taken, or proposed to be taken to address any accidental, unauthorised or unlawful processing of the Personal Information; or

(d) any Personal Information Breach including measures to mitigate its possible adverse effects.;

4.1.9. immediately, following any unauthorised or unlawful Personal Information processing or Personal Information Breach, ensure that it co-ordinates and co-operates with the Company's handling of the matter, including:

(a) assisting with any investigation;

(b) providing the Company with physical access to any facilities and operations affected;

(c) facilitating interviews with the Operator employees, former employees and others involved in the matter;

(d) making available all relevant records, logs, files, data reporting and other materials required to comply with all Data Protection Legislation or as otherwise reasonably required by the Company; and

(e) taking reasonable and prompt steps to mitigate the effects and to minimise any damage resulting from the Personal Information Breach or unlawful Personal Information processing.

(f) to not inform any third party of any Personal Information Breach without first obtaining the Company's prior written consent, except when required to do so by law.

(g) agrees that the Company has the sole right to determine: (a) whether to provide notice of the Personal Information Breach to any Data Subjects, supervisory authorities, regulators, law enforcement agencies or others, as required by law or regulation or in the Company discretion, including the contents and delivery method of the notice; and (b) whether to offer any type of remedy to affected Data Subjects, including the nature and extent of such remedy.

(h) will cover all reasonable expenses associated with the performance of the obligations under clause this clause 4.1 unless the matter arose from the Company's specific instructions, negligence, wilful default or breach of this Agreement / Addendum, in which case the Company will cover all reasonable expenses.

(i) will also reimburse the Company for actual reasonable expenses that the Company incurs when responding to a Personal Information Breach to the extent that the Operator caused such a Personal Information Breach, including all costs of notice and any remedy.

4.1.10. not use the Personal Information for any direct marketing or advertising, research, or statistical purposes, *unless expressly authorised to do per its mandate* and when conducting such activity ensure that this is done strictly in compliance with the requirements of POPIA and its regulations especially those applicable to direct marketing detailed under section 69;

4.1.11. not treat the Personal Information as its own, it expressly acknowledging that it has been tasked with processing the Personal Information in its capacity as the Company's Operator and agent, and that ownership of all the records housing the Personal Information and any records comprising such Personal Information pertaining to the Data Subject, will always remain with the Company;

4.1.12. not sell, alienate, or otherwise part with the Personal Information or any of the records housing the Personal Information, save with the Company's prior written consent;

4.1.13. where it is allowed to transfer the Personal Information onwards to a Sub Operator, for the purposes of performing its mandate, conclude a "Sub Operator agreement" with the Sub Operator which compels the third party receiving the Personal Information to maintain the confidentiality and security of the Personal Information. Sub Operator agreements will house the same terms and conditions as contained in this Agreement/Addendum, and which must be concluded before the Personal Information is transferred to the Sub Operator.

4.1.14. ensure that any person acting under the authority of the Operator, including any employee or Sub Operator, shall be obligated to process the Personal Information only on instructions from the Operator and strictly in accordance with this Agreement/Addendum, read together with the Sub Operator Agreement, where applicable.

4.2. The Operator warrants that it has the legal authority to give the above-mentioned warranties and fulfil the undertakings set out in this Agreement/Addendum.

4.3. The Company, in order to ascertain compliance with the warranties and undertakings housed under this Agreement/Addendum, will have the right on reasonable notice and during regular business hours, to view and or audit, either by itself or through an independent agent, the Operator's facilities, files, and any other data processing documentation needed for the required

review, audit and or independent or impartial inspection. The Operator undertakes to provide all necessary assistance which may be needed to give effect to this right.

5. LIABILITY OF THE OPERATOR AND THIRD-PARTY RIGHTS

5.1. In the event of the Operator, the Sub Operator or their respective employees or agents failing to comply with any of the provisions of POPIA or breaching any of the warranties and undertakings contained under this Agreement/Addendum or the Sub Operator Agreement (where applicable), then in such an event, the Operator shall be liable for all damages it or the Sub Operator may have caused in consequence of said breach or non-compliance, including patrimonial, non-patrimonial and punitive damages suffered by the Company and or the Data Subject(s).

5.2. The Operator indemnifies and holds the Company including its directors, employees and any affected Data Subjects harmless against any such loss, damage, action or claim which may be brought by whomsoever against the Company or any of its directors employees or Data Subjects, or against any of the Companies affiliated or their directors and employees, and the Operator agrees to pay all or any such amounts on demand.

5.3. At the request of the Company, the Operator will provide the Company with evidence of financial resources sufficient to fulfil its responsibilities set out under this Agreement/Addendum which may include insurance coverage or other forms of collateral.

6. APPLICABLE LAW

The laws of South Africa shall apply to this Agreement/Addendum, regardless of where the Personal Information is, will be, or was processed.

7. TERMINATION

7.1. In the event of:

7.1.1. any other agreements, between the parties and to which these terms apply, being terminated for any reason;

7.1.2. the processing of the Personal Information by the Operator being completed in accordance with this Agreement/Addendum;

7.1.3. the transfer of Personal Information to the Operator being suspended by the Company for whatever reason;

7.1.4. the Sub Operator is in breach of the Sub Operator Agreement;

7.1.5. the Operator being in breach of its obligations under this Agreement/Addendum and or has failed to comply with POPIA, and has failed when called upon to do so by the Company, to rectify the breach or area of non-compliance;

7.1.6. the Operator is in substantial or persistent breach of any warranties or undertakings given by it under the Agreement/Addendum, notwithstanding that the Company has

not given the Operator notice of such breach;

7.1.7. an application is filed for the placing of the Operator under business rescue, under administration, or winding up whether interim or final, which application is not dismissed within the applicable period for such dismissal under applicable law; or any equivalent event in any jurisdiction occurs,

then the Company without prejudice to any other rights, which it may have against the Operator, shall be entitled to terminate the Agreement/Addendum as well as the Sub Operator Agreement where applicable.

7.2. The parties agree that the termination of the Agreement / Addendum at any time, and or the Sub Operator agreement, where applicable, for whatever reason, does not exempt them from the rights and obligations set out under this Agreement / Addendum and applicable Data Protection Legislation, with regards to the processing of the Personal Information.

7.3. In the event of the Agreement / Addendum being terminated the Operator undertakes to:

7.3.1. restore and or transfer back to the Company all and any Personal Information which has been provided to the Operator for processing, including that held by the Sub Operator, whether same has been processed or not, and or which has been processed, together with any related documentation and or information. All aforementioned documentation must without exception, be returned to the Company within a period of 30 (thirty) days from date of service of the termination notice.

7.3.2. to confirm in writing when the transfer under clause 7.3.1 takes place, that all such Personal Information will be kept confidential as per the provisions of clause 4.1 and that it will not under any circumstances use the aforementioned information for whatsoever reason.

7.4. Notwithstanding termination of the Agreement / Addendum, the clauses 4, 5, 6 and 7.2 will survive any such termination.

8. GENERAL

8.1. Variation

The parties may not modify the provisions of this Agreement / Addendum including the annexures, unless such variation is reduced to writing and signed by the parties.

8.2. In the event of any conflict or inconsistency between the terms of the Agreement / Addendum and the agreements that may be in place to which this Agreement / Addendum is being read with, then the terms, and conditions in so far as the processing of the Personal Information is concerned, as set out under this Agreement / Addendum will take precedence and govern its interpretation, application, and construction.

8.3. All notices to be provided in terms of this Agreement / Addendum must be sent to the Information Officer by email at: ..... (Add details)

Concluded on …… at …….

_____

For and Behalf of the Company

Name:

Capacity:

Concluded on …… at …….

_____

For and on behalf of the Operator

Name:

Capacity:

Operator Agreement Revision 1/2021	Updated: 28/07/2022

ANNEXURE A

MANDATE TO PROCESS

DESCRIPTION OF THE PERSONAL DATA WHICH THE OPERATOR WILL PROCESS

Purpose(s):

Description of the Personal Information belonging to the Data Subject(s) which the Operator has been asked to process in terms of this Operator Agreement

Description of Data Subject	*Eg. vendors and suppliers.*

PERSONAL DETAILS	**MANNER AND FORM AND RECORD DETAILS**
General ☐ Name ☐ Identifying number ☐ Age ☐ Birthdate ☐ Language ☐ Physical and postal address ☐ e-mail address ☐ Telephone number ☐ Location information ☐ Other identifiers ☐ Gender ☐ Marital status ☐ Vehicle registration number	Further information:
Race and gender ☐ Gender ☐ Race ☐ Colour ☐ Ethnic origin ☐ National origin	
Religion and belief ☐ Religion ☐ Conscience ☐ Belief ☐ Culture	
Sexual orientation ☐ Sex ☐ Sexual orientation	

Deviant behaviour and Criminal history ☐ Criminal history	
Education ☐ Education history ☐ Employment history ☐ Psychometrics	
Physical and medical ☐ Medical history ☐ Physical health well-being ☐ Pregnancy ☐ Disability ☐ Mental health well-being ☐ Psychometrics	
Financial history ☐ Financial history	
Biometrics ☐ Blood typing, ☐ Fingerprinting ☐ DNA analysis ☐ Retinal scanning ☐ Voice recognition ☐ Alco/blood concentration	
Personal opinions ☐ Personal opinions, views or preferences of the Data Subject	
Views or opinions of another individual about the Data Subject ☐ Views or opinions of another individual about the Data Subject	

Security access control **Biometrics** **Photographs and CCTV** ☐ Photographs and CCTV footage if an individual can be identified by the footage	
Biometrics ☐ Blood type ☐ Fingerprinting ☐ Alco/blood concentration ☐ Fingerprinting	
Children Information pertaining to children such as ☐ Name ☐ Next of kin ☐ Parents ☐ Address ☐ Telephone details ☐ Email ☐ School	

3. Duration of the Processing of Personal Data

The Processing of the Personal Information will be carried out over the periods set out below:

DURATION	

4. Location of Personal Data Processing

The Processing of the Personal Information will be carried out at the following locations:

LOCATIONS	

None of the abovementioned Personal Data will be transferred outside SOUTH AFRICA.

5. Disclosure and other Operators (or Data Processors) to be used
Recipients
The Personal Information belonging to the abovementioned Data Subjects may only be disclosed to the following recipients or categories of recipients:

Sensitive Data (If Appropriate)

The personal data transferred concerns the following categories of sensitive data:

Sub Processors or Operators

The Processing of the Personal Information will be carried out by the Operator and the following Sub-Operators or Processors:

Name of Sub- Processor(s)	Localization	Type of Processing

Any modification to the above listing shall be agreed in writing between the Parties, through an Amendment to this Operator Agreement (see Annexure B).

6. Maximum Duration of Personal Data Retention and Deletion Rules

The Operator will return the Personal Information to .....within 30 (thirty) days.

Where the Operator is not required to return the Personal Information, then the Operator will retain the Personal Information for a period of .....months/years from the date of termination of the Agreement, and after such period it will delete the Personal Information as follows:

DELETION details	

ANNEXURE B

ONWARDS TRANSMISSION NOTE

…… (Individual or Legal entity name), an Operator acting on behalf of the Company, have agreed to provide you .....with the following information, which we have been asked to process by the Company on their behalf:

1. DETAILS OF THE DATA SUBJECT/S AND OWNER OF THE PERSONAL INFORMATION

……

……..

2. DETAILS OF THE PERSONAL INFORMATION

……

……..

3. REASON OR PURPOSE WHY YOU NEED TO PROCESS THE PERSONAL INFORMATION

……

……..

We have obtained permission from the Company and the Data Subject, as indicated below, to provide you with the abovementioned information, which is provided to you on the terms detailed below.

By accepting and receiving the Personal Information you undertake to comply with and abide by these terms:

4. CONDITIONS AND TERMS OF USE AND IMPLIED CONSENT TO COMPLY
(NOTE TO OPERATOR- SEE CLAUSES IN THE OPERATOR AGREEMENT RELEVANT TO SUB OPERATORS)

- You will keep the Personal Information private and confidential;
- You may only use the Personal Information for the purpose described above and for no other purpose;
- You will safeguard the Personal Information;
- You will in particular ensure that the Personal Information is kept safe and secure from unlawful or unauthorized access, and you will ensure that the integrity of the information is not compromised or altered in any manner;
- When using the Personal Information, you will comply with the processing conditions and provisions set out under a law known as the Protection of Personal Information Act, 4 of 2013, (POPIA);
- You agree to indemnify the Data Subject against all and any damages which may be incurred by them as a result of your non-compliance with the above undertakings.

Furthermore, you acknowledge that the Company and/or the Data Subject may institute legal action against you under the provisions recorded under POPIA should you breach the abovementioned terms.

1. **Signed by the Company …… date ……**

2. **I, the abovementioned data subject, agree to the above onwards transmission of my Personal Information.**

   Signed by Data Subject …… date ……

   Signed by Recipient …… date ……

ANNEXURE C

TECHNICAL AND ORGANISATIONAL MEASURES FOR DATA PROCESSING TO BE IMPLEMENTED BY THE OPERATOR

***Operator's security / privacy policies to be attached to this Annexure C.**

1. PHYSICAL ACCESS CONTROL

Safeguarding admission and access to processing systems against unauthorized parties.

The following technical and organizational measures have been implemented by the Operator for the processing of Personal Information described in this Agreement / Addendum (applicable fields marked with an "X")

- ☐ Alarm system
- ☐ Automatic access control system
- ☐ Locking system with code lock
- ☐ Biometric access barriers
- ☐ Light barriers / motion sensors
- ☐ Manual locking system including key regulation
- ☐ Visitor logging
- ☐ Chip cards / transponder locking system
- ☐ Video monitoring of access door
- ☐ Safety locks
- ☐ Personnel screening by gatekeeper / reception
- ☐ Careful selection of cleaning and security staff

2. DATA ACCESS CONTROL / USER CONTROL

Prevention of third parties using automatic processing systems with equipment for data transmission.

The following technical and organisational measures have been implemented by the Operator for the processing of Personal Information described in this Agreement / Addendum (applicable fields marked with an "X")

- ☐ Authentication with username / password (per valid password regulations)
- ☐ Access to online system requires a second factor of authentication (multi-factor authentication)
- ☐ Usage of intrusion detection systems
- ☐ Usage of up - to - date anti-virus software
- ☐ Usage of well-configured software firewall
- ☐ Regular installation of system software patches
- ☐ Creation of unique user profiles
- ☐ Assignment of user profiles to IT systems
- ☐ Usage of VPN technology

☐ Encryption of mobile data storage media

☐ Encryption of data storage media in laptops

☐ Usage of central smartphone administration software (e.g. for the external erasure of data)

☐ De-activation procedures when employee(s) leave the employment of the Operator organization, revoking access rights.

3. DATA USAGE CONTROL / DATA STORAGE MEDIA CONTROL / MEMORY CONTROL

Ensuring that the parties authorised to use an automated processing system only have access to the Personal Information appropriate for their access authorization.

Prevention of unauthorized reading, copying, changing or erasure of data storage media (data storage media control).

Prevention of unauthorized entry of Personal Information and unauthorised access to it, changing and deleting save Personal Information (memory control).

The following technical and organisational measures have been implemented by the Operator for the processing of Personal Information described in this Agreement / Addendum (applicable fields marked with an "X");

☐ Roles and authorisations based on a "need to know principle"

☐ Periodic reviews of access rights

☐ Number of administrators reduced to only the "essentials"

☐ Logging of access to applications, in particular the entry, change and erasure of data

☐ Physical erasure of data storage media before reuse

☐ Use of shredders or service providers

☐ Administration of rights by defined system administrators

☐ Password guidelines, including password length and changing passwords

☐ Secure storage of data storage media

☐ Proper destruction of data storage media

☐ Logging of destruction

4. TRANSFER CONTROL / TRANSPORTATION CONTROL

Ensuing that the confidentiality and integrity of data is protected during the transfer of Personal Information and the transportation of data storage media (e.g. through powerful encryption of data transmission, closed envelopes used in mailings, encrypted saving on data storage media).

The following technical and organisational measures have been implemented by the Operator for the processing of Personal Information described in this Agreement / Addendum (applicable fields marked with an "X");

☐ Establishment of dedicated lines for VPN tunnels

☐ Use of most current version of Transport Layer Security (TLS)

☐ Encrypted data transmission on the Internet (such as HTTPS, SFTP etc.)

- ☐ Email encryption
- ☐ Documentation of the recipients of data and time frames of planned transmission or agreed erasure deadlines
- ☐ In case of physical transportation; careful selection of transportation personnel and vehicles
- ☐ Transmission of data in an anonymized or pseudonymized form
- ☐ In case of physical transportation; secure containers / packaging; Strong data encryption.

5. ENTRY CONTROL / TRANSMISSION CONTROL

Ensuring that it is possible to subsequently review and establish which Personal Information has been entered or changed at what time and by whom in automated processing systems, for instance through logging (entry control).

Depending on the system, ensuring that it is possible to review and determine to which offices or locations Personal Information has been transmitted or provided using equipment for data transmission, or to which offices or locations it could be transmitted (transmission control).

The following technical and organisational measures have been implemented by the Operator for the processing of Personal Information described in this Agreement / Addendum (applicable fields marked with an "X");

- ☐ Logging of the entry, change and erasure of data
- ☐ Traceability of the entry, change and erasure of data through unique usernames (not user groups)
- ☐ Assignment of rights for the entry, change and erasure of data based on an authorization concept
- ☐ Creating an overview showing which data can be entered, changed and deleted with which applications
- ☐ Maintaining forms from which data is taken over in automated processing

6. AVAILABILITY CONTROL / RESTORATION / RELIABILITY / DATA INTEGRITY

Ensuring that systems used can be restored in case of disruption (restorability).

Ensuring that all systems functions are available and that any malfunctions are reported (reliability).

Ensuring that saved Personal Information is protected from accidental destruction or loss (availability control).

The following technical and organisational measures have been implemented by the Operator for the processing of Personal Information described in this Agreement / Addendum (applicable fields marked with an "X");

- ☐ Uninterruptible Power Supply (UPS)
- ☐ Devices for monitoring temperature and moisture in server rooms
- ☐ Alarms for unauthorized access to server rooms
- ☐ Test of data restorability

- ☐ Storing data back-ups in a separate and secure location
- ☐ In flood areas the server is located abo e the possible flood level
- ☐ Air conditioning units in server rooms
- ☐ Protected outlet strips in server rooms
- ☐ Fire extinguishers in server rooms
- ☐ Creating a back-up and recovery concept
- ☐ Creating an emergency plan

7. SEPARATION CONTROL / SEPARABILITY

Ensuring that data processed for different purposes can be processed separately.

The following technical and organisational measures have been implemented by the Operator for the processing of Personal Information described in this Agreement / Addendum;

- ☐ Physically separated storing on separate systems or data storage media
- ☐ Including purpose attributions / data fields in data sets
- ☐ Establishing database rights
- ☐ Logical client separation
- ☐ For pseudonymized data" separation of mapping file and storage on a separate and secured IT system
- ☐ Separation of production and testing systems.

8. INCIDENT MANAGEMENT

- ☐ Ensuring that, in the event of a security breach of personal data, the effect of the breach is minimized, and the correct notification procedures are implemented as per the Agreement/Addendum.
- ☐ Maintains up to date incident response plan which includes responsibilities and methods of assessment of information security events, classification thereof, incident response plans and procedures.
- ☐ Regularly testing of incident response plans with "tabletop" exercises to bring about constant improvements to the plan.

9. AUDIT

The Operator regularly tests, assesses and evaluates the effectiveness of the Technical and Organisational Measures outlined above.

- ☐ Conducts regular internal audits of its security practices.
- ☐ Ensures Personnel are aware of and comply with technical and organisational measures as described above.
- ☐ Maintains a register of security incidents.

10. LIST OF SUB OPERATORS

If Sub Operators are hired (for instance for hosting, providing computing centre space, operating software used to process Personal Information, etc.) for the processing of Personal Information, the implementation of technical and organizational measures by the respective Sub Operator must be regulated through appropriate agreements.

The following Sub Operators have been contracted:

☐ Name of Sub Operator; _____

☐ Name of Sub Operator; _____

☐ Name of Sub Operator; _____

☐ Name of Sub Operator; _____