THE INDEPENDENT REGULATORY BOARD FOR AUDITORS

[IRBA]

STANDARD DATA CROSS BOARDER OPERATOR AGREEMENT / ADDENDUM

APPLICABLE TO ALLTRANSFER OF PERSONAL INFORMATION TO ANY COUNTRY OUTSIDE THE REPUBLIC OF SOUTH AFRICA

1. INTRODUCTION

1.1 The Protection of Personal Information Act, 4 of 2013 (POPIA) is a data protection privacy law which as its main function and objective, regulates and controls the processing of Personal Information by a Responsible Party.

1.2 IRBA, in its capacity as a 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 a number of persons, including legal entities and individuals, who are referred to as Data Subjects under the Data Processing Laws, including POPIA.

1.3 IRBA is obligated to comply with the Data Processing Laws, including POPIA and the Data Protection conditions housed under POPIA with respect to the processing of all and any Personal Information pertaining to all and any Data Subjects.

1.4 In order for IRBA to pursue its mandate and its related operational and business interests, IRBA may from time to time have to transfer Personal Information to third parties, including those situated in South Africa, and those who may be situated in another country, outside South Africa, who will process such Personal Information:

- in their own right as a Responsible Parties, or
- alternatively who will process Personal Information as Operators on behalf of IRBA,

1.5 In terms of sections 20, 21 and section 72 of POPIA where IRBA as a Responsible Party provides another with Personal Information which it is responsible for, for processing, then IRBA has a duty to ensure that it concludes a written agreement or contract with the recipient of the Personal Information in terms of which the Recipient contractually undertakes to:

- only process or use Personal Information which has been provided to it by the Responsible Party, for processing, in accordance with the mandate or instruction issued to it by the Responsible Party;
- treat such Personal Information, as confidential;
- not disclose the Personal Information to any other person, unless required by law or in the course of the proper performance of its duties;
- establish and maintain adequate safeguards and security measures in respect of the information which it is processing on behalf of the Responsible Party, in this case being IRBA, which are designed to keep that Personal Information safe and secure from misuse, abuse and/or unauthorised use or access.

1.7 IRBA is desirous of providing Personal Information to a third party (hereinafter referred to as the “Recipient”) and in order to ensure that the Personal Information is correctly processed in a manner which does not impinge on the Data Subject’s rights under POPIA, the Recipient of the Personal Information undertakes to comply with the terms and conditions set out under this Personal Information Transfer Agreement / Addendum.

2. DEFINITIONS

2.1 The parties must take note of the following definitions, which will be used throughout this Personal Information Transfer Agreement, unless the context indicates a contrary meaning:

2.1.1 **“Agreement”** means, **in the absence of any other agreements** which may be in place as between the parties, this Agreement which will govern the relationship as between the parties in relation to the processing of Personal Information;

2.1.2 **"Addendum"** means, **where there are other agreements**, in place as between the parties, and which agreements describe the terms and conditions applicable to the parties’ relationship, including any standard terms and conditions, this Addendum, which Addendum will be read together with the other agreements aforementioned, and which Addendum will govern the relationship as 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, judgment, 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 Subject(s)”** means the person(s) who own(s) the Personal Information which in terms of this Agreement / Addendum, is to be processed by the Recipient;

2.1.5 "**Data Protection Legislation**" means any data protection or data privacy laws applicable from time to time, including but not limited to POPIA, the Electronic Communications and Transactions Act 26 of 2005 and the Consumer Protection Act 68 of 2008, the General Data Protection Regulation (GDPR) the UK Data Privacy Act (UKDPA) and the Californian Privacy Act (CPA);

2.1.6 **“IRBA”** shall mean the Independent Regulatory Board for Auditors who has provided the Recipient with certain Personal Information belonging to its Data Subjects, to process in accordance with the terms of this Agreement / Addendum**;**

2.1.7 "**parties**" means the IRBA and the Recipient ;

2.1.8 **"person"** means an identifiable, living, natural person, or an identifiable, existing juristic person;

2.1.9 **"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, employment details , 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;

- 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.

2.1.10 "**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, wheresoever occurring.

2.1.11 **"process" or "processing"** means any operation or activity or any set of operations, whether or not by automatic means, performed by the Recipient concerning a Data Subject's Personal Information, where so ever occurring 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 so as 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 "**POPIA**" means the Protection of Personal Information Act 4 of 2013;

2.1.14 **"Recipient"** means the person or entity receiving Personal Information from the Responsible Party, whether in its capacity as a Responsible Party or as an Operator, in a country situated outside South Africa, as the case may be;

2.1.15 "**Responsible Party**" shall have the meaning given to it in terms of POPIA.

2.2 Capitalised terms not otherwise defined in this Agreement / Addendum shall bear the meanings given to them in the Agreement / Addendum. Reference to a '*clause*' is to a clause in the Agreement / Addendum, unless otherwise stated or implied form the context in which it appears.

2.3 If there is a conflict between any provision in this Agreement / Addendum and any other agreements which may be in place as between the parties, then, in so far as the conflict concerns the processing of Personal Information, the provision appearing in this Agreement / Addendum shall prevail.

2.4 For purposes of interpretation, in the case of the Agreement / Addendum, the terms set out hereunder shall at all times be read together with the terms housed under the other agreements which may be in place as between the parties, which documents shall constitute one and the same agreement, and except for the additions contemplated in this Agreement / Addendum all the provisions of the terms housed under the other agreements which may be in place as between the parties, remain unchanged and are, with effect from the time that the Recipient is asked to process Personal Information on behalf of IRBA, amended or supplemented by this Agreement / Addendum, and the provisions of the Agreement / Addendum shall apply *mutatis mutandis* to all the other agreements which may be in place as between the parties for the duration of the Agreement / Addendum.

2.5 No agreement varying, adding to, deleting from or consensually cancelling this Agreement / Addendum, and no waiver of any right under this Agreement / Addendum, shall be effective unless reduced to writing and signed by or on behalf of the Parties.

3. MANDATE TO PROCESS

IRBA hereby gives the Recipient certain Personal Information, to process as described under **Annexure "C"**.

4. OBLIGATIONS OF THE RECIPIENT

4.1 The Recipient expressly warrants and undertakes that it will:

4.1.1 process the Personal Information strictly as described under **Annexure "C"** and any specific instructions provided to it by IRBA from time to time;

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

4.1.3 treat the Personal Information as confidential and only disclose, transfer and/or hand over the Personal Information to those person(s) who are employed by it, and who need to process the Personal Information in accordance with the mandate to process as a Recipient and/or in terms of the Agreement / Addendum under strict undertakings of confidentiality;

4.1.4 in addition to the provisions of clause 4.1.3, treat the Personal Information as confidential and only disclose, transfer and/or hand over the Personal Information to third parties under specific instructions as issued by IRBA in writing from time to time or where required by law and only once it has provided IRBA with adequate warning of this requirement to disclose and the related details thereof, including the identity of the person who is to receive the Personal Information, the reason for the disclosure and confirmation that the person to whom the Personal Information is to be disclosed to, has signed the POPIA onwards transmission notice attached hereto marked **Annexure "A";**

4.1.5 ensure that it has and will continue to have in place, appropriate technical and organizational measures to protect and safeguard the Personal Information against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, including Industry Best Practices, which provide a level of security appropriate to the risk represented by the processing and the nature of the Personal Information to be protected and which safeguards comply with the requirements set out under POPIA, and in addition, which measures are in line with the requirements described under the attached Company Security Service Level Requirements, marked **Annexure "B"**;

4.1.6 implement such measures to ensure a level of security appropriate to the risk involved, including as appropriate:

a) the pseudonymisation and encryption of Personal Information;
b) the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;
c) the ability to restore the availability and access to Personal Information in a timely manner in the event of a physical or technical incident; and
d) a process for regularly testing, assessing and evaluating the effectiveness of security measures.

4.1.7 process the Personal Information strictly in accordance with POPIA and the POPIA processing conditions and any other Data Privacy Laws which may be in place in the Country or area where the Recipient is located and where it is using the Personal Information, provided that the POPIA provisions at all times will take precedence;

4.1.8 not use the Personal Information for any direct marketing or advertising, research or statistical purposes, unless expressly authorised to do as 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;

4.1.9 where processing the Personal Information as an Operator, not treat the Personal Information as its own. To this end, the recipient expressly acknowledges that it has been tasked with processing the Personal Information in its capacity as IRBA'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 IRBA;

4.1.10 not sell, alienate or otherwise part with the Personal Information or any of the records housing the Personal Information, save with IRBA's prior written consent and which is required in order for it to comply with its mandate;

4.1.11 where it has to pass the Personal Information to a sub-Recipient, or sub-Operator, as the case may be, as per its mandate or in terms of the Agreement / Addendum, ensure that such party concludes a "sub-Recipient or sub-Operator Agreement" with it and IRBA, which compels the third party receiving the Personal Information to respect and maintain the confidentiality and security of the Personal Information, which sub-Recipient or sub-Operator Agreement will house the same terms and conditions as contained in this Agreement / Addendum, and which shall be concluded before the Personal Information is transferred to the sub-Recipient or sub-Operator.

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

4.1.13 promptly and without undue delay notify IRBA if any Personal Information is lost or destroyed or becomes damaged, corrupted, or unusable. The Recipient will restore such Personal Information at its own expense.

4.1.14 without undue delay notify IRBA 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 IRBA 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.

4.1.15 Immediately, following any unauthorised or unlawful Personal Information processing or Personal Information Breach, ensure that it co-ordinates and co-operates with IRBA's handling of the matter, including:

(a) assisting with any investigation;

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

(c) facilitating interviews with the Recipient's 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 IRBA; 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.

4.1.16 do not inform any third party of any Personal Information Breach without first obtaining IRBA's prior written consent, except when required to do so by law.

4.1.17 agrees that IRBA has the sole right to determine whether:

a) 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 IRBA's discretion, including the contents and delivery method of the notice; and
b) to offer any type of remedy to affected Data Subjects, including the nature and extent of such remedy.

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

4.1.19 will also reimburse IRBA for actual reasonable expenses that IRBA incurs when responding to a Personal Information Breach to the extent that the Recipient caused such a Personal Information Breach, including all costs of notice and any remedy.

4.2 The Recipient 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 IRBA, 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 Recipient's facilities, files, and any other data processing documentation

needed for the required review, audit and/or independent or impartial inspection and the Recipient undertakes to provide all necessary assistance which may be needed to give effect to this right.

5. LIABILITY OF THE RECIPIENT AND THIRD-PARTY RIGHTS

5.1 In the event of the Recipient, the sub-Recipient / sub-Operator or their respective employees or agents breaching any of the warranties and undertakings housed under this Agreement / Addendum or the sub-Recipient / sub -Operator Agreement where applicable, or failing to comply with any of the provisions of POPIA and/or the 8 POPIA Personal Information processing conditions, then in such an event, the Recipient shall be liable for all and any damages it or the sub-Recipient may have caused in consequence of said breach or non-compliance, including patrimonial, non-patrimonial and punitive damages suffered by IRBA and/or the Data Subject(s) and the Recipient indemnifies and holds IRBA including its directors, employees and all and any affected Data Subjects harmless against any such loss, damage, action or claim which may be brought by whomsoever against IRBA or any of its directors, employees, or Data Subjects, or against any of IRBA's affiliated companies, or their directors or employees, and agrees to pay all and any such amounts on demand.

5.2 At the request of IRBA, the Recipient will provide IRBA with evidence of financial resources sufficient to fulfil its responsibilities set out under this Agreement / Addendum and the Recipient Agreement, which may include insurance coverage.

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 actually processed.

7. TERMINATION

7.1 In the event of:

7.1.1. any other agreements, as between the Parties and to which this Agreement / Addendum applies, being terminated for whatsoever reason;

7.1.2. the transfer of Personal Information to the Recipient being temporarily suspended by IRBA for longer than one month, for whatever reason;

7.1.3. the Recipient being in breach of its obligations under the Agreement or the Addendum, as the case may be, or has failed to comply with POPIA or the 8 Information Processing Principles, or any other applicable Data Privacy Laws, and has failed when called upon to do so by IRBA to rectify the breach or area of non-compliance;

7.1.4. the Recipient is in substantial or persistent breach of any warranties or undertakings given by it under the Agreement or the Addendum, as the case may be, notwithstanding that IRBA has not given the Recipient notice of such breach;

7.1.5. the sub-Recipient / sub-Operator is in breach of the sub-Recipient / sub-Operator Agreement;

7.1.6. an application is filed for the placing of the Recipient 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 IRBA, without prejudice to any other rights which it may have against the Recipient, shall be entitled to terminate the Agreement or the Addendum, as the case may be, as well as where applicable, the sub-Recipient Agreement.

7.2 The Parties agree that the termination of the Agreement or the Addendum, as the case may be, at any time, and/or the sub-Recipient Agreement, where applicable, in any circumstances and for whatever reason, does not exempt them from the rights and obligations set out under the Agreement or the Addendum, as the case may be, with regards to the processing of the Personal Information**,** read together with the obligations under POPIA.

7.3 In the event of the Agreement or the Addendum, being terminated whenever, and for whatsoever reason, the Recipient undertakes to:

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

7.3.2 to confirm in writing simultaneously 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 or the Addendum, as the case may be, and for whatsoever reason, the clauses 4, 5, 6 and 7.2 will survive any such termination.

8. GENERAL

8.1 The parties may not modify the provisions of the Agreement or the Addendum, as the case may be, including any annexures, unless such variation is reduced to writing and signed by the Parties.

8.2 The Agreement / Addendum, save where the contrary is stated, will be subject to and governed by the terms set out under the Agreement / Addendum. In the event of any conflict or inconsistency between the terms of the Agreement / Addendum and the other agreements which 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 the Agreement / Addendum will take precedence and govern its interpretation, application and construction.

8.3 All notices to be provided in terms of the Agreement or the Addendum, as the case may be, must be sent to the respective Company's Information Officer or Deputy Information Officer by email: which details are as follows:

Information Officer
Name: Imre Nagy
Address: Building 2, Greenstone Hill Office Park, Emerald Boulevard, Modderfontein, 1609
Tel: 087 940 8826

Email: POPIA@irba.co.za

Deputy Information Officer
Name: Rebecca Moeketsi Motsepe
Address: Building 2, Greenstone Hill Office Park, Emerald Boulevard, Modderfontein, 1609
Tel: 087 940 8803
CEmail: POPIA@irba.co.za

ANNEXURE "A"

ONWARDS TRANSMISSION NOTE

ONWARDS TRANSMISSION NOTE

We, ……. the Recipient acting on behalf of IRBA, have agreed to provide you with the following information, which we have been asked to process by IRBA on their behalf in our capacity as a Recipient, as defined under POPIA:

1. **DETAILS OF THE DATA SUBJECT 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 IRBA 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**

- 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 unauthorised access, and you will ensure that the integrity of the information is not compromised or altered in any manner;

- When using the information, you will comply with the processing conditions and provisions set out under the Protection of Personal Information Act, 4 of 2013, (POPIA);
- You agree to indemnify the Data Subject, IRBA and its employees and directors, 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 IRBA and/or the Data Subject may institute legal action against you under the provisions housed under POPIA should you breach the abovementioned terms.

1. Signed by IRBA

……

……

2. Signed by Data Subject

I, the abovementioned Data Subject agrees to the above onwards transmission of my Personal Information.

……

……

3. Signed by Recipient

……

……

ANNEXURE "B"

TECHNICAL AND ORGANIZATIONAL MEASURES FOR DATA PROCESSING TO BE IMPLEMENTED BY THE RECIPIENT

1. Physical Access Control

Safeguarding admission / access to processing systems with which processing is carried out against unauthorized parties (e.g. through physical property protection: fence, gatekeeper, personnel barrier, turnstile, door with card reader, camera surveillance, organizational property security, regulation on access authorizations, access registration)

The following technical and organizational measures have been implemented by the Recipient for the processing of Personal Information described in this Agreement / Addendum:

☐	Alarm system
☐	Automatic access control system
☐	Locking system with code lock
☐	Biometric access barriers
☐	Light barriers/motion sensors
☐	Manual locking system including key regulation (key book, key issue)
☐	Visitor logging
☐	Careful selection of security staff
☐	Chip cards/transponder locking systems
☐	Video monitoring of access doors
☐	Safety locks
☐	Personnel screening by gatekeeper/reception
☐	Careful selection of cleaning staff
☐	Obligation to wear employee/guest ID cards

2. Data Access Control / User Control

Prevention of third parties using automatic processing systems with equipment for data transmission (authentication with user and password).

The following technical and organizational measures have been implemented by the Recipient for the processing of Personal Information described in this Agreement / Addendum.

☐	Authentication with username / password (passwords assigned based on the valid password regulations)
☐	Usage of intrusion detection systems
☐	Usage of anti-virus software
☐	Usage of a software firewall
☐	Creation of 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)

3. Data Usage Control / Data Storage Media Control / Memory Control

Prevention of unauthorized reading, copying, changing or erasure of data storage media (data storage media control), Prevention of unauthorized entry of Personal Information and unauthorized access to it, changing and deleting saved Personal Information (memory control).

Ensuring that the parties authorized to use an automated processing system only have access to the Personal Information appropriate for their access authorization (e.g. through authorization concepts, passwords, regulations for leaving IRBA and for moving employees to other departments.) (data usage control).

The following technical and organizational measures have been implemented by the Recipient for the processing of Personal Information described in this Agreement / Addendum:

☐	Roles and authorizations based on a *"need to know principle"*
☐	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, incl. password length and changing passwords
☐	Secure storage of data storage media
☐	Proper destruction of data storage media (DIN 66399)
☐	Logging of destruction

4. Transfer Control / Transportation Control

Ensuring 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 transmissions, closed envelopes used in mailings, encrypted saving on data storage media).

The following technical and organizational measures have been implemented by the Recipient for the processing of Personal Information described in this Agreement / Addendum:

☐	Establishment of dedicated lines or VPN tunnels
☐	Encrypted data transmission on the Internet (such as HTTPS, SFTP, etc.)
☐	E-mail 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

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 / locations Personal Information has been transmitted or provided using equipment for data transmission, or to which offices/locations it could be transmitted (transmission control).

The following technical and organizational measures have been implemented by the Recipient for the processing of Personal Information described in this Agreement / Addendum:

☐	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 a disruption (restorability).

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

Ensuring that saved Personal Information cannot be damaged through system malfunctions (data integrity).

Ensuring that Personal Information is protected from accidental destruction or loss (availability control), e.g. by implementing appropriate back-up and disaster recovery concepts.

The following technical and organizational measures have been implemented by the Recipient for the processing of Personal Information described in this Agreement / Addendum:

☐	Uninterruptible Power Supply (UPS)
☐	Devices for monitoring temperature and moisture in server rooms
☐	Fire and smoke detector systems
☐	Alarms for unauthorized access to server rooms
☐	Tests of data restorability
☐	Storing data back-ups in a separate and secure location
☐	In flood areas the server is located above 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 (for instance through logical separation of customer data, specialized access controls (authorization concept), separating testing and production data).

The following technical and organizational measures have been implemented by the Recipient 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 (software-based)
☐	For pseudonymized data: separation of mapping file and storage on a separate, secured IT system
☐	Separation of production and testing systems

8. List of sub-Recipients

If sub-processors 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-Recipient must be regulated through appropriate contract data processing agreements.

The following sub Recipients have been hired:

☐	Name:
☐	Name:
☐	Name:
☐	Name:
☐	Name:

Please attach sub-Recipient Agreements

ANNEXURE "C"

DETAILS OF THE PERSONAL INFORMATION FOR PROCESSING

DETAILS OF THE PROCESSING

The Recipient may process personal Information as follows:

DETAILS OF THE DATA SUBJECT

The Personal Information Processed concern the following Data Subjects:

PURPOSE FOR PROCESSING

CATEGORIES OF DATA

The Personal Information transferred concern the following categories of data:

DETAILS OF THE DATA SUBJECT'S SPECIAL PERSONAL INFORMATION
