OPERATOR AGREEMENT / ADDENDUM

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 The WCGRB, 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 The WCGRB 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 the WCGRB to pursue its mandate and its related operational and business interests, the WCGRB may from time to time ask third parties to process certain Personal Information on its behalf, which Personal Information it has obtained from its Data Subjects.

1.5 In relation to the processing of Personal Information belonging to Data Subjects in South Africa, in terms of section 20 of POPIA, if the WCGRB discloses Personal Information which it has collected from Data Subjects to another for the purpose of processing or further processing such Personal Information on its behalf, hereinafter referred to as “the Operator” then any such processing must be subject to a written agreement concluded between the WCGRB, as the Responsible Party, and the Operator, which 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 WCGRB;

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

1.5.3 keep all the Personal Information held by the Operator on behalf of the WCGRB and/or belonging to the WCGRB Data Subjects, confidential;

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

1.6 The WCGRB is desirous of providing the person (individual and/or a legal entity) to whom this Addendum / Agreement applies (the Operator) with certain Personal

Information, which the WCGRB would like the Operator to process on its behalf, and the Operator has agreed to process the Personal Information on behalf of the WCGRB, which processing will be subject to the terms and conditions set out in this Operator Agreement.

2. DEFINITIONS

2.1 The parties must take note of 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** 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 Operator, on behalf of WCGRB;

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), where applicable.

2.1.6 **"the WCGRB"** shall mean the Western Cape Gaming and Racing Board, who has mandated the Operator to process certain Personal Information belonging to Data Subjects on its behalf, in accordance with the terms of this Agreement / Addendum and where applicable any detailed mandate which is attached hereto marked Annexure "C";

2.1.7 **"Operator"** the person who has been mandated by the WCGRB in terms of the Agreement / Addendum to processes Personal Information belonging to certain Data Subject(s) on its behalf;

2.1.8 "**parties**" means the parties to this Agreement / Addendum;

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

2.1.10 **"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.

2.1.11 "**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.

2.1.12 **"process or processing"** means any operation or activity or any set of operations, whether or not 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;

2.1.13 **"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.

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

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

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 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 Operator is asked to process Personal Information on behalf of the WCGRB, 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

The WCGRB hereby grants to the Operator a mandate to process certain Personal Information on its behalf, as per **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 its mandate and any specific instructions provided to it by the WCGRB 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 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 an Operator 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 where under any specific instructions as issued by the WCGRB in writing from time to time or where required by law and only once it has provided the WCGRB 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 which is housed on and can be downloaded from the WCGRB website, https://www.wcgrb.co.za/notices/.

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 WCGRB Security Service Level Requirements, marked **Annexure "B"**, which must be completed by the Operator, where applicable

4.1.6 process the Personal Information strictly in accordance with POPIA and the POPIA processing conditions;

4.1.7 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;

4.1.8 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 WCGRB'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 WCGRB;

4.1.9 not sell, alienate or otherwise part with the Personal Information or any of the records housing the Personal Information;

4.1.10 where it is allowed to make use of a sub-operator, as per its mandate or in terms of the Agreement / Addendum, ensure that such party concludes a "sub-operator agreement" with it, annexed hereto and marked **Annexure "C"** and the WCGRB which compels the third party receiving the Personal Information to respect and maintain the confidentiality and security of the Personal Information, which 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-operator.

4.1.11 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, and in particular the Sub-operator Agreement, where applicable.

4.1.12 notify the WCGRB immediately where it has reasonable grounds to believe that the Personal Information, which has been provided to it including any Personal Information, which it has processed and which pertains to the Agreement, has been lost, destroyed, or accessed or acquired by any unauthorised person and in such event, immediately: make available to the WCGRB the details of the Personal Information Breach; comply with all instructions and directions given by the WCGRB; take all measures necessary to determine the scope of the compromise and to restore the integrity of the Personal Information so compromised, including where applicable the WCGRB's infrastructure; provide all information which may be requested by the WCGRB, co-operate fully with WCGRB in relation to any notifications which may be made by the WCGRB to any regulator, Data Subjects, or any other person; and co-operate fully with the WCGRB in relation to any investigations that the WCGRB or any regulator, may initiate or which may be initiated by an investigator or other authority.

4.1.13 provide the WCGRB with all assistance and co-operation requested by the WCGRB in relation to any requests or complaints received from any person or entity, including

requests for the deletion, updating or correction of Personal Information which it is processing on behalf of the WCGRB.

4.1.14 provide, on request, all information, data and materials required by the WCGRB to confirm its compliance with its obligations in this Agreement / Addendum. The information shall be provided at no additional cost where provided in an electronic format only. The information shall be provided to the WCGRB promptly and in any event within 5 (five) business days of the request, provided that if the WCGRB is unable to receive the information within this period, then such information will be provided as soon as is practically possible.

4.1.15 comply with all reasonable directions and instructions which may be given by the WCGRB regarding the processing of Personal Information in terms of the Agreement / Addendum. It is further agreed that any directions or instructions which are required for purposes of ensuring compliance with any applicable laws, including Data Protection Legislation, shall be deeded reasonable.

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 WCGRB, 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 and 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 breaching any of the warranties and undertakings housed under this Agreement / Addendum or the sub-operator agreement here applicable, or failing to comply with any of the provisions of POPIA and/or the 8 POPIA Personal Information conditions, then in such an event, the Operator shall be liable for all and any 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 WCGRB and/or the Data Subject(s) and the Operator indemnifies and holds the WCGRB 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 the WCGRB or any of its directors , employees, or Data Subjects, or against any of the WCGRB'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 the WCGRB, the Operator will provide the WCGRB with evidence of financial resources sufficient to fulfil its responsibilities set out under the Agreement, and the Operator 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 Addendum applies, being terminated for whatsoever reason;

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

7.1.3 the Operator 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, and has failed when called upon to do so by the WCGRB to rectify the breach or area of non-compliance;

7.1.4 the Operator 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 the WCGRB has not given the Operator notice of such breach;

7.1.5 the sub-operator is in breach of the sub-operator agreement;

7.1.6 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 WCGRB without prejudice to any other rights which it may have against the Operator, shall be entitled to terminate the Agreement or the Addendum, as the case may be, as well as where applicable, the sub-operator 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-operator agreement, where applicable, in any circumstances and for whatever reason, does not exempt them from the rights and obligations set out under this 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 Operator undertakes to:

7.3.1 restore and/or transfer back to the WCGRB 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 of which documentation must without exception, be returned to the WCGRB 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, as the case may be, 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 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 WCGRB Information Officer by email: primo@wcgrb.co.za

_____

Signed by WCGRB **Date:** _____

_____

Signed by Operator **Date:** _____

ANNEXURE "A"

MANDATE TO PROCESS

DETAILS OF PROCESSING

1. **Service rendered and/or Goods delivered in terms of the Service Level Agreement entered into between the WCGRB and the Operator:**

2. **Mandate in terms of the Processing Notice:**

SUMMARY OF THE PURPOSE OF COLLECTION	**Lawfulness Consent required**
Due diligence purposes - legitimate purpose: To carry out a due diligence before we decide to engage or interact with you or to do business with you, including obtaining and verifying your credentials, including your business details, and where applicable your medical status, health history and related records, education, qualifications and employment history, credit and financial status and history, tax status, B-BBEE status, and or any performance or vendor related history. **Lawfulness – YES; Consent required – NO**	
Contract purposes - assessment and conclusion of a contract: To investigate whether we are able or willing to conclude a contract with you based on the findings of any due diligence detailed above, and if the assessment is in order, to conclude a contract with you. **Lawfulness – YES; Consent required – NO**	
To process transactions and render or provide or receive goods and services - **conclusion of a contract**: To perform under any contract which has been concluded with you, including carrying out all contractual obligations, exercising all contractual rights, assessing or communicating requirements, and/or responding to, or submitting queries, complaints, returns or engaging in general feedback, or acting in such a manner as to personalize any goods or services, and to make recommendations related to us and/or to your operations or activities. **Lawfulness – YES; Consent required – NO**	
Attending to financial matters pertaining to any transaction - conclusion of a contract: To administer accounts or profiles related to you including registrations, subscriptions, purchases, billing events, payments of fees, costs and charges, and taxes, calculations, quoting, invoicing, receipt of payments or payment of refunds, reconciliations and financial management in general. **Lawfulness – YES; Consent required – NO**	

Communications- legitimate purpose: To make contact with you and to communicate with you generally or in respect of our or your requirements, or instructions.

Lawfulness – YES; Consent required – NO

Risk assessment and anti-bribery and corruption matters-legitimate purpose: To carry out vendor, organizational and enterprise wide risk assessments, and due diligences, in order to detect and prevent bribery, corruption, fraud and abuse, to comply with Anti Bribery and Corruption (ABC) laws, as well as to identify and authenticate your access to and to provide you with access to our services or premises and generally to ensure the security and protection of all persons including employees, and persons when entering or leaving our sites and operations or facilities and/or to exercise our rights and to protect our and others' rights and/or property, including to take action against those that seek to violate or abuse our systems, services, licensees, stakeholders, or employees and/or other third parties where applicable.

Lawfulness – YES; Consent required – NO

Legal obligations, litigation, insurance and public duties: To ensure that all service providers are complying with the law and their various legal obligations, including the requirement to register with regulators, obtain and hold permits and certificates, register for VAT, Tax, PAYE, SDL, COIDA and UIF, customs and excise, in order to ensure that all legal levies and fees are paid, to ensure that service providers have submitted legal or statutory reports or have provided various regulatory or statutory notices or returns, in order to litigate and/or to pursue or defend legal claims or collections, to attend to insurance claims and related procedures, to respond to a request or order from a SAPS official, investigator or court official, regulator, or public authority.

Lawfulness – YES; Consent required – NO

Operational issues - compliance with laws and manage the contract: To communicate, enforce and ensure that you comply with our policies, including in relation to legal obligations, claims or actions or legal requirements and conducting investigations and incident responses, including reviewing your communications in these situations in accordance with relevant internal policies and applicable law.

Lawfulness – YES; Consent required – NO

Occupational health - **compliance with laws:** To manage occupational health and absence and fitness for work and notifying family members in emergencies.

Lawfulness – YES; Consent required – NO

Travel - contractual: To facilitate business travel, travel-related support including conference attendance, bookings, and emergency support services.

Lawfulness – YES; Consent required – NO

B-BBEE - compliance with laws: To comply with B-BBEE and to monitor or report B-BBEE requirements, opportunities and related diversity issues, including using your details in B-BBEE reports and score cards. **Lawfulness – YES; Consent required – NO**
Security purposes - legitimate purpose and to comply with laws: to permit you access to our offices, facilities, manufacturing or parking areas, as well as to controlled areas, for the purposes of monitoring via CCTV, your interaction and access in and from our facilities described above, and for general risk management, security and emergency incident control purposes as well as for data and cybersecurity purposes. **Lawfulness – YES; Consent required – NO**
Internal research and development purposes - **consent required:** To conduct internal research and development for new content, products, and services, and to improve, test, and enhance the features and functions of our current goods and services. **Lawfulness – YES; Consent required – NO**

3. Categories of Data Subjects:

☐Clients	☐Former employees
☐ Visitors	☐ Apprentices/ interns
☐ Event participants	☐ Employees relatives
☐ Service users	☐ Consultants
☐ Communication participants	☐ Sales representatives
☐ Subscribers	☐ Shareholders / bodies
☐ Interested parties	☐ Contact persons for business
☐ Supplier and/ or Service Provider (individual contacts at these vendors)	☐ Suppliers and service providers
☐ Employees	☐ Business partners
☐ Applicants	☐ Other please specify:

4. Type of Personal Information

General data/ private contact details

- ☐ Names Personal profiles
- ☐ Image
- ☐ Private address data
- ☐ Date of birth
- ☐ ID card data (e.g. Passport, Social Security, Driving License)
- ☐ Other please specify:

_____

Contract data

- ☐ Settlement and payment data
- ☐ Bank details/ credit card data
- ☐ Financial Standing/ Creditworthiness
- ☐ Contract histories
- ☐ Other please specify:

_____

Professional data

- ☐ Personal Details
- ☐ Position and Employment Details
- ☐ Performance Management
- ☐ Qualification and Education Details
- ☐ Salary or Social Security Data
- ☐ Absence from Work
- ☐ Other please specify:

_____

Service and IT usage data

☐ Device identifiers
☐ Usage and connection data
☐ Image / video data
☐ Telecommunication data/ message content
☐ Audio / voice data
☐ Identification data
☐ Access data
☐ Authorization
☐ Meta data
☐ Other please specify: _____

Special categories of Personal Information

☐ Race or Ethnic Origin
☐ Physical or Mental Health
☐ Biometric Data
☐ Trade Union Membership
☐ Religious or Philosophical Beliefs
☐ Political Opinions
☐ Genetic Data
☐ Sexual Life
☐ Criminal Offences, Convictions or Judgments
☐ Other please specify:

_____

_____
Signed by WCGRB **Date:** _____

_____
Signed by Operator **Date:** _____

ANNEXURE "B"

TECHNICAL AND ORGANIZATIONAL MEASURES FOR DATA PROCESSING BY THE OPERATOR

The WCGRB will provide limited access to the Operator and/or employees of the Operator to render the services to the WCGRB and process certain Personal Information on behalf of the WCGRB, as agreed to between the parties. The access granted will be password protected and the necessary security measures will be put in place by the WCGRB.

The Operator must complete the sections below, where applicable:

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 Operator 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
- ☐ Miscellaneous:

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 Operator for the processing of Personal Information described in this Agreement / Addendum.

☐	Authentication with user name/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)
☐	Miscellaneous:

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 the company and for moving employees to other departments) (data usage control).

The following technical and organizational measures have been implemented by the Operator 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
☐	Miscellaneous:

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 Operator 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
☐	Miscellaneous:

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 Operator 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 user names (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
☐	Miscellaneous:

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 Operator 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
☐	Miscellaneous:

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 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 (software-based)
☐	For pseudonymized data: separation of mapping file and storage on a separate, secured IT system
☐	Separation of production and testing systems
☐	Miscellaneous:

8. List of Sub-Operators

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-Operator must be regulated through appropriate contract data processing agreements.

The following sub-operators have been hired:

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

Please attach sub-operator Agreements as Annexure C / delete if not applicable