ANNEXURE "C"

SUB - OPERATOR AGREEMENT

between

WESTERN CAPE GAMBLING AND RACING BOARD
(Hereinafter referred to as **"WCGRB")**

and

……

(Hereinafter referred to as the **"Operator")**

and

……

(Hereinafter referred to as the **"Sub-Operator")**

1. INTRODUCTION

1.1 In terms of section 20 of POPIA, where a Responsible Party asks other parties (hereinafter referred to as "an Operator") to process Personal Information or further process Personal Information belonging to its Data Subjects on its behalf, whether in South Africa or outside South Africa**,** then any such processing must be subject to a written agreement concluded between the parties which contractually obliges the Operator to:

1.1.1 comply with the provisions of POPIA and the POPIA processing conditions when processing such Personal Information on behalf of the WCGRB;

1.1.2 only process the Personal Information in accordance with the mandate or written instructions received from the Responsible Party and or in accordance with the provisions set out under **Annexure "A" and "B"**;

1.1.3 keep all the Personal Information on behalf of the Responsible Party and / or belonging to the Responsible Party's Data Subjects, confidential;

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

1.2 Furthermore, where any Operator is desirous of appointing a sub-Operator to process any Personal Information on its behalf and which belongs to the Responsible Party's Data Subjects, then in such an event any such processing must be subject to a written agreement concluded between the Responsible Party, the Operator and the sub-Operator which contractually obliges the sub-Operator to comply with the requirements set out under clause 1.1.1 - 1.1.4 above.

1.3 The Operator is desirous of providing the sub-Operator with certain Personal Information which pertains to certain of the WCGRB Data Subjects, for processing on its behalf, and WCGRB has agreed that this may take place subject to the terms and conditions set out under this sub-Operator Agreement.

2. DEFINITIONS

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

2.1.1 **"Data Subject (s)"** means the person (s) who own (s) the Personal Information which is to be processed by the sub-Operator on behalf of the Operator in terms of this sub-Operator Agreement;

2.1.3 "**WCGRB**" shall mean

Western Cape Gambling and Racing Board, 100 Fairway Close, Parow, 7500, who has mandated the Operator to process certain Personal Information belonging to Data Subjects on its behalf, in accordance with the terms of an Operator Agreement and who has in turn agreed that the Operator may sub contract certain of its processing duties and obligations to the sub-Operator;

2.1.4 **"Operator"** means (*insert full details and address*)…… ……..……..…….. who has been mandated by the WCGRB in terms of a Service-level Agreement and an Operator Agreement to processes Personal Information belonging to certain Data Subject (s) on its behalf;

2.1.5 **"Operator Agreement"** means the Operator Agreement concluded between WCGRB and the Operator;

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

2.1.7 **"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.

2.1.8 **"process or processing"** means any operation or activity or any set of operations, whether or not by automatic means, performed by the sub-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;

2.1.9 **"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.

2.1.10 **"sub-Operator"** means the party who has been appointed by the Operator, on approval by WCGRB, to process certain Personal Information on its behalf in terms of this sub-Operator Agreement;

2.1.11 **"sub- Operator Agreement"** means this sub-Operator Agreement.

3. MANDATE TO PROCESS

The Operator hereby grants to the sub-Operator a mandate to process certain Personal Information, which mandate is set out under **Annexure "A"** attached hereto, on its behalf for the purpose and period set out under **Annexure "A"** and WCGRB agrees that this sub-processing may take place on the terms set out under this sub-Operating Agreement.

4. OBLIGATIONS OF THE SUB- OPERATOR

4.1 The sub-Operator expressly warrants and undertakes that it will:

4.1.1 process the Personal Information strictly in accordance with its mandate set out under the sub-Operator Agreement read together with **Annexure "A" and "B"** and any specific instructions provided to it by the WCGRB or the Operator from time to time;

4.1.2 not use the Personal Information for any other purpose, save for the purpose set out under this sub-Operator Agreement and **Annexure "A"**;

4.1.3 only disclose, transfer and / or hand over the Personal Information to those person(s) identified under item of **Annexure "A"**;

4.1.4 save for the provisions housed under clause 4.1.3, treat the Personal Information as confidential and not disclose the Personal Information to any other person unless 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 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, and which in addition, provides 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, which measures are in line with the requirements described under the attached WCGRB Security Service Level Requirements, marked **Annexure "B"**;

4.1.6 notify the Operator and 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, has been lost, destroyed, or accessed or acquired by any unauthorised person;

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

4.1.8 not use the Personal Information for any direct marketing or advertising, research or statistical purposes, unless expressly authorised to do as described under **Annexure "A",** read together with the Agreement, 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 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 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 WCGRB;

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

4.1.11 ensure that any person acting under the authority of the sub-Operator, including any employee or sub-Operator, shall be obligated to process the Personal Information only on instructions from the sub-Operator and strictly in accordance with this sub-Operator Agreement.

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

4.3 The WCGRB, in order to ascertain compliance with the warranties and undertakings housed under this sub-Operator Agreement, 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 sub-Operator's (and where applicable any sub-Operator's) facilities, files, and any other data processing documentation needed for the required review, audit and / or independent or impartial inspection and the sub - 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 sub-Operator or their respective employees or agents breaching any of the warranties and undertakings housed under this sub-Operator agreement, or failing to comply with any of the provisions of POPIA

and / or the POPIA Personal Information conditions or principles, then in such an event, the sub-Operator shall be liable for all and any damages it may have caused in consequence of said breach or non-compliance, including patrimonial, non-patrimonial and punitive damages suffered by the and / or any of its Data Subject(s) and the sub-Operator indemnifies and holds the WCGRB including its directors, employees or its affiliated companies, or their directors or employees and its 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 its Data Subjects, or against any of its affiliated companies, or their directors or employees, and Data Subjects and agrees to pay all and any such amounts on demand.

5.2 At the request of the WCGRB, or the Operator, the sub-Operator will provide the WCGRB, or the Operator with evidence of financial resources sufficient to fulfil its responsibilities set out under the sub-Operator Agreement, and in particular to cover any of its liabilities set out under clause 5 above, which may include insurance coverage.

6. APPLICABLE LAW

The laws of South Africa shall apply to this sub-Operator Agreement, regardless of where the Personal Information is, will be, or was actually processed.

7. TERMINATION

7.1 In the event of:

7.1.1 the Agreement being terminated for whatsoever reason;

7.1.2 the Operator Agreement being terminated for whatsoever reason;

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

7.1.4 the sub-Operator being in breach of its obligations under the sub-Operator Agreement or has failed to comply with POPIA or the Information Processing Principles, and has failed when called upon to do so by the WCGRB, or the Operator to rectify the breach or area of non-compliance;

7.1.5 the sub-Operator is in substantial or persistent breach of any warranties or undertakings given by it under the sub-Operator Agreement, notwithstanding that the WCGRB, or the Operator has not given the sub-Operator notice of such breach;

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

7.2 The Parties agree that the termination of the sub-Operator Agreement at any time, in any circumstances and for whatever reason, does not exempt them from the rights and obligations set out under this sub-Operator Agreement with regards to the processing of the Personal Information detailed under **Annexure "A" and "B",** read together with the obligations under POPIA.

7.3 In the event of the sub-Operator Agreement being terminated whenever, and for whatsoever reason, the sub-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 sub-Operator for processing, including that held by any sub-Operators, 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 sub-Operator Agreement 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 this sub-Operator Agreement including the information in **Annexure "A" and "B"** unless such variation is reduced to writing and signed by the Parties.

8.2 **Notices**

All notices to be provided in terms of the Sub-Operator Agreement must be sent to the WCGRB's Information Officer at: primo@wcgrb.co.za.

_____

Signed by WCGRB **Date: _____**

_____

Signed by Operator **Date: _____**

LIST OF ATTACHMENTS

ANNEXURE "A"

Mandate and Details of Processing

ANNEXURE "B"

Technical and organizational measures for contract data processing implemented by the contractor

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 ☐ Religious or Philosophical Beliefs

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

_____

ANNEXURE "B"

TECHNICAL AND ORGANIZATIONAL MEASURES FOR DATA PROCESSING BY THE SUB-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 sub -Operator for the processing of Personal Information described in this sub-Operator

☐	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 sub-Operator for the processing of Personal Information described in this sub-Operator Agreement:

☐	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 sub-Operator for the processing of Personal Information described in this sub-Operator Agreement:

☐	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

☐	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 sub-Operator for the processing of Personal Information described in this sub-Operator Agreement:

☐	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 sub-Operator for the processing of Personal Information described in this sub-Operator Agreement:

☐	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 sub-Operator for the processing of Personal Information described in this sub-Operator Agreement:

☐	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 sub-Operator for the processing of Personal Information described in this sub-Operator Agreement:

☐	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 center 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, where applicable.