fusion
software

125 JAN SMUTS AVENUE
PARKWOOD
JOHANNESBURG
2193
TEL: 0861 387 466
FAX: 0866 123 176
INFOFUSIONSOFTWARE.CO.ZA

Fusion Software Third Party Data Processor Agreement Addendum to original Agreement

entered into by and between

____

Proprietary

(**"The Client "**)

Registration number			
Signed at		**Date**	
	Signature --		
Name		who warrants that they are duly authorised to sign	
Designation			

And

FUSION SOFTWARE

Proprietary Limited

(**"the Service Provider"**)

Registration number	2017/249376/07		
Signed at	Killarney, JHB	**Date**	30 June 2021
	--		
Name	David Tayler	who warrants that they are duly authorised to sign	
Designation	CEO/POPIA OFFICER		

in respect of the Principal Agreement concluded between the Parties

1. DEFINITIONS

1.1 This Addendum is issued pursuant to the Principal Agreement and, where expressly provided to the contrary herein, shall be subject to the terms and conditions contained therein, including, without limitation, the definitions and rules of interpretation set out in the Principal Agreement. Accordingly, capitalised expressions and words in this Addendum shall, unless defined otherwise in clause 1.2 below, bear the meaning assigned to such expressions and words in the Principal Agreement.

1.2 Meanings of expressions and words used in this document. In this Addendum the following expressions and words have the meanings assigned to them below and derivative expressions and words will have a corresponding meaning: -

1.2.1 **“Addendum**" means this document, together with its schedules;

1.2.2 "**Addendum Effective Date**" means the date of signature of this Addendum by the Party signing last in time;

1.2.3 "**Authorised Subcontractors**" means those subcontractors set out in Schedule 3 which are specifically authorised by Fusion Software to sub-process Fusion Software Personal Information on the basis set out in clause 7, as such schedule may be amended by the Parties in writing from time to time during the term of the Principal Agreement;

1.2.4 "**Fusion Software Personal Information**" means the data described in Schedule 1 and any other Personal Information processed by Service Provider on behalf of “The Client” pursuant to or in connection with the Principal Agreement;

1.2.5 "**Data Protection Laws”** means POPI, GDPR and any other applicable data protection laws which will be applicable

1.2.6 "**Data Subject**" shall have the meaning ascribed thereto in POPIA; "**EEA**" means the European Economic Area, comprising the Member States of the European Union plus Iceland, Liechtenstein and Norway;

1.2.7 “**Erasure"** and "**Erase**" means the removal or destruction of Personal Information such that it cannot be recovered or reconstructed;

1.2.8 "**GDPR**" means the EU General Data Protection Regulation 2016/679 of the European Parliament and of the Council;

1.2.9 "**Incident**" means a security breach leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, Fusion Software or “The Clients” Personal Information transmitted, stored or otherwise processed;

1.2.10 "**Information Officer**" shall have the meaning ascribed thereto in POPI and includes a Data Protection Officer contemplated in GDPR;

1.2.11 "**Parties**" means collectively “The Client” and Fusion Software; and the term **"Party"** refers to either of them, as the context may require;

1.2.12 "**Personal Information**" shall have the meaning ascribed thereto in POPI;

1.2.13 "**POPI**" means the Protection of Personal Information Act, 2013. Any term not defined in this Addendum or the Principal Agreement shall, if applicable, have the meaning ascribed thereto in POPI;

1.2.14 "**Principal Agreement"** means the Agreement concluded between the Parties with an Effective Date of ________________________________as amended by this Addendum and any other amendments thereto;

1.2.15 “**Products”** means the products to be supplied by the Service Provider to “The Client” pursuant to the Principal Agreement;

1.2.16 "**Process", "Processing"** and **"Processed**" shall have the meaning ascribed thereto in POPI;

1.2.17 "**Services**" means the services to be supplied by the Service Provider to "The Client" pursuant to the Principal Agreement;

1.2.18 "**Special Categories of Personal Information**" shall have the meaning ascribed thereto in POPI;

1.2.19 "**Staff**" means any director, employee, agent, consultant, contractor or other representative of a Party or its subcontractors involved in the provision of Products or Services;

1.2.20 "**Standard Contractual Clauses**" means the standard contractual clauses for the transfer of Personal Information to Service Providers established in Third Countries, as approved by the European Commission Decision 2010/87/EU, or any set of clauses approved by the European Commission which amends, replaces or supersedes such clauses; and

1.2.21 "**Third Country**" means any country outside the Republic of South Africa or the EEA which is not the subject of a valid adequacy decision by the European Commission on the protection of Personal Information in Third Countries.

2 INTRODUCTION

The Parties hereby agree that, with effect from the Addendum Effective Date, the terms and conditions set out in this Addendum shall be added to and form part of the Principal Agreement.

3 DATA PROCESSING TERMS

3.1 Compliance with Addendum. When providing the Services and/or Products to "The Client" pursuant to the Principal Agreement, the Service Provider shall strictly Process "The Clients" Personal Information on behalf of "The Client" in accordance with the terms of this Addendum and applicable Data Protection Laws.

3.2 Standard of performance. The Service Provider shall maintain all the technical and organisational measures to comply with the requirements set forth in the Addendum and its Schedules, including, without limitation, those set out in Schedule 2.

4 PROCESSING OF "THE CLIENTS" PERSONAL INFORMATION

4.1 Processing. The Service Provider shall only Process "The Clients" Personal Information for the purposes set out in Schedule 2.

4.2 Restrictions. The Service Provider shall not Process or alter "The Clients" Personal Information or disclose or permit the disclosure of "The Client's" Personal Information to any third party other than in accordance with "The Client's" documented instructions; unless such Processing is required by any law to which the Service Provider is subject. The Service Provider shall, to the extent permitted by such law, inform "The Client's" of that legal requirement before Processing the Personal Information and comply with "The Client's" instructions to minimise, to the extent possible, the scope of the disclosure, unless instructed otherwise by "The Client".

4.3 Limited consent. For the purposes set out in clause 3.1 above, "The Client" hereby consents to the transfer by the Service Provider of "The Client's" Personal Information to the recipients listed in Schedule 2, including the Service Providers located in Third Countries, subject to the Service Provider complying with the provisions of clause 1212.

5 RELIABILITY AND NON–DISCLOSURE

5.1 Staff access. The Service Provider shall take reasonable steps to ensure the reliability of any member of Staff who may have access to "The Clients" Personal Information, ensuring in each case that access is strictly limited to those individuals who require access to the relevant Clients Personal Information.

5.2 Requirements for Staff access. Fusion Software will ensure that all Staff which have a duty to process "The Clients" Personal Information:

5.2.1 are informed of the confidential nature of the Clients Personal Information and are aware of the Service Provider's obligations under this Addendum and the Principal Agreement in relation to "The Clients" Personal Information.

5.2.2 have undertaken appropriate training or certifications in relation to the Data Protection Laws or any other training or certifications requested by "The Client". Should there be no request from "The Client"; "The Client" will be satisfied and will be adequate with Fusion Software training on Personal information and POPIA Act.

5.2.3 are subject to written confidentiality undertakings; and

5.2.4 when accessing "The Clients" Personal Information, are subject to user authentication and login processes in accordance with this Addendum, the Principal Agreement and the applicable Data Protection Laws.

6 PERSONAL INFORMATION SECURITY

6.1 Technical and organisational measures. The Service Provider shall implement appropriate technical and organisational measures in respect of "The Clients" Personal Information to ensure a level of security appropriate to the risk associated with such Processing, including but not limited to:

6.1.1 pseudonymisation and encryption;

6.1.2 the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;

6.1.3 the ability to restore the availability and access to "The Clients" Personal Information in a timely manner in the event of a physical or technical Incident; and

6.1.4 a process for regularly testing, assessing, and evaluating the effectiveness of the technical and organisational measures implemented for ensuring the security of "The Client's" Personal Information together with the specific requirements set out in Schedule 2.

6.2 Risk Assessment. In assessing the appropriate level of security, the Service Provider shall take into account the risks that are presented by Processing, in particular from accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to "The Clients" Personal Information transmitted, stored or otherwise processed.

7 DATA SUBJECT RIGHTS

7.1 Notification. The Service Provider shall promptly notify "The Client" if it receives a request from a Data Subject, a supervisory authority and /or other competent authority under any applicable Data Protection Laws with respect to "The Clients" personal information if "The Client" is hosted on our servers.

7.2 Assistance by Service Provider. The Service Provider shall, at a quoted cost to "The Client" provide "The Client" with all assistance required by "The Client" to respond to requests received from Data Subjects in terms of the relevant Data Protection on Laws and shall comply with any assessment, enquiry, notice or investigation under any Data protection Laws with respect to "The Client" personal Information or this Addendum, which shall include without limitation:

7.2.1 the provision of all data requested by “The Client” within a reasonable timescale specified by “The Client” in each case, including full details and copies of the complaint, compliment, communication or request and any of “The Client’s” Personal Information it holds in relation to the requesting Data Subject;

7.2.2 where applicable, providing such assistance as is reasonably requested by “The client” to enable “The Client” to comply with the relevant request within the timescales prescribed by the Data Protection Laws; and

7.2.3 implementing any additional technical and organisational measures as may be reasonably required by “The Client” to allow “The Client” to respond effectively to relevant complaints, communications or requests.

8 PERSONAL INFORMATION BREACH

8.1 Notice of breach. The Service Provider shall notify “The Client” without undue delay and, in any case, within a reasonable time frame of becoming aware of or reasonably suspecting a Personal Information Breach. The Service Provider will provide “The Client” with sufficient information to allow “The Client” to meet any obligations to report a Personal Information Breach under the Data Protection Laws. Such notification shall as a minimum:

8.1.1 describe the nature of the Personal Information Breach, the categories and numbers of Data Subjects affected, and the categories and numbers of Personal Information records affected;

8.1.2 communicate the name and contact details of the Service Provider's Information Officer or other relevant contact from whom more information may be obtained;

8.1.3 describe the estimated risk posed by and the likely consequences of the Personal Information Breach; and

8.1.4 describe the measures taken or proposed to be taken to address the Personal Information Breach.

8.2 Service Provider Obligations. The Service Provider shall, within reason co-operate with "The Client" and take such reasonable steps as requested by "The Client" to assist in the investigation, mitigation and remediation of each Personal Information Breach. All commercial instructions are for the clients interests and therefore need to be agreed to.

8.3 Notification of Personal Information Breach. In the event of a Personal Information Breach, the Service Provider shall not inform any third party without "The Clients" prior consent, unless notification is required by the applicable Data Protection Laws to which the Service Provider is subject, in which case the Service Provider shall, to the extent permitted by such law, inform "The Client" of that legal requirement, provide a copy of the proposed notification and consider any comments made by "The Client" before notifying the Personal Information Breach.

9 DATA PROTECTION IMPACT ASSESSMENT AND PRIOR CONSULTATION

The Service Provider shall provide reasonable assistance to "The Client" with any data protection impact assessments which are required under Article 35 of GDPR or any other Data Protection Laws and with any prior consultations to any supervisory authority which are required under Article 36 of GDPR, in each case solely in relation to Processing of "The Client's" Personal Information by the Service Provider on behalf of "The Client" and considering the nature of the processing and information available to the Service Provider.

10 ERASURE OR RETURN OF "THE CLIENT'S" PERSONAL INFORMATION

10.1 The Service Provider shall promptly and, in any event, within 90 days:

10.1.1 cessation of processing of "The Clients" Personal Information by the Service Provider; or

10.1.2 termination of the Principal Agreement, by mutual agreement of "The Client" and The Service provider (such choice to be notified to Service Provider in writing) either:

10.1.2.1 return a complete copy of all "The Clients" Personal Information in its, or any Authorised Subcontractor's, possession or control to "The Clients" by secure file transfer in such format as such data is in at the time of such request, or, on the written direction of "The Client", in flat file format, and securely Erase, or procure the Erasure of, all other copies of "The Client" Personal Information in its, or any Authorised Subcontractor's, possession or control; or

10.1.2.2 Erase, or procure the Erasure of, all copies of "The Client" Personal Information in the possession or under the control of the Service Provider or any Authorised Subcontractor, and in each case, provide a written notice to "The Client" that it has complied fully with the requirements of this clause 0.

10.2 **Right of retention**. The Service Provider may retain "The Client's" Personal Information to the extent required by any applicable law, and only to the extent and for such period as required by such law, and always provided that Service Provider shall ensure the confidentiality of all such Clients Personal Information and shall ensure that such Personal Information is only Processed as necessary for the purposes specified by the applicable law requiring its retention and for no other purpose.

11 AUDIT RIGHTS

The Service Provider shall make available to "The Client", upon request, all information necessary to demonstrate compliance with this Addendum and allow for, audits and inspections by an auditor mandated and agreed to; by "The Client", of any premises where the Processing of "The Clients" Personal Information takes place. The Service Provider shall permit the Auditor to inspect, audit and copy any relevant records, processes and systems so that "The Client" may satisfy itself that the provisions of this Addendum are being complied with, subject to the Auditor being subject to non-disclosure obligations similar to those set out in the Principal Agreement.

12 INTERNATIONAL TRANSFERS OF "THE CLIENTS" PERSONAL INFORMATION

The Service Provider shall not process "The Clients" Personal Information nor permit any person other than an Authorized Subcontractor to process "The Clients" Personal Information in a Third Country, unless authorized in writing by "The Client" in advance, via an amendment to Schedule 2 to this Addendum.

13 CODES OF CONDUCT AND CERTIFICATION

At the request of "The Client", the Service Provider shall comply with any Code of Conduct approved by a regulator pursuant to Chapter 7 of POPI or Article 40 of GDPR and obtain any certification under the applicable Data Protection Laws, to the extent that they relate to the processing of "The Clients" Personal Information.

14 EXTENT OF VARIATION

The Principal Agreement shall only be varied as expressly recorded in this Addendum, it being expressly recorded that all remaining terms and conditions of the Principal Agreement shall remain in full force and effect.

15 GENERAL

15.1 Counterparts. This Addendum may be executed in any number of counterparts each of which shall be deemed to be an original and all of which when taken together shall constitute one and the same agreement.

15.2 Precedence. Should there be any conflict between the provisions of this Addendum and those contained in the Principal Agreement, the provisions of this Addendum will prevail. In such event the Parties undertake to conform to the provision of this Addendum and to take whatever steps may be necessary to give effect to the provisions as set out herein.

15.3 Disputes. Any disputes relating to the Addendum shall be resolved in accordance with the dispute resolution provisions of the Principal Agreement.

15.4 Termination. Subject to this section, the Parties agree that this Addendum and the Standard Contractual Clauses shall terminate automatically upon termination of the Principal Agreement or expiry, or termination of all service contracts entered into by the Service Provider with The Client, pursuant to the Principal Agreement, whichever is later.

15.5 Survival. Any obligations imposed on the Service Provider under this Addendum in relation to the Processing of Personal Information shall survive any termination or expiration of the Principal Agreement.

15.6 Breach. Any breach of this Addendum shall constitute a material breach of the Principal Agreement.

15.7 Validity. Should any provision of this Addendum be invalid or unenforceable, then the remainder of this Addendum shall remain valid and in force. The invalid or unenforceable provision shall be either:

15.7.1 be amended as necessary to ensure its validity and enforceability, while preserving the Parties' intentions as closely as possible or, if this is not possible,

15.7.2 construed in a manner as if the invalid or unenforceable part had never been contained therein.

SCHEDULE 1

DETAILS OF PROCESSING OF "THE CLIENT'S" PERSONAL INFORMATION

This schedule 1 document includes certain details of the Processing of "The Clients" Personal Information as required by Data Protection Laws

1. Subject matter and duration of the Processing of "The Clients" Personal Information

The subject matter and duration of the Processing of "The Clients" Personal Information are set out in the Principal Agreement and this Addendum.

2. The nature and purpose of the Processing of "The Clients" Personal Information:

____

____

3. The type of "The Clients" Personal Information to be processed:

____

____

4. The categories of Data Subject to whom "The Clients" Personal Information relates:

____

____

SCHEDULE 2

TECHNICAL AND ORGANISATIONAL MEASURES

The Service Provider shall be responsible for implementing Organisational and Technical measures which comply with best practice and applicable Data Protection Laws. Without limiting the generality of the foregoing, such measures shall include the following.

1. ORGANISTATIONAL SECURITY MEASURES

1.1 Security Management

1.1.1 **Security policy and procedures**. The Service Provider must document a security policy with regard to the Processing of Personal Information.

1.1.2 Roles and responsibilities.

1.1.2.1 Roles and responsibilities assigned to Staff related to the Processing of The Client Personal Information must be clearly defined and allocated in accordance with the Service Provider's security policy.

1.1.2.2 During internal re-organisations or terminations or changes of employment, revocation of rights and responsibilities of Staff, appropriate hand-over procedures must be clearly defined.

1.1.3 **Access Control Policy**: Specific access control rights must be allocated to each Staff role involved in the Processing of “The Clients” Personal Information, following the "need-to-know" principle.

1.1.4 **Resource/asset management**: The Service Provider must maintain a register of the IT Staff used for the Processing of “The Clients” Personal Information (hardware, software, and network). A specific person must be assigned the task of maintaining and updating the register (e.g., IT officer).

1.1.5 **Change management**: The Service Provider must ensure that all changes to the IT system are registered and monitored by a specific person (e.g., IT or security officer). Regular monitoring of this process must be provided for.

1.2 Incident response and business continuity

1.2.1 Incident’s handling / Personal Information breaches:

1.2.1.1 An Incident response plan with detailed procedures must be defined to ensure effective and orderly response to Incidents pertaining to “The Clients” Personal Information.

1.2.1.2 The Service Provider will report any security Incident that has resulted in a loss, misuse, or unauthorized acquisition of any "The Clients" Personal Information, to "The Clients" in writing without undue delay.

1.2.2 Business continuity: The Service Provider shall establish the main procedures and controls to be followed in order to ensure the required level of continuity and availability of the IT system Processing "The Clients" Personal Information (in the event of an Incident/Personal Information breach).

1.3 **Human resources**

1.3.1 Confidentiality of personnel: The Service Provider shall ensure that all Staff understand their responsibilities and obligations related to the Processing of "The Clients" Personal Information. Roles and responsibilities must be clearly communicated during the pre-employment and/or induction process.

The Service Provider shall ensure that all Staff are adequately informed about the security controls of the IT system that relate to their everyday work. Staff involved in the Processing of "The Clients" Personal Information must also be properly informed about relevant data protection requirements and legal obligations through regular awareness campaigns.

2.**Technical security measures**

2.1 Access control and authentication

2.1.1 An access control system applicable to all users accessing the IT system shall be implemented. The system must allow for the creating, approving, reviewing and deleting of user accounts.

2.1.2 The use of shared user accounts must be avoided. In cases where this is necessary, it is must be ensured that all users of the shared account have the same roles and responsibilities.

2.1.3 When granting access or assigning user roles, the "need-to-know principle" shall be observed in order to limit the number of users having access to "The Clients" Personal Information only to those who require it for achieving the Service Provider's Processing purposes.

2.1.4 Where authentication mechanisms are based on passwords, the Service Provider shall implement very strong password control parameters including length, character complexity, and non-repeatability.

2.1.5 The authentication credentials (such as user ID and password) shall never be transmitted unprotected over the network.

2.2 **Logging and monitoring**: Log files shall be activated for each system or application used for the Processing of BBD Personal Information. They include all types of access to data (view, modification, deletion).

2.3 Security of data at rest

2.3.1 Server/Database security

2.3.1.1 Database and applications servers must be configured to run using a separate account, with minimum OS privileges to function correctly.

2.3.1.2 Database and applications servers must only Process "The Client's" Personal Information that is actually needed to Process in order to achieve its Processing purposes.

2.3.2 Workstation security:

2.3.2.1 Users must not be able to deactivate or bypass security settings.

2.3.2.2 Anti-virus applications and detection signatures must be configured on a regular basis.

2.3.2.3 Users must not have privileges to install or deactivate unauthorised software applications.

2.3.2.4 The system must have session time-outs when the user has not been active for a certain time period.

2.3.2.5 Critical security updates released by the operating system developer must be installed regularly.

2.4 Network/Communication security.

2.4.1 Whenever access is performed through the Internet, communication must be encrypted through cryptographic protocols.

2.4.2 Traffic to and from the IT system must be monitored and controlled through firewalls and intrusion detection systems.

2.5 Back-ups:

2.5.1 Backup and data restore procedures must be defined, documented and clearly linked to roles and responsibilities.

2.5.2 Backups must be given an appropriate level of physical and environmental protection consistent with the standards applied on the originating data.

2.5.3 Execution of backups must be monitored to ensure completeness.

2.6 Execution of backups devices:

2.6.1 Mobile and portable device management procedures must be defined and documented establishing clear rules for their proper use.

2.6.2 Mobile devices that are allowed to access the information system must be pre-registered and pre-authorised.

2.7 Application lifecycle security. During the development lifecycle, best practice, state of the art and well acknowledged secure development practices or standards must be followed**.**

2.8 Data deletion/disposal:

2.8.1 Software-based overwriting must be performed on media prior to their disposal. In cases where this is not possible (CD's, DVD's, etc.) physical destruction must be performed.

2.8.2 Shredding of paper and portable media used to store “The Clients” Personal Information must be carried out.

2.9 **Physical security**: The physical perimeter of the IT system infrastructure must not be accessible by non-authorised personnel. Appropriate technical measures (e.g. intrusion detection system, chip-card operated turnstile, single-person security entry system, locking system, etc) or organisational measures (e.g., security guard) shall be set in place to protect security areas and their access points against entry by unauthorised persons.

SCHEDULE 3

TECHNICAL AND ORGANISATIONAL MEASURES

If applicable – please include a list of Authorised Subcontractors as at the Addendum Effective Date to be included here. Please include full legal name, processing activity, location of service centre(s)]

No.	Authorised Subcontractor (full legal name)	Processing activity	Location of service centres.
1.			