DATA PROCESSING ADDENDUM

This Data Processing Addendum ("DPA") is entered into on _____ (the **"Effective Date"**) by and between _____ (the **"Customer"**) and Afi Technologies Inc. (**"Afi"**).

This DPA amends the Terms of Service, Master Subscription Agreement, Order Form or/and other agreements between Afi and the Customer for the purchase of online services (referred together as "**Main Agreement**"), only to the extent the Service is used to Process Personal Data covered. In the event of a conflict between this DPA and the Main Agreement concerning the subject matter hereof, the terms of this DPA will govern.

Each of Afi and the Customer may be referred to herein as a "**Party**" and together as the "**Parties**".

The Parties are entering into this DPA to ensure that appropriate safeguards are in place to protect such Personal Data in accordance with Applicable Data Protection Laws.

Definitions

1.1 The following definitions are used in this DPA:

a) "**Adequate Country**" means a country or territory that is recognized under European Data Protection Laws as providing adequate protection for Personal Data.

b) "**Affiliate**" means any entity that directly or indirectly controls, is controlled by, or is under common control with the subject entity, where "control" refers to the power to direct or cause the direction of the subject entity, whether through ownership of voting securities, by contract or otherwise.

c) "**Applicable Data Protection Laws**" means all laws and regulations that are applicable to the processing of Personal Data under the Main Agreement, including European Data Protection Laws and the CCPA.

d) "**European Data Protection Laws**" means all laws and regulations of the European Union, the European Economic Area, their member states, Switzerland, and the United Kingdom applicable to the processing of Personal Data under the Main Agreement (including, where applicable, (i) Regulation 2016/679 of the European Parliament and of the Council on the protection of natural persons with regard to the Processing of Personal Data and on the free movement of such data (General Data Protection Regulation) (the "**EU GDPR**"); (ii) the EU GDPR as saved into United Kingdom law by virtue of section 3 of the United Kingdom's European Union (Withdrawal) Act 2018 (the "**UK GDPR**"); (iii) the EU e-Privacy Directive (Directive 2002/58/EC); and (iv) any and all applicable national data protection laws made under, pursuant to or that apply in conjunction with any of (i), (ii) or (iii)).

e) "**CCPA**" means the California Consumer Privacy Act of 2018 (Cal. Civ. Code § 1798.100 - 1798.199, 2018).

f) "**Controller**" means an entity that determines the purposes and means of the processing of Personal Data.

g) "**Data Subject Request**" means a request made by or on behalf of a Data Subject to exercise a right for access to, rectification, objection, erasure or other applicable right recognized by the GDPR of that Data Subject's Personal Data.

h) "**Personal Data**" means all data which is defined as '*personal data*', '*personal information*', or '*personally identifiable information*' (or analogous term) under Applicable Data Protection Laws.

i) "**Processor**" means an entity which processes Personal Data on behalf of the Controller, including an entity to which another entity discloses a natural individual's personal information for a business purpose pursuant to a written contract that requires the entity receiving the information to only retain, use, or disclose Personal Data information for the purpose of providing the Service.

j) "**processing**", "**data subject**", and "**supervisory authority**" will have the meanings ascribed to them in European Data Protection Law.

k) "**Restricted Transfer**" means: (i) where the EU GDPR or Swiss Federal Act on Data Protection applies, a transfer of Personal Data from the European Economic Area or Switzerland (as applicable) to a country outside of the European Economic Area or Switzerland (as applicable) which is not subject to an adequacy determination by the European Commission or Swiss Federal Data Protection and Information Commissioner (as applicable); and (ii) where the UK GDPR applies, a transfer of Personal Data from the United Kingdom to any other country which is not based on adequacy regulations pursuant to Section 17A of the United Kingdom Data Protection Act 2018.

l) "**Service**" means software products and all related services provided by Afi that Processes Personal Data covered by this DPA.

m) "**SCCs**" means: (i) where the EU GDPR or Swiss Federal Act on Data Protection applies, the contractual clauses annexed to the European Commission's Implementing Decision 2021/914 of 4 June 2021 on standard contractual clauses for the transfer of Personal Data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council ("**EU SCCs**"); and (ii) where the UK GDPR applies, standard data protection clauses adopted pursuant to or permitted under Article 46 of the UK GDPR ("**UK SCCs**").

n) "**UK Addendum**" means the template addendum issued by the UK ICO and laid before the UK Parliament in accordance with s119A of the Data Protection Act 2018 on 2 February 2022, as revised under Section 18, which amends the SCCs.

No Sale of Personal Data

With respect to all Personal Data it processes in its role as a Processor or sub-processor, Afi warrants that it will: not sell, retain, use or disclose the Personal Data for any purpose other than for the specific purpose of performing the services to which the Customer subscribes, nor for any commercial purpose other than providing the services. Afi will not use the Personal Data for the purposes of marketing or advertising. For the avoidance of any doubt, Afi shall not sell or share information as those terms are defined under the CCPA.

Duration of Processing/Term of DPA

This DPA and Afi's Processing of Personal Data will terminate automatically upon termination of the Main Agreement and of any post termination period during which Afi makes Personal Data available for export by Customer, until its final deletion.

Controller/Processor Roles

For purposes of this DPA, the parties agree that Afi is a Processor or sub-processor, as applicable, of Personal Data and the Customer is the data controller or processor.

Customer represents and warrants to Afi that Customer has the right and authority to appoint Afi as a Processor and provide instructions to Afi, and such actions have been authorized by the appropriate Controller of the Personal Data.

Afi agrees that it will process all Personal Data in accordance with its obligations pursuant to this DPA and that Customer discloses Personal Data to Afi only for the performance of the Service.

Customer has sole responsibility for the quality, ongoing accuracy, legality and scope of Personal Data and the means by which Customer acquired Personal Data.

Processing of Personal Data

Afi will Process the Personal Data only on the instructions of Customer, including through Customer's use and configuration of the features within the service. Customer instructs Afi to Process the Customer Personal Data:

(a) to provide the applicable service and related technical and administrative support consistent with the Main Agreement and this DPA;
(b) as further instructed via Customer's use of the service; and
(c) to comply with other reasonable instructions provided by Customer (via email or support tickets) that are consistent with the nature and scope of the service.

As soon as practicable upon becoming aware Afi will inform Customer if, in its opinion, an instruction violates the terms of the Applicable Data Protection Laws.

Subject Matter and Nature of Processing

The subject matter and scope of Processing is Afi's provision of the Service, including related technical and administrative support (through management portals or otherwise) that is the subject of the Main Agreement. Afi will Process Personal Data that is provided directly or indirectly by Customer, its clients or end users to Afi for the purpose of providing the Service that is the subject of the Main Agreement.

Security

Afi maintains commercially reasonable technical and organizational measures to ensure a level of security appropriate to the risks that are presented by the processing of Personal Data to protect against accidental or unlawful access, destruction, loss or alteration of Personal Data under its control. Afi may modify such measures, provided that any changes will not result in a material degradation of the security measures. The measures include, without limitation, the security measures set out in Annex 2 ("**Security Measures**").

The Service may make available certain Customer controlled security features, which may include multi-factor authentication, administrative access controls and local encryption. Customer is responsible for securing Personal Data under its control, including but not limited to properly configuring and using available Customer controlled security features.

Personal Data Breach

If Afi becomes aware of and confirms a breach of Afi's security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data in Afi's custody, including Afi's sub-processors, for the purpose of providing the service, Afi will, without undue delay, notify Customer and exercise best efforts to mitigate the effects and to minimize any damage resulting from such a security incident.

Customer agrees that an unsuccessful security incident will not be subject to this section. An unsuccessful security incident includes but is not limited to things such as attempts at unauthorized access to Personal Data or to any of Afi's infrastructure storing Personal Data, pings and other broadcast attacks on firewalls or edge servers, port scans, unsuccessful log-on attempts, denial of service attacks, packet sniffing (or other unauthorized access to traffic data that does not result in access beyond IP addresses or headers).

Afi's obligation to report or respond to a security incident will not be construed as an acknowledgement of any fault or liability of Afi with respect to the security incident. Afi will have no obligation to respond to any incidents caused by Customer or anyone acting with Customer's authorization.

Duty of Confidentiality

Afi ensures that its personnel engaged in the processing Personal Data are under obligations of confidentiality.

Data Subject Requests

If Afi receives a Data Subject Request related to the services, to the extent it is able to do so, and it is legally permitted, Afi will notify Customer and/or direct the Data Subject to make the request directly to Customer.

Customer is responsible for responding to any Data Subject Requests. Taking into account the nature of the Processing, Afi will provide Customer with commercially reasonable assistance in responding to a Data Subject Request, to the extent legally permitted, if such Data Subject Request is reasonably possible and is required under the Applicable Data Protection Laws. If and to the extent legally permitted, Customer will be responsible for any costs arising from Afi's assistance. If required by the relevant Applicable Data

Protection Laws Afi will at no extra charge to the Customer provide reasonable assistance to facilitate such Data Subject Request.

Data Deletion

Within a reasonable amount of time following expiration or termination of the applicable Main Agreement or completion of the services, other than to the extent required to comply with applicable law, Afi will delete all Personal Data processed pursuant to this DPA.

Audit

Afi will cooperate with any Customer audit to verify Afi's compliance with its obligations under this DPA by making available, subject to non-disclosure obligations, third party audit reports, where available, descriptions of security controls and other information reasonably requested by Customer regarding Afi's security practices and compliance with the obligations under the Applicable Data Protection Laws in relation to its processing of Personal Data

Governing Law

Unless set forth otherwise in the Main Agreement, then the DPA is governed and construed by the laws of the State of California without reference to the conflicts of law provisions, and the Parties irrevocably consent to the exclusive personal jurisdiction of the courts of San Francisco, California.

Sub-processing

Customer acknowledges and agrees that Afi may engage third party sub-processors for the specific purposes of carrying out the services. Afi will not sell or otherwise disclose Personal Data to third parties for commercial purposes.

Customer hereby consents to the use of sub-processors as described in this section. A current list of sub-processors includes:

Alphabet Inc., Mountain View, CA	Google Cloud Platform (GCP) is used by Afi to host the Service, including for storage and processing of the data
Amazon.com, Inc., Seattle, WA	Amazon Web Services (AWS) is used by Afi to host the Service, including for storage and processing of the data
Stripe, Inc., San Francisco, CA	Afi uses Stripe to accept payments, manage subscriptions and invoicing.
HubSpot, Inc., Cambridge, MA	HubSpot is used by Afi to manage and automate the sales processes.
Zendesk, San Francisco, CA	Afi uses Zendesk to manage and automate the technical support services.

Afi will provide prior notification, by updating the list of sub-processors and/or providing notice in the applicable service, of a new sub-processor before authorizing such new sub-processor to have access to Customer's Personal Data in connection with the provision of the applicable services.

Customer may reasonably object to Afi's use of a new sub-processor by notifying Afi promptly in writing, explaining the reasonable grounds for objection, within ten (10) business days following Afi's notice described above. Afi will use commercially reasonable efforts to make available to Customer a change to Customer's configuration or use of the services to avoid use of the objected to new sub-processor. If Afi is unable to make available such change within a reasonable period of time, not to exceed thirty (30) days, either party as its sole remedy may terminate the applicable Main Agreement. In such case, Afi will refund any prepaid fees covering the remainder of the term applicable to such services.

Afi will use only sub-processors that have executed written contracts with Afi containing obligations that are substantially similar to those of Afi under this DPA. Afi will be liable for the acts and omissions of its sub-processors to the same extent Afi would be liable if performing the services of each sub-processor directly under the terms of this DPA.

Transfers of Personal Data

Certain Afi services allow Customer the ability to use a data centers located in the European Economic Area and in the United Kingdom ("European Data Centers") for Processing of Personal Data. Certain data related to technical and administrative support for a Service or its management portal ("Metadata") may be hosted in the U.S. even if Customer uses a European Data Center.

If the transfer of Personal Data from Customer to Afi is a Restricted Transfer, then it will be subject to the appropriate SCCs as follows:

1.1 in relation to Personal Data that is protected by the EU GDPR, the EU SCCs will apply as follows:

(a) Module Two will apply where the Customer is a Controller and Module Three will apply where the Customer is a Processor;

(b) in Clause 7, the optional docking clause will apply;

(c) in Clause 9, Option 2 will apply;

(d) in Clause 11, the optional language shall not apply;

(e) in Clause 13 and Annex 1.C, Customer shall maintain records of the applicable Member States and competent supervisory authority, which shall be made available to Afi on request;

(f) in Clause 17, option 1 shall apply and the SCCs shall be governed by Irish law;

(g) in Clause 18(b), disputes shall be resolved before the courts of Ireland;

(h) in Annex 1.A, the 'data importer' shall be Afi and the 'data exporter' shall be Customer and any Affiliates that have acceded to the SCCs pursuant to this DPA;

(i) in Annex 1.B, the description of the transfer is as described in Annex 1 of this DPA;

(j) in Annex 2, the technical and organization measures are as follows: (i) Those measures implemented by Afi as described in Annex 2 of this DPA.

(k) the sub-processors for Annex III shall be as described in Sub-processing section of this DPA.

1.2 in relation to Personal Data that is protected by the UK GDPR, the UK SCCs will apply modified as follows:

(a) the SCCs shall be modified and interpreted in accordance with Part 2 of the UK Addendum, which shall be deemed incorporated into and form an integral part of the DPA;

(b) Tables 1, 2 and 3 in Part 1 of the UK Addendum shall be deemed completed with the information set out in Annex 1 and Annex 2 of the DPA, and Table 4 in Part 1 of the UK Addendum shall be deemed completed by selecting "neither party";

(c) any conflict between the terms of the SCCs and the UK Addendum will be resolved in accordance with Section 10 and Section 11 of the UK Addendum.

1.3 in relation to Personal Data that is protected by the Swiss Federal Act on Data Protection (as amended or replaced), the EU SCCs, completed as set out about in Section 1.1(a) of this DPA, will apply to transfers of such Personal Data, except that:

(a) the competent supervisory authority in respect of such Personal Data will be the Swiss Federal Data Protection and Information Commissioner;

(b) the governing law will be the laws of Switzerland;

(c) references to "Member State(s)" in the EU SCCs will be interpreted to refer to Switzerland, and data subjects located in Switzerland will be entitled to exercise and enforce their rights under the EU SCCs in Switzerland; and

(d) references to the "General Data Protection Regulation", "Regulation 2016/679" or "GDPR" in the SCCs will be understood to be references to the Swiss Federal Act on Data Protection (as amended or replaced).

1.4 in the event that any provision of this DPA contradicts, directly or indirectly, the SCCs, the SCCs will prevail.

Legal Requests

In Afi's role as a Processor or sub-Processor, as applicable, if Afi receives a subpoena, court order, warrant or other legal demand from law enforcement or any public or judicial authority seeking the disclosure of Personal Data, Afi will attempt to redirect the governmental body to request such Personal Data directly from Customer. As part of this effort, Afi may provide Customer's basic contact information to the governmental body. If compelled to disclose Personal Data to a governmental body, then Afi will give Customer reasonable notice of the legal demand to allow Customer to seek a protective order or other appropriate remedy, unless Afi is legally prohibited from doing so.

Limitation of Liability

Notwithstanding anything to the contrary in the Main Agreement or the DPA and to the extent permitted by law, each party's liability arising out of the DPA, the SCCs or any data protection agreements in connection with the Service, whether in contract, tort or under any other liability, shall remain subject to the limitation of liability section of the Main Agreement and any reference in such section to the liability of a party means the aggregate liability of that party and all of its Affiliates under the Agreement and this DPA. Customer agrees that any regulatory penalties incurred by Afi that arise in connection with Customer's failure to comply with its obligations under this DPA or any laws or regulations including Applicable Data Protection Laws shall reduce Afi' liability under the Main Agreement and the DPA as if such penalties were liabilities to Customer under the Main Agreement and the DPA.

Notices

Notice to Afi under this DPA should be sent to privacy@afi.ai. If Customer is not the primary administrator for the service (for example, a client who purchases the service from a managed service provider) Customer acknowledges and agrees that Afi will communicate all notices related to this DPA via email or through the Service with the party that is the primary administrator for the Service.

If Customer is the primary administrator for the Service (for example, a managed service provider that manages the services for its client) Customer acknowledges and agrees that it is responsible for receiving and promptly relaying all notices related to this DPA received via email or through the Service to the appropriate parties, including those notices required by applicable law.

It is Customer's responsibility to maintain current, accurate contact information within the applicable administrative portal for the Service for purposes of facilitating all notices.

General

Afi reserves the right to modify this DPA, including if different GDPR recognized compliance standards become available, or as needed to maintain compliance with the GDPR or other applicable law.

By signing below, each party acknowledges that it has read and understood the terms of this DPA and agrees to be bound by them

Afi Technologies Inc

Name: _____

Title: _____

Signature: _____

Customer: _____

Name: _____

Title: _____

Signature: _____

Annex 1. Description of the Details of Processing

Data exporter

Data Exporter is the legal entity specified in the Customer signature section of this DPA.

Data importer

The data importer is Afi Technologies Inc, a provider of cloud-to-cloud backup and restoration solutions which processes personal data upon the instructions of the data exporter in accordance with the Main Agreement.

Data Subjects

Customer may submit Personal Data to the Services, the extent of which is determined and controlled by Customer in its sole discretion, and which may include but is not limited to Personal Data relating to the following categories of data subjects:

- Prospects, customers, business partners and vendors of Customer (who are natural persons)
- Employees or contact persons of Customer's prospects, customers, business partners and vendors
- Employees, agents, advisors, freelancers of Customer (who are natural persons)

Categories of Data

Customer may submit Personal Data to the Services, the extent of which is determined and controlled by Customer in its sole discretion, and which may include but is not limited to the following categories of Personal Data:

- First and last name
- Position and Employer
- Contact information (company, email, phone, physical business address)
- ID data
- Professional life data
- Personal life data
- Localization data

Special categories of data

Customer may submit special categories of Personal Data to the Services, the extent of which is determined and controlled by Customer in its sole discretion, and which is for the sake of clarity Personal Data with information revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade-union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation.

Nature and purpose of processing

Processing of Personal Data by data importer necessary for the purpose of performance of the Services pursuant to the Main Agreement.

Competent supervisory authority

The data exporter's competent supervisory authority will be determined in accordance with the EU GDPR.

The frequency of the transfer

Continuous for the period of the service agreement or subscription.

Annex 2. Technical and Organizational Security Measures

This Appendix forms part of the Standard Contractual Clauses. A description of the technical and organizational security measures implemented by the data importer in accordance with Standard Contractual Clauses is set out below.

We make all reasonable efforts to ensure a level of security appropriate to the risk associated with the processing of Personal Data. We maintain organizational, technical and administrative measures designed to protect Personal Data within our organization against unauthorized access, destruction, loss, alteration or misuse.

Encryption in Transit

All customer data is encrypted in transit using an up to date TLS1.2 or newer protocol.

Encryption at Rest

All data at rest is encrypted with AES 256 encryption. No customer content is stored in an unencrypted format on the storage. In addition, customers have the option to use their own encryption key (Google KMS, AWS KMS or Azure KMS) for encryption at rest.

Storage and Hosting

Afi infrastructure, including Afi-managed cloud storage and Afi application, is hosted in Google Cloud, which holds the following compliance certifications: SOC1, SOC2, SOC3, ISO 9001, ISO 27001, MPAA, FISMA, FERPA, CJIS, CSA, DIACAP, FedRAMP, ITAR, FIPS 140- 2, G-Cloud.

Afi cloud infrastructure services and data storage are deployed in Google Cloud Platform that prevents physical access to the data and implements access control using Google Single Sign-On.

Afi application has no on-premises or local components.

MFA and Access Management

Login to all customer services is provided via Google and Microsoft OAuth2 login that support 2FA.

Afi enforces 2FA for all its internal systems and services and its personnel is required to use it at all times. Accounts with privileged access to the systems and services provide only limited revocable role-based access rights via GCP platform.

No account credentials are stored on a persistent storage in an unencrypted format.

Audit and Assessment

Afi performs a annual security assessment of its systems and processes. The assessment is performed in collaboration with a reputable independent audit firm and is based on the trust services criteria set forth in TSP section 100, 2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality and Privacy (AICPA, Trust Services Criteria).

Afi also performs regular, at least once a year, assessments of the public-facing systems, vulnerability and penetration testing. Results of such assessments are made available to the customers upon request.

Security awareness

Afi maintains set of documents that define security and privacy policies. All employees are required to read and sign this document. Afi conducts security and privacy trainings mandatory to all employees, as well as the onboarding training for all new employees.