EUROPEAN DATA PROCESSING AGREEMENT (EU Standard Contractual Clauses)

Revised October 13th, 2021

This European Data Processing Addendum ("DPA") is entered into on _____ (the "Effective Date") by and between

with a principal place of business located at (the "Customer") and Afi Technologies Inc., a Delaware company with its registered office in 8 The Green, Suite #10711, Dover, DE 19901 and its associate(s) ("Afi").

This DPA amends the Afi Terms of Use available at afi.ai/terms only to the extent the Product is used to Process Personal Data covered under the GDPR.

Definitions

"Standard Contractual Clauses" means the standard contractual clauses annexed to the European Commission's Decision (EU) 2021/914 of 4 June 2021, in the form set out at Annex 4; as may be amended, superseded or replaced.

"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.

"Controller", "Data Subject", "Processor", Processing" will have the meaning set forth in Article 4 of the GDPR.

"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.

"GDPR" means Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the Processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC.

"Personal Data" means information relating to an identified or identifiable natural person (Data Subject) covered under the GDPR that is directly or indirectly submitted, stored or Processed via use of the Product by Customer, its Affiliates, clients or end users.

"Product" means a Product and all related services provided by Afi that Processes Personal Data covered by this DPA.

"Subprocessor" means a third party that, by reason of its role in performing services on behalf of Afi with respect to Afi's provision of a Product, may have logical access to Personal Data covered by this DPA.

Effectiveness

This DPA is effective from February 20, 2018.

In the event of a conflict between this DPA and the Terms of Use concerning the subject matter hereof, the terms of this DPA will govern.

Duration of Processing/Term of DPA

This DPA and Afi's Processing of Personal Data will terminate automatically upon termination of the Terms of Use 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 of Personal Data. This DPA does not apply where Afi is a Controller of Personal Data.

Customer may act either as a Controller or Processor, as applicable, of Personal Data. If Customer is not the Controller of Personal Data, 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.

Customer has sole responsibility for the quality, ongoing accuracy, legality and scope of Personal Data and the means by which Customer acquired Personal Data. Customer represents and warrants that it has sufficient rights and all third party consents as may be necessary and appropriate for the use of the Personal Data with the Product and that its submission of Personal Data to Afi will comply with the GDPR and all applicable laws.

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 Product. Customer instructs Afi to Process the Customer Personal Data

(a) to provide the applicable Product and related technical and administrative support consistent with the Terms of Use and this DPA;
(b) as further instructed via Customer's use of the Product; 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 Product.

Afi will inform Customer if, in its opinion, an instruction violates the terms of the GDPR.

Subject Matter and Nature of Processing

The subject matter and scope of Processing is Afi's provision of the Product, including related technical and administrative support (through management portals or otherwise) that is the subject of the Terms of Use. 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 Product that is the subject of the Terms of Use.

Data Subject Requests

If Afi receives a Data Subject Request related to the Product, 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 consistent with the functionality of the Product and is required under applicable law. To the extent legally permitted, Customer will be responsible for any costs arising from Afi's assistance.

Duty of Confidentiality

Afi ensures that its personnel engaged in the processing Personal Data have committed to maintain the confidentiality of Personal Data by requiring such personnel to execute written confidentiality agreements.

Data Deletion

Within a reasonable amount of time following expiration or termination of the applicable Terms of Use plus any post termination period during which Customer has the ability to export Personal Data, Afi will delete Personal Data. Customer hereby instructs Afi to delete all Personal Data after such period. It is Customer's responsibility to export any Personal Data prior to its deletion.

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 covered by the GDPR in Afi's custody or control, 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 equipment or facilities 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.

Subprocessing

Customer acknowledges and agrees that Afi Affiliates may be retained as Subprocessors and that Afi and its Affiliates respectively may engage third party Subprocessors as needed to provide a Product. Customer hereby consents to the use of Subprocessors as described in this section.

A current list of Subprocessors includes:

- Google Cloud Platform and Amazon Web Services for infrastructure hosting
- HubSpot, Salesforce and Zendesk for customer relationship management
- Atlassian Jira for automated support ticketing

Afi will provide prior notification, by updating the list of Subprocessors and/or providing notice in the applicable Product, of a new Subprocessor before authorizing such new Subprocessor to have access to Customer's Personal Data in connection with the provision of the applicable Product.

Customer may reasonably object to Afi's use of a new Subprocessor 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 Product to avoid use of the objected to new Subprocessor. 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 Terms of Use with respect only to those services which cannot be provided by Afi without the use of the objected-to new Subprocessor. In such case, Afi will refund any prepaid fees covering the remainder of the term applicable to such Product.

Afi will use only Subprocessors 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 Subprocessors to the same extent Afi would be liable if performing the services of each Subprocessor directly under the terms of 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 policies.

Taking into account the nature of the Processing and the information available to Afi, Afi will provide, at Customer's cost if legally allowed, commercially reasonable cooperation and assistance to Customer regarding Customer's compliance obligations described in Articles 32-36 of the GDPR.

Limitation of Liability

The exclusions and limitations of liability set forth in the applicable Terms of Use will not apply with respect to claims of breach of confidentiality and breach of data security obligations.

Security

Afi maintains commercially reasonable technical and organizational measures 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 Product may make available certain Customer controlled security features, which may include multi-factor authentication, administrative access controls and local encryption. Afi makes available best practices for Customer to adopt to help protect against accidental or unlawful access, destruction, loss or alteration of Personal Data. Customer is responsible for securing Personal Data under its control, including but not limited to properly configuring and using available Customer controlled security features.

Transfers of Personal Data

Certain Products 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 Product or its management portal ("Metadata") may be hosted in the U.S. even if Customer uses a European Data Center.

Governing Law

This DPA is governed by the law of England and Wales and is subject to the exclusive jurisdiction of the courts of England and Wales.

Notices

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

If Customer is the primary administrator for a Product (for example, a managed service provider that manages a Product 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 Product 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 Product 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.

IN WITNESS WHEREOF, the Parties have executed this European Data Processing Agreement.

Afi

Name: _____

Title: _____

Signature: _____

Customer: _____

Name: _____

Title: _____

Signature: _____

Annex 4 – Standard Contractual Clauses

Module Two: Transfer Controller to Processor (C2P)

SECTION I

Clause 1

Purpose and scope

(a) The purpose of these standard contractual clauses is to ensure compliance with the requirements of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 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) for the transfer of personal data to a third country.

(b) The Parties:

i. the natural or legal person(s), public authority/ies, agency/ies or other body/ies (hereinafter "entity/ies") transferring the personal data, as listed in Annex I.A. (hereinafter each "data exporter"), and

ii. the entity/ies in a third country receiving the personal data from the data exporter, directly or indirectly via another entity also Party to these Clauses, as listed in Annex I.A. (hereinafter each "data importer")

have agreed to these standard contractual clauses (hereinafter: "Clauses").

(c) These Clauses apply with respect to the transfer of personal data as specified in Annex I.B.

(d) The Appendix to these Clauses containing the Annexes referred to therein forms an integral part of these Clauses.

Clause 2

Effect and invariability of the Clauses

(a) These Clauses set out appropriate safeguards, including enforceable data subject rights and effective legal remedies, pursuant to Article 46(1) and Article 46 (2)(c) of Regulation (EU) 2016/679 and, with respect to data transfers from controllers to processors and/or processors to processors, standard contractual clauses pursuant to Article 28(7) of Regulation (EU) 2016/679, provided they are not modified, except to select the appropriate Module(s) or to add or update information in the Appendix. This does not prevent the Parties from including the standard contractual clauses laid down in these Clauses in a wider contract and/or to add other clauses or additional safeguards, provided that they do not contradict, directly or indirectly, these Clauses or prejudice the fundamental rights or freedoms of data subjects.

(b) These Clauses are without prejudice to obligations to which the data exporter is subject by virtue of Regulation (EU) 2016/679.

Clause 3

Third-party beneficiaries

(a) Data subjects may invoke and enforce these Clauses, as third-party beneficiaries, against the data exporter and/or data importer, with the following exceptions:

i. Clause 1, Clause 2, Clause 3, Clause 6, Clause 7;
ii. Clause 8 - Clause 8.1(b), 8.9(a), (c), (d) and (e);
iii. Clause 9 - Clause 9(a), (c), (d) and (e);

iv. Clause 12 - Clause 12(a), (d) and (f);
v. Clause 13;
vi. Clause 15.1(c), (d) and (e);
vii. Clause 16(e);
viii. Clause 18 - Clause 18(a) and (b).

(b) Paragraph (a) is without prejudice to rights of data subjects under Regulation (EU) 2016/679.

Clause 4

Interpretation

(a) Where these Clauses use terms that are defined in Regulation (EU) 2016/679, those terms shall have the same meaning as in that Regulation.

(b) These Clauses shall be read and interpreted in the light of the provisions of Regulation (EU) 2016/679.

(c) These Clauses shall not be interpreted in a way that conflicts with rights and obligations provided for in Regulation (EU) 2016/679.

Clause 5

Hierarchy

In the event of a contradiction between these Clauses and the provisions of related agreements between the Parties, existing at the time these Clauses are agreed or entered into thereafter, these Clauses shall prevail.

Clause 6

Description of the transfer(s)

The details of the transfer(s), and in particular the categories of personal data that are transferred and the purpose(s) for which they are transferred, are specified in Annex I.B.

Clause 7

Docking clause

(a) An entity that is not a Party to these Clauses may, with the agreement of the Parties, accede to these Clauses at any time, either as a data exporter or as a data importer, by completing the Appendix and signing Annex I.A.

(b) Once it has completed the Appendix and signed Annex I.A, the acceding entity shall become a Party to these Clauses and have the rights and obligations of a data exporter or data importer in accordance with its designation in Annex I.A.

(c)The acceding entity shall have no rights or obligations arising under these Clauses from the period prior to becoming a Party.

SECTION II - OBLIGATIONS OF THE PARTIES

Clause 8

Data protection safeguards

The data exporter warrants that it has used reasonable efforts to determine that the data importer is able, through the implementation of appropriate technical and organisational measures, to satisfy its obligations under these Clauses.

8.1 Instructions

(a) The data importer shall process the personal data only on documented instructions from the data exporter. The data exporter may give such instructions throughout the duration of the contract.

(b) The data importer shall immediately inform the data exporter if it is unable to follow those instructions.

8.2 Purpose limitation

The data importer shall process the personal data only for the specific purpose(s) of the transfer, as set out in Annex I.B, unless on further instructions from the data exporter.

8.3 Transparency

On request, the data exporter shall make a copy of these Clauses, including the Appendix as completed by the Parties, available to the data subject free of charge. To the extent necessary to protect business secrets or other confidential information, including the measures described in Annex II and personal data, the data exporter may redact part of the text of the Appendix to these Clauses prior to sharing a copy, but shall provide a meaningful summary where the data subject would otherwise not be able to understand the its content or exercise his/her rights. On request, the Parties shall provide the data subject with the reasons for the redactions, to the extent possible without revealing the redacted information. This Clause is without prejudice to the obligations of the data exporter under Articles 13 and 14 of Regulation (EU) 2016/679.

8.4 Accuracy

If the data importer becomes aware that the personal data it has received is inaccurate, or has become outdated, it shall inform the data exporter without undue delay. In this case, the data importer shall cooperate with the data exporter to erase or rectify the data.

8.5 Duration of processing and erasure or return of data

Processing by the data importer shall only take place for the duration specified in Annex I.B. After the end of the provision of the processing services, the data importer shall, at the choice of the data exporter, delete all personal data processed on behalf of the data exporter and certify to the data exporter that it has done so, or return to the data exporter all personal data processed on its behalf and delete existing copies. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit return or deletion of the personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process it to the extent and for as long as required under that local law. This is without prejudice to Clause 14, in particular the requirement for the data importer under Clause 14(e) to notify the data exporter throughout the duration of the contract if it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under Clause 14(a).

8.6 Security of processing

(a) The data importer and, during transmission, also the data exporter shall implement appropriate technical and organisational measures to ensure the security of the data, including protection against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access to that data (hereinafter "personal data breach"). In assessing the appropriate level of security, the Parties shall take due account of the state of the art, the costs of implementation, the nature, scope, context and purpose(s) of processing and the risks involved in the processing for the data subjects. The Parties shall in particular consider having recourse to encryption or pseudonymisation, including during transmission, where the purpose of processing can be fulfilled in that manner. In case of pseudonymisation, the additional information for attributing the personal data to a specific data subject shall, where possible, remain under the exclusive control of the data exporter. In complying with its obligations under this paragraph, the data importer shall at least implement the technical and organisational measures specified in Annex II. The data importer shall carry out regular checks to ensure that these measures continue to provide an appropriate level of security.

(b) The data importer shall grant access to the personal data to members of its personnel only to the extent strictly necessary for the implementation, management and monitoring of the contract. It shall ensure that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

(c) In the event of a personal data breach concerning personal data processed by the data importer under these Clauses, the data importer shall take appropriate measures to address the breach, including measures to mitigate its adverse effects. The data importer shall also notify the data exporter without undue delay after having become aware of the breach. Such notification shall contain the details of a contact point where more information can be obtained, a description of the nature of the breach (including, where possible, categories and approximate number of data subjects and personal data records concerned), its likely consequences and the measures taken or proposed to address the breach including, where appropriate, measures to mitigate its possible adverse effects. Where, and in so far as, it is not possible to provide all information at the same time, the initial notification shall contain the information then available and further information shall, as it becomes available, subsequently be provided without undue delay.

(d) The data importer shall cooperate with and assist the data exporter to enable the data exporter to comply with its obligations under Regulation (EU) 2016/679, in particular to notify the competent supervisory authority and the affected data subjects, taking into account the nature of processing and the information available to the data importer.

8.7 Sensitive data

Where the transfer involves personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, or biometric data for the purpose of uniquely identifying a natural person, data concerning health or a person's sex life or sexual orientation, or data relating to criminal convictions and offences (hereinafter "sensitive data"), the data importer shall apply the specific restrictions and/or additional safeguards described in Annex I.B.

8.8 Onward transfers

The data importer shall only disclose the personal data to a third party on documented instructions from the data exporter. In addition, the data may only be disclosed to a third party located outside the European Union (in the same country as the data importer or in another third country, hereinafter "onward transfer") if the third party is or agrees to be bound by these Clauses, under the appropriate Module, or if:

i. the onward transfer is to a country benefitting from an adequacy decision pursuant to Article 45 of Regulation (EU) 2016/679 that covers the onward transfer;

ii. the third party otherwise ensures appropriate safeguards pursuant to Articles 46 or 47 Regulation of (EU) 2016/679 with respect to the processing in question;

iii. the onward transfer is necessary for the establishment, exercise or defence of legal claims in the context of specific administrative, regulatory or judicial proceedings; or

iv. the onward transfer is necessary in order to protect the vital interests of the data subject or of another natural person.

Any onward transfer is subject to compliance by the data importer with all the other safeguards under these Clauses, in particular purpose limitation.

8.9 Documentation and compliance

(a) The data importer shall promptly and adequately deal with enquiries from the data exporter that relate to the processing under these Clauses.

(b) The Parties shall be able to demonstrate compliance with these Clauses. In particular, the data importer shall keep appropriate documentation on the processing activities carried out on behalf of the data exporter.

(c) The data importer shall make available to the data exporter all information necessary to demonstrate compliance with the obligations set out in these Clauses and at the data exporter's request, allow for and contribute to audits of the processing activities covered by these Clauses, at reasonable intervals or if there are indications of non-compliance. In deciding on a review or audit, the data exporter may take into account relevant certifications held by the data importer.

(e) The data exporter may choose to conduct the audit by itself or mandate an independent auditor. Audits may include inspections at the premises or physical facilities of the data importer and shall, where appropriate, be carried out with reasonable notice.

(d) The Parties shall make the information referred to in paragraphs (b) and (c), including the results of any audits, available to the competent supervisory authority on request.

Clause 9

Use of sub-processors

(a) The data importer has the data exporter's general authorisation for the engagement of sub-processor(s) from an agreed list. The data importer shall specifically inform the data exporter in writing of any intended changes to that list through the addition or replacement of sub-processors at least 30 business days in advance, thereby giving the data exporter sufficient time to be able to object to such changes prior to the engagement of the sub-processor(s). The data importer shall provide the data exporter with the information necessary to enable the data exporter to exercise its right to object.

(b) Where the data importer engages a sub-processor to carry out specific processing activities (on behalf of the data exporter), it shall do so by way of a written contract that provides for, in substance, the same data protection obligations as those binding the data importer under these Clauses, including in terms of third-party beneficiary rights for data subjects. The Parties agree that, by complying with this Clause, the data importer fulfils its obligations under Clause 8.8. The data importer shall ensure that the sub-processor complies with the obligations to which the data importer is subject pursuant to these Clauses.

(c)The data importer shall provide, at the data exporter's request, a copy of such a sub-processor agreement and any subsequent amendments to the data exporter. To the extent necessary to protect business secrets or other confidential information, including personal data, the data importer may redact the text of the agreement prior to sharing a copy.

(d) The data importer shall remain fully responsible to the data exporter for the performance of the sub-processor's obligations under its contract with the data importer. The data importer shall notify the data exporter of any failure by the sub-processor to fulfil its obligations under that contract.

(e)The data importer shall agree a third-party beneficiary clause with the sub-processor whereby - in the event the data importer has factually disappeared, ceased to exist in law or has become insolvent - the data exporter shall have the right to terminate the sub-processor contract and to instruct the sub-processor to erase or return the personal data.

Clause 10

Data subject rights

(a) The data importer shall promptly notify the data exporter of any request it has received from a data subject. It shall not respond to that request itself unless it has been authorised to do so by the data exporter.

(b) The data importer shall assist the data exporter in fulfilling its obligations to respond to data subjects' requests for the exercise of their rights under Regulation (EU) 2016/679. In this regard, the Parties shall set out in Annex II the appropriate technical and organisational measures, taking into account the nature of the processing, by which the assistance shall be provided, as well as the scope and the extent of the assistance required.

(c) In fulfilling its obligations under paragraphs (a) and (b), the data importer shall comply with the instructions from the data exporter.

Clause 11

Redress

(a) The data importer shall inform data subjects in a transparent and easily accessible format, through individual notice or on its website, of a contact point authorised to handle complaints. It shall deal promptly with any complaints it receives from a data subject.

(b) In case of a dispute between a data subject and one of the Parties as regards compliance with these Clauses, that Party shall use its best efforts to resolve the issue amicably in a timely fashion. The Parties shall keep each other informed about such disputes and, where appropriate, cooperate in resolving them.

(c) Where the data subject invokes a third-party beneficiary right pursuant to Clause 3, the data importer shall accept the decision of the data subject to:

i. lodge a complaint with the supervisory authority in the Member State of his/her habitual residence or place of work, or the competent supervisory authority pursuant to Clause 13;

ii. refer the dispute to the competent courts within the meaning of Clause 18.

(d) The Parties accept that the data subject may be represented by a not-for-profit body, organisation or association under the conditions set out in Article 80(1) of Regulation (EU) 2016/679.

(e)The data importer shall abide by a decision that is binding under the applicable EU or Member State law.

(f) The data importer agrees that the choice made by the data subject will not prejudice his/her substantive and procedural rights to seek remedies in accordance with applicable laws.

Clause 12

Liability

(a) Each Party shall be liable to the other Party/ies for any damages it causes the other Party/ies by any breach of these Clauses.

(b) The data importer shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages the data importer or its sub-processor causes the data subject by breaching the third-party beneficiary rights under these Clauses.

(c) Notwithstanding paragraph (b), the data exporter shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages the data exporter or the data importer (or its sub-processor) causes the data subject by breaching the third-party beneficiary rights under these Clauses. This is without prejudice to the liability of the data exporter and, where the data exporter is a processor acting on behalf of a controller, tothe liability of the controller under Regulation (EU) 2016/679 or Regulation (EU) 2018/1725, as applicable.

(d)The Parties agree that if the data exporter is held liable under paragraph (c) for damages caused by the data importer (or its sub-processor), it shall be entitled to claim back from the data importer that part of the compensation corresponding to the data importer's responsibility for the damage.

(e) Where more than one Party is responsible for any damage caused to the data subject as a result of a breach of these Clauses, all responsible Parties shall be jointly and severally liable and the data subject is entitled to bring an action in court against any of these Parties.

(f) The Parties agree that if one Party is held liable under paragraph (e), it shall be entitled to claim back from the other Party/ies that part of the compensation corresponding to its / their responsibility for the damage.

(g) The data importer may not invoke the conduct of a sub-processor to avoid its own liability.

Clause 13

Supervision

(a) The supervisory authority with responsibility for ensuring compliance by the data exporter with Regulation (EU) 2016/679 as regards the data transfer, as indicated in Annex I.C, shall act as competent supervisory authority.

(b) The data importer agrees to submit itself to the jurisdiction of and cooperate with the competent supervisory authority in any procedures aimed at ensuring compliance with these Clauses. In particular, the data importer agrees to respond to enquiries, submit to audits and comply with the measures adopted by the supervisory authority, including remedial and compensatory measures. It shall provide the supervisory authority with written confirmation that the necessary actions have been taken.

SECTION III - LOCAL LAWS AND OBLIGATIONS IN CASE OF ACCESS BY

PUBLIC AUTHORITIES

Clause 14

Local laws and practices affecting compliance with the Clauses

(a) The Parties warrant that they have no reason to believe that the laws and practices in the third country of destination applicable to the processing of the personal data by the data importer, including any requirements to disclose personal data or measures authorising access by public authorities, prevent the data importer from fulfilling its obligations under these Clauses. This is based on the understanding that laws and practices that respect the essence of the fundamental rights and freedoms and do not exceed what is necessary and proportionate in a

democratic society to safeguard one of the objectives listed in Article 23(1) of Regulation (EU) 2016/679, are not in contradiction with these Clauses.

(b) The Parties declare that in providing the warranty in paragraph (a), they have taken due account in particular of the following elements:

(i) the specific circumstances of the transfer, including the length of the processing chain, the number of actors involved and the transmission channels used; intended onward transfers; the type of recipient; the purpose of processing; the categories and format of the transferred personal data; the economic sector in which the transfer occurs; the storage location of the data transferred;

(ii) the laws and practices of the third country of destination- including those requiring the disclosure of data to public authorities or authorising access by such authorities - relevant in light of the specific circumstances of the transfer, and the applicable limitations and safeguards;

(iii) any relevant contractual, technical or organisational safeguards put in place to supplement the safeguards under these Clauses, including measures applied during transmission and to the processing of the personal data in the country of destination.

(c) The data importer warrants that, in carrying out the assessment under paragraph (b), it has made its best efforts to provide the data exporter with relevant information and agrees that it will continue to cooperate with the data exporter in ensuring compliance with these Clauses.

(d)The Parties agree to document the assessment under paragraph (b) and make it available to the competent supervisory authority on request.

(e) The data importer agrees to notify the data exporter promptly if, after having agreed to these Clauses and for the duration of the contract, it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under paragraph (a), including following a change in the laws of the third country or a measure (such as a disclosure request) indicating an application of such laws in practice that is not in line with the requirements in paragraph (a).

(f) Following a notification pursuant to paragraph (e), or if the data exporter otherwise has reason to believe that the data importer can no longer fulfil its obligations under these Clauses, the data exporter shall promptly identify appropriate measures (e.g. technical or organisational measures to ensure security and confidentiality) to be adopted by the data exporter and/or data importer to address the situation. The data exporter shall suspend the data transfer if it considers that no appropriate safeguards for such transfer can be ensured, or if instructed by the competent supervisory authority to do so. In this case, the data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses. If the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise. Where the contract is terminated pursuant to this Clause, Clause 16(d) and (e) shall apply.

Clause 15

Obligations of the data importer in case of access by public authorities

15.1 Notification

(a) The data importer agrees to notify the data exporter and, where possible, the data subject promptly (if necessary with the help of the data exporter) if it:

(i) receives a legally binding request from a public authority, including judicial authorities, under the laws of the country of destination for the disclosure of personal data transferred pursuant to these Clauses; such

notification shall include information about the personal data requested, the requesting authority, the legal basis for the request and the response provided; or

(ii) becomes aware of any direct access by public authorities to personal data transferred pursuant to these Clauses in accordance with the laws of the country of destination; such notification shall include all information available to the importer.

(b) If the data importer is prohibited from notifying the data exporter and/or the data subject under the laws of the country of destination, the data importer agrees to use its best efforts to obtain a waiver of the prohibition, with a view to communicating as much information as possible, as soon as possible. The data importer agrees to document its best efforts in order to be able to demonstrate them on request of the data exporter.

(c)Where permissible under the laws of the country of destination, the data importer agrees to provide the data exporter, at regular intervals for the duration of the contract, with as much relevant information as possible on the requests received (in particular, number of requests, type of data requested, requesting authorities, whether requests have been challenged and the outcome of such challenges, etc.).

(d)The data importer agrees to preserve the information pursuant to paragraphs (a) to (c) for the duration of the contract and make it available to the competent suspensory authority on request.

(e) Paragraphs (a) to (c) are without prejudice to the obligation of the data importer pursuant to Clause 14(e) and Clause 16 to inform the data exporter promptly where it is unable to comply with these Clauses.

15.2 Review of legality and data minimisation

(a) The data importer agrees to review the legality of the request for disclosure, in particular whether it remains within the powers granted to the requesting public authority, and to challenge the request if, after careful assessment, it concludes that there are reasonable grounds to consider that the request is unlawful under the laws of the country of destination, applicable obligations under international law and principles of international comity. The data importer shall, under the same conditions, pursue possibilities of appeal. When challenging a request, the data importer shall seek interim measures with a view to suspending the effects of the request until the competent judicial authority has decided on its merits. It shall not disclose the personal datarequested until required to do so under the applicable procedural rules. These requirements are without prejudice to the obligations of the data importer under Clause 14(e).

(b) The data importer agrees to document its legal assessment and any challenge to the request for disclosure and, to the extent permissible under the laws of the country of destination, make the documentation available to the data exporter. It shall also make it available to the competent supervisory authority on request.

(c)The data importer agrees to provide the minimum amount of information permissible when responding to a request for disclosure, based on a reasonable interpretation of the request.

SECTION IV - FINAL PROVISIONS

Clause 16

Non-compliance with the Clauses and termination

(a) The data importer shall promptly inform the data exporter if it is unable to comply with these Clauses, for whatever reason.

(b) In the event that the data importer is in breach of these Clauses or unable to comply with these Clauses, the data exporter shall suspend the transfer of personal data to the data importer until compliance is again ensured or the contract is terminated. This is without prejudice to Clause 14(f).

(c)The data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses, where:

(i) the data exporter has suspended the transfer of personal data to the data importer pursuant to paragraph (b) and compliance with these Clauses is not restored within a reasonable time and in any event within one month of suspension;

(ii) the data importer is in substantial or persistent breach of these Clauses; or

(iii) the data importer fails to comply with a binding decision of a competent court or supervisory authority regarding its obligations under these Clauses.

In these cases, it shall inform the competent supervisory authority such non-compliance. Where the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise.

(d) Personal data that has been transferred prior to the termination of the contract pursuant to paragraph (c) shall at the choice of the data exporter immediately be returned to the data exporter or deleted in its entirety. The same shall apply to any copies of the data. The data importer shall certify the deletion of the data to the data exporter. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit the return or deletion of the transferred personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process the data to the extent and for as long as required under that local law.

(e) Either Party may revoke its agreement to be bound by these Clauses where (i) the European Commission adopts a decision pursuant to Article 45(3) of Regulation (EU) 2016/679 that covers the transfer of personal data to which these Clauses apply; or (ii) Regulation (EU) 2016/679 becomes part of the legal framework of the country to which the personal data is transferred. This is without prejudice to other obligations applying to the processing in question under Regulation (EU) 2016/679.

Clause 17

Governing law

These Clauses shall be governed by the law of one of the EU Member States, provided such law allows for third-party beneficiary rights. The Parties agree that this shall be the law of the Republic of Ireland.

Clause 18

Choice of forum and jurisdiction

(a) Any dispute arising from these Clauses shall be resolved by the courts of an EU Member State.

(b) The Parties agree that those shall be the courts of the jurisdiction specified in Clause 17.

(c) A data subject may also bring legal proceedings against the data exporter and/or data importer before the courts of the Member State in which he/she has his/her habitual residence.

(d) The Parties agree to submit themselves to the jurisdiction of such courts.

Data exporter:

[CUSTOMER: PLEASE COMPLETE AND SIGN:]

Name: _____

Position: _____

Address: _____

Signature_____

(stamp of organisation)

Data importer:

Name (written out in full): _____

Position: _____

Address: _____

Annex 1 to the Standard Contractual Clauses

This Appendix forms part of the Standard Contractual Clauses.

A description of the Details of Processing is set out below.

Data exporter

Data Exporter is the legal entity specified in Section 12.4.1 of the DPA.

Data importer

The data importer is 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 terms of the 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)
- Customer's Users authorized by Customer to use the Services

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
- Title
- Position
- Employer
- Contact information (company, email, phone, physical business address)

- ID data
- Professional life data
- Personal life data
- Localisation data

Special categories of data (if appropriate)

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.

Processing operations

The objective of Processing of Personal Data by data importer is the performance of the SCC Services pursuant to the Agreement.

Data exporter:

[CUSTOMER: PLEASE COMPLETE AND SIGN:]

Name: _____

Position: _____

Address: _____

Signature_____
(stamp of organisation)

Data importer:

Name (written out in full): _____

Position: _____

Address: _____

Annex 2 to the Standard Contractual Clauses

This Appendix forms part of the Standard Contractual Clauses.

A description of the technical and organisational security measures implemented by the data importer in accordance with Standard Contractual Clauses is set out below.

General measures

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. Your Personal Data is only accessible to a limited number of personnel who need access to the information to perform their duties.

Access and authentication

Afi maintains commercially reasonable technical and organizational measures to protect against accidental or unlawful access, destruction, loss or alteration of Personal Data under its control.

Afi software is designed in a way to make it impossible for Afi employees or subcontractors to access encrypted customer data. We conduct regular privacy & security trainings with employees and executives.

Storage of Data

Afi infrastructure is hosted in Google Cloud, and we use Google Security Model that provides top-level security of the 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 is US-EU Privacy Shield certified and we're compliant with all major data protection regulations (including GDPR, HIPPA and CCPA).

All data is encrypted in transit by use of TLS1.x protocol and using AES 256 encryption. All storage types we use provide encryption at rest. Additionally, data is encrypted using AES256 by per-customer key.

Local user access

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 Sing-on.
Login to all services is provided via Google OAuth2 login with 2FA as an obligatory requirement.

Accounts with privileged access to the system 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.
Sensitive customer data such as account or billing information is accessed only via protected devices compliant with the company data protection policies and is never sent via unprotected communication channels.

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 quarterly security and privacy trainings mandatory to all employees, as well as the onboarding training for all new employees.

Afi conducts quarterly security reviews by internal Security team.
Afi works with Google Cloud to ensure the security and reliability of its service, in addition to:
- following a Secure Software Development Life Cycle (SSDLC);

- performing quarterly security-related trainings for R&D and DevOps teams;

- conducting regular vulnerability assessments;
- running paid Bug Bounty programs;

- encrypting customer data in transit and at rest;

- adhering to other internal policies as described in this document.

Data exporter:

[CUSTOMER: PLEASE COMPLETE AND SIGN:]

Name: _____

Position: _____

Address: _____

Signature_____
(stamp of organisation)

Data importer:

Name (written out in full): _____

Position: _____

Address: _____

Annex 3 to the Standard Contractual Clauses

This Appendix forms part of the Standard Contractual Clauses.

The List of Sub-Processors used by the data importer are listed in accordance with Clause 9(a) of the Standard Contractual Clauses are set out in Annex 2 of the DPA:

Alphabet Inc.	Google Cloud Platform (GCP) offered by Google is a cloud computing service. GCP is compliant with SOC 1/2/3, ISO/IEC 27001, PCI DSS and other major security regulations. Afi uses GCP to host its container-based distributed application using Google Kubernetes engine, as well as to store the backup data using encrypted geo-redundant cloud storage.
Amazon.com, Inc.	Amazon Web Services (AWS) is a subsidiary of Amazon providing an on-demand cloud computing service. AWS is compliant with SOC 1/2/3, ISO/IEC 27001, PCI DSS and other major security regulations. We use Amazon Elastic Kubernetes Service to host our application, and store the backup data using encrypted geo-redundant cloud storage.
Stripe, Inc.	Stripe offers payment processing and anti-fraud tools which Afi uses to accept payments from customers, manage subscriptions, and perform transaction reporting. Stripe is certified as a PCI Level 1 Service Provider, which is the most stringent level of certification available in the payments industry.
HubSpot, Inc.	HubSpot provides tools for customer relationship management (CRM), social media marketing, lead generation and web analytics. It has TRUSTe certification for Enterprise Privacy and its IT is audited as part of the Sarbanes Oxley compliance. Afi uses HubSpot CRM and analytics tools to manage and automate our sales processes.
Zendesk	Zendesk is a helpdesk software provider. It is compliant with SOC 2/3, ISO 27001 and other security regulations. Afi uses Zendesk to accept the customer support tickets, manage and automate the technical support services.

Data exporter:

[CUSTOMER: PLEASE COMPLETE AND SIGN:]

Name: _____

Position: _____

Address: _____

Signature_____
(stamp of organisation)

Data importer:

Name (written out in full): _____

Position: _____

Address: _____