# **EUROPEAN DATA PROCESSING AGREEMENT** (EU Standard Contractual Clauses)

*Revised September 29th, 2020*

This European Data Processing Addendum ("DPA") is entered into on ____________ (the "Effective Date") by and between ______________________________________________________________________________, a _____________________________________________ company with a principal place of business located at ______________________________________________________________________________________ (the "Customer") and KLTM Solutions LLC, a Delaware limited liability company with its registered office in 8 The Green, Suite A, Dover, DE 19901 ("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

"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 KLTM Solutions LLC, 8 The Green, Suite A, Dover, DE 19901. 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.

**KLTM Solutions LLC**

Name: ______________________________

Title: ________________________________

Signature: ___________________________

______________________________________

Name: ______________________________

Title: ________________________________

Signature: ___________________________

# Standard Contractual Clauses

For the purposes of Article 26(2) of Directive 95/46/EC for the transfer of personal data to processors established in third countries which do not ensure an adequate level of data protection

*[CUSTOMER: PLEASE COMPLETE]*

Name of the data exporting organisation: ____________________________

Address: _________________________________________________________

e-mail: ____________________

(the data exporter)

And

Name of the data importing organisation: KLTM Solutions LLC

Address: 8 The Green, Suite A, Dover, Delaware, USA 19901

e-mail: privacy@afi.ai

(the data importer)

each a “party”; together “the parties”,

HAVE AGREED on the following Contractual Clauses (the Clauses) in order to adduce adequate safeguards with respect to the protection of privacy and fundamental rights and freedoms of individuals for the transfer by the data exporter to the data importer of the personal data specified in Appendix 1.

*Clause 1*

### ***Definitions***

For the purposes of the Clauses:

(a) '*personal data*', '*special categories of data*', '*process/processing*', '*controller*', '*processor*', '*data subject*' and '*supervisory authority*' shall have the same meaning as in Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data;

(b) '*the data exporter*' means the controller who transfers the personal data;

(c) *'the data importer'* means the processor who agrees to receive from the data exporter personal data intended for processing on his behalf after the transfer in accordance with his instructions and the terms of the Clauses and who is not subject to a third country's system ensuring adequate protection within the meaning of Article 25(1) of Directive 95/46/EC;

(d) *'the subprocessor'* means any processor engaged by the data importer or by any other subprocessor of the data importer who agrees to receive from the data importer or from any other subprocessor of the data importer personal data exclusively intended for processing activities to be carried out on behalf of the data exporter after the transfer in accordance with his instructions, the terms of the Clauses and the terms of the written subcontract;

(e) *'the applicable data protection law'* means the legislation protecting the fundamental rights and freedoms of individuals and, in particular, their right to privacy with respect to the processing of personal data applicable to a data controller in the Member State in which the data exporter is established;

(f) *'technical and organisational security measures'* means those measures aimed at protecting personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing.

*Clause 2*

### *Details of the transfer*

The details of the transfer and in particular the special categories of personal data where applicable are specified in Appendix 1 which forms an integral part of the Clauses.

*Clause 3*

### *Third-party beneficiary clause*

1. The data subject can enforce against the data exporter this Clause, Clause 4(b) to (i), Clause 5(a) to (e), and (g) to (j), Clause 6(1) and (2), Clause 7, Clause 8(2), and Clauses 9 to 12 as third-party beneficiary.

2. The data subject can enforce against the data importer this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8(2), and Clauses 9 to 12, in cases where the data exporter has factually disappeared or has ceased to exist in law unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law, as a result of which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity.

3. The data subject can enforce against the subprocessor this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8(2), and Clauses 9 to 12, in cases where both the data exporter and the data importer have factually disappeared or ceased to exist in law or have become insolvent, unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law as a result of which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity. Such third-party liability of the subprocessor shall be limited to its own processing operations under the Clauses.

4. The parties do not object to a data subject being represented by an association or other body if the data subject so expressly wishes and if permitted by national law.

*Clause 4*

### *Obligations of the data exporter*

The data exporter agrees and warrants:

(a) that the processing, including the transfer itself, of the personal data has been and will continue to be carried out in accordance with the relevant provisions of the applicable data protection law (and, where applicable, has been notified to the relevant authorities of the Member State where the data exporter is established) and does not violate the relevant provisions of that State;

(b) that it has instructed and throughout the duration of the personal data processing services will instruct the data importer to process the personal data transferred only on the data exporter's behalf and in accordance with the applicable data protection law and the Clauses;

(c) that the data importer will provide sufficient guarantees in respect of the technical and organisational security measures specified in Appendix 2 to this contract;

(d) that after assessment of the requirements of the applicable data protection law, the security measures are appropriate to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing, and that these measures ensure a level of security appropriate to the risks presented by the processing and the nature of the data to be protected having regard to the state of the art and the cost of their implementation;

(e) that it will ensure compliance with the security measures;

(f) that, if the transfer involves special categories of data, the data subject has been informed or will be informed before, or as soon as possible after, the transfer that its data could be transmitted to a third country not providing adequate protection within the meaning of Directive 95/46/EC;

(g) to forward any notification received from the data importer or any subprocessor pursuant to Clause 5(b) and Clause 8(3) to the data protection supervisory authority if the data exporter decides to continue the transfer or to lift the suspension;

(h) to make available to the data subjects upon request a copy of the Clauses, with the exception of Appendix 2, and a summary description of the security measures, as well as a copy of any contract for subprocessing services which has to be made in accordance with the Clauses, unless the Clauses or the contract contain commercial information, in which case it may remove such commercial information;

(i) that, in the event of subprocessing, the processing activity is carried out in accordance with Clause 11 by a subprocessor providing at least the same level of protection for the personal data and the rights of data subject as the data importer under the Clauses; and

(j) that it will ensure compliance with Clause 4(a) to (i).

*Clause 5*

### ***Obligations of the data importer***

The data importer agrees and warrants:

(a) to process the personal data only on behalf of the data exporter and in compliance with its instructions and the Clauses; if it cannot provide such compliance for whatever reasons, it agrees to inform promptly the data exporter of its inability to comply, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract;

(b) that it has no reason to believe that the legislation applicable to it prevents it from fulfilling the instructions received from the data exporter and its obligations under the contract and that in the event of a change in this legislation which is likely to have a substantial adverse effect on the warranties and obligations provided by the Clauses, it will promptly notify the change to the data exporter as soon as it is aware, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract;

(c) that it has implemented the technical and organisational security measures specified in Appendix 2 before processing the personal data transferred;

(d) that it will promptly notify the data exporter about:

(i) any legally binding request for disclosure of the personal data by a law enforcement authority unless otherwise prohibited, such as a prohibition under criminal law to preserve the confidentiality of a law enforcement investigation,

(ii) any accidental or unauthorised access, and

(iii) any request received directly from the data subjects without responding to that request, unless it has been otherwise authorised to do so;

(e) to deal promptly and properly with all inquiries from the data exporter relating to its processing of the personal data subject to the transfer and to abide by the advice of the supervisory authority with regard to the processing of the data transferred;

(f) at the request of the data exporter to submit its data processing facilities for audit of the processing activities covered by the Clauses which shall be carried out by the data exporter or an inspection body composed of independent members and in possession of the required professional qualifications bound by a duty of confidentiality, selected by the data exporter, where applicable, in agreement with the supervisory authority;

(g) to make available to the data subject upon request a copy of the Clauses, or any existing contract for subprocessing, unless the Clauses or contract contain commercial information, in which case it may remove such commercial information, with the exception of Appendix 2 which shall be replaced by a summary description of the security measures in those cases where the data subject is unable to obtain a copy from the data exporter;

(h) that, in the event of subprocessing, it has previously informed the data exporter and obtained its prior written consent;

(i) that the processing services by the subprocessor will be carried out in accordance with Clause 11; and

(j) to send promptly a copy of any subprocessor agreement it concludes under the Clauses to the data exporter.

### *Clause 6*

### ***Liability***

1. The parties agree that any data subject, who has suffered damage as a result of any breach of the obligations referred to in Clause 3 or in Clause 11 by any party or subprocessor is entitled to receive compensation from the data exporter for the damage suffered.

2. If a data subject is not able to bring a claim for compensation in accordance with paragraph 1 against the data exporter, arising out of a breach by the data importer or his subprocessor of any of their obligations referred to in Clause 3 or in Clause 11, because the data exporter has factually disappeared or ceased to exist in law or has become insolvent, the data importer agrees that the data subject may issue a claim against the data importer as if it were the data exporter, unless any successor entity has assumed the entire legal obligations of the data exporter by contract of by operation of law, in which case the data subject can enforce its rights against such entity.

   The data importer may not rely on a breach by a subprocessor of its obligations in order to avoid its own liabilities.

3. If a data subject is not able to bring a claim against the data exporter or the data importer referred to in paragraphs 1 and 2, arising out of a breach by the subprocessor of any of their obligations referred to in Clause 3 or in Clause 11 because both the data exporter and the data importer have factually disappeared or ceased to exist in law or have become insolvent, the subprocessor agrees that the data subject may

issue a claim against the data subprocessor with regard to its own processing operations under the Clauses as if it were the data exporter or the data importer, unless any successor entity has assumed the entire legal obligations of the data exporter or data importer by contract or by operation of law, in which case the data subject can enforce its rights against such entity. The liability of the subprocessor shall be limited to its own processing operations under the Clauses.

*Clause 7*

### *Mediation and jurisdiction*

1. The data importer agrees that if the data subject invokes against it third-party beneficiary rights and/or claims compensation for damages under the Clauses, the data importer will accept the decision of the data subject:

   (a) to refer the dispute to mediation, by an independent person or, where applicable, by the supervisory authority;

   (b) to refer the dispute to the courts in the Member State in which the data exporter is established.

2. The parties agree that the choice made by the data subject will not prejudice its substantive or procedural rights to seek remedies in accordance with other provisions of national or international law.

*Clause 8*

### *Cooperation with supervisory authorities*

1. The data exporter agrees to deposit a copy of this contract with the supervisory authority if it so requests or if such deposit is required under the applicable data protection law.

2. The parties agree that the supervisory authority has the right to conduct an audit of the data importer, and of any subprocessor, which has the same scope and is subject to the same conditions as would apply to an audit of the data exporter under the applicable data protection law.

3. The data importer shall promptly inform the data exporter about the existence of legislation applicable to it or any subprocessor preventing the conduct of an audit of the data importer, or any subprocessor, pursuant to paragraph 2. In such a case the data exporter shall be entitled to take the measures foreseen in Clause 5 (b).

*Clause 9*

### *Governing Law*

The Clauses shall be governed by the law of the Member State in which the data exporter is established.

*Clause 10*

### *Variation of the contract*

The parties undertake not to vary or modify the Clauses. This does not preclude the parties from adding clauses on business related issues where required as long as they do not contradict the Clause.

*Clause 11*

### *Subprocessing*

1. The data importer shall not subcontract any of its processing operations performed on behalf of the data exporter under the Clauses without the prior written consent of the data exporter. Where the data importer subcontracts its obligations under the Clauses, with the consent of the data exporter, it shall do so only by way of a written agreement with the subprocessor which imposes the same obligations on the subprocessor as are imposed on the data importer under the Clauses. Where the subprocessor fails to fulfill its data protection obligations under such written agreement the data importer shall remain fully liable to the data exporter for the performance of the subprocessor's obligations under such agreement.

2. The prior written contract between the data importer and the subprocessor shall also provide for a third-party beneficiary clause as laid down in Clause 3 for cases where the data subject is not able to bring the claim for compensation referred to in paragraph 1 of Clause 6 against the data exporter or the data importer because they have factually disappeared or have ceased to exist in law or have become insolvent and no successor entity has assumed the entire legal obligations of the data exporter or data importer by contract or by operation of law. Such third-party liability of the subprocessor shall be limited to its own processing operations under the Clauses.

3. The provisions relating to data protection aspects for subprocessing of the contract referred to in paragraph 1 shall be governed by the law of the Member State in which the data exporter is established.

4. The data exporter shall keep a list of subprocessing agreements concluded under the Clauses and notified by the data importer pursuant to Clause 5(j), which shall be updated at least once a year. The list shall be available to the data exporter's data protection supervisory authority.

## *Clause 12*

### *Obligation after the termination of personal data processing services*

1. The parties agree that on the termination of the provision of data processing services, the data importer and the subprocessor shall, at the choice of the data exporter, return all the personal data transferred and the copies thereof to the data exporter or shall destroy all the personal data and certify to the data exporter that it has done so, unless legislation imposed upon the data importer prevents it from returning or destroying all or part of the personal data transferred. In that case, the data importer warrants that it will guarantee the confidentiality of the personal data transferred and will not actively process the personal data transferred anymore.

2. The data importer and the subprocessor warrant that upon request of the data exporter and/or of the supervisory authority, it will submit its data processing facilities for an audit of the measures referred to in paragraph 1.

**On behalf of the data exporter:**

*[CUSTOMER:  PLEASE COMPLETE AND SIGN:]*

Name: ___________________________________

Position: ___________________________________

Address: ___________________________________

Signature_____________________________
(stamp of organisation)

**On behalf of the data importer:**

Name (written out in full): ________________________________

Position: ________________________________

Address: 8 the Green, Suite A, Dover, Delaware 19901, the US

## APPENDIX 1 TO THE STANDARD CONTRACTUAL CLAUSES

This Appendix forms part of the Clauses and must be completed and signed by the parties.

The Member States may complete or specify, according to their national procedures, any additional necessary information to be contained in this Appendix.

**Data exporter**

The data exporter is (please specify briefly your activities relevant to the transfer):

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

**importer**

The data importer is (please specify briefly activities relevant to the transfer):

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 personal data transferred will be subject to the following basic processing activities (please specify):

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

*[CUSTOMER: PLEASE SIGN]*

DATA EXPORTER

Name: ____________________________

Authorised Signature ________________

DATA IMPORTER

Name: ___________________________

Authorised Signature ______________

## APPENDIX 2 TO THE STANDARD CONTRACTUAL CLAUSES

This Appendix forms part of the Clauses and must be completed and signed by the parties.

Description of the technical and organisational security measures implemented by the data importer in accordance with Clauses 4(d) and 5(c):

### Afi Security Controls

### 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.

*[CUSTOMER: PLEASE SIGN]*

DATA EXPORTER

Name: ___________________________________

Authorised Signature _______________________

DATA IMPORTER

Name: ___________________________

Authorised Signature ________________