

**DATA PROCESSING ADDENDUM**

This Data Processing Addendum (“**Addendum**”) forms part of the Master Subscription Agreement or other similar type agreement pertaining to the Processing of Customer Personal Data (the “**Agreement**”) between Apttus Corporation (“**APTTUS**”) and Customer (collectively the “**Parties**”). This Addendum does not replace nor supersede any pre-existing obligations of the Parties; but rather augments such obligations in context of certain applicable laws and regulations pertaining to the handling and processing of Customer Personal Data.

**HOW TO EXECUTE THIS DPA:**

1. Complete the information required for “Customer Designated POC” on page 4;
2. Complete the information as the data exporter on pages 7 and 12;
3. Sign where indicated on pages 5, 12, and 14; **and**
4. Return the signed Addendum to APTTUS via [data-privacy@apttus.com](mailto:data-privacy@apttus.com)

This Addendum shall become legally binding once APTTUS receives a validly completed and signed copy from Customer.

This Addendum shall not become legally binding, unless Customer has executed a valid Agreement and/or Order Form pursuant to such an Agreement.

**1. Subject Matter and Duration.**

**a) Subject Matter.** This Addendum reflects the Parties’ commitment to abide by Applicable Data Protection Laws concerning the Processing of Customer Personal Data in connection with APTTUS’ execution of the Agreement. All capitalized terms that are not expressly defined in this Data Processing Addendum will have the meanings given to them in the Agreement. If and to the extent language in this Addendum or any of its Exhibits conflicts with the Agreement, this Addendum shall control.

**b) Duration and Survival.** This Addendum will become legally binding upon the Effective Date of the Agreement or upon the date upon which both Parties have signed this Addendum, if it is completed after the Effective Date of the Agreement. APTTUS will Process Customer Personal Data until the relationship terminates as specified in the Agreement. APTTUS’ obligations and Customer’s rights under this Addendum will continue in effect so long as APTTUS Processes Customer Personal Data.

**2. Definitions.**

For the purposes of this Addendum, the following terms and those defined within the body of this Addendum apply.

**a) “Applicable Data Protection Law(s)”** means the relevant data protection and data privacy laws, rules and regulations to which the Customer Personal Data are subject. “Applicable Data Protections Law(s)” shall include, but not be limited to, EU General Data Protection Regulation 2016/679 (“GDPR”).

**b) “Customer Personal Data”** means Personal Data pertaining to Customer’s users or employees located in the European Economic Area Processed by APTTUS. The Customer Personal Data and the specific uses of the Customer Personal Data are detailed in **Exhibit A** attached hereto, as required by the GDPR.

**c) “Controller”** means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the Processing of Personal Data.

**d) “Personal Data”** shall have the meaning assigned to the terms “personal data” or “personal information” under Applicable Data Protection Law(s).

**e) “Process,” “Processes,” “Processing,” “Processed”** means any operation or set of operations which is performed on data or sets of data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination, or otherwise making available, alignment or combination, restriction, erasure, or destruction.

**f) “Processor”** means a natural or legal person, public authority, agency or other body which Processes Customer Personal Data on behalf of Customer subject to this Addendum.

**g) “Security Incident(s)”** means the breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Customer Personal Data Processed by APTTUS.

- h)** “**Services**” means any and all services that APTTUS performs under the Agreement.
- i)** “**Third Party(ies)**” means APTTUS’ authorized contractors, agents, vendors and third party service providers that Process Customer Personal Data (i.e. subprocessors).

### **3. Data Use and Processing.**

- a)** Compliance with Laws. Customer Personal Data shall be Processed in compliance with the terms of this Addendum and all Applicable Data Protection Law(s).
- b)** Documented Instructions. APTTUS and its Third Parties shall Process Customer Personal Data only in accordance with the documented instructions of Customer or as specifically authorized by this Addendum, the Agreement, or any applicable Statement of Work. APTTUS will, unless legally prohibited from doing so, inform Customer in writing if it reasonably believes that there is a conflict between Customer’s instructions and applicable law or otherwise seeks to Process Customer Personal Data in a manner that is inconsistent with Customer’s instructions.
- c)** Authorization to Use Third Parties. To the extent necessary to fulfill APTTUS’ contractual obligations under the Agreement or any Statement of Work, Customer hereby authorizes APTTUS to engage Third Parties (including subprocessors). Any Third Party Processing of Customer Personal Data shall be consistent with Customer’s documented instructions and comply with all Applicable Data Protection Law(s).
- d)** APTTUS and Third Party Compliance. APTTUS agrees to (i) enter into a written agreement with Third Parties regarding such Third Parties’ Processing of Customer Personal Data that imposes on such Third Parties (including subprocessors) data protection and security requirements for Customer Personal Data that are compliant with Applicable Data Protection Law(s); and (ii) remain responsible to Customer for APTTUS’ Third Parties’ failure to perform their obligations with respect to the Processing of Customer Personal Data.
- e)** Right to Object to Third Parties. APTTUS shall make available to Customer a list of Third Parties that Process Customer Personal Data upon reasonable request. Prior to engaging any new Third Parties that Process Customer Personal Data, APTTUS will notify Customer via email and allow Customer thirty (30) days to object. If Customer has legitimate objections to the appointment of any new Third Party, the parties will work together in good faith to resolve the grounds for the objection for no less than thirty (30) days, and failing any such resolution, Customer may terminate the part of the service performed under the Agreement that cannot be performed by APTTUS without use of the objectionable Third Party. APTTUS shall refund any pre-paid fees to Customer in respect of the terminated part of the Service.
- f)** Confidentiality. Any person or Third Party authorized to Process Customer Personal Data must agree to maintain the confidentiality of such information or be under an appropriate statutory or contractual obligation of confidentiality.
- g)** Personal Data Inquiries and Requests. APTTUS agrees to comply with all reasonable instructions from Customer related to any requests from individuals exercising their rights in Personal Data granted to them under Applicable Data Protection Law(s) (“**Privacy Request**”). At Customer’s request and without undue delay, APTTUS agrees to assist Customer in answering or complying with any Privacy Request in so far as it is possible.
- h)** Data Protection Impact Assessment and Prior Consultation. APTTUS agrees to provide reasonable assistance at Customer’s expense to Customer where, in Customer’s judgement, the type of Processing performed by APTTUS is likely to result in a high risk to the rights and freedoms of natural persons (e.g., systematic and extensive profiling, Processing sensitive Personal Data on a large scale and systematic monitoring on a large scale, or where the Processing uses new technologies) and thus requires a data protection impact assessment and/or prior consultation with the relevant data protection authorities.
- i)** Demonstrable Compliance. APTTUS agrees to keep records of its Processing in compliance with Applicable Data Protection Law(s) and provide any necessary records to Customer to demonstrate compliance upon reasonable request.

### **4. Cross-Border Transfers of Personal Data.**

- a)** Cross-Border Transfers of Personal Data. Customer authorizes APTTUS and its Third Parties to transfer Customer Personal Data across international borders, including from the European Economic Area to the United States. Any cross-border transfer of Customer Personal Data must be supported by an approved adequacy mechanism.

b) Standard Contractual Clauses. At Customer's request, the Parties will execute and rely upon Standard Contractual Clauses in **Exhibit B** to act as the adequacy mechanism to support the transfer and Processing of Customer Personal Data to the United States.

## 5. Information Security Program.

a) APTTUS agrees to implement appropriate technical and organizational measures designed to protect Customer Personal Data as required by Applicable Data Protection Law(s) and as may be further described in the Agreement (the "**Information Security Program**"). Such measures shall include:

i) The ability to ensure the ongoing confidentiality, integrity, availability of APTTUS' Processing and Customer Personal Data;

ii) The ability to restore the availability and access to Customer Personal Data in the event of a physical or technical incident;

iii) A process for regularly testing, assessing and evaluating of the effectiveness of the APTTUS' Information Security Program to ensure the security of Customer Personal Data from reasonably suspected or actual accidental or unlawful destruction, loss, alteration, unauthorized disclosure or access.

## 6. Security Incidents.

a) Security Incident Procedure. APTTUS will deploy and follow policies and procedures to detect, respond to, and otherwise address Security Incidents including procedures to (i) identify and respond to reasonably suspected or known Security Incidents, mitigate harmful effects of Security Incidents, document Security Incidents and their outcomes, and (ii) restore the availability or access to Customer Personal Data in a timely manner.

b) Notice. APTTUS agrees to provide prompt written notice without undue delay and within the time frame required under Applicable Data Protection Law(s) (but in no event longer than forty-eight (48) hours) to Customer's Designated POC if it knows or reasonably suspects that a Security Incident has taken place. Such notice will include all available details required under Applicable Data Protection Law(s) for Customer to comply with its own notification obligations to regulatory authorities or individuals affected by the Security Incident.

## 7. Audits.

a) Right to Audit; Permitted Audits. APTTUS shall make available to Customer and its regulators all information necessary to demonstrate compliance with Applicable Data Protection Laws and this Addendum. Customer and its regulators shall have the right to inspect APTTUS' architecture, systems, and documentation which are relevant to the security and integrity of Customer Personal Data, or as otherwise required by a governmental regulator:

i) Following any notice from APTTUS to Customer of an actual or reasonably suspected Security Incident involving Customer Personal Data;

ii) Upon Customer's reasonable belief that APTTUS is not in compliance with Applicable Data Protection Laws, this Addendum or its security policies and procedures under the Agreement;

iii) As required by governmental regulators;

iv) Or otherwise in accordance with GDPR regulations.

b) Audit Terms. Any audits described in this Section shall be:

i) Conducted by Customer or its regulator, or through a third party independent contractor selected by one of these parties.

ii) Conducted during reasonable times.

iii) Conducted upon reasonable advance notice to APTTUS.

iv) Of reasonable duration and shall not unreasonably interfere with APTTUS' nor Third Party day-to-day operations.

v) Conducted in such a manner that does not violate any agreement between APTTUS and its cloud providers.

c) Third Parties. In the event that Customer conducts an audit through a third party independent auditor or a third party accompanies Customer or participates in such audit, such third party shall be required to enter into a non-disclosure agreement containing confidentiality provisions substantially similar to those set forth in the Agreement to protect APTTUS’s and APTTUS’s customers’ confidential and proprietary information. For the avoidance of doubt, regulators shall not be required to enter into a non-disclosure agreement.

d) Audit Results. Upon APTTUS’ request, after conducting an audit, Customer shall notify APTTUS of the manner in which APTTUS does not comply with any of the applicable security, confidentiality or privacy obligations or Applicable Data Protection Laws herein. Upon such notice, APTTUS shall make any necessary changes to ensure compliance with such obligations at its own expense and without unreasonable delay and shall notify Customer when such changes are complete. Notwithstanding anything to the contrary in the Agreement, Customer may conduct a follow-up audit within six (6) months of APTTUS’ notice of completion of any necessary changes. To the extent that a APTTUS audit and/or Customer audit identifies any material security vulnerabilities, APTTUS shall remediate those vulnerabilities within fifteen (15) days of the completion of the applicable audit, unless any vulnerability by its nature cannot be remedied within such time, in which case the remediation must be completed within a mutually agreed upon time not to exceed sixty (60) days.

**8. Data Storage and Deletion.**

a) Data Storage. APTTUS will abide by the following with respect to storage of Customer Personal Data:

i) APTTUS will not store or retain any Customer Personal Data except as necessary to perform the Services under the Agreement.

ii) APTTUS uses subprocessors’ cloud service which processes and stores Personal Data in one or more countries. Customer may contact APTTUS for any queries regarding countries where Customer Personal Data is Processed or stored.

b) Data Deletion. APTTUS will abide by the following with respect to deletion of Customer Personal Data:

i) Within thirty (30) calendar days of the Agreement’s expiration or termination, or sooner if requested by Customer, APTTUS will securely destroy (per subsection (iii) below) all copies of Customer Personal Data (including automatically created archival copies).

ii) Upon Customer’s request, APTTUS will promptly return to Customer a copy of all Customer Personal Data within thirty (30) days and, if Customer also requests deletion of the Customer Personal Data, will carry that out as set forth above. Deletion of Customer Personal Data will be conducted in accordance with standard industry practices.


iii) Upon Customer’s request, APTTUS will provide evidence that APTTUS has deleted all Customer Personal Data. APTTUS will provide the “Certificate of Deletion” within thirty (30) dates of Customer’s request.

**9. Contact Information.**

a) APTTUS and the Customer agree to designate a point of contact for urgent privacy and security issues (a “Designated POC”). The Designated POC for both parties are:

- APTTUS Designated POC: data-privacy@apttus.com
- Customer Designated POC:

**APTTUS Corporation**  
a(n) Delaware Corporation

Signature:  \_\_\_\_\_  
 Printed Name: Pranita Lakhwara  
 Title: CIO  
 Date: 12/20/2018

**Customer:** \_\_\_\_\_

Signature: \_\_\_\_\_  
 Printed Name: \_\_\_\_\_  
 Title: \_\_\_\_\_  
 Date: \_\_\_\_\_

**Exhibit A**

1.1 Subject Matter of Processing	The subject matter of Processing is the Services pursuant to the Agreement.
1.2 Duration of Processing	The Processing will continue until the expiration or termination of the Agreement.
1.3 Categories of Data Subjects	<p>Includes the following:</p> <ul style="list-style-type: none"> <li>• Prospects, customers, business partners and vendors of Customer (who are natural persons)</li> <li>• Employees or contact persons of Customer's prospects, customers, business partners and vendors</li> <li>• Employees, agents, advisors, freelancers of Customer (who are natural persons)</li> <li>• Customer's users authorized by Customer to use the Services</li> </ul>
1.4 Nature and Purpose of Processing	<p>Includes the following:</p> <p>Nature: Processing in APTTUS' "Quote-to-Cash" SaaS applications (to the extent purchased by Customer) of the data uploaded by Customer to such applications.</p> <p>The purpose of Processing of Customer Personal Data by APTTUS is the performance of the Services pursuant to the Agreement.</p>
1.5 Types of Personal Information	<p>Includes the following:</p> <ul style="list-style-type: none"> <li>• First and last name</li> <li>• Title</li> <li>• Position</li> <li>• Employer</li> <li>• Contact information (company, email, phone, physical business address)</li> <li>• Identification Data (notably email addresses and phone numbers)</li> <li>• Electronic identification data (notably IP addresses and mobile device IDs)</li> </ul>

**Exhibit B**

**Standard Contractual Clauses (Processors)**

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.

Name of the data exporting organisation:

Address:

Tel.: \_\_\_\_\_; fax: \_\_\_\_\_; e-mail: \_\_\_\_\_

Other information needed to identify the organization (if applicable)

.....  
(the data **exporter**)

And

Name of the data importing organisation: APTTUS Corporation

Address: 1400 Fashion Island Blvd, Suite 100, San Mateo, CA 94404

Tel.: (650) 445-7700; e-mail: legal@apttus.com

Other information needed to identify the organisation: N/A

(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;
  - (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 or 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 fulfil 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:**

Name (written out in full):  
 Position:  
 Address:  
 Other information necessary in order for the contract to be binding (if any):

Signature.....

**On behalf of the data importer:**

Name (written out in full): Praniti Lakhwara  
 Position: CIO & DPO  
 Address: 1400 Fashion Island Blvd, Suite 100, San Mateo, CA 94404

DocuSigned by:  
 Signature *Praniti Lakhwara*  
 460819EB77894B8.....

**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 the Customer identified above.

**Data importer**

The data importer is: APTTUS Corporation, 1400 Fashion Island Blvd, Suite 100, San Mateo, CA 94404.

**Data subjects**

The personal data transferred concern the following categories of data subjects:

Data exporter may submit Personal Data to the Services, the extent of which is determined and controlled by the data exporter 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 data exporter (who are natural persons)
- Employees or contact persons of data exporter's prospects, customers, business partners and vendors
- Employees, agents, advisors, freelancers of data exporter (who are natural persons)
- Data exporter's Users authorized by data exporter to use the Services.

**Categories of data**

The personal data transferred concern the following categories of data:

Data exporter may submit Personal Data to the Services, the extent of which is determined and controlled by the data exporter 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
- Connection data
- Localisation data

**Special categories of data (if appropriate)**

The personal data transferred concern the following special categories of data:

Not applicable.

**Processing operations**

The personal data transferred will be subject to the following basic processing activities:

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



**DATA EXPORTER**

Name:.....

Authorised Signature .....

**DATA IMPORTER**

Name: Praniti Lakhwara

Authorised Signature .....  
DocuSigned by:  
Praniti Lakhwara  
460049EB77894B8

**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):**

Data importer will maintain administrative, physical, and technical safeguards for protection of the security, confidentiality and integrity of Customer Personal Data, as described in the Data Processing Addendum and the Agreement. Data Importer will not materially decrease the overall security of the Services during a subscription term.