# Data Processing Addendum

**(Updated May 18, 2021)**

This Data Processing Addendum ("***DPA***") forms part of the Cloud Automation Agreement or Software License Agreement (each, as applicable, the "***Agreement***") between Automation Anywhere, Inc. ("***AAI***") and the customer identified in such Agreement ("***Customer***") and reflects the parties' agreement with regard to the processing of Customer Personal Data. Customer enters into this DPA on behalf of itself and, to the extent required under applicable Data Protection Law, in the name and on behalf of its Authorized Affiliates, if and to the extent AAI processes Customer Personal Data for which such Authorized Affiliates qualify as the Controller. All capitalized terms not defined herein shall have the meaning set forth in the Agreement. In providing the Service to Customer pursuant to the Agreement, AAI may process Customer Personal Data on behalf of Customer and the parties agree to comply with the following provisions with respect to any Customer Personal Data. For additional clarity and at its discretion, AAI may amend this DPA but any such amendment(s) shall not materially increase Customer's liabilities and/or obligations nor shall it materially decrease AAI's obligations and/or liabilities unless required by applicable law.

## DEFINITIONS

"Applicable Data Protection Laws" means all laws and regulations, to the extent applicable to the Processing of Personal Data under the Agreement, which may include without limitation the GDPR and other laws and regulations of the European Union, the European Economic Area and their member states, Switzerland, the United Kingdom and the CCPA.

"Affiliate" means any entity not under sanctions or embargo restrictions by the U.S. Government that directly or indirectly controls, is controlled by, or is under common control with the subject entity. "Control," for purposes of this definition, means possessing, directly or indirectly, the power to direct or cause the direction of the management, policies and operations of such entity, whether through ownership of voting securities, by contract or otherwise.

"Authorized Affiliate" means any of Customer's Affiliate(s) which (a) is subject to the data protection laws and regulations of the European Union, the European Economic Area and/or their member states, Switzerland and/or the United Kingdom, and (b) is permitted to use the Service pursuant to the Agreement between Customer and AAI, but has not signed its own Order Form with AAI and is not a "Customer" as defined under the Agreement.

"CCPA" means the California Consumer Privacy Act (Cal. Civ. Code § 1798.100 et. seq.) and any derivative or related legislation as amended, extended, repealed and replaced or re-enacted.

"Controller" means the entity which determines the purposes and means of the Processing of Personal Data.

**"*Customer Data*"** means the electronic data or information, including Personal Data, submitted by Customer to the Services or through AAI's support portal.

“Customer Personal Data” means Personal Data which is Processed by AAI on behalf of Customer in connection with the Service.

“Data Subject” means the identified or identifiable person to whom Customer Personal Data relates; an identifiable person is one who can be defined, directly or indirectly, in particular by reference to an identifier such as a name, identification number, location data, an online identifier. For purposes of this DPA, references to Data Subject shall also include, to the extent applicable, references to “Consumers” as defined under the CCPA.

“GDPR” means the 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 (General Data Protection Regulation).

“Personal Data” has the meaning set forth in the Applicable Data Protection Laws or, to the extent not so defined under Applicable Data Protection Laws, means any information relating to a Data Subject; For clarity and in the case of any contradiction, the type of Personal Data processed by AAI is specified in Appendix 1 of the Standard Contractual Clauses.

“Processing” (including, as applicable, “Process”, “Processed” and “Processes”) means any operation or set of operations which is performed upon Personal 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 and/or as defined under Applicable Data Protection Laws.

“Processor” means the entity which Processes Personal Data on behalf of the Customer.

“Service” means (i) the support and maintenance that AAI provides to Customer (the “***Support Services***”) as part of the Software and to the extent applicable (ii) AAI’s cloud-based software-as-a-service applications (the “***Cloud Services***”), in each case as provided by or on behalf of AAI under the Agreement.

“Standard Contractual Clauses” means the Standard Contractual Clauses for the transfer of Personal Data or SCoPD from the European Economic Area to third countries (controller to controller transfers), approved by the European Commission in Decision 2004/915/EC, dated 27 December 2004, and (ii) where AAI is a Processor, the Standard Contractual Clauses for the transfer of Personal Data or SCoPD from the European Economic Area to third countries (controller to processor transfers), approved by the European Commission in Decision 2010/87/EU, dated 5 February 2010.

“Subprocessor” means an entity engaged by AAI only for the performance of the Processing under this DPA and as specifically authorized in advance in writing by Customer.

Terms capitalized but not defined herein shall have the meanings ascribed to them in the Agreement.

**DPA TERMS**

AAI and Customer hereby enter into this DPA effective upon the earlier of execution of the Agreement or the last signature date below. This DPA is incorporated into and forms a part of the Agreement.

**1. PROCESSING OF CUSTOMER DATA**

**a. Provision of the Service.** AAI provides the Service to Customer under the Agreement. In connection with the Service, the parties anticipate that AAI may Process Customer Data that contains Customer Personal Data.

**b. The Parties' Roles.** The parties acknowledge and agree that (i) with respect to Customer's Personal Data and/or SCoPD processed by AAI for the provision of the Service, AAI shall be a Processor (or a 'service provider' for purposes of CCPA) and Customer shall be a Controller (or a 'Business' for purposes of CCPA), and (ii) with respect to any other Personal Data and/or SCoPD including (without limitation) such data processed for Service Improvement, each party shall be a separate Controller (or a 'Business' for purposes of CCPA) and each party shall be responsible for its compliance with the applicable Privacy Laws with respect to the Customer's Personal Data and/or SCoPD.

**c. Customer's General Instruction.** By entering into this DPA, Customer instructs AAI to process Customer Personal Data only in accordance with Applicable Data Protection Laws: (a) for the purpose of providing the Service which may include collection, recording, organizing, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction of Customer Personal Data; (b) as documented in the Agreement including this DPA; and/or (c) as further documented in any other written instructions given by Customer and acknowledged by AAI as constituting instructions for purposes of this DPA.

**d. Customer's Responsibilities.** Customer shall, in its use of the Service, Process Customer Personal Data in accordance with the requirements of Applicable Data Protection Laws. For the avoidance of doubt, Customer's instructions for the Processing of Customer Personal Data shall comply with Applicable Data Protection Laws. Customer shall have sole responsibility for the accuracy, quality, and legality of Customer Personal Data and the means by which Customer acquired Customer Personal Data. Notwithstanding anything to the contrary in this Agreement, Customer shall not provide AAI with any Customer Personal Data not specified in Appendix 1 of the Standard Contractual Clauses, and shall not provide AAI with Customer Personal Data unless Customer complies with Applicable Data Protection Laws, including without limitation, applicable security and confidential measures set forth in GDPR Article 32. Customer accepts full liability for any breaches of its responsibilities in this Section 1(d).

**e. AAI's Responsibilities.** AAI shall keep Customer Personal Data confidential and shall only Process Customer Personal Data on behalf of and in accordance with Customer's documented instructions for Processing in accordance with the Agreement. AAI shall not be required to comply with Customer's instructions if such instructions would

violate Applicable Data Protection Laws. Customer acknowledges and agrees that if in AAI's opinion, a documented instruction violates Applicable Data Protection Laws, including without limitation, the GDPR or other Union or Member State data protection provisions, AAI shall promptly inform Customer in writing, which includes an e-mail. In this event, AAI reserves the right, subject to notification to Customer (which includes by email with a copy sent by registered letter, to suspend the Processing resulting from the violative instruction, without prejudice to the continuation of the Agreement and/or Customer's obligation to pay any fees or other sums due under the Agreement. Except as otherwise set forth in this DPA and/or in the Agreement, AAI shall not Process Customer Personal Data for any purpose other than to perform the Service or as otherwise permitted by Applicable Data Protection Laws.

f. **Details and Scope of the Processing.** The subject matter of Processing Customer Personal Data by AAI is the performance of the applicable Service pursuant to the Agreement. The duration of the Processing, the nature, and purpose of the Processing, the types of Customer Personal Data Processed, and categories of Data Subjects, under this DPA are further specified in Appendix 1 to the Standard Contractual Clauses.

## 2. RIGHTS OF DATA SUBJECTS

a. **Data Subject Requests.** To the extent legally permitted and relevant under Applicable Data Protection Laws and in AAI's capacity as a Processor, AAI shall promptly notify Customer if it receives a request from a Data Subject to exercise the Data Subject's rights under applicable law, including without limitation, right of access, right to rectification, restriction of Processing, erasure ("right to be forgotten"), data portability, object to the Processing or its right not to be subject to an automated individual decision making ("***Data Subject Request***"). Taking into account the nature of the Processing, AAI shall assist Customer through appropriate commercially reasonable organizational and technical measures, for the fulfillment of Customer's obligation to respond to a Data Subject Request under Applicable Data Protection Laws. In addition and to the extent Customer, in its use of the Service, does not have the ability to address a Data Subject Request or a similar request under CCPA, AAI shall, upon Customer's written request, provide commercially reasonable efforts to assist Customer in responding to such Data Subject Request, to the extent that AAI is legally authorized to do so, and to the extent the response to such Data Subject Request is required under Applicable Data Protection Laws.

## 3. AAI PERSONNEL

a. **Confidentiality.** AAI shall ensure that its personnel engaged in the Processing of Customer Personal Data are informed of the confidential nature of the Customer Personal Data, have received appropriate training regarding their responsibilities and have executed written confidentiality agreements.

b. **Reliability.** AAI shall take commercially reasonable steps to ensure the reliability of any AAI personnel engaged in the Processing of Customer Personal Data.

c. **Limitation.** AAI shall ensure that AAI's access to Customer Personal Data is limited to those personnel assisting in the provision of the Service in accordance with the Agreement.

## 4. SUBPROCESSORS

**a. AAI's Subprocessors.** AAI has instructed or authorized the use of Subprocessors to assist AAI with respect to the performance of AAI's obligations under the Agreement. A list of AAI's Subprocessors is attached to this DPA as Appendix 3. If AAI intends to change any of the Subprocessors listed on Appendix 3, AAI shall provide thirty (30) days' notice to Customer, via e-mail and/or through the support portal, for a Subprocessor identified as a "cloud provider" in this DPA (i.e., third-party companies where Customer Data is stored), thereby giving Customer the opportunity to reasonably object to such changes. Currently, such AAI Subprocessors are Amazon and Salesforce. For all other Subprocessors, AAI shall provide reasonable notice. If Customer wishes to object to any such changes, it can do so by following any process implemented by AAI in its notification to Customer or via registered letter sent to:

Attention: Legal Department (Chief Privacy Officer)
Automaton Anywhere, Inc.
633 River Oaks Pkwy
San Jose, CA 95134
United States of America

AAI shall respond to such objections within a reasonable time frame so long as such objections have a reasonable basis. Further, AAI shall enter into a contract with the Subprocessor whereby AAI shall require the Subprocessor to comply with obligations no less onerous than AAI's obligations under this DPA. In particular, the Subprocessor shall contractually commit to implement appropriate technical and organizational measures for protection of the security, confidentiality and integrity of Customer Data.

**b. Liability for Subprocessors.** AAI shall be liable for the acts and omissions of its Subprocessors to the same extent AAI would be liable if performing the services of each Subprocessor directly under the terms of this DPA, except as otherwise set forth in the Agreement.

## 5. CUSTOMER OBLIGATIONS

**a. Nature of Customer Personal Data.** For Support only, Customer acknowledges and agrees that, except as otherwise set forth in this Section 5, Customer Personal Data provided or made available to AAI for Processing in connection with the Service shall consist of business contact information, in the form of support ticket authentication data, relating to Customer's employees, agents or contractors only ("***Business Contact Data***"). Business Contact Data contains the following categories of data: First and Last Name, Role, Title, Position, Location, Employer and Contact Information (company, email, phone, physical business address), Username and IP Address.

**b. Disclosure of Customer End User Information.** For Support only and to the extent Customer, in its sole discretion, deems it necessary to disclose or otherwise provide to AAI any Customer Personal Data other than Business Contact Data (for example, but not limited to, a screen shot containing Customer Personal Data related to any of Customer's end users), Customer shall notify AAI in writing and in advance that it intends to disclose such Customer Personal Data to AAI, pursuant to a process as

specified by AAI. Such process is currently delineated when Customer submits a ticket in AAI's support portal.

**c. Lawful Basis**. To the extent relevant under Applicable Data Protection Laws, Customer shall have a lawful basis for Processing all Customer Data it provides to AAI, including without limitation providing such Customer Data to AAI. If at any time during the Term of the Agreement, Customer discovers that it does not have a lawful basis for Processing Personal Data, including, without limitation, disclosing or transferring the same to AAI, then it shall notify AAI in writing immediately and AAI upon such notification will cease processing that Customer Data.

**d. Customer Warranty**. Customer acknowledges that its failure to comply with Section 5(b) above means that AAI may be unable to comply with its obligations as set forth in Section 2(a) above and/or enable some and/or all of a Data Subject's rights or Consumer's rights (e.g., deletion). As such, Customer warrants it will comply with Sections (5)b and will provide AAI notice when it provides Personal Data to AAI during the provisioning of support, and (ii) to the extent Customer does not comply with the obligations specified in subsection (i) above, AAI's failure to comply with its obligations under Section 2(a) shall not be considered a breach of this DPA.

## 6. SECURITY

**a. General Obligations.** Both AAI and Customer will take and implement, and AAI will contractually require its Subprocessors to take and implement, all appropriate technical and organizational security and confidentiality measures, and regularly update them, to ensure a level of security appropriate to the risk related to the Processing of the Customer Personal Data and protect Customer Personal Data particularly against any accidental or unlawful destruction, loss, alteration or unauthorized disclosure or access (whether such Customer Personal Data is on AAI's or Customer's systems or facilities, in transit or being disposed of). AAI shall ensure that Customer Personal Data communicated by or obtained from Customer is logically segregated except as specified in the Agreement.

## 7. PERSONAL DATA BREACH

**a.** Successful Security Incident/Data Breach. A "***Successful Security Incident***" (Breach) means accidental, unauthorized or unlawful access to, destruction of, loss of, alteration of or unauthorized disclosure of Customer Data while being Processed and under the control of AAI during the use of the Services. In the event of a Successful Security Incident, AAI shall notify the Customer about the Successful Security Incident without undue delay after becoming aware of it (or within the time frame required by applicable law). The report shall detail the following, if known; (i) the nature of the unauthorized use or disclosure; (ii) who made the unauthorized use or received the unauthorized disclosure; (iii) the steps AAI has taken to mitigate any deleterious effect of the unauthorized use or disclosure; (iv) the corrective actions AAI will take to prevent future similar incidents; (v) maintain a record of all information relating to the successful Security Incident including the results of its own investigations and any supervisory or regulatory authorities' investigations (v) all actions taken as may be required by applicable Privacy Laws.

**b.** 11.9 Unsuccessful Security Incident. AAI has no obligation to report or respond to an Unsuccessful Security Incident, and any response by AAI shall not be construed as an acknowledgement by AAI of any fault or liability. An "***Unsuccessful Security Incident***" means an incident that results in no unauthorized access to Customer Data or to any of AAI's equipment or facilities storing Customer Data, and may include, without limitation, dropped or denied network traffic, denied access attempts to systems and applications, alerts from security devices or services, pings and other broadcast attacks on firewalls or edge servers, denial of service attacks, packet sniffing (or other unauthorized access to traffic data that does not result in access to Customer Data) or similar incidents.

**c.** AAI shall reimburse Customer for all reasonable costs associated with providing notification to Data Subjects and supervisory authorities, solely to the extent it is demonstrated that the Breach was caused by AAI, its Subprocessors or its agents.

## 8. AUDITS

Upon 30 days written notice by Customer and subject to the confidentiality obligations set forth in the Agreement, AAI shall make available to Customer AAI's procedures relevant to the protection of Customer Personal Data in the form of AAI's third-party certifications and audit reports ("***Audit Records***"), to the extent that AAI makes them generally available to its customers. Customer shall contact AAI in accordance with the "Notices" Section of the Agreement to request Audit Records. In the event of the occurrence of a Successful Security Incident involving Customer Data, Customer shall have the right to request an on-site audit of the AAI facilities involved in the Processing of the Customer Data. Before the commencement of any such on-site audit, Customer and AAI shall mutually agree upon the scope, timing, and duration of the audit. The provisions in this section shall by no means derogate from or materially alter the provisions on audits as specified in the Standard Contractual Clauses.

## 9. RETENTION AND DELETION OF CUSTOMER DATA

AAI shall delete Customer Personal Data processed in connection with (a) its provision of the Support Services within 90 days after the associated help desk ticket is closed, (b) its provision of the Cloud Services within 30 days after completion of the applicable Processing activity involving such Customer Personal Data, provided always that (c) AAI shall delete Business Contact Data within 30 days after expiration or termination of the Agreement, in each case unless otherwise required by law.

## 10. AUTHORIZED AFFILIATES

**a. Contractual Relationship.** The parties acknowledge and agree that, by executing the Agreement, the Customer enters into the DPA on behalf of itself and, as applicable, in the name and on behalf of its Authorized Affiliates, thereby establishing a separate DPA between AAI and each such Authorized Affiliate subject to the provisions of the Agreement and this Section 10 and Section 11. Each Authorized Affiliate agrees to be bound by the obligations under this DPA and, to the extent applicable, the Agreement. For the avoidance of doubt, an Authorized Affiliate is not and does not become a party to the Agreement and is only a party to this DPA. All access to and use of the Service by Authorized Affiliates must comply with the terms and conditions of the Agreement and DPA and any violation of the terms and conditions of the Agreement or DPA by an Authorized Affiliate shall be deemed a violation by Customer.

b. **Communication.** The Customer that is the contracting party to the Agreement shall remain responsible for coordinating all communication with AAI under this DPA and be entitled to make and receive any communication in relation to this DPA on behalf of its Authorized Affiliates.

c. **Rights of Authorized Affiliates.** Where an Authorized Affiliate becomes a party to this DPA, it shall to the extent required under Applicable Data Protection Laws be entitled to exercise the rights and seek remedies under this DPA, subject to the following:

   i. Except where Applicable Data Protection Laws require the Authorized Affiliate to exercise a right or seek any remedy under this DPA against AAI directly by itself, the parties agree that (1) solely the Customer that is the contracting party to the Agreement shall exercise any such right or seek any such remedy on behalf of the Authorized Affiliate, and (2) the Customer that is the contracting party to the Agreement shall exercise any such rights under this DPA not separately for each Authorized Affiliate individually but in a combined manner for all of its Authorized Affiliates together (as set forth, for example, in Section ii, below).

   ii. The parties agree that the Customer that is the contracting party to the Agreement shall, when carrying out an on-site audit under Section 8 above, take all reasonable measures to limit any impact on AAI including, to the extent reasonably possible, combining several audit requests carried out on behalf of different Authorized Affiliates in one single audit.

**11. LIMITATION OF LIABILITY**

a. **LIABILITY FOR SUPPORT SERVICES.** EACH PARTY'S AND ALL OF ITS AFFILIATES' LIABILITY, TAKEN TOGETHER IN THE AGGREGATE, ARISING OUT OF OR RELATED TO A SUCCESSFUL SECURITY INCIDENT ARISING FROM CUSTOMER'S USE OF THE SUPPORT SERVICES PROVIDED BY AAI UNDER THE AGREEMENT AND/OR THIS DPA, AND ALL DPAS BETWEEN AUTHORIZED AFFILIATES AND AAI, WHETHER IN CONTRACT, TORT OR UNDER ANY OTHER THEORY OF LIABILITY, SHALL NOT EXCEED THE TOTAL FEES PAID BY CUSTOMER AND ITS AUTHORIZED AFFILIATES UNDER THE AGREEMENT IN THE TWELVE (12) MONTHS PRECEDING THE INCIDENT OUT OF WHICH THE LIABILITY AROSE.

b. **LIABILITY FOR CLOUD SERVICES.** AAI'S AGGREGATE LIABILITY ARISING OUT OF OR RELATED TO A SUCCESSFUL SECURITY INCIDENT ARISING FROM CUSTOMER'S USE OF THE CLOUD SERVICES PROVIDED BY AAI UNDER THE AGREEMENT AND/OR THIS DPA, WHETHER IN CONTRACT, TORT OR UNDER ANY OTHER THEORY OF LIABILITY, SHALL NOT EXCEED TWO TIMES (2X) THE TOTAL FEES PAID BY CUSTOMER AND ITS AUTHORIZED AFFILIATES UNDER THE AGREEMENT IN THE TWELVE (12) MONTHS PRECEDING THE INCIDENT OUT OF WHICH THE LIABILITY AROSE.

For the avoidance of doubt, AAI's and its Affiliates' total liability for all claims from the Customer and all of its Authorized Affiliates arising out of or related to the Agreement and each DPA shall apply in the aggregate for all claims under both the Agreement and all DPAs established under this Agreement, including by Customer and all Authorized Affiliates, and, in particular, shall not be understood to apply individually and severally to Customer and/or any Authorized Affiliate that is a contractual party to any such DPA.

**12. EUROPEAN SPECIFIC PROVISIONS.** The terms set forth in this Section 12 apply to the extent Customer Personal Data is subject to GDPR:

**a. GDPR.** AAI will Process Customer Personal Data in accordance with the GDPR requirements directly applicable to AAI's provision of the Service to Customer.

**b. Data Protection Impact Assessment.** Upon Customer's request, AAI shall provide Customer with reasonable cooperation and assistance needed to fulfill Customer's obligations under the GDPR to carry out a data protection impact assessment related to Customer's use of the Service, to the extent Customer does not otherwise have access to the relevant information, and to the extent such information is available to AAI. AAI shall provide reasonable assistance to Customer in the cooperation or prior consultation with any supervisory authority in the performance of its tasks related to this Section of this DPA, to the extent required under the GDPR.

**c. Transfers of Customer Personal Data**. Customer acknowledges and agrees that AAI will transfer Customer Personal Data outside of the European Union, the European Economic Area or their member states, Switzerland and/or the United Kingdom, as part of the provision of the Service, to countries that are not recognized by the European Commission as providing an adequate level of protection for Personal Data. The onward transfer of Customer Personal Data shall occur via the Standard Contractual Clauses or other approved method.

**d. Standard Contractual Clauses.** The Standard Contractual Clauses apply to: (i) the legal entity that has executed the Standard Contractual Clauses as the data exporter and its Authorized Affiliates and, (ii) the Affiliates of Customer established within the European Economic Area, Switzerland and the United Kingdom, which have signed Order Forms for the Service. For the purpose of the Standard Contractual Clauses, the aforementioned entities shall be deemed "data exporters."

**13. LEGAL EFFECT**

This DPA shall only become legally binding between Customer and AAI when (a) Customer signs this DPA or, (b) when this DPA is incorporated by reference into an executed Agreement (via a "click to accept" procedure online or through written signature) (c) when the Customer utilizes AAI's support ticket process and the Customer does not already have a executed DPA with AAI.

**14. ORDER OF PRECEDENCE**

This DPA is incorporated into and forms part of the Agreement. For matters not addressed under this DPA, the terms of the Agreement apply. In the event of a conflict between the terms of the Agreement and this DPA, the terms of this DPA will control. In the event of a

conflict between the terms of the DPA and Standard Contractual Clauses, the Standard Contractual Clauses will prevail.

## STANDARD CONTRACTUAL CLAUSES

### 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: _____

(the data **exporter**)

And

Name of the data importing organisation: Automation Anywhere, Inc.

Address: 633 River Oaks Parkway, San Jose, CA 95134

Tel.:_____; fax:_____; e-mail: privacy@automationanywhere.com

Other information needed to identify the organisation:

(the data **importer**)

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

HAVE AGREED on thefollowing 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.

Background

The data exporter has entered into a data processing addendum (“DPA”) with the data importer. Pursuant to the terms of the DPA, it is contemplated that services provided by the data importer will involve the transfer of personal data to data importer. Data importer is located in a country not ensuring an adequate level of data protection. To ensure compliance with Directive 95/46/EC and applicable data protection law, the controller agrees to the provision of such Services, including the processing of personal data incidental thereto, subject to the data importer’s execution of, and compliance with, the terms of these Clauses.

*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 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 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:

Signature…….

**On behalf of the data importer:**

Name (written out in full):

Position:
Address: 633 River Oaks Parkway, San Jose, CA 95134

Signature…….

## 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 legal entity that has executed the Data Processing Addendum based on the Standard Contractual Clauses as a Data Exporter established within the European Economic Area and Switzerland that have purchased the Services on the basis of one or more Order Form(s).

**Data importer**

The data importer is:

Automation Anywhere, Inc.

**Data subjects**

The Personal Data transferred concern the following categories of data subjects:

- Actual customers of Customer and their employees
- Employees of Customer
- Suppliers of Customer and their employees

**Categories of data**

The Personal Data transferred concern the following categories of data:

- First and Last Name
- Phone Number
- Company Name
- Title
- Location (Country)
- IP Addresses
- Special Categories of Personal Data as determined by Customer
- Other personal data as determined by Customer
- Telemetry and usage data including but not limited to: (user-name, password, device IDs, audit logs, and error logs)

**Processing operations**

The Personal Data transferred will be subject to the following basic processing activities:

The objective of Processing of Personal Data by the data importer is the performance of the Services pursuant to the Agreement. The Processing of Personal Data will primarily be performed in the United States, Japan, India, and/or Poland but may be performed in any country where AAI has a presence.

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.

AAI shall maintain administrative, physical and technical safeguards for protection of the security, confidentiality and integrity of Customer Data, including Personal Data, which is processed in connection with AAI's provision of the Services ("Technical and Organizational Measures"). AAI requires its sub-processors to also maintain appropriate Technical and Organizational Measures. AAI regularly monitors compliance with these safeguards. AAI will not materially decrease the overall security protections applied to Personal Data during the term of the Services. Technical and Organizational Measures applicable to Salesforce, in its capacity as AAI's sub-processor, can be found at:

https://www.salesforce.com/content/dam/web/en_us/www/documents/legal/misc/salesforce-security-privacy-and-architecture.pdf

and

https://developer.salesforce.com/docs/atlas.en-us.securityImplGuide.meta/securityImplGuide/salesforce_security_guide.htm

Note: AAI utilizes Salesforce's Sales, Service and Community Clouds and has implemented Salesforce Platform Encryption (At Rest and In Motion).

DATA EXPORTER

Name:

Authorised Signature

DATA IMPORTER

Name:

Authorised Signature

## APPENDIX 3 TO THE STANDARD CONTRACTUAL CLAUSES

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

The list of subprocessors approved by the data importer as of the effective date of the DPA is as set forth below:

| **Subprocessor** | **Purpose** |
|---|---|
| | |
| Salesforce for Support | Service Cloud -Customer Support Ticketing System<br>Single Sign-On – User Authentication<br>Community Cloud – For External Customer Community<br>Einstein – for Chat Bot and Data Analytics |
| Grazitti Interactive | Search Unify – Search Functionality |
| Microsoft Azure | Authentication and Virtual Machines in Lab Environments |
| JIRA by Atlassian | Engineering Bug Tracking System |
| Amazon AWS | Virtual Machines in Lab Environments |
| Sapient | Virtual Machines in Lab Environments |
| Qualtrics | Support Case Close Survey v2 |
| Whatfix | Support – Worldwide Customer Onboarding |

DATA EXPORTER

Name:
Authorised Signature

DATA IMPORTER

Name: