

DATA PROCESSING ADDENDUM

(Updated December 27, 2023)

This Data Processing Addendum ("**DPA**") is entered into and forms part of the Cloud Automation Agreement or On-Premise License Agreement (including their former designations of Master License Agreement and Software License Agreement, respectively) or any other agreement under which AAI provides Services to Customer which does not exclude the processing of Personal Data - each, as applicable, the "**Agreement**") between the customer identified in such Agreement ("**Customer**") and Automation Anywhere, Inc. ("**AAI**"). Customer and AAI are each referred to as a "**Party**" and collectively as the "**Parties**". 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 Personal Data for which such Authorized Affiliates qualify as the Controller. AAI may modify 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 Privacy Law (as defined below).

All capitalized terms not defined herein shall have the meaning set forth in the Agreement. In providing Services 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.

1. Definitions. The terms used in this DPA shall have the meanings set forth in this DPA or as defined by Applicable Privacy Law, whichever is broader. Capitalized terms not otherwise defined herein or defined by Applicable Privacy Law shall have the meaning given to them in the Agreement. The following terms have the meanings set forth below:

1.1 "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.

1.2 "Authorized Affiliate" means any of Customer's Affiliate(s) which (a) is subject to Applicable Privacy Law, and (b) is permitted to use the Services 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.

1.3 "Applicable Privacy Law" means all laws and regulations, aside from Chinese privacy laws, applicable to the Processing of Customer Personal Data under the Agreement including, without limitation: (a) the California Consumer Privacy Act as amended by the California Privacy Rights Act and any binding regulations promulgated thereunder ("**CCPA**"), (b) the Colorado Privacy Act ("**CPA**"), (c) the Virginia Consumer Data Protection Act ("**VCDPA**"), (d) the Connecticut Data Protection Act ("**CTDPA**"), (e) the Utah Consumer Privacy Act ("**UCPA**") (f) the General Data Protection Regulation (Regulation (EU) 2016/679) ("**EU GDPR**"), (g) the Swiss Federal Act on Data Protection ("**FADP**"), (h) the EU GDPR as it forms part of the law of England and Wales by virtue of section 3 of the European Union (Withdrawal) Act 2018 and the UK Data Protection Act 2018 (the "**UK GDPR**"); and (i) the Argentine Law 25,326 Personal Data Protection Law ("**PDPL**"); in each case, as updated, amended or replaced from time to time.

1.4 “**EEA**” means the European Economic Area.

1.5 “**Data Subject**” means an identified or identifiable natural person, or such other similar term as may be defined by Applicable Privacy Law.

1.6 “**Personal Data**” means (a) personal data, personal information, personally identifiable information, or similar term as defined by Applicable Privacy Law or (b) if not defined by Applicable Privacy Law, any information that relates to a Data Subject; in each case, to the extent Processed by AAI, on behalf of Customer, in connection with AAI’s performance of the Services.

1.7 “**Privacy Authority**” means any competent supervisory authority, attorney general, or other regulator with responsibility for privacy or data protection matters.

1.8 “**Process**”, “**Processes**”, “**Processing**” or “**Processed**” means any operation or set of operations, as defined in the Applicable Privacy Law, performed upon Personal Data whether or not by automatic means, including collecting, recording, organizing, storing, adapting or altering, retrieving, consulting, using, disclosing, making available, aligning, combining, blocking, erasing and destroying Personal Data.

1.9 “**Restricted Transfer**” means: (a) where EU GDPR applies, a transfer of Personal Data to a country outside the EEA that is not subject to an adequacy determination, (b) where UK GDPR applies, a transfer of Customer Personal Data from the United Kingdom to any other country that is not subject to an adequacy determination, (c) where FADP applies, a transfer of Customer Personal Data to a country outside Switzerland that is not subject to an adequacy determination, and (d) with respect to any other country where Applicable Privacy Law apply that restrict overseas transfers, an overseas transfer to a country that is not subject to an adequacy decision or otherwise requires some form of transfer mechanism to be implemented in order to comply with such Applicable Privacy Law (such transfer being any “**Other Restricted Transfer**”).

1.10 “**Security Incident**” means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Personal Data while being processed by AAI. For purposes of this DPA, Security Incident shall also include any other similar term as defined by Applicable Privacy Law. Security Incidents do not include unsuccessful attempts or activities that do not compromise the security of Customer Personal Data, including unsuccessful log-in attempts, pings, port scans, denial of service attacks or other network attacks on firewalls or networked systems.

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

1.12 “**Standard Contractual Clauses**” means (a) with respect to restricted transfers (as such term is defined under Applicable Privacy Law) which are subject to the EU GDPR and /or the FADP, the Controller-to-Processor standard contractual clauses, as set out in the European Commission’s Implementing Decision (EU) 2021/914 of 4 June 2021 on standard contractual clauses for the transfer of personal data to third countries pursuant to GDPR, as may be amended or replaced by the European Commission from time to time (the “**EU SCCs**”), (b) with respect to restricted transfers subject to the UK GDPR, the International Data Transfer DPA

to the EU Commission Standard Contractual of 21 March 2022, as may be amended or replaced by the UK Information Commissioner's Office from time to time (the "**UK SCCs**"), (c) with respect to restricted transfers subject to Argentina's PDPL, the standard international transfer contractual clauses contained in Appendix II (provision of services), as set out in Regulation No. 60-E/2016 ("**Argentinian SCCs**"), and (d) with respect to restricted transfers subject to other Applicable Privacy Law, such other standard contract clauses as may be required to be implemented between AAI and Customer ("**Other Applicable Transfer Clauses**").

1.13 "Subprocessor" means any third party or AAI Affiliate engaged by AAI to Process Personal Data on behalf of AAI.

2. Scope. This DPA applies to AAI as a Processor of Personal Data and to Customer as a Controller or Processor of Personal Data, and to AAI's Processing of Personal Data under the Agreement to the extent such Processing is subject to Applicable Privacy Law. This DPA is governed by the governing law of the Agreement unless otherwise set forth herein or required by Applicable Privacy Law.

3. Processing Requirements.

3.1 AAI shall comply with all Applicable Privacy Law in the Processing of Personal Data and only Process Personal Data for the purposes of providing the Services and in accordance with Customer's instructions, which shall include Processing for purposes of performing the Services in accordance with the Agreement. AAI shall promptly inform Customer if (a) in AAI's opinion, an instruction from Customer violates Applicable Privacy Law; or (b) AAI is required by applicable law to otherwise Process Personal Data, unless AAI is prohibited by that law from notifying Customer.

3.2 AAI shall provide to Customer such cooperation, assistance and information as Customer may reasonably request to enable it to comply with its obligations under Applicable Privacy Law and co-operate and comply with the directions or decisions of a relevant Privacy Authority, in each case (a) solely to the extent applicable to AAI's provision of the Services, and (b) within such reasonable time as would enable Customer to meet any time limit imposed by the Privacy Authority.

4. Customer Responsibilities

4.1 Customer shall, in its use of the Services, Process Personal Data in accordance with the requirements of Applicable Data Protection Law, including without limitation in accordance with any requirements to obtain consent, or other legal basis, for processing by, or transfer to, AAI. For the avoidance of doubt, Customer's instructions for the Processing of Personal Data shall comply with Applicable Data Protection Law. 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.

4.2 Support. Customer acknowledges and agrees that Personal Data provided or made available to AAI for Processing in connection with support shall consist of business contact information only, in the form of support ticket authentication data, relating to Customer's employees, agents or contractors only ("**Support Authentication Data**"). Support Authentication 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. Customer and its users are prohibited from submitting

attachments to, or screensharing with, support when such attachments or screensharing contain Personal Data or protected health information.

5. Subprocessors.

5.1 Customer generally authorizes AAI to engage Subprocessors to Process Personal Data. Customer further agrees that AAI may engage its Affiliates as Subprocessors. AAI will maintain an up-to-date list of its Subprocessors, including their functions and locations. AAI's current Subprocessor list is attached hereto as Exhibit C to this DPA ("**DPA Exhibit C**").

5.2 AAI may update the Subprocessor List from time to time. At least 30 days before any new Subprocessor Processes any Customer Personal Data, AAI will add such Subprocessor to the Subprocessor List and notify Customer through email and the support portal.

5.3 If Customer wishes to object to a new Subprocessor based on reasonable data protection concerns, it can do so within 30 days after notice of a new Subprocessor by following any process described by AAI in its notification to Customer or via registered letter sent to:

Attention: Legal Department (Privacy Counsel)
Automaton Anywhere, Inc.
633 River Oaks Pkwy
San Jose, CA 95134
United States of America
privacy@automationanywhere.com

AAI shall respond to such objections within a reasonable time frame so long as such objections have a reasonable basis.

5.4 AAI will: (a) enter into a written agreement with each Subprocessor, imposing data processing and protection safeguards substantially the same as those set out in Exhibit B to this DPA ("**DPA Exhibit B**"), and (b) remain liable for compliance with the obligations of this DPA and for any acts or omissions of a Subprocessor that cause AAI to breach any of its obligations under this DPA.

6. Security of Personal Data.

6.1 In addition to any data security provisions in the Agreement, AAI represents and warrants that it has implemented and will maintain reasonable and appropriate physical, technical, organizational and administrative safeguards to preserve and protect the confidentiality, security, integrity, availability, and authenticity of the Personal Data and to protect against Security Incidents, including the security measures set forth in DPA Exhibit B.

6.2 AAI shall ensure personnel who Process Personal Data either enter into written confidentiality agreements or are subject to statutory obligations of confidentiality.

6.3 Customer is responsible for reviewing the information made available by AAI relating to data security and making an independent determination as to whether the Services meet Customer's requirements and legal obligations under Applicable Privacy Law.

6.4 Customer is solely responsible for complying with Security Incident notification laws applicable to Customer and fulfilling any obligations to give notices to government authorities, affected individuals or others relating to any Security Incidents.

7. Breach Notification.

7.1 AAI will (a) notify Customer without undue delay and, in any event, not later than 72 hours, after becoming aware of a Security Incident affecting Customer and (b) make reasonable efforts to identify the cause of the Security Incident, mitigate the effects, and remediate the cause to the extent within AAI's reasonable control. Customer acknowledges that AAI's notification of a Security Incident is not an acknowledgement by AAI of its fault or liability.

7.2 Upon Customer's request and taking into account the nature of the applicable Processing, AAI will assist Customer by providing, when available, information reasonably necessary for Customer to meet its Security Incident notification obligations under Applicable Data Protection Law.

8. Data Protection Impact Assessment. Upon Customer's request and taking into account the nature of the applicable Processing, AAI will provide Customer with assistance in fulfilling Customer's obligations under Applicable Privacy Law to carry out a data protection impact or similar risk assessment related to Customer's use of the Services, to the extent such information is available to AAI, including, if required by Applicable Privacy Law, to assist Customer in consultations with relevant Privacy Authorities.

9. Audit Rights. Upon 30 days' written notice by Customer and subject to the confidentiality obligations set forth in the Agreement, AAI shall make available to Customer its procedures relevant to the protection of Customer Personal Data in the form of AAI's third-party certifications and audit reports to the extent that AAI makes them generally available to its customers ("**Audit Records**"). Customer may request Audit Records through AAI's compliance portal at <https://www.automationanywhere.com/compliance-portal>. In the event of a Security Incident, Customer shall have the right to request a copy of the most recent Audit Records, a root cause of the Security Incident report, a remediation plan, and upon completion, a copy of a remediation report showing any identified root cause remediated.

10. Deletion of Personal Data. Unless instructed earlier by Customer or subject to an earlier deletion schedule by the specific Services in accordance with Documentation (as defined in the Agreement), 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 and (b) its provision of the Cloud Services within 30 days after termination of the Agreement, in each case unless otherwise required by law. Notwithstanding the foregoing, back up files will be deleted within seven months after termination of the Agreement.

11. CCPA. In the event of AAI Processing the Personal Data of Data Subjects who are California consumers under the CCPA, the required contractual clauses of the CCPA, as may be amended or replaced from time to time, are incorporated herein. Customer and AAI hereby acknowledge and agree that in no event shall the transfer of Personal Data from Customer to AAI constitute a sale of Personal Data or transfer of Personal Data for valuable consideration to AAI,

and that nothing shall be construed as providing for the sale or transfer for valuable consideration of Personal Data to AAI. AAI shall not: (a) sell or share Personal Data; (b) retain, use, or disclose Personal Data for any purpose other than to perform the Services; (c) retain, use, or disclose Personal Data outside of the direct business relationship between Customer and AAI; or (d) combine Personal Data with personal information that AAI receives from or on behalf of another business or person, or that it collects from its own interactions with individuals, unless otherwise permitted by the CCPA. Furthermore, (i) the specific Business Purpose(s) for which AAI is processing Personal Data is contained in the Agreement and AAI acknowledges that Customer is disclosing the Personal Data to AAI only for the limited and specified Services set forth in the Agreement; (ii) AAI shall comply with all applicable sections of the CCPA, including providing the same level of privacy protection as required of Customer by the CCPA with respect to the Personal Data as specified in DPA Exhibit B ; (iii) Customer has the right to take reasonable and appropriate steps to ensure AAI uses the Personal Data in a manner consistent with Customer's obligations under the CCPA, and such steps will be in the form of receiving copies of AAI's Audit Records. To the extent steps beyond the review of Audit Records is required by the CCPA, and so long as there is a mutual agreement as to the scope of the assessment in advance, AAI shall allow Customer or its designee (who shall not be a competitor of AAI and shall enter into an appropriate confidentiality agreement with AAI), upon 30-day notice during normal business hours, and at Customer's expense, assess AAI's compliance with the CCPA specifically as to Customer's Personal Data; (iv) Customer has the right, upon written notice, to take reasonable and appropriate steps to stop and remediate AAI's unauthorized use of personal information; (v) AAI shall notify the Customer, should it determine that AAI can no longer meet its obligations with respect to Customer's Personal Data under the CCPA; and (vi) AAI and Customer shall enable each other to comply with consumer requests regarding the Personal Data which are made pursuant to the CCPA by forwarding any applicable consumer request made pursuant to the CCPA by email to Customer (in case of notice necessary to Customer) or to privacy@automationanywhere.com if notice is necessary to AAI and provide the other party with any information necessary to comply with the request. AAI will include the restrictions and the requirements of the CCPA in any contracts with subcontractors who process Personal Data and will notify Customer of any new Subprocessor in accordance with Section 5 herein.

12. Restricted Transfers.

12.1 EU Transfers. In the event of a Restricted Transfer to a recipient outside of the EEA, then such transfers shall be governed by the EU SCCs (Module Two for Controller to Processor transfers and Module Three for Processor to Processor transfers), which shall be entered into and incorporated into this DPA by this reference and:

- (a) Customer is the "data exporter" and AAI is the "data importer";
- (b) Where applicable the following applies:
 - (i) the optional docking clause in Clause 7 does not apply;
 - (ii) in Clause 9, Option 2 will apply, the minimum time period for prior notice of a new Subprocessor shall be 30 days, and AAI shall fulfill its notification obligations by notifying Customer of any new Subprocessor in accordance with this DPA;
 - (iii) in Clause 11, the optional language does not apply;
 - (iv) in Clause 13, all square brackets are removed with the text remaining;
 - (v) in Clause 17, Option 1 will apply, and the EU SCCs will be governed by Irish law;

- (vi) in Clause 18(b), disputes will be resolved before the courts of Ireland;
- (vii) Exhibit A of this DPA (“**DPA Exhibit A**”)(Subject Matter and Details of Processing) and/or the order form contains the information required in Annex 1 of the EU SCCs; and
- (viii) DPA Exhibit B (Details of the Technical and Organizational Measures) contains the information required in Annex 2 of the EU SCCs.

12.2 Swiss Transfers. In the event of a Restricted Transfer to a recipient outside of Switzerland, then such transfers shall be governed by the EU SCCs as set forth in Section 12.1 above, which shall be entered into and incorporated into this DPA by reference and modified as follows:

- (a) in Clause 13 the competent supervisory authority shall be the Swiss Federal Data Protection and Information Commissioner;
- (b) in Clause 17 (Option 1), the EU SCCs will be governed by the laws of Switzerland;
- (c) in Clause 18(b), disputes will be resolved before the courts of Switzerland;
- (d) the term Member State must not be interpreted in such a way as to exclude Data Subjects in Switzerland from enforcing their rights in their place of habitual residence in accordance with Clause 18(c); and
- (e) all references to the EU GDPR in this DPA are also deemed to refer to the FADP.

12.3 UK Transfers. In the event of a Restricted Transfer to a recipient outside of the United Kingdom, then such transfers shall be governed by the UK SCCs, which shall be entered into and incorporated into this DPA by reference and:

- (a) in Table 1 of the UK SCCs, the parties’ key contact information is located in DPA Exhibit A and/or the order form;
- (b) in table 2 of the UK SCCs, the EU SCCs shall apply, including the Appendix Information and with only the following modules, clauses or optional provisions of the EU SCCs brought into effect for the purposes of this DPA:
 - (i) The applicable Module is Controller to Processor or Processor to Processor, as applicable;
 - (ii) the optional docking clause in Clause 7 does not apply;
 - (iii) in Clause 9, Option 2 will apply, the minimum time period for prior notice of a new Subprocessor shall be 30 days, and AAI shall fulfill its notification obligations by notifying Customer of any new Subprocessor in accordance with this DPA;
 - (iv) in Clause 11, the optional language does not apply;
- (c) in Table 3 of the UK SCCs
 - (i) the list of parties is located in DPA Exhibit A ;
 - (ii) the description of transfer is located in DPA Exhibit A ;
 - (iii) Annex II is located in DPA Exhibit B ; and
 - (iv) The list of Subprocessors is as set forth in DPA Exhibit C .
- (d) in Table 4 to the UK SCCs, neither party can terminate the DPA due to a change in law (the respective box is deemed checked).
- (e) incorporated herein are Part 2 (Mandatory Clauses) of the Approved Addendum, being the template Addendum B.1.0 issued by the ICO and laid before Parliament in accordance with s119A of the Data Protection Act

2018 on 2 February 2022, as it is revised under Section 18 of those Mandatory Clauses.

12.4 Argentinian Transfers. In the event of a Restricted Transfer to a recipient outside of Argentina, then such transfers shall be governed by Appendix II (provision of services) of the Argentinian SCCs, which shall be entered into and incorporated into this DPA by reference and:

- (a) DPA Exhibit A and DPA Exhibit B provide details of the Restricted Transfer and Technical and Organizational Measures; and
- (b) Disputes relating to the Argentinian SCC shall be governed by applicable Argentinian law and resolved before the courts of Argentina.

12.5 Other Restricted Transfers. In the event of any Other Restricted Transfer, such transfers shall be governed by such Other Applicable Transfer Clauses as may be required under Applicable Privacy Law, which shall be entered into and incorporated into this DPA by reference and:

- (a) DPA Exhibit A and DPA Exhibit B provide details of the Restricted Transfer and Technical and Organizational Measures; and
- (b) Disputes relating to the Other Restricted Transfer shall be governed by the applicable laws of the country from which the Other Restricted Transfer takes place and resolved before the courts of such country.

AAI shall provide a signed copy of the applicable Standard Contractual Clauses upon request.

13. Data Subject Requests.

13.1 Upon Customer's request and taking into account the nature of the applicable Processing, AAI will assist Customer by appropriate technical and organizational measures, insofar as possible, in complying with Customer's obligations under Applicable Privacy Law to respond to requests from individuals to exercise their rights under Applicable Privacy Law, provided that Customer cannot reasonably fulfill such requests independently (including through use of the Services).

13.2 If AAI receives a request from a Data Subject in relation to the Data Subject's Personal Data, AAI will notify Customer and advise the Data Subject to submit the request to Customer (but not otherwise communicate with the Data Subject regarding the request except as may be required by Applicable Privacy Law), and Customer will be responsible for responding to any such request.

14. Authorized Affiliates.

14.1 The parties acknowledge and agree that, by executing the Agreement, the Customer enters into this 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. 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 Services 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.

14.2 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.

14.3 Where an Authorized Affiliate becomes a party to this DPA, it shall to the extent required under Applicable Privacy Law, be entitled to exercise the rights and seek remedies under this DPA, subject to the following: Except where Applicable Privacy Law require the Authorized Affiliate to exercise a right or seek any remedy under this DPA against AAI directly by itself, the parties agree that (i) 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 (ii) 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.

15. Limitation of Liability.

THE RESPECTIVE LIABILITIES OF AAI AND CUSTOMER, AND EACH OF THEIR AFFILIATES AND/OR AUTHORIZED AFFILIATES, UNDER THIS DPA, SHALL BE LIMITED IN ACCORDANCE WITH THE APPLICABLE LIMITATIONS OF LIABILITY CONTAINED IN THE AGREEMENT.

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 such DPAs, 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.

16. 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).

17. Order of Precedence. In the event of inconsistencies between the provisions of the Standard Contractual Clauses and this DPA or other agreements between the Parties regarding the processing of Personal Data, the order of precedence shall be: the applicable Standard Contractual Clauses, followed by the DPA, followed by other agreements between the Parties.

DPA EXHIBIT A
Details of the Processing of Personal Data

A. LIST OF PARTIES

Data exporter(s):

1. Customer Name: As specified in the Order Form

Customer Trading Name (if different):

Customer Main Address (if a company registered address): As specified in the Order Form

Customer's Official Registration Number (if any) (company number or similar identifier):

Customer's key contact person's name: As specified in the Order Form

Key contact's position: As specified in the Order Form

Key contact's contact details: As specified in the Order Form

Customer's DPO's name and contact information (if any):

Customer's EU Representative name and contact information (if any):

Activities relevant to the data transferred under these Clauses: Submitting data (which may include Personal Data) to the Services for Processing in accordance with the Agreement between Customer and Automation Anywhere Inc.

Role: Controller or Processor

Data importer:

1. Name: Automation Anywhere, Inc.

Trading Name (if different):

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

Official Registration Number (if any) (company number or similar identifier): Delaware Secretary of State file number 6944468

Key contact person's name, position and contact details: Shannon Salerno, Director, Legal – Product and Privacy Counsel, privacy@automationanywhere.com

Activities relevant to the data transferred under these Clauses: Processing data (which may include Personal Data) submitted by Customer's users to the Services, and collecting Personal Data from users of the Services, each for Processing in accordance with the Agreement between Customer and Automation Anywhere Inc.

Role: Processor

Categories of data subjects whose personal data is transferred

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

1. Actual customers of Customer and their employees

2. Employees of Customer
3. Suppliers of Customer and their employees
4. Any other data subjects' Personal Data submitted to the Services by Customer

Categories of personal data transferred

1. Personal Data as determined by Customer
2. Telemetry and usage data including but not limited to: username, user email address, password, device IDs, audit logs, product features used, and error logs.
3. Support Authentication Data for provisioning of support services:
 - First and Last Name
 - Phone Number
 - Company Name
 - Title
 - Location (Country)
 - IP Addresses
 - E-Mail

Sensitive data transferred (if applicable) and applied restrictions or safeguards that fully take into consideration the nature of the data and the risks involved, such as for instance strict purpose limitation, access restrictions (including access only for staff having followed specialised training), keeping a record of access to the data, restrictions for onward transfers or additional security measures.

As determined by Customer with the technical and organizational security measures described in DPA Exhibit B.

The frequency of the transfer (e.g. whether the data is transferred on a one-off or continuous basis).

Continuous for the duration of the services

Nature of the processing

Collection, recording, analysis, structure, host, transfer, erasure, and any other activity customer instructs the services to perform on the Personal Data. Data Importer shall process Personal Data for purposes of the provision of services to the Data Exporter, in accordance with the terms and conditions of this DPA and the Agreement.

Purpose(s) of the data transfer and further processing

Provision of automation and/or automation discovery services, and support for such services (if applicable), as further specified in the Agreement and Order Form.

The period for which the personal data will be retained, or, if that is not possible, the criteria used to determine that period

As specified in the section titled "Deletion of Personal Data" in this DPA.

For transfers to (sub-) processors, also specify subject matter, nature and duration of the processing

See DPA Exhibit C– Subprocessor List – continuous for duration of the use of the applicable service.

DPA EXHIBIT B

Details of the Technical and Organizational Measures

In addition to maintaining ISO27001:2013, ISO22301:2019, Type 2 SOC 1, and Type 2 SOC 2 certifications Processing Personal Data under the Agreement, AAI has implemented and shall maintain its written comprehensive data protection program that includes the following safeguards:

- Appropriate user authentication controls, including secure methods of assigning, selecting, and storing access credentials and restricting access to active users.
- Secure access controls, including controls that limit access to Customer Personal Data to individuals who have a demonstrable genuine business need-to-know, supported by appropriate policies, protocols, and controls to facilitate access authorization, establishment, modification, and termination.
- Appropriate and timely adjustments to AAI's data protection program based on: periodic risk assessments; regular comprehensive evaluations (such as third-party assessments) of the AAI's data protection program; monitoring and regular testing of the effectiveness of safeguards, including vulnerability assessment and penetration testing; and a review of safeguards at least annually and whenever there is a material change in AAI's technical environment or business practices that may implicate the confidentiality, availability, integrity, or security of the data importer's information systems.
- Appropriate ongoing training and awareness programs designed to ensure workforce members and others acting on AAI's behalf are aware of and adhere to AAI's data protection program's policies, procedures, and protocols.
- Appropriate monitoring of information systems in a manner designed to ensure data integrity and prevent loss or unauthorized access to, or acquisition, use, or disclosure of, Personal Data.
- Appropriate technical security measures designed to prevent unauthorized intrusions and access, including firewall protection, antivirus protection, security patch management, logging of access to or use or disclosure of Personal Data, and intrusion detection.
- Appropriate use of encryption of Personal Data submitted to the Services.
- With respect to storage of Personal Data, contracting with subprocessors who have appropriate facility security measures, including access controls, designed to prevent unauthorized access to premises, information systems, and data.
- Safeguards ensuring disposal of Personal Data renders that data permanently unreadable and unrecoverable.
- Additional technical and organizational measures for the use of the software portion of the Services, along with certifications and SOC2 Type 2 report, can be found at the following link:

<https://www.automationanywhere.com/compliance-portal>

- For Support, AAI utilizes Salesforce's Sales, Service and Community Clouds and has implemented Salesforce Platform Encryption (At Rest and In Motion). Additional technical and organizational measures for the use of Support can be found at the following links:

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

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

DPA EXHIBIT C

Subprocessor List

Notes:

Intelligent Automation Co-Pilot for Business Users is formerly known as Automation Co-Pilot and AARI.

Process Discovery is formerly known as Fortress IQ.

References herein to "A360 cloud" include the following products: Automation 360 Pure Cloud - Base Package, Intelligent Automation - Enterprise Platform Plus Bundle, Intelligent Automation Co-Pilot for Business Users, Intelligent Automation Co-Pilot for Automators (Base, Plus, and Premium), Document Automation, Bot Insights, Discovery Bot, and IQ Bot

Subprocessor Legal Name	Applicable Services	Function of Subprocessor	Subprocessor Privacy Contact	Address of the Subprocessor
Google, LLC	The following Cloud Products: A360 Cloud	Cloud hosting infrastructure, file and data storage services	855-548-2777 https://support.google.com/policies/contact/general_privacy_form	1600 Amphitheatre Parkway, Mountain View, California 94043, United States
Google, LLC	The following Cloud Products: IQ Bot and Document Automation	Data extraction using Google Document AI, Vision AI optical character recognition, Apigee	855-548-2777 https://support.google.com/policies/contact/general_privacy_form	1600 Amphitheatre Parkway, Mountain View, California 94043, United States

Amazon Web Services, Inc. (subsidiary of Amazon.com, Inc.)	The following Cloud Products: A360 Cloud	Cloud hosting infrastructure, provisioning service, file and data storage services, data base and reporting	https://pages.awscloud.com/DSAR_RTf.html Amazon Web Services, Inc., 410 Terry Avenue North, Seattle, WA 98109-5210, ATTN: AWS Legal	410 Terry Avenue North Seattle, WA 98109-5210, United States
Microsoft Corporation	The following Cloud Products: IQ Bot and Document Automation	Microsoft forms recognizer	https://www.microsoft.com/en-us/concern/privacyrequest-other	One Microsoft Way, Redmond, Washington 98052 United States
Microsoft Corporation	The following Cloud Products: Document Automation and Intelligent Automation Co-Pilot for Automators	Large language model	https://www.microsoft.com/en-us/concern/privacyrequest-other	One Microsoft Way, Redmond, Washington 98052 United States
Cockroach Labs Inc	The following Cloud Products: A360 Cloud	Database	info@cockroachlabs.com	125 W 25th Street 11th Floor New York, NY 10001, United States
Auth0, Inc. (subsidiary of Okta, Inc.)	The following Cloud Products: A360	Single Signon - Automation Anywhere OAuth implementation; OAuth authorization support	privacy@okta.com	10800 NE 8th Street, Ste. 600, Bellevue, WA, 98004, United States

PixieBrix, Inc.	The following Cloud Products: Intelligent Automation - Co-Pilot for Business Users	Function integrations for Google Chrome extensions	privacy@pixiebrix.com	245 8th Ave 1083, New York, NY 10011 United states
Pendo.io, Inc.	All Cloud and On-Premise Services aside from Process Discovery	In-product guides, spotlights, informational tips and other contextual user assistance elements within the product to help onboard and educate users about Automation Anywhere solutions; Anonymized user analytics to understand usage patterns of Automation Anywhere's product; In product user notifications; User feedback on product features	gdpr@pendo.io	301 Hillsborough St Ste 1900, Raleigh, North Carolina, 27603, United States

Provectus IT, Inc.	A360 Cloud	Engineering resources	legal@provectus.com	125 University Avenue, Suite 295, Palo Alto, California, 94301, United States
Waverley Software, Inc.	A360 Cloud	Engineering resources	info@waverleysoftware.com	855 El Camino Real, 13A-222, Palo Alto, CA 94301-2305, United States
Sumo Logic, Inc.	The following cloud products: A360 Cloud and Process Discovery	Event logging, cloud monitoring, telemetry collection	privacy@sumologic.com	855 Main St Ste 100, Redwood City, California, 94063, United States
Elasticsearch, Inc	The following cloud products: A360 Cloud and Process Discovery	Database and reporting	privacy@elastic.co	800 W El Camino Real, Suite 350, Mountain View, CA 94040 United States
Innodata Inc.	Document Automation and Process Discovery	Data labeling and categorization	legal@innodata.com	55 Challenger Rd, Ridgefield Park, NJ 07660, United States
Google, LLC	Process Discovery	Cloud hosting, infrastructure, optical character recognition, Google Kubernetes Engine - open source container orchestration technology	855-548-2777 https://support.google.com/policies/contact/general_privacy_form	1600 Amphitheatre Parkway, Mountain View, California 94043, United States

Trantor Inc.	Process Discovery	Engineering resources	info@trantorinc.com	3723 Haven Avenue Suite 107,119,120, Menlo Park, CA 94025 United States
Shibumi.com, Inc.	COE Manager	Pipeline and ROI tracking for automations, support escalation for COE Manager, and professional services for customization requests	privacy@shibumi.com	50 Washington Street Suite 302E, Norwalk, CT 06854 United States
Movate Inc.	Customer Support	Support resources across international timezones	privacy.officer@csscorp.com ; privacy.officer@movate.com	5600 Tennyson, Parkway Suite 255, Plano TX - 75024, United States
Qualesce LLC	Customer Support for SAP Accelerator	Product specific customer support	info@qualesce.com	2591 Dallas Parkway, STE 300. Frisco, Texas 75043, United States
Gainsight, Inc.	Customer Support in the form of a Customer Community	External customer community	privacy@gainsight.com	350 Bay Street, Suite 100, San Francisco, CA 94133 United States

Salesforce, Inc.	Customer Support Application	Cloud Provider & Customer Support Ticketing System; Single Sign On - User Authentication for access to Knowledgebase and forums; Community Cloud - Knowledge base and external customer community, and customer self service tool for provisioning and license management	privacy@salesforce.com ; datasubjectrequest@salesforce.com ; legal@salesforce.com	Salesforce Tower. 415 Mission Street, 3rd Floor. San Francisco, CA 94105 United States
Grazitti Interactive LLP/ Grazitti Interactive, Inc.	Customer Support Application	Locate information across multiple applications	privacy@searchunify.com	Plot No – 198, Industrial Area Phase 2, Panchkula, Haryana – 134113, India/ 340 E Middlefield Rd, Mountain View, CA 94043, United States

Atlassian Corporation Plc/ Atlassian, Inc.	Customer Support Application	Bug tracking and management system	privacy@atlassian.com	Level 6, 341 George Street, Sydney, NSW 2000, Australia/ 350 Bush Street Floor 13, San Francisco, CA 94104, United States
SupportLogic, Inc.	Customer Support Application	Artificial intelligence customer support case review for escalation avoidance	security@supportlogic.io ; dpo@supportlogic.io ; privacy@supportlogic.io	356 Santana Row 1000 San Jose, CA 95128, United States
Zoho Corporation	Customer Support Application	Support chat, analytics, and workflows	legal@zohocorp.com ; privacy@zohocorp.com	4141 Hacienda Drive, Pleasanton, CA 94588, United States
Tableau Software, Inc. (subsidiary of Salesforce, Inc.)	Customer Support Application	Data visualization software	legal@salesforce.com ; privacy@salesforce.com	Salesforce Tower. 415 Mission Street, 3rd Floor. San Francisco, CA 94105 United States
Qualtrics International Inc.	Customer Support Application	Support and Customer Success surveys	notice@qualtrics.com	333 West River Park Drive Provo, Utah 84604, United States
CodeGlo Tech & Marketing LLC	Customer Support Application	Artificial intelligence and large language model to assist with customer support case resolution	legalteam@codeglo.com	342 N Water St, Milwaukee, WI 53203, USA

One Realm, Inc.	Customer Support Application	Artificial intelligence and large language model to assist with customer support case resolution	info@getodin.ai	One Realm Inc (Odin AI) 4011 Adriatic St Oxnard, CA 93035
Adobe Inc.	All Cloud and On-Premise Services	Product updates messaging and critical product communications	privacyofficer@marketo.com	345 Park Avenue San Jose, CA 95110-2704, United States
Amazon Web Services, Inc. (subsidiary of Amazon.com, Inc.)	All Cloud and On-Premise Services	Critical product communications	https://pages.awscloud.com/DSAR_RTF.html Amazon Web Services, Inc., 410 Terry Avenue North, Seattle, WA 98109-5210, ATTN: AWS Legal	410 Terry Avenue North Seattle, WA 98109-5210, United States
Zoomin Software, Inc.	Technical Documentation	Documentation portal to provide AAI's technical documentation	privacy@zoominsoftware.com	33 West 60th St., 11th Floor, New York NY 10023

AAI may also engage one or more of the following AAI Affiliates as Subprocessors to deliver some or all of the Services provided to Customer:

Subprocessor Name	Location
Automation Anywhere, Inc.	California, United States

Automation Anywhere Software Pvt. Ltd.	India
Automation Anywhere UK Limited	United Kingdom
Automation Anywhere Australia Pty. Ltd.	Australia
Automation Anywhere Singapore Pte. Ltd.	Singapore
Automation Anywhere Japan, Co., Ltd.	Japan
Automation Anywhere GmbH	Germany
Automation Anywhere Canada Ltd.	Canada
Automation Anywhere HK Limited	Hong Kong
Automation Anywhere Korea LLC	South Korea
Automation Anywhere France (SAS)	France
Automation Anywhere South Africa (Pty) Ltd.	South Africa
Automation Anywhere FZ-LLC	United Arab Emirates
SmartForce Tecnologia, Consultoria e Servicos Ltda	Brazil
Workforce Digital, S.A. de C.V.	Mexico