Data Processing Addendum

(Updated October 21, 2021)

This Data Processing Addendum ("**DPA**") 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 - 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 Laws, 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. AAI may modify this DPA but any such modifications shall not materially increase Customer's liabilities and/or obligations hereunder, nor shall they materially decrease AAI's obligations and/or liabilities hereunder, unless required by Applicable Data Protections Laws.

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 United States (including but not limited to the CCPA) and the GDPR and other laws and regulations of the European Union, the European Economic Area and their member states (the "**EEA**"), Switzerland and the United Kingdom.

"**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 Affiliates which are (a) subject to the data protection laws and regulations of the European Union, the EEA, Switzerland and/or the United Kingdom, and (b) permitted to use the Service pursuant to the Agreement between Customer and AAI, but have not signed a separate Order Form with AAI and are 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 Cloud 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, or 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 (a) with respect to the European Union, 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) (the "**EU GDPR**") and (b) with respect to the United Kingdom, the United Kingdom General Data Protection Regulation (the "**UK GDPR**").

"**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 person. The type of Personal Data Processed by AAI is specified in Exhibit A.

"**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.

"**SCoPD**" means "Special Categories of Personal Data" as defined in the GDPR.

"**Service**" means (i) the support and maintenance that AAI provides to Customer under the Agreement (the "**Support Services**") 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, with respect to transfers subject to (i) the UK GDPR, the Standard Contractual Clauses for the Transfer of Customer Personal Data to Data Processors Established In Third Countries pursuant to Commission Decision 2010/87/EU of 5 February 2010, and (ii) the EU GDPR, the applicable module (Module 1: Controller to Processor; or Module 2: Controller to Controller) of the standard contractual clauses as set out in the European Commission's Decision 2021/914 of 4 June 2021, in each case as may be amended, updated, or replaced from time to time.

"**Subprocessor**" means an entity engaged by AAI only for Processing under this DPA.

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 execution of the Agreement. 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).

c. **Compliance with Applicable Data Protections Laws.** Each party shall comply fully with Applicable Data Protection Laws in undertaking each of its respective obligations under this DPA.

d. **Customer's General Instruction.** By entering into this DPA, Customer instructs AAI to Process Customer Personal Data: (a) for the purpose of providing the Service; (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.

e. **Customer's Responsibilities.** 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 DPA, Customer shall not provide AAI with any Customer Personal Data (i) not specified in Exhibit A hereto, and (ii) unless Customer complies with Applicable Data Protection Laws, including without limitation, applicable security and confidentiality measures set forth in GDPR Article 32.

f. **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 and/or DPA. 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, AAI shall promptly inform Customer in writing, which may be via email. In this event, AAI reserves the right, upon notification to Customer (which may be via 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.

g. **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 Exhibit A hereto.

2. RIGHTS OF DATA SUBJECTS

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, objections 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 a 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 its 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 Exhibit C. If AAI intends to change any of the Subprocessors listed on Exhibit C, AAI shall provide thirty (30) day notice to Customer, via email and/or through the support portal, for a Subprocessor identified as a "cloud provider" in Exhibit C (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, Google 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 described 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.

5. CUSTOMER OBLIGATIONS

a. **Support Authentication Data.** For Support Services only, Customer acknowledges and agrees that, except as otherwise set forth in this Section 5, Customer Personal Data provided to AAI for Processing in connection with the Service shall consist of business contact information 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.

b. **Other Personal Data.** For Support Services only and to the extent Customer, in its sole discretion, deems it necessary to provide to AAI any Customer Personal Data other than Support Authentication Data (for example, but not limited to, a screen shot containing Customer Personal Data related to any of Customer's end users), Customer shall check the appropriate box when submitting a support ticket to indicate that it intends to disclose such Customer Personal Data to AAI. In the event Customer fails to comply with the preceding sentence, AAI shall have no obligation to assist Customer with Data Subject Requests under Section 2 above and AAI's failure to assist under such circumstances shall not be considered a breach of this DPA.

c. **Lawful Basis**. To the extent relevant under Applicable Data Protection Laws, Customer shall have a lawful basis for Processing, and providing to AAI, all Customer Data. If at any time during the Term of the Agreement, Customer discovers that it does not have a lawful basis for Processing Personal Data or 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.

6. SECURITY

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's technical and organizational security and confidentiality measures are described in Exhibit B hereto. AAI shall ensure that Customer Personal Data received from Customer is logically segregated.

7. DATA BREACH

a. <u>Successful Security Incident/Data Breach</u>. A "***Successful Security Incident***" means accidental, unauthorized or unlawful access to, destruction of, loss of, alteration of or unauthorized disclosure of Customer Data while being Processed by AAI. In the event of a Successful Security Incident, AAI shall notify the Customer without undue delay after becoming aware of it, but in no event longer than 72 hours. Such notification 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; and (v) all actions taken as may be required by Applicable Data Protection Laws. AAI shall 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.

b. <u>Unsuccessful Security Incident</u>. 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. <u>Reimbursement of Costs</u>. 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 Successful Security Incident was caused by AAI, or its Subprocessors.

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 its 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 may request Audit Records through AAI's compliance portal. Following 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 Support Authentication 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

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 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 that AAI may, without Customer's prior written consent, transfer and Process the Personal Data in a foreign jurisdiction outside the EEA, provided such transfer is either (i) to a country or territory which has been formally recognized by the European Commission or the United Kingdom, as applicable, as affording the Personal Data an adequate level of protection, or (ii) the transfer of such personal data is, as between AAI (as data importer) and Customer (as data exporter), undertaken pursuant to the Standard Contractual Clauses, the terms of which are incorporated into this DPA by reference and can be found at: https://ec.europa.eu/info/system/files/1_en_annexe_acte_autonome_cp_part1_v5_0.pdf and https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/international-transfers-after-uk-exit/sccs-after-transition-period/, for the EC and UK, respectively.

   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 EEA, 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 become legally binding between Customer and AAI when (a) this DPA is incorporated by reference into an executed Agreement or (b) Customer utilizes AAI's support ticket process and the Customer does not already have a DPA in place with AAI.

14. ORDER OF PRECEDENCE

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 provisions of the Standard Contractual Clauses and this DPA the Agreement, the Standard Contractual Clauses shall control, but only with respect to Personal Data transferred outside of the EEA. The information set forth in Exhibit A constitutes (i) applicable designations of optional clauses under, and (ii) the information required to be included in the schedules and appendices to, the Standard Contractual Clauses, and the parties' agreement to the terms of this DPA is deemed to also constitute agreement to the Standard Contractual Clauses to the extent the same may be required to be separately executed. AAI shall provide a signed copy of the Standard Contractual Clauses upon request.

EXHIBIT A
Details of the Processing of Personal Data

Data Exporter
The Data Exporter is _____
insert full legal name

Data Importer; Nature and Purpose of Processing

The Data Importer is AAI. The Data Importer provides Support Services to the Data Exporter under the Agreement, in the course of which it Processes certain Personal Data as a Processor.

Data Subjects

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

Categories of Data

The Personal Data transferred includes the following categories of data:
1. Other Personal Data as determined by Customer
2. Telemetry and usage data including but not limited to: username, password, device IDs, audit logs, 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

Special Categories of Data (if applicable)

The Personal Data transferred includes the following SCoPD (please specify):
1. As determined by Customer

Location of Processing

The Processing of Personal Data will primarily be performed in the United States, Costa Rica, Japan, India, Singapore and/or Poland but may be performed in any country where AAI has a presence.

Processing Instructions

Data Importer shall Process Personal Data for purposes of the provision of the Service to the Data Exporter, in accordance with the terms and conditions of this DPA and the Agreement.

Obligations and Rights of Data Exporter

The obligations and rights of the Data Exporter are set forth in the Agreement and this DPA.

Governing Law

With respect to transfers subject to the EU GDPR, the Standard Contractual Clauses shall be subject to the governing law of the Member State in which Customer is primarily established or, in the event that the Customer does not have a primary establishment, shall be subject to the governing law of Ireland.

Technical and organizational measures

Data Importer implements and maintains industry standard technical and organizational measures to protect the security of Personal Data that it processes in connection with its Services. Such measures include, as appropriate to the nature of the Personal Data processed, but are not limited, to the measures set forth in Exhibit B.

Optional Clauses Designations Under the EU Standard Contractual Clauses

For purposes of both Module 1 (Controller to Controller) and Module 2 (Controller to Processor):

Clause 7 (docking clause) is not included

For purposes of Module 2 (Controller to Processor):

Clause 9 - the parties agree that Option 2 (general written authorization for the engagement of Subprocessors) shall apply.

EXHIBIT B
Details of the Technical and Organizational Measures

AAI's security TOMs for the Cloud Services can be found at the following link:

https://www.automationanywhere.com/certification-reports.

AAI's security TOMs for Support Services 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 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).

EXHIBIT C
Subprocessors List

The list of Subprocessors approved by the Data Exporter as of the date of this DPA is as set forth below:

Subprocessor	Purpose
Google Cloud (Cloud Provider)	Infrastructure for Automation 360 Cloud Service
Salesforce for Support (Cloud Provider)	Service Cloud -Customer Support Ticketing System Single Sign-On – User Authentication Community Cloud – For External Customer Community 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 (Cloud Provider)	Infrastructure for Automation 360 Cloud Service
Amazon AWS	Virtual Machines in Lab Environments
Pendo	Support Case Close Survey v2
Pendo	Support – Worldwide Customer Onboarding