COPADO DATA PROCESSING AGREEMENT

This Data Processing Agreement ("DPA") is incorporated into Customer's governing agreement with Copado and forms part of the written contract for Customer's access and use of the Copado Services (also defined as "Tools") (the "Agreement") between the applicable Copado entity as set forth in the Agreement ("Copado," "we," "us" or "our") and its customer ("Customer," "you" or "your"). This DPA applies to Personal Data provided by Customer and each Data Controller in connection with your use of the Services. All capitalized terms not defined herein shall have the meaning set forth in the Agreement.

1. Scope

1.1. **Purpose**. This DPA is implemented as part of a framework in relation to data collection and processing, and Data Protection Law.

1.2. **Governance**. Customer will bind any other Data Controller it permits to use the Service to the terms of this DPA and will be solely responsible for administration of all approvals, consents, instructions or requests from other Data Controllers. Customer agrees that it shall be Copado's sole point of contact and to accept all information and notices on behalf of its other Data Controllers. Customer is solely responsible for distributing any information and notices to its other Data Controllers.

2. Roles and Responsibilities

2.1. **Roles.** Copado shall be Data Processor and Customer and those entities that it permits to use the Services shall be the Data Controller(s).

2.2. **Responsibilities.** The Appendices are incorporated into this DPA and (1) set forth the nature and purpose of processing, (2) Copado's Technical and Organizational Measures designed to secure Personal Data, (3) Copado's active Subprocessor list, and (4) additional obligations arising under Data Protection Law. Each party agrees to comply with its respective obligations under Data Protection Law. Customer is solely responsible for determining whether the Services meet Customer's requirements and legal obligations under Data Protection Law.

2.3. **Documentation and Records of Processing.** Each party is responsible for its own documentation requirements under Data Protection Law. If Customer is unable to utilize the functionality of the Services to obtain the information required to adequately maintain records of processing related to Personal Data, Copado agrees to reasonably assist Customer to obtain such data, subject to the terms of the Agreement and technical limitations.

3. Copado Obligations

3.1. **Instructions from Customer.** Copado will follow instructions received from Customer with respect to Personal Data unless such instructions are in violation of applicable law or require modifications to the Services. Should Copado be unable to comply with Customer's instructions, it will notify Customer. Customer understands and agrees that names, email addresses, and password are required to effectively use the Services and if Customer requests a deletion of such information, this may result in the termination of a user account and/or Customer's ability to use the Services.

3.2. **Data Processing.** To process Personal Data, Copado and its Subprocessors will use personnel who are informed of the confidential nature of Personal Data and any applicable requirements under the Data Protection Law. Copado and its Subprocessors will train individuals having access to Personal Data in data security and data privacy measures.

3.3. **Technical and Organizational Measures.** Copado agrees to implement technical and organizational measures as is commercially reasonable under the circumstances taking into account the Personal Data processed in the Services. Copado and its Subprocessors may modify the controls stated in Appendix 2 at any time without notice or consent from Customer if such modifications do not materially decrease the overall security of the Services.

3.4. **Security Breach Notification.** Copado will notify Customer without undue delay if it becomes aware of any Security Breach. For purposes of clarity, Customer is solely responsible and liable for its User's access credentials and all actions taken by its Users.

3.5. **Data Subject Requests.** If Customer is unable to process data subject requests using the functionality of the Services, Copado agrees to reasonably assist Customer in processing such data subject requests in accordance with Customer's instructions and Data Protection Law. If a data subject or data protection authority contacts Copado directly with an inquiry related to Customer, Copado will notify Customer of such request and shall only respond to such request by informing the data subject or data protection authority to contact Customer.

3.6. **Data Protection Impact** Assessment. If Customer is required by Data Protection Law to perform a data protection impact assessment, Copado shall provide reasonably requested documents necessary to show Copado's compliance with this DPA.

4. Subprocessors

4.1. **Authorized Subprocessors.** Customer agrees and provides general authorization for Copado to use Subprocessors to fulfill its contractual obligations under this DPA or to provide certain services on its behalf. The Subprocessors currently engaged by Copado to carry out processing activities on behalf of Customer are set forth in Appendix 3. At least 30 days before Copado engages any new Subprocessor to carry out processing activities on behalf of Customer, Copado will inform Customer (by email or by posting within the Services) of that update. If Customer has a legitimate objection to a new Subprocessor under Data Protection Law, then without prejudice to any other termination rights Customer has under the Agreement and subject to the applicable terms and conditions, Customer shall have 30 days to terminate the Agreement. If Customer does not terminate the Agreement within the specified time frame, Customer consents to Copado's use of the new Subprocessor(s). The Parties agree that Copado may replace a Subprocessor without notice where such replacement is reasonably necessary due to urgent operational or security issues ("Emergency Replacement"). In the event of an Emergency Replacement, Copado shall inform Customer (by email or by posting within the Services) without undue delay.

4.2. **Subprocessor Obligations.** Where Copado utilizes any Subprocessor as described above (i) Copado will restrict the Subprocessor's access to Personal Data only to what is necessary to maintain the Service or to provide the Service to Customer in accordance with the Agreement and Copado will prohibit the Subprocessor from accessing Personal Data for any other purpose; (ii) Copado will enter into a written agreement with the Subprocessor and, to the extent that the Subprocessor is performing the same data processing services that are being provided by Copado under this DPA, Copado will impose on the Subprocessor the same or similar contractual obligations that Copado has under this DPA; and (iii) Copado will remain responsible for its compliance with the obligations of this DPA and for any acts or omissions of the Subprocessor's that cause Copado to breach any of Copado's obligations under this DPA.

5. Certifications and Audits

5.1. **Customer Audits.** Customer (or its third-party regulator) or a mutually agreeable third party auditor, may audit Copado's control environment and security practices relevant to Personal Data processed only if: (a) Copado has not provided reasonably sufficient evidence of its compliance with the Technical and Organizational Measures in Appendix 2; (b) A Security Breach has occurred; (c) Customer or another Data Controller has reasonable grounds to suspect that Copado is not in compliance with its obligations under this DPA; or (d) An audit is formally requested by Customer's or another Data Controller's data protection authority. Where Customer audits Copado's environment, Copado will reasonably support Customer in its audit processes subject to the restrictions set forth in Section 5.2. Upon Customer's request, security documentation of Copado or its applicable Subprocessor(s) can be provided to Customer.

5.2. **Audit Restrictions.** The Customer audit will be limited to once in any twelve-month period and limited in scope and timing as reasonably agreed in advance between the Parties and, in all events, subject to Copado's security policies and procedures. Copado and Customer will use current certifications or other audit reports to minimize duplicative or repetitive audits. Customer and Copado will each bear their own expenses of audit unless the Customer is auditing under Section 5.1 (c) (unless such audit reveals a breach by Copado in which case Copado shall bear its own expenses of audit) or 5.1(d). In those cases, Customer will bear both its own expense as well as the cost of Copado's internal resources required to conduct the audit. If an audit determines that Copado has breached its obligations under the Agreement, Copado will remedy the breach at its own cost.

6. Data Export and Deletion

6.1. **Export and Deletion.** If Customer is unable to access or delete its Personal Data during the term of the Agreement, Copado shall reasonably assist Customer with a request to retrieve Personal Data in a mutually agreeable format, subject to the Agreement, Data Protection Law, and technical limitations. Any data deletion obligations as set forth in the Agreement shall apply to Personal Data processed in accordance with this DPA.

7. International Transfers

7.1. **Location of Processing.** The Copado data processing location will default to the United States unless Customer elects to utilize Copado's EU-based* data processing location during implementation (*other geography-specific locations may be available based on the subscriptions purchased by Customer). For Copado Essentials, the data processing location will be in the United States.

7.2. **Application of the Standard Contractual Clauses.** The Parties enter into and incorporate the Standard Contractual Clauses if Personal Data is transferred from the EEA, either directly or via onward transfer, to any country not recognized by the European Commission as providing an adequate level of protection for Personal Data (as described in the GDPR). Notwithstanding the foregoing, the Standard Contractual Clauses (or obligations the same as those under the Standard Contractual Clauses) will not apply if Copado has adopted an alternative recognized compliance standard, including without limitation Binding Corporate Rules for Processors, for the lawful transfer of Personal Data (as defined in the GDPR) outside the EEA. Further, to the extent the Standard Contractual Clauses apply, the terms of this DPA clarify the respective obligations within the Standard Contractual Clauses and nothing in this DPA shall be construed to conflict with the terms of the Standard Contractual Clauses. The optional docking clause in Clause 7 and the optional language in clause 11 shall not apply. Option 2 of Clause 9 shall apply under the basis of the general authorization for subcontractors provided in this DPA. The governing law of the Standard Contractual Clauses shall be the law of the Netherlands.

7.3. **Application of the UK Standard Contractual Clauses.** The Parties enter into and incorporate the UK Standard Contractual Clauses if Personal Data is transferred from the United Kingdom to any country not recognized by the UK adequacy regulations or the European Commission "adequacy decision." Further, to the extent the UK Standard Contractual Clauses apply, the terms of this DPA clarify the respective obligations within the UK Standard Contractual Clauses and nothing in this DPA shall be construed to conflict with the terms of the Standard Contractual Clauses. The Parties further agree that the "Parties' details" shall be as stated in the Agreement and the "Key Contact" shall be the contact listed in an Order Form or the Agreement. The module in operation shall be Module 2. The selected or optional clauses shall be the same as those reflected in Section 7.2. The Appendix Information in Table 3 shall be as stated in Annex I of the EEA SCCs. Both Importer and Exporter shall be checked in Table 4.

7.4. **Appendices.** If and to the extent the UK Standard Contractual Clauses or the Standard Contractual Clauses (collectively, "EEA SCCs") apply, Annex I of the EEA SCCs shall be deemed completed with the information set out in Appendix 1 to this DPA; Annex II of the EEA SCCs shall be deemed completed with the information set out in Appendix 2 to this DPA; and Annex III of the EEA SCCs shall be deemed completed with the information set out in Appendix 3 to this DPA.

8. Definitions

Capitalized terms not defined herein will have the meanings given to them in the Agreement.

"Data Controller" means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of Personal Data.

"Data Processor" means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the Data Controller.

"Data Protection Law" means any applicable international, national, federal, state, or local data privacy or data protection laws, regulations, or orders, as amended or introduced from time to time, which may include without limitation, Regulation (EU) 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data ("EU GDPR"); the United Kingdom Data Protection Act 2018, and the EU GDPR as amended and incorporated into UK law under the UK European Union (Withdrawal) Act 2018) ("UK GDPR"); the New Federal Act on Data Protection (nFADP); the California Consumer Privacy Act, as amended by the California Privacy Rights Act; and similar state-specific data privacy and data protection legislation.

"Data Subject" means an identified or identifiable natural person.

"EEA" means the European Economic Area, namely the European Union Member States along with Iceland, Norway and Lichtenstein.

"Personal Data" means any information relating to a Data Subject. For the purposes of this DPA, it includes only personal data entered by Customer or its Users into the Services. It also includes personal data supplied to or accessed by Copado or its Subprocessors in order to provide support under the Agreement.

"Security Breach" means a confirmed (1) accidental or unlawful access to or acquisition of Customer Personal Data by an unauthorized third party, or (2) similar incident involving Personal Data for which a Data Processor is required under applicable law to provide notice to the Data Controller.

"Services" means Copado's software platform purchased by Customer in an Order Form and as further described in the Documentation.

“Standard Contractual Clauses” or sometimes referred to the “EU Model Clauses” means the Standard Contractual Clauses (Module 2 – Controller to Processor) or any subsequent version thereof released by the Commission (which will automatically apply). The current Standard Contractual Clauses are located at: https://commission.europa.eu/law/law-topic/data-protection/international-dimension-data-protection/standard-contractual-clauses-scc_en.

“UK Standard Contractual Clauses” means the International Data Transfer Addendum to the Standard Contractual Clauses, available at https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/international-transfers/international-data-transfer-agreement-and-guidance/.

“Subprocessor” means Copado Affiliates and third parties engaged by Copado or Copado’s Affiliates to process personal data.

Accepted and agreed to as of the Effective Date by the authorized representative of each Party:

COPADO

By: ______________________________________

Name: ______________________________________

Title: ______________________________________

Date: ______________________________________

CUSTOMER

By: ______________________________________

Name: ______________________________________

Title: ______________________________________

Date: ______________________________________

Appendix 1 – Data Processing Description

This Appendix 1 shall serve as Appendix 1 to the Standard Contractual Clauses, if applicable.

Description of the Parties

The Data Exporter is the Customer that subscribed to use the Services and any Affiliates or Users permitted by Customer to use the Services.

The Data Importer is Copado, its Affiliates, and its Subprocessors that provide and support the Services.

Subject Matter, Duration, and Purpose of Processing

Personal Data may be processed for the purposes of providing and supporting the Copado Services, as set forth in the Agreement. The processing will be ongoing during the duration of the Agreement and the subject matter is in the context of providing the Services.

Categories of Data Subjects and Types of Personal Data for Processing

Customer may submit Personal Data of its Users into the Services. The Services only require Personal Data in the form of name and email for authentication, authorization, and process outcome notification purposes. Customer is contractually prohibited from entering Restricted Information into the Services. For any Copado Robotic Testing products or services, Customer acknowledges that best practices involve the use of robotic testing in a test environment with test data. Customer is in control of any additional Personal Data processed using robotic testing.

Special Categories of Data

Customer is strictly prohibited from including sensitive data or special categories of data (as defined in GDPR) in its Customer Data submitted into the Service.

Contact Information of Processor

Copado Entity	Address	Region
Copado Limited Company number 11719338	8 Devonshire Square, London EC2M 4YJ, United Kingdom	United Kingdom
Copado Inc.	330 N. Wabash Ave., Fl 23, Chicago, IL 60611	North and South America
Copado Netherlands B.V. Dutch trade register number 30263556	Barbara Strozzilaan 201 | 1083 HN Amsterdam	EMEA
Copado Australia Pty Ltd (Copado Essentials contracts via this entity)	Azure Group Pty Ltd, Level 10, 171 Clarence Street, Sydney NSW 2000	APAC

Appendix 2 - Copado Technical and Organizational Measures

This Appendix 2 contains a high-level description of Copado's Technical and Organizational Data Security and Privacy Measures. All capitalized terms used but not defined in this Addendum have the meanings assigned to them in the Agreement. Copado agrees to implement and maintain the following measures:

I. General Security Practices

Copado shall maintain commercially reasonable technical and organizational measures designed to protect the security, confidentiality and integrity of Customer Materials. These technical and organizational measures are further outlined within this ISE and are evaluated annually as part of Copado's independent third party security audit. Copado may adjust the security controls listed herein, provided that it will not materially decrease the overall security of the Services during a subscription term. During the term of the Agreement, Copado shall maintain, at its own expense an audit certification by an independent outside audit firm, and shall provide or make available to Customer, upon request, a copy of each of its ISO27001 and SOC 2 Type II reports, which shall be updated at least annually. If the third party audit discovers any deficiencies, Copado shall work with the third party auditor to remediate any such deficiencies to remedy such findings in a timely manner.

II. Business Controls

1. External Scanning

On an annual basis, Copado agrees to perform penetration tests on Copado systems. Copado agrees to review the results of such tests and classify any discovered vulnerabilities in accordance with Copado's internal policies governing vulnerability classification. Copado agrees to remediate any confirmed vulnerabilities in accordance with said standards. Copado agrees to maintain records of testing and remediation activities based on findings from its penetration tests.

2. Training

Copado requires all employees to undergo security training upon hire and annually thereafter. Copado requires additional role-based security training for personnel that is relevant to their business function. Copado's Information Security Management Team regularly reviews the content of the training and will update it based on any changes in Copado's security risk assessment.

III. Application Design Controls

1. Single Sign-On

Copado uses SAML based single sign-on to access and operate the Services.

2. Password Policy

Copado maintains the following password controls for systems used to host its Services:

- 16 character password minimum with a 64 character limit;
- Do not use secret questions as a sole password reset requirements;
- Require email verification of a password change request;
- Require current password in addition to the new password during password change;
- Store passwords in a hashed and salted format using a memory-hard or CPU- hard one-way hash function; and
- Enforce appropriate account lockout and brute-force protection on account access.

3. Patching

Copado maintains a vulnerability patch management process designed to identify and remediate vulnerabilities. Copado regularly and periodically patches and/or takes other corrective actions to remediate known or discovered vulnerabilities to all components of the application stack in a commercially reasonable risk-based timeframe, giving greater priority to vulnerabilities with a higher severity rating.

4. Logging

Copado agrees to maintain the following security logs for thirty (30) days:

- User authentications;
- Read, write, delete operations on application and system users and objects; and
- Security settings changes (including disabling logging.

5. Additional Application Security Controls

Copado shall develop, implement, maintain, and use commercially reasonable security measures including, (i) encryption during the transmission of Customer Materials, (ii) the installation and maintenance of firewalls, (iii) industry-standard anti-virus software, (iv) an intrusion and vulnerability management program, and (v) endpoint detection tools on any systems that process Customer Materials. Copado uses TLS 1.2+ based encryption to protect data in transit between systems and encryption at rest for all data storages and backups in its cloud-based infrastructure.

IV. Application implementation controls

1. Vulnerability Prevention

Copado developers are trained and instructed to follow guidelines designed to prevent vulnerabilities including those in the OWASP Top Ten, for example:

- Authorization bypass. Example: accessing other customers' data or admin features from a regular account.
- Insecure session ID. Example: guessable token; token stored in an insecure location (e.g., cookie without secure and http Only flags set).
- Injections. Example: SQL injection, NoSQL injection, XXE, OS command injection
- Cross-site scripting. Example: calling insecure Javascript functions, performing insecure DOM manipulations, echoing back user input into HTML without escaping.
- Cross-site request forgery. Example: accepting requests with an Origin header from a different domain.
- Use of vulnerable libraries. Example: using server-side frameworks or javascript libraries with known vulnerabilities.

V. Operational controls

1. Physical Access

Copado Services use IaaS vendors that validate physical security of relevant facilities using the following access controls:

- 24x7 Security guards;
- Internal and external video cameras;
- Formal access and visitor procedures;
- Entrance security controls, such as badge readers, biometric identification mechanisms, and/or physical locks;
- Alarmed emergency exit points;
- Fire detection alarms and protection equipment; and
- Redundant and emergency power sources.

2. Logical Access

Copado limits systems and Customer Materials access exclusively to the users with a legitimate need. Copado deactivates redundant accounts and expired access grants in a timely manner. Copado performs regular reviews of access to validate need to know.

VI. Business Continuity and Disaster Recovery

Copado maintains a formal business continuity and disaster recovery plan that is reviewed and tested annually. Additionally, Copado IaaS vendors are required to utilize data redundancy for system restoration and disaster recovery. System restoration and disaster recovery controls include daily backups. In the event of a disaster that results in the loss of the data center in which Customer Materials is stored, Copado shall exercise commercially reasonable efforts to restore the Services from such backups.

Appendix 3 - Subprocessors

Entity Name	**Type of Service**	**Geographic Location**
Amazon Web Services, Inc.	Amazon Web Service (AWS); fail-over and hosting for testing functionality	United States** or European Union*
Google LLC	Google Cloud Platform (GCP); hosting; Artificial Intelligence Services via Google VertexAI.	For GCP hosting: United States, United Kingdom, European Union, or Australia* For Google VertexAI: United States, Singapore, Australia or European Union*
Salesforce	Cloud Application Platform; hosting; support ticket tracking; User Interface.	United States or European Union*
ngrok, LLC	Provides connectivity to Customer on-premise resources for Copado, to the extent selected and downloaded onto customer's system(s)	United States or European Union*
SendGrid	Email notification platform; usage and data (email addresses) are based on the customer's specific configuration	United States or European Union*
Intercom**	Customer Support; Customer chat functionality	United States (within AWS)
ChargeBee**	Order generation software	United States (within AWS)
Copado Affiliates	Copado's affiliated entities may provide support, professional services, or other maintenance or management of the Services.	United States, European Union, United Kingdom, Canada, India, Australia, Vietnam
Key		
* Location is consistent and follows the location selection for Copado instance	(i.e., if the Copado instance is in the U.S., all Subprocessors are also in the U.S.)	
** For Copado Essentials Only	This does not apply to Copado's enterprise software offering.	

Appendix 4

California Consumer Privacy Act and U.S. Data Protection and Privacy Requirements

1. In accordance with Section 1798.140(j) and 1798.140(ag) of the California Consumer Privacy Act ("**CCPA**") as amended by the California Privacy Rights Act ("**CPRA**") and accompanying regulations (collectively referred to as **"CCPA"**), Copado agrees to comply with the terms and conditions of this Appendix 4. In addition to its foregoing obligations in the DPA, Copado agrees that it has and shall:
   a. not Sell or Share the Personal Data received from Customer;
   b. not retain, use, or disclose Personal Data Collected pursuant to the Agreement for any other purpose other than for the specific purpose of performing the Services specified in the Agreement and accompanying Schedules; including retaining, using or disclosing data for a Commercial Purpose (defined below) other than providing services in the Agreement and accompanying Schedules;
   c. not retain, use, or disclose Personal Data Collected pursuant to the Agreement outside of the direct business relationship between Copado and Customer;
   d. not further Collect (defined below), Sell (defined below), Share (defined below) or use Personal Data Collected pursuant to the Agreement without Customer's prior express written consent, and only as necessary to perform the stated business purpose; and
   e. not combine the Personal Data that Copado receives from, or on behalf of, Customer with Personal Data that it receives from, or on behalf of, another person or persons, or collects from Copado's own interaction with the Data Subject, except as otherwise permitted by the CCPA.
2. Copado agrees that:
   a. it shall notify Customer in writing if it determines it cannot comply with Customer's lawful instructions for use of Personal Data Collected pursuant to the Agreement;
   b. Upon notice to Customer under subsection (a), Customer is entitled to suspend the processing of Personal Data Collected pursuant to the Agreement;
   c. It grants Customer the right to request information necessary to monitor and assess Copado's compliance with this Agreement and the CCPA, including by but not limited to, requesting information related to Copado's independent third-party security assessments, audits, and other technical and operational testing, a maximum of once every twelve months (or otherwise in accordance with the audit rights in the DPA);
   d. It grants Customer the right to take reasonable and appropriate steps to validate that Copado uses the Personal Data Collected pursuant to the Agreement in a manner consistent with Customer's obligations under the CCPA; and
   e. If it contracts with another entity that supplements the services to Customer and involves the processing of Personal Data, it shall have a contract with the subcontractor that complies with the CCPA and accompanying regulations, and other applicable Data Protection Laws. Copado shall remain fully responsible for the compliance with the terms and conditions of the Agreement by any such Subprocessor.
3. For purposes of this Appendix, capitalized terms used herein shall have the meanings set forth in the Agreement (including the DPA) unless they are defined below:
   a. "Commercial Purpose" means to advance a person's commercial or economic interests, such as by inducing another person to buy, rent, lease, join, subscribe to, provide, or exchange products, goods, property, information, or services, or enabling or effecting, directly or indirectly, a commercial transaction.
   b. "Collects," "collected," or "collection" means buying, renting, gathering, obtaining, receiving, or accessing any Personal Data pertaining to a Data Subject by any means.
   c. "Cross-context behavioral advertising" means the targeting of advertising to a Data Subject based on the Data Subject's Personal Data obtained from the Data Subject's activity across businesses, distinctly-branded websites, applications, or services, other than the business, distinctly-branded website, application, or service with which the Data Subject intentionally interacts.
   d. "Sell" means selling, renting, releasing, disclosing, disseminating, making available, transferring, or otherwise communicating orally, in writing, or by electronic or other means, a Data Subject's Personal Data by the business to another business or a third party for monetary or other valuable consideration.
   e. "Share" means sharing, renting, releasing, disclosing, disseminating, making available, transferring, or otherwise communicating orally, in writing, or by electronic or other means, a Data Subject's Personal Data by the business to a third party for cross-context behavioral advertising, whether or not for monetary or other valuable consideration, including transactions between a business and a third party for cross-context behavioral advertising for the benefit of a business in which no money is exchanged.
   f. The terms "Data Subject" and "Personal Data" as used herein have the meanings ascribed to them above in the Addendum, and include the terms "Consumer" and "Personal Information" as used in applicable Data Protection Laws.
4. To the extent that similar laws of the United States provide for or require similar contract terms, this appendix will be deemed to address such requirements, to the extent permissible by law or regulations.