DATA PROCESSING AGREEMENT

Last Updated June 1, 2026

This Data Processing Agreement ("**DPA**") forms part of and is governed by the Cogito API Service Terms available at: https://cogito.decart.ai/legal/terms ("**Agreement**") executed by and between Decart.ai Inc. ("**Decart.ai**") and the Developer, as such terms are defined in the Agreement. All capitalized terms not defined herein shall have the meaning set forth in the Agreement.

This DPA is effective as of the date on which the Developer first accesses Service, Account or uses the API or LLM ("**Effective Date**"). The term of this DPA coincides with the term of the Agreement and terminates upon expiration or earlier termination (as set forth in Section 6 of the Agreement), or, if later, on the date when Decart.ai ceases all Processing of Developer Data.

WHEREAS, Decart.ai provides Developer with the Services as defined under the Agreement; and

WHEREAS, as part of the Services Decart.ai will Process Developer Data, which includes Personal Data (as defined below) on behalf of the Developer, in accordance with the terms of this DPA and all applicable Data Protection Laws.

1. DEFINITIONS

1.1. "**Adequate Country**" is a country that at the time of the provision of the relevant Services, has been recognized as providing adequate protection by the European Commission based on Art. 45 GDPR.

1.2. The terms "**Business**", "**Business Purpose**", "**Consumer**", "**Controller**", "**Database Owner**", "**Personal Data Breach**", "**Processing**" (and "**Process**"), "**Processor**", "**Holder**", "**Service Provider**", "**Sale**" "**Sell**" and "**Share**", "**Special Categories of Personal Data**", "**Sensitive Data**" and "**Supervisory Authority**", shall all have the same meanings as ascribed to them under the applicable Data Protection Laws. "**Data Protection Law**" means any and all applicable privacy and data protection laws and regulations (including, where applicable, EU Data Protection Law, UK Data Protection Laws, Swiss Data Protection Laws, Israeli Data Protection Law and the U.S. Data Protection Laws) as may be amended or superseded from time to time.

1.3. "**Data Subject**" means an identified or identifiable natural person. "**Data Privacy Framework**" or "**DPF**" means the EU-U.S. Data Privacy Framework, the UK Extension to the EU-U.S. Data Privacy Framework and the Swiss-U.S. Data Privacy Framework self-certification programs (as applicable) operated by the U.S. Department of Commerce; as may be amended, superseded, or replaced.

1.4. "**Developer Data**" means any Input and Output (as defined in the Agreement) containing Personal Data, including, to the extent applicable, End User Personal Data, Processed by Decart.ai in the course of providing the Services, all as detailed in **Annex I** attached herein.

1.5. "**DPF Principles**" means the Principles and Supplemental Principles available at:

https://www.dataprivacyframework.gov/program-articles/Participation-Requirements-Data-Privacy-Framework-(DPF)-Principles ; as may be amended, superseded or replaced.

1.6. "**EEA**" means the European Economic Area.

1.7. "**European Data Protection Law**" means, collectively, the laws and regulations of the European Union, the EEA, their member states, and the United Kingdom, applicable to the Processing of Personal Data, including (where applicable): (i) "**EU Data Protection Laws**"- EU General Data Protection Regulation (Regulation 2016/679) ("**EU GDPR**"); Regulation 2018/1725; and the e-Privacy Directive (Directive 2002/58/EC), as amended (**e-Privacy Law**); (ii) "**UK Data Protection Laws**" - the Data Protection Act 2018 (DPA 2018), as amended, and EU GDPR as incorporated into UK law as amended ("**UK GDPR**" and collectively with the EU

GDPR shall be referred to herein as the "**GDPR**"); (iii) "**Swiss Data Protection Laws**" or "**FADP**" - the Swiss Federal Data Protection Act (dated June 19, 1992, as of March 1, 2019) ("**FDPA**") and the Ordinance on the Federal Act on Data Protection ("**FODP**"); (iv) any national data protection laws made under, pursuant to, replacing or succeeding the EU GDPR or the e-Privacy Law; (v) any amendment or legislation replacing or updating any of the foregoing; and (vi) any judicial or administrative interpretation of any of the above, including any binding judicial or administrative interpretation of any of the above, or approved certification mechanisms issued by any relevant Supervisory Authority.

1.8. "**Instructions**" means the written, documented instructions provided by the Developer to Decart.ai directing Decart.ai to perform a specific or general action with regard to Developer Data.

1.9. "**Israeli Data Protection Laws**" means, collectively, the: (i) Israeli Protection of Privacy Law, 5741-1981 (as amended under Amendment 13); (ii) the regulations promulgated pursuant thereto, including the Israeli Protection of Privacy (Data Security) Regulations, 5777-2017 and the Israeli Protection of Privacy (Transfer of Data to Databases Abroad) Regulations, 5761-2001; (iii) any amendments or legislation replacing or updating any of the foregoing; and (iv) any judicial or administrative interpretation of any of the above, including any binding guidance, guidelines, codes of practice, approved codes of conduct or certification mechanisms approved by the Israeli Privacy Protection Authority.

1.10. "**Personal Data**" means any information relating to a Data Subject uploaded by or for Developer or Developer's agents, employees, or contractors to the Service as Developer Data, including "Personal Information," "Special Categories of Data," or "Highly Sensitive Data," or "Sensitive Data" or equivalent terms under applicable Data Protection Law.

1.11. "**Security Incident**" means any accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Developer Data. Any Personal Data Breach will comprise a Security Incident.

1.12. "**Standard Contractual Clauses**" or "**SCCs**" means: (i) the standard contractual clauses for

the transfer of Personal Data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council adopted by the European Commission Decision 2021/914 of 4 June 2021, which may be found at: https://eur- lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32021D0914&from=EN and

incorporated herein by reference ("**EU SCC**"); (ii) the UK "International Data Transfer Addendum to the European Commission Standard Contractual Clauses" available at: available at https://ico.org.uk/media/for-organisations/documents/4019539/international-data-transfer-addendum.pdf and

incorporated herein by reference ("**UK SCC**"); or (iii) the applicable standard data protection clauses issued, approved or recognized by the Swiss Federal Data Protection and Information Commissioner ("**Swiss SCC**").

1.13. "**US Data Protection Laws**" means federal and state privacy laws applicable to the Decart.ai Processing activities of Developer Data under this DPA, and any implementing regulations and amendment thereto, including without limitation the: (i) California Consumer Privacy Act (Cal. Civ. Code §§ 1798.100 - 1798.199) of 2018 including as modified by the California Privacy Rights Act as well as all regulations promulgated thereunder from time to time ('**CCPA**'); and (ii) (xx) other state privacy laws. All as amended or superseded from time to time and including any implementing regulations and amendments thereto.

2. ROLES AND DETAILS OF PROCESSING

2.1. The parties acknowledge and agree that, in connection with their respective obligations under the Agreement, and with respect to the Processing of Developer Data, Decart.ai is acting as a Data Processor (or Sub-processor, as applicable) and Developer is acting as a Data Controller (or Processor, on behalf of its End Users, as applicable). Each party will comply with Data Protection Law to which it is subject in the performance on this DPA.

2.2. Notwithstanding the above, Decart.ai shall remain the owner and Data Controller of the Usage Data (as defined in the Agreement) and certain Developer Account information, including contact information, transactions records, credit purchases and other commercial information of the Developer or Authorized Users. This information is processed by Decart.ai to manage the customer relationship, customer success, provide support, address bugs, facilitate security, provide maintenance and carry out core business functions such as accounting, billing, and filing taxes.

2.3. The Developer shall be exclusively responsible for defining the lawful basis for Processing Developer Data, including by obtaining any required consent and providing any required disclosures under applicable Data Protection Laws. Decart.ai shall act based on such lawful basis and Instructions provided by the Developer.

2.4. The subject matter and duration of the Processing carried out by Decart.ai on behalf of the Developer, the nature and purpose of the Processing, the type of Personal Data and categories of Data Subjects are described in **Annex I** attached hereto.

2.5. The Developer acknowledges and agrees that, as part of the Processing, the Developer Data will be processed using the LLM which may incorporate Artificial Intelligence features and technologies, as described in the Agreement .

3. PROCESSING OF PERSONAL DATA

3.1. Decart.ai represents and warrants that it shall Process Developer Data, on behalf of the Developer, solely for the purpose of providing the Services, in accordance with the Instructions. Notwithstanding the above, in the event Decart.ai is required under applicable laws, including Data Protection Law, to Process Developer Data other than as instructed by Developer, it shall make reasonable efforts to inform the Developer of such requirement prior to Processing such Developer Data, unless prohibited under applicable law.

3.2. Decart.ai shall inform Developer without undue delay (unless otherwise required by law) in the event that, according to Decart.ai's reasonable discretion, any of the Instructions infringes applicable laws, and Decart.ai shall have the right to immediately cease and suspend any such Processing activity related to the infringing Instruction.

3.3. Decart.ai shall provide reasonable cooperation and assistance to the Developer in ensuring compliance with its obligation to carry out data protection impact assessments and prior consultations with Supervisory Authorities or other competent data privacy authorities to the extent required under applicable Data Protection Laws, provided that, Decart.ai shall only be required to assist as for information which is reasonably available to Decart.ai and Developer does not have reasonable access to such information.

3.4. Decart.ai shall ensure that the staff or any other person authorized to Process the Developer Data has committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

3.5. Where US Data Protection Laws are applicable, Decart.ai will: (i) not Sell or Share Personal

Data; (ii) use Personal Data for the Business Purpose(s) set forth in the Agreement, and not retain, use, or disclose Personal Data, except where permitted by applicable Data Protection Law, for any purpose other than the Business Purpose(s) or outside of the direct business relationship between Decart.ai and Developer; (iii) notify Developer if it determines it can no longer meet its obligations under applicable Data Protection Law; (iv) not combine Personal Data, except to the extent permitted by applicable Data Protection Laws, with personal information that Decart.ai receives from, or on behalf of, other persons or with personal information Decart.ai collects from its own interactions with Consumers; (v) by complying with the obligations set out in Section 8 of this DPA, permit Developer to take reasonable and appropriate steps to ensure Decart.ai Processes Personal Data in a manner consistent with Developer's obligations under applicable Data Protection Laws; and (vi) work together with Developer in good faith to remediate any allegedly unauthorized use of Personal Data, if Developer reasonably believes that Decart.ai is Processing Personal Data in an unauthorized manner and provides Decart.ai with reasonable written notice of such belief.

4. DATA SUBJECTS RIGHTS AND REQUESTS

4.1. It is agreed that where Decart.ai receives a data subject request or a request from a regulator or authority in respect to Developer Data, where applicable, Decart.ai will notify the Developer of such request and direct the Data Subject or the applicable authority to the Developer in order to enable the Developer to respond directly to the Data Subject's or the applicable authority's request, unless otherwise required under applicable laws or otherwise prohibited.

4.2. Decart.ai will reasonably cooperate and assist Developer in responding to such request, provided that the Developer cannot reasonably fulfill such obligations independently with help of available in the documentation, the website or any other self-service feature provided by Decart.ai.

5. SUB-PROCESSING

5.1. The Developer acknowledges that Decart.ai may transfer Developer Data to and otherwise interact with third party data Processors ("**Sub-Processor**"). The Developer hereby authorizes Decart.ai to engage and appoint such Sub-Processors as listed in **Annex III**, as well as permits each Sub-Processor to appoint a Sub-Processor on its behalf. Decart.ai may continue to use those Sub-Processors already engaged by it or to engage an additional or replace an existing Sub-Processors to Process Developer Data, subject to the provision of a thirty (30) days prior notice of its intention to do so to the Developer (via email correspondence or through the Account). In case the Developer has not objected to the adding or replacing of a Sub-Processor within such notice period, such Sub-Processor shall be deemed approved by the Developer. In the event the Developer objects to the adding or replacing of a Sub-Processor, within such notice period, Decart.ai may, under Decart's sole discretion, suggest the engagement of a different Sub-Processor for the same course of services, or otherwise terminate the Agreement where the Services cannot be reasonably provided under such circumstances, without liability to Developer.

5.2. Decart.ai shall, where it engages any Sub-Processor, impose, through a legally binding contract between Decart.ai and the Sub-Processor, data protection obligations that are no less onerous than, and provide at least the same level of protection as, those set out in this DPA. Decart.ai shall ensure that such contract will require the Sub-Processor to provide sufficient guarantees to implement appropriate technical and organizational measures in

such a manner that the Processing will meet the requirements of Data Protection Laws.

5.3. Decart.ai shall remain responsible to the Developer for the performance of the Sub-Processor's obligations in accordance with this DPA.

6. TECHNICAL AND ORGANIZATIONAL MEASURES

6.1. Taking into account the state of the art, the costs of implementation and the nature, scope, context, and purposes of Processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, and without prejudice to any other security standards agreed upon by the parties, Decart.ai hereby confirms that it has implemented and will maintain appropriate physical, technical and organizational measures to protect the Developer Data as required under Data Protection Laws to ensure lawful Processing of Developer Data and safeguard Developer Data from unauthorized, unlawful or accidental processing, access, disclosure, loss, alteration or destruction.

6.2. The parties acknowledge that security requirements are constantly changing, and that effective security requires frequent evaluation and regular improvement of outdated security measures. The security measures implemented and maintained by Decart.ai are further detailed in **Annex II**.

7. SECURITY INCIDENT

7.1. Decart.ai will notify the Developer without undue delay (and no later than 48 hours) upon becoming aware of any Security Incident concerning Developer Data and will take necessary steps to remediate, minimize any effects of and investigate any Security Incident and to identify its cause. Upon Developer's request, Decart.ai will reasonably co-operate with the Developer and provide the Developer with such assistance and information as it may reasonably require in connection with the containment, investigation, or mitigation of the Security Incident. Developer is solely responsible for determining whether to notify the relevant supervisory or regulatory authorities and impacted Data Subjects in relation to any Security Incident and for providing such notice.

7.2. Decart.ai will notify the Developer in writing and will keep the Developer informed of any material developments in connection with the Security Incident. Decart.ai's notification or compliance with its obligations under this Section shall not be construed as an acknowledgment by Decart.ai of any fault or liability with respect to the Security Incident.

8. AUDIT RIGHTS

8.1. Decart.ai shall maintain accurate written records of all categories of processing activities carried out on behalf of Developer under this DPA and shall make such records available to the supervisory authority as reasonably required under Data Protection Laws. In case such records are provided to Developer they shall be considered Decart.ai‘s confidential information and shall be subject to confidentiality obligations.

8.2. Developer may audit Decart.ai’s compliance with this DPA and Data Protection Laws by requesting a certificate issued for security verification reflecting the outcome of an audit conducted by a third party auditor (e.g.,ISO27001 certificate) or a comparable certification or other security certification of an audit conducted by a third-party auditor, within twelve (12) months as of the date of Developer's request.

8.3. Alternatively, in the event the records and documentation provided subject to Section 8.1

and 8.2 above are not sufficient for the purpose of demonstrating compliance, Decart.ai shall make available, solely upon prior reasonable written notice and no more than once per calendar year (except in case of severe data security incidents, e.g. data breaches resulting in a risk to the rights and freedoms of natural persons), to a reputable auditor nominated by the Developer, information necessary to reasonably demonstrate compliance with this DPA and Data Protection Laws, and shall allow for audits, including inspections, by such reputable auditor solely in relation to the Processing of the Developer Data ("**Audit**") in accordance with the terms and conditions hereunder. The auditor shall be subject to standard confidentiality obligations (including third parties). Decart.ai may object to an auditor appointed by the Developer in the event Decart.ai reasonably believes the auditor is not suitably qualified or is a competitor of Decart.ai. Developer shall bear all expenses related to the Audit and shall (and ensure that each of its auditors shall) over the course of such Audit, avoid causing any damage, injury, or disruption to Decart.ai's premises, equipment, personnel and business while its personnel are on those premises in the course of such Audit.

8.4. Nothing in this DPA will require Decart.ai to either disclose to Developer or its third-party auditor, or to allow Developer or its third-party auditor to access: (i) data related to other customers or partners; (ii) Decart.ai's internal accounting or financial information; (iii) any trade secret of Decart.ai or its Affiliates; (iv) any information that, in Decart's reasonable opinion, could compromise the security of any Decart.ai's systems or cause any breach of its obligations under applicable law or its security or privacy obligations to any third party; or (v) any information that Developer or its third-party auditor seeks to access for any reason other than the good faith fulfillment of Developer's obligations under the Data Protection Laws.

9. CROSS BORDER PERSONAL DATA TRANSFERS

9.1. Where European Data Protection Laws apply to the transfer of Personal Data from the EEA, UK or Switzerland, such transfers will be subject to measures as are necessary to ensure the transfer is in compliance with European Data Protection Laws, which include (without limitation) at least one of the following: (i) transferring such Personal Data to a recipient that is covered by a suitable framework or other legally adequate transfer mechanism recognized by the relevant authorities or courts as providing an adequate level of protection for Personal Data, including to an Adequate Country or data privacy and transfer frameworks such as the DPF; (ii) to a recipient that has achieved binding corporate rules authorization in accordance with applicable European Data Protection Law; or (iii) to a recipient that has executed the Standard Contractual Clauses.

9.2. When Developer and Decart.ai rely on the SCC to facilitate a transfer to a third country the following shall apply:

a) For Transfer of Personal Data from the EEA the EU SCC shall apply and completed as follows: **(1)** Module II (Controller to Processors) will apply; **(2)** In Clause 7 the optional docking clause will not apply; **(3)** In Clause 9, option 2 (general written authorization) shall apply for the Sub-Processors listed in the Sub-Processors list and the method for appointing Sub-Processor shall be as set forth in the Sub-Processing Section of the DPA; **(4)** In Clause 11, the optional language will not apply, and Data Subjects shall not be able to lodge a complaint with an independent dispute resolution body; **(5)** In Clause 17, option 1 shall apply, and the EU SCC shall be governed by the law of the Republic of Ireland; **(6)** In Clause 18(b) the parties choose the competent courts of the Republic of Ireland, as their choice of forum and jurisdiction; **(7) Annex I(A) of the EU SCC** is completed as follows: Developer is

the Data Exporter, Decart.ai is the Data Importer, the parties' contact details Agreement Effective Date; **Annex I(B) of the EU SCC** is completed as set out in Annex I of this DPA; **Annex I(C) of the EU SCC** shall identify the competent supervisory authority/ies as the supervisory authority Republic of Ireland; **(8) Annex II of the EU SCC** is deemed completed with the information set out in **Annex II** of this DPA; **(9) Annex III of the EU SCC** shall be completed with the list of Sub-Processors.

b) For transfer of Personal Data from the UK, the UK SCC shall apply and completed as follows: **(1) Table 1** shall be completed as set forth in section (a)(7) above; **(2) Table 2** shall be completed as set forth in Section (a)(1) - (a)(4) above; **(3) Tables 3** shall be completed as follows: **Annex 1A** shall be completed with relevant information as set out in Section (a)(7) above; **Annex 1B** shall be completed with relevant information as set out in **Annex I** of this DPA; **Annex II** shall be completed with relevant information as set out in the trust center; **Annex III** shall be completed with the list of sub-processors; **(4) Table 4** shall be completed with the "neither party" option; and **(5)** Any conflict between the terms of the EU SCC and the UK SCC will be resolved in accordance with Section 10 and Section 11 of the UK SCC.

c) For transfer of Personal Data from Switzerland, the Swiss SCC shall apply in with following modifications (i) references to "Regulation (EU) 2016/679" will be interpreted as references to the Swiss DPA; (ii) references to "EU", "Union" and "Member State law" will be interpreted as references to Swiss law; and (iii) references to the "competent supervisory authority" and "competent courts" will be replaced with the "the Swiss Federal Data Protection and Information Commissioner" and the "relevant courts in Switzerland".

10. TERM, TERMINATION AND CONFLICT

10.1. This DPA shall be effective as of the Effective Date and shall remain in force until the Agreement terminates or as long as Decart.ai Processes Developer Data.

10.2. Following the termination or expiration of this DPA, Decart.ai shall, upon Developer's written request, delete Developer Data Processed on behalf of the Developer and certify to the Developer that it has done so, or, return Developer Data to the Developer and delete existing copies, unless applicable law or regulatory requirements requires that Decart.ai continue to store Developer Data. Until the Developer Data is deleted or returned, the parties shall continue to ensure compliance with this DPA. In any case, Decart.ai reserves the right to delete any Developer Data 60-days from deletion of the Account.

10.3. In the event of a conflict between the terms and conditions of this DPA and the Agreement the Agreement shall prevail. For the avoidance of doubt, in the event Standard Contractual Clauses have been executed between the parties, the terms of the Standard Contractual Clauses shall prevail over those of this DPA. Except as set forth herein, all of the terms and conditions of the Agreement shall remain in full force and effect as between Developer and Decart.ai.

ANNEX I
DETAILS OF PROCESSING

This Annex I includes certain details of the Processing of Personal Data as required under the Data Protection Laws.

A. LIST OF PARTIES

Data exporter:

- Name: Developer's name as identified in the Account
- Address: Developer's address as identified in the Account
- Contact person's name and contact details: Developer's contact details as specified in the Account
- Activities relevant to the data transferred under these clauses: Receipt of the Services
- Signature and date: These clauses shall be deemed executed and entered into by Developer as of the DPA Effective Date.
- Role: The data exporter's role shall be Controller or Processor specified in Section 2.1 of the DPA.

Data importer:

- Name: Decart.ai Inc.
- Address: 1007 N Orange St, Fl 10, Wilmington, Delaware, 19801, United States.
- Contact person's name, position and contact details: dpo@decart.ai
- Activities relevant to the data transferred under these Clauses: Provision of the Services
- Signature and date: These clauses shall be deemed executed and entered into by Decart.ai as of the DPA Effective Date.
- Role: The data importer's role shall be Processor.

B. DESCRIPTION OF TRANSFER

Categories of Data Subjects:

The Developer, Authorized User or End Users or any individual that the Developer, Authorized User or End Users uploaded personal data about such individual while using the Services, as part of the Input.

Categories of Personal Data or Special Categories of Personal Data:

Any content, information, text or otherwise submitted through the Services (including within the Input), or behavior insights, engagement, and communication with the End User, Developer, or Authorized User (to the extent applicable).

Nature of the processing:

Collection, transmission, organization, communication, transfer, host and other types of processing for the purpose of providing the Services as set out and subject to the limitations in the Agreement by Decart.ai.

Purpose(s) of Processing:

To provide the Developer (including Authorized Users) to use the Services, including API access and use of LLM, and to enable the generation of Output in response to Input.

Retention Period:

Subject to the retention limitations set forth in the Agreement, Personal Data shall be retained for as long as it is necessary to provide the Services or as is required by applicable law. For clarity, Decart.ai does not use Input or Output to train, fine-tune, or improve artificial intelligence or machine learning models, and does not retain or use Input or Output for any other commercial purpose, except as required by applicable law.

Process Frequency:

Continuous basis.

ANNEX II

TECHNICAL AND OPERATIONAL SECURITY MEASURES

This Technical and Operational Security Measures Annex (**Security Annex**) forms part of, and is incorporated by reference into, the Data Processing Agreement ("DPA") between Decart.ai Inc. (Processor) and Developer (Customer). Capitalized terms used but not defined in this Security Annex have the meanings given in the DPA and in the Cogito API Service Terms available at: https://cogito.decart.ai/legal/terms ("**Agreement**") executed by and between Decart.ai and the Developer. This Security Annex describes the technical and organizational measures implemented and maintained by the Processor, in its capacity as a "processor", to ensure a level of security appropriate to the risk when providing API-based inference services for LLMs and related generative AI services that may Process the Customer's Personal Data on the Customer's behalf.

1. **Information Security Management System (ISMS).** Processor shall maintain an Information Security Management System (ISMS), including supporting policies and procedures, aligned with applicable security-related industry standards. The Processor's ISMS shall be designed to protect the confidentiality, integrity, and availability of the Services and Customer Personal Data, and to support the Processor's compliance with Applicable Laws relating to the Processing of Customer Personal Data and the provision of the Services.

2. **Substantial Identification and authentication mechanisms.** Processor shall ensure that access to the systems shall include substantial Identification and authentication mechanisms, including multi factor authentication mechanisms where required.

3. **Access Permissions.** Processor shall determine access permissions for authorized users to the Systems in accordance with each role's responsibilities. Access permissions shall be granted only to the extent required to perform the applicable role. The Processor shall keep an up-to-date record of roles, user permissions granted to such roles, and the authorized users performing such roles ("**Access Registry**"), and shall review the Access Registry to ensure proper management based on the role-based authorization concept. Immediately following the termination of an authorized user's role, the Processor shall revoke that user's permissions and, to the extent practicable, change passwords for any Systems to which the authorized user may have had access or knowledge of passwords.

4. **Access Control**. Processor shall establish and implement physical and electronic controls and safeguards to protect Systems used to manage, Process, or store Customer Personal Data against unauthorized access, disclosure, modification, destruction, interference, or downtime, in a manner consistent with industry standards. This includes ensuring that only authorized persons can access Customer Personal Data processing systems and that, during Processing, Customer Personal Data cannot be read, copied, modified, or deleted without authorization. Specific measures include:

    4.1. **Physical Access Control**. Processor utilizes third-party Sub-Processor cloud infrastructure providers to host and process Customer Personal Data. Customer acknowledges that physical access controls are maintained by such Sub-processors in accordance with their respective security certifications (e.g., SOC 2 Type II, ISO 27001). Processor shall monitor Sub-Processor's compliance through its sub-processor management program.

    4.2. **Electronic Access Control**. Processor shall monitor and record access to the systems used in connection with Customer Personal Data by implementing an appropriate automated monitoring mechanism for its systems ("**Monitoring**

Systems"). A record of each user's access to the Systems (a "**Log**") shall include: (i) the user's identity; (ii) the Customer Personal Data accessed and the time of the access attempt; (iii) the system component to which access was attempted; (iv) the access type and scope; and (v) whether access was granted or denied. The Monitoring Systems shall not permit disabling or modification of their operation and shall detect such modification or disabling and send alerts to those responsible. Logs shall be retained for at least twelve (12) months from the date of creation and shall be made available to Customer upon request for audit or investigation purposes. The Processor shall notify its authorized users of the existence of the Monitoring Systems.

5. **Security Operations.** Processor shall maintain a documented patch management plan or patching process and shall provide it to Customer upon request. The Processor shall update and apply security patches to its systems and endpoint devices on a regular basis.
6. **Secure Development/Code Review.** Processor shall follow a secure development lifecycle for its applications and systems. Processor shall conduct, or have an independent security organization conduct, an application security code review.
7. **Security Testing.** Processor shall conduct vulnerability scanning and penetration testing of applications and devices that handle Customer Personal Data at least annually. Processor shall remediate critical and high-level risks identified by such scans.
8. **Timely Response to Vulnerabilities.** Processor shall remediate, within industry best-practice timelines, security vulnerabilities that may impact Customer Personal Data.
9. **Network Security.** Processor shall maintain the security of the Systems in accordance with practices consistent with industry standards. Such security shall include, at a minimum: (i) the use of anti-virus and anti-malware systems; (ii) the use of firewall systems; and (iii) physically and logically segregating infrastructure that Processes Customer Personal Data from infrastructure that Processes non-Customer Personal Data.
10. **System Mapping and Risk Assessment.** Processor shall maintain up-to-date documentation detailing, with respect to Customer Personal Data and the Systems used to Process it, the following: (i) an up-to-date inventory of digital assets, including at least each asset's owner and risk level; and (ii) network topology. Processor shall conduct an information security risk assessment at least once every eighteen (18) months and shall update its information security procedures and safeguards accordingly.
11. **Endpoint Security Requirements.** Endpoint devices used by Processor to access Systems or exchange Customer Personal Data must meet Processor's security standards and the provisions of this Security Annex. This includes, without limitation, ensuring that: (i) anti-virus and anti-malware software is installed, active, and up to date; (ii) endpoint devices have strong password policies enforced; and (iii) disk encryption is enabled where applicable.
12. **Portable Devices Restrictions.** Processor shall continuously document the connection of portable devices of any type to Systems containing Customer Personal Data. Such connections and use shall be permitted only with prior authorization. Processor shall also ensure that downloading Customer Personal Data onto portable devices is prohibited.
13. **Secure Customer Personal Data Destruction and Return.** Processor shall retain Customer Personal Data only for the period necessary to provide the Services. Upon termination of the Agreement, Processor shall return to Customer all Customer Personal Data and delete it (including from its archives), unless otherwise requested by Customer in writing. If Customer provides written consent for Processor to retain Customer Personal Data after

termination, Processor shall retain Customer Personal Data in accordance with Processor's Customer Personal Data retention policy, subject to confidentiality obligations and applicable legal requirements.

14. **Backups.** Processor shall maintain a procedure for regular backups of Customer Personal Data and all relevant Systems and software. Such procedure shall ensure that: (i) Customer Personal Data is securely stored in backups using the same security protocols required for the primary environment; (ii) restoration of Customer Personal Data may be performed only with Customer's prior written permission; and (iii) Processor shall document any restoration, including the identity of the person who performed the restoration and details of the information restored.

15. **Sub-Processor Relationships.** Processor shall contractually flow down the material obligations of this Security Annex to each subcontractor utilized in the provision of the Services. Processor shall remain responsible for the acts and omissions of its subcontractors and shall regularly monitor, review, and audit subcontractor security controls.

16. **Annual Assessments, Audits, and Certifications.** Processor shall conduct annual information security assessments and audits of its systems and operations relevant to the Processing of Customer Personal Data. Processor represents and warrants that it maintains current SOC 2 Type 2, ISO 27001 and ISO 42001 certifications, and shall provide evidence of such certifications to Customer upon request and standard confidentially obligations.

17. **Human Resource Security.** Processor shall provide annual training to all personnel who have access to Customer Personal Data. Such training shall cover the protection of Customer Personal Data, applicable security procedures and protocols, and cyber security awareness. Processor shall ensure that such personnel are appropriately vetted and are bound by written confidentiality obligations, and that they complete such training prior to being granted access to Customer Personal Data.

18. **Incident Management Program.** Processor shall maintain and implement a documented information security event management process, including incident reporting, response, prioritization, escalation, and remediation.

19. **Business Continuity and Disaster Recovery.** Processor shall document and maintain a Business Continuity and Disaster Recovery Plan in accordance with industry best practices and consistent with industry standards and shall perform an annual disaster recovery plan exercise.

ANNEX III

LIST OF SUB-PROCESSORS

Name	Processing Activity	Sub-Processor Location
Amazon Web Services	Cloud provider	USA
Google Cloud Platform (GCP)	Cloud provider	USA
CoreWeave	Cloud provider	USA
Vercel	Hosting provider	USA
Neon	Database provider	USA
Stripe	Payment processor	USA
Resend	Email delivery provider	USA
Slack	Communication provider	USA
Google Sign-In	Authentication provider	USA
Datadog	Observability and monitoring provider	USA
PostHog	Analytics provider	USA