Data Processing Addendum

Last Updated: March 9, 2026

This Data Processing Addendum ("**DPA**") governs Cognition AI, Inc. ("**Licensor**")'s processing of Customer Personal Data that Licensor processes on behalf of and under the instruction of Customer through Licensor's enterprise or software services as applicable ("**Services**") under the terms of certain agreement(s) between Customer and Licensor governing the Customer's use of the Services (the "**Agreement**"), and is hereby incorporated into the Agreement. To the extent there is a conflict between the Agreement and this DPA, this DPA takes precedence unless the Agreement expressly overrides particular terms of this DPA.

1. **Definitions**. For the purposes of this DPA, the following terms shall have the meanings set out below. Capitalized terms used but not defined in this DPA shall have the meanings given in the Agreement. All other terms in this DPA not otherwise defined in the Agreement shall have the corresponding meanings given to them in Data Protection Laws.

   a. "**Account Data**" means Personal Data provided by or on behalf of Customer (including its users) solely for purposes of administering, provisioning, or managing the Customer's relationship with Licensor, including the names or contact information of individuals authorized by Customer to access Customer's account.

   b. "**Customer Data**" means (i) data, information, and other content, in any form or medium, that Customer (including its users) submits, posts, or otherwise transmits through the Services, or (ii) data that is generated and made available to Customer by the Services through use of such data, in each case excluding Account Data.

   c. "**Customer Personal Data**" means any Personal Data included within Customer Data that Licensor processes on behalf of Customer to provide the Services that is defined as "personal data", "personal information" or similar terms under any Data Protection Law.

   d. "**Data Protection Laws**" means, as applicable, EU/UK Privacy Laws, US Privacy Laws and any similar law of any other jurisdiction which relates to data protection, privacy or the processing of Personal Data, in each case, as applicable and in force from time to time, and as amended, consolidated, re-enacted or replaced from time to time.

   e. "**EU/UK Privacy Laws**" means, as applicable: (i) the General Data Protection Regulation 2016/679 (the "**GDPR**"); (ii) the Privacy and Electronic Communications Directive 2002/58/EC; (iii) the UK Data Protection Act 2018, the UK General Data Protection Regulation as defined by the UK Data Protection Act 2018 as amended by the Data Protection, Privacy and Electronic Communications (Amendments etc.) (EU Exit) Regulations 2019 (together with the UK Data Protection Act 2018, the "UK GDPR"), and the Privacy and Electronic Communications Regulations 2003; and (iv) any relevant law, directive, order, rule, regulation or other binding instrument which implements any of the above, in each case, as applicable and in force from time to time, and as amended, consolidated, re-enacted or replaced from time to time.

   f. "**US Privacy Laws**" means, as applicable, the California Consumer Privacy Act ("**CCPA**"), Colorado Privacy Act, Connecticut Data Privacy Act, Delaware Personal Data Privacy Act, Florida Digital Bill of Rights, Indiana Consumer Data Protection Act, Iowa Consumer Data Protection Act, Montana Consumer Data Privacy Act, Oregon Consumer Privacy Act, Tennessee Information Protection Act, Texas Data Privacy and Security Act, Utah Consumer Privacy Act, and Virginia Consumer Data Protection Act, and any similar law of any other state related to the processing of Personal Data.

2. **Relationship and Roles of the Parties**

   a. **Licensor as a Processor**. Customer is the entity that determines the purposes and means for which Customer Personal Data is processed ("**Data Controller**"), and Licensor processes Customer Personal Data on the Data Controller's behalf and in accordance with the Data Controller's written instructions ("**Data Processor**"). The terms "Data Controller" and "Data

Processor" shall have the same meaning as those similar concepts used in applicable Data Protection Laws. Licensor and Customer each agree to comply with their respective obligations under Data Protection Laws.

b. **Licensor as an Independent Controller of Account Data**. Notwithstanding anything to the contrary in this DPA, the parties acknowledge and agree that Licensor may process Account Data as a Data Controller solely to (a) manage and administer its relationship with Customer, including business user access management and account provisioning; (b) detect, prevent, or investigate security incidents, fraud, and other abuse or misuse of the Services; and (c) comply with applicable legal or regulatory obligations. In each case in accordance with applicable Data Protection Law, this DPA, the Agreement, and the Licensor Privacy Policy.

3. **Customer Personal Data Processing Requirements**. Licensor agrees to use Customer Personal Data solely for the nature, purpose, and duration of the processing identified in the Agreement and in this DPA. For clarity, as Data Processor, Licensor will not sell or share Customer Personal Data, nor will Licensor use, disclose, retain, or otherwise process Customer Personal Data (i) for a purpose other than the specific purpose of providing the Services; (ii) outside of the direct business relationship between Licensor and Customer and the written instructions received from Customer; and (iii) in a manner inconsistent with applicable Data Protection Laws. The parties agree that any Customer Personal Data exchanged between them in connection with the Agreement is not consideration from either party to the other with respect to the Agreement or otherwise. Where the Customer Personal Data is subject to the CCPA, Licensor will not combine any Customer Personal Data with any Personal Data that Licensor receives from or on behalf of another party, or collects from its own interactions with individuals, except as otherwise permitted under the CCPA. The foregoing sentence does not apply to Customer Personal Data that has been anonymized, aggregated, or de-identified to the extent the Agreement permits or instructs Licensor to process or use Customer Personal Data that is anonymized, aggregated, or de-identified. In such cases, Licensor will (i) adopt reasonable measures to prevent such de-identified data from being used to infer information about, or otherwise being linked to, a particular natural person or household; (ii) not make attempts to re-identify the information, except solely for the purpose of determining whether its de-identification process function as designed; and (iii) before sharing de-identified data with any other party, contractually obligate such recipients to comply with the requirements of this/provision.

4. **Subprocessors**. Licensor may disclose Customer Personal Data to Licensor's sub-processors as necessary to deliver the Services or to help satisfy its obligations in accordance with this DPA ("**Subprocessor**"), and Customer hereby consents to the use of such Subprocessors. Licensor will enter into contractual arrangements with each Subprocessor binding them to provide a comparable level of data protection to that provided for in the Agreement and this DPA. Licensor agrees to be liable for the acts and omissions of its Subprocessors to the same extent Licensor would be liable under the terms of the DPA if it performed such acts or omissions itself, subject to the limitations of liabilities set forth in the Agreement. A list of Licensor's current Subprocessors is set forth in Appendix C to this DPA. Licensor may update Appendix C from time to time by posting an updated DPA on its website. If Customer objects to a newly added Subprocessor on reasonable grounds relating to the protection of Customer Personal Data, Customer may cease use of the Services. Continued use of the Services after an update to Appendix C constitutes Customer's acceptance of the updated Subprocessor list.

5. **Notifications to Customer**. Licensor will inform Customer if Licensor determines that an instruction from Customer violates any applicable Data Protection Laws and/or if Licensor can no longer meet its obligations under this DPA. If Licensor is required by Data Protection Laws to process any Customer Personal Data for reasons outside of the Agreement, Licensor will inform Customer in advance of any such processing, unless prohibited by law. Licensor will provide Customer prompt notice if Licensor becomes aware of a legally required request for disclosure of Customer Personal Data to law enforcement authorities, unless prohibited by law.

6. **Data Subject Rights**. If Customer's data subjects submit a complaint or request with respect to access to or the rectification, erasure, restriction, portability, objection, blocking, or deletion of Customer Personal Data directly to Licensor, Licensor will inform the Customer and will not

respond to such a request without Customer's prior written authorization. Licensor will provide reasonable assistance to Customer, by appropriate technical and organization measures, insofar as this is possible, to provide information necessary to respond to such requests.

7. **Security and Breach Prevention**. Licensor will maintain reasonable and appropriate organizational and technical security measures to protect against unauthorized or accidental access, loss, alteration, disclosure or destruction of Customer Personal Data, and protect the rights of the Customer Personal Data subjects. Licensor will take steps to ensure that Licensor personnel are protecting the security, privacy, and confidentiality of Customer Personal Data consistent with the requirements of this DPA, and require that persons employed by Licensor and other persons engaged to perform on its behalf to be subject to a duty of confidentiality with respect to the Customer Personal Data and to comply with the data protection obligations applicable to Licensor under the Agreement and this DPA. Licensor will inform Customer without undue delay if Licensor becomes aware of any breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or unauthorized access to Customer Personal Data processed by Licensor for Customer ("**Data Breach Incident**") by Licensor, its Subprocessors, or any other third parties acting on Licensor's behalf. Licensor will provide reasonable assistance to Customer for investigation of any Data Breach Incident.

8. **Customer Assistance, Audits, and Assessments**. Licensor will cooperate with assessments or audits performed by or on behalf of Customer to confirm that Licensor is processing Customer Personal Data in a manner consistent with this DPA and Data Privacy Laws ("**Audits**") on the condition that: (i) the Audit is required by law; (ii) where permitted by law, Licensor may first provide a summary of the results of a third-party audit or certification report ("**Third-Party Certification**") to demonstrate compliance with its obligations under this DPA or Applicable Data Protection Laws; (iii) the Audit occurs if such Third-Party Certification is not sufficient to demonstrate Licensor's compliance with the obligations set out in this DPA and applicable Data Protection Laws; (iv) Licensor is given at least 30 days advance written notice of the Audit; (v) the parties mutually agree upon the scope, time, and duration of the Audit; (vi) the Audit is at the Customer's sole expense; and (vii) the Audit is conducted in a manner that is minimally disruptive to Licensor's business. Any information provided to Customer under this section, such as results of such Audits and any Third-Party Certifications, shall be the Confidential Information of Licensor. Where required by law, Licensor grants Customer the right to stop and remediate unauthorized use of Customer Personal Data. Licensor will provide commercially reasonable assistance to Customer for the preparation of data protection impact assessments with respect to the processing of Customer Personal Data by Licensor, and where necessary, provide consultations with any supervisory authority with jurisdiction over such processing.

9. **Customer Obligations**. Customer represents and warrants that it has and will maintain throughout the term all necessary rights, consents, and authorizations to provide Customer Personal Data to Licensor, and that it shall only transfer Customer Personal Data to Licensor using secure, reasonable and appropriate mechanisms to the extent these mechanisms are within Customer's control. Customer authorizes Licensor to use, disclose, retain, and otherwise process Customer Personal Data as contemplated by the Agreement, this DPA, and/or other processing instructions provided by Customer to Licensor. Customer acknowledges and agrees that Customer, not Licensor, is responsible for certain design and configuration decisions related to the Services, and the secure implementation of these decisions that complies with applicable Data Protection Laws.

10. **International Transfers**. Licensor will process Customer Personal Data only on documented instructions from Customer, including transfers to a third country or an international organization, unless required to do so by applicable Data Protection Laws. Where Customer Personal Data that originates in the European Economic Area is transferred to a country outside of Europe that is not subject to an adequacy decision, Licensor will do so in accordance with the standard contractual clauses adopted by the EU Commission on June 4, 2021 ("**SCC**") which are hereby incorporated into this DPA by reference and deemed entered into and completed as follows: (i) Module 2 (Controller to Processor) of the SCCs apply when Customer is a controller and Licensor is processing Customer Personal Data as a processor; (ii) Module 3 (Processor to Processor) of the SCCs apply when the Customer is a processor and Licensor is processing Customer Personal Data

as a subprocessor. For each of these modules, the following applies: (a) Clause 7 (Docking Clause) does not apply; (b) In Clause 9(a), Option 2 (General Written Authorization) is selected, and the minimum time period for prior notice shall be as set forth in Section 7 of this DPA; (c) the optional language in Clause 11 (Redress) does not apply; (d) the square brackets (“\[“ and “\]”) in Clause 13 (Supervision) are hereby removed; (e) In Clause 17 (Governing Law), Option 1 is selected, and the parties agree that the SCCs will be governed by the law of the EU member state in which the data exporter is located; (f) in Clause 18 (Choice of Forum and Jurisdiction), the parties agree that any disputes arising from the SCCs shall be resolved by the courts of the EU member state in which the data exporter is located. The information required in Annex I and II of the SCCs are included in Appendix A and B of this DPA. Customer Personal Data that originates from Switzerland and is transferred to a country outside of Switzerland that is not subject to an adequacy decision shall be processed in accordance with the SCCs, with the following changes: (I) the term “EU member state” must not be interpreted to exclude data subjects from bringing legal proceedings before the courts in their place of habitual residence of Switzerland in accordance with Clause 18(c); and (II) the Swiss Federal Data Protection and Information Commissioner shall act as the competent supervisory authority insofar as the relevant data transfer is governed by the Swiss Federal Act on Data Protection. For Customer Personal Data transfers originating from the United Kingdom and to a country outside of the United Kingdom that is not subject to an adequacy decision, the parties will comply with the terms of the Mandatory Clauses of the Approved Addendum, being the template Addendum B.1.0 issued by the Information Commissioner’s Office and laid before Parliament in accordance with s119A of the Data Protection Act 2018 on February 2, 2022, as revised under Section 18 of the Mandatory Clauses (“**UK Addendum**”). The information required for Part One of the UK Addendum is set out in Appendix A of this DPA, as applicable. For the purposes of Table 4 of Part One of the UK Addendum, either party may end the UK Addendum when it changes.

11. **Term and Termination**. This DPA will remain in effect for as long as Licensor is processing Customer Personal Data on Customer’s behalf, or until the termination of the Agreement, and all Customer Personal Data has been returned or deleted in accordance with this DPA. Upon termination of this DPA, Licensor will direct each Subprocessor to delete Customer Personal Data within thirty (30) days of the termination, unless prohibited by law. To the extent Licensor is required to retain any Customer Personal Data to comply with applicable legal or regulatory obligations, including record retention requirements, Licensor will isolate and protect such data for further processing and delete it as soon as such obligations are satisfied.

APPENDIX A: COGNITION AI DPA

SCC ANNEX I

-

LIST OF PARTIES

Data Exporter(s): Customer
Role: For the purposes of SCC Module 2, Customer is a controller. For the purposes of SCC Module 3, Customer is a processor.

Data Importer(s): Identity and contact details of the data importer(s), including any contact person with responsibility for data protection.

Company Name: Cognition AI, Inc.

Address: 550 Third Street, San Francisco, CA 94107

Contact person's name, position, and contact details: Sampriti Panda, Head of Security, sampriti@cognition.ai

Activities relevant to the data transferred under these Clauses: Performance of the Services pursuant to the Agreement.

Role: Processor

-

DESCRIPTION OF TRANSFER

Categories of data subjects whose personal data is transferred

Any data subjects whose Personal Data is processed by Licensor on behalf of Customer to provide Services.

Categories of personal data transferred

Any categories of Customer Personal Data processed on behalf of Customer when providing Services such as any Personal Data included in Customer Data (as defined in the Agreement), or otherwise accessed by Licensor when providing support.

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

No sensitive data is intended to be transferred, unless a user voluntarily and unexpectedly submits it.

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

Continuous.

Nature of the processing

The performance of the Services as described in the Agreement.

Purpose(s) of the data transfer and further processing

The performance of the Services as described in the Agreement.

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

During the term of the Agreement.

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

The performance of the Services as described in the Agreement.

-

COMPETENT SUPERVISORY AUTHORITY

Identify the competent supervisory authority/ies in accordance with Clause 13

The data protection authority of the EU member state in which the data exporter is located.

APPENDIX B: COGNITION AI DPA

SCC ANNEX II

-

TECHNICAL AND ORGANIZATIONAL MEASURES TO ENSURE THE SECURITY OF THE DATA

Licensor has put in place technical and organizational security measures to protect Customer Personal Data:

Authentication and Authorization Controls. Licensor maintains best practices for authenticating and authorizing employee permissioning and service access:

- Licensor uses single sign-on (SSO) to authenticate to third-party services. Role Based Access Controls (RBAC) are used when provisioning internal access to the Services via Okta;

- Multi-factor authentication is used by employees;

- Review and approval processes for any access requests to services storing Customer Personal Data;* Established procedures for promptly revoking access rights upon employee separation;

- Use of a third-party identity access management service to manage Customer identity (SSO);

- Separation of Customer Personal Data by organization account.

Security. Licensor maintains best practices for securing and operating its cloud infrastructure, including the following measures:

- Separate production and non-production environments;

- Primary backend resources are deployed behind a VPN;

- All employees are issued company devices and prohibited from using personal devices;

- All devices are provisioned via MDM, and devices are protected in the event of physical loss;

- Keys for cryptographic protected are securely managed and stored in AWS KMS;

- Services logs are monitored for security and availability;

- Licensor's maintains the following policies and standards: (1) information security policy; (2) computer and network security policy; (3) access control policy; (4) asset management policy; (5) incident management response policy;

- Licensor maintains a SOC 2 Type I certification.

Data Controls. Licensor maintains best practices to prevent the unauthorized reading, modification or disclosure of data at rest and during transfer:

- All data transmission is encrypted in transit and at rest;

- Production software is routinely monitored via logging, error handling and monitoring dashboards of live metrics. Unusual application states (ie. unusually high error rates, slowness, failures) trigger alerts which are promptly investigated;

- Employee access to the Services follows the principle of least privilege, such that only employees with the relevant roles have access to the Services environment;

- Customer Personal Data submitted to the Services is only used in accordance with the terms of the DPA, Agreement, and any other applicable contractual agreements in place with Customer.

Personnel. Licensor ensures all personnel are vetted and trained with respect to security practices.

- Licensor requires all personnel to complete security training at least annually;

- All employees are run through background checks.

APPENDIX C

LIST OF SUBPROCESSORS

Entity	Purpose	Location
Microsoft Azure *	core processing	United States
AWS *	core processing, profile data, logs, and indices	United States
Google Cloud **	core processing, profile data, logs, and indices	United States
Auth0 *	profile data	United States
Sentry **	system logs	United States
Datadog **	system logs	United States
Zendesk ***	support contacts	United States
Pylon ***	support contacts	United States
Decagon ***	Support Chatbot	United States
Agumbe (Cognition India) ***	Support Workflow	India

* Devin only
** Windsurf Only
*** Devin and Windsurf

The following entities to the extent Customer Personal Data is included in the Customer Data submitted as input to The Cognition Platform.

Entity	Purpose	Location
OpenAI **	core processing	United States
Anthropic **	core processing	United States
Google/Vertex *	core processing	United States
AWS/Bedrock *	core processing	United States
Databricks *	core processing	United States
xAI *	core processing	United States
Snowflake *	core processing	United States

* Windsurf Only, if enabled
** Devin and Windsurf (if enabled as to Windsurf)

Devin for Terminal (CLI) may use subprocessors for both Devin and Windsurf