

Data Processing Addendum

Effective Date: June 2026

This Data Processing Addendum ("DPA") supplements the Terms and Conditions or other written agreement governing Customer's use of the Services (the "Agreement") entered into by and between Customer and Poll the People, Inc. (dba: CustomGPT.ai) ("Company"). This DPA is incorporated into the Agreement and applies automatically where Customer's use of the Services involves the processing of Personal Data. Customer enters into this DPA on behalf of itself and, to the extent required under applicable Data Protection Laws, in the name and on behalf of its Affiliates, if any. This DPA incorporates the terms of the Agreement, and any terms not defined in this DPA have the meanings set forth in the Agreement.

1. Definitions

1.1 "Affiliate" means (i) an entity of which a party directly or indirectly owns fifty percent (50%) or more of the stock or other equity interest, (ii) an entity that owns at least fifty percent (50%) or more of the stock or other equity interest of a party, or (iii) an entity which is under common control with a party by having at least fifty percent (50%) or more of the stock or other equity interest of such entity and a party owned by the same person, but such entity shall only be deemed to be an Affiliate so long as such ownership exists.

1.2 "Authorized Subprocessor" means a third party who has a need to know or otherwise access Customer's Personal Data to enable Company to perform its obligations under this DPA or the Agreement, and who is either (1) listed in Exhibit B or on Company's then-current subprocessor list, or (2) subsequently authorized under Section 4.2 of this DPA.

1.3 "Company Account Data" means personal data that relates to Company's relationship with Customer, including the names or contact information of individuals authorized by Customer to access Customer's account and billing information of individuals that Customer has associated with its account. Company Account Data also includes any data Company may need to collect for the purpose of managing its relationship with Customer, identity verification, or as otherwise required by applicable laws and regulations.

1.4 "Company Usage Data" means Service usage data collected and processed by Company in connection with the provision of the Services, including without limitation data used to identify the source and destination of a communication, activity logs, and data used to optimize and maintain performance of the Services, and to investigate and prevent system abuse; provided, however, that Company Usage Data shall not include Customer content, prompts, outputs, uploaded documents, Confidential Information, Personal Data, or other information that identifies Customer or Customer users.

1.5 "Data Exporter" means Customer.

1.6 "Data Importer" means Company.

1.7 "Data Protection Laws" means any applicable laws and regulations in any relevant jurisdiction relating to the use or processing of Personal Data, including: (i) the California Consumer Privacy Act of 2018, as amended by the California Privacy Rights Act of 2020 ("CCPA"), (ii) the General Data Protection Regulation (Regulation (EU) 2016/679) ("EU GDPR") and the EU GDPR as it forms part of the law of England and Wales by virtue of section 3 of the European Union (Withdrawal) Act 2018 (the "UK GDPR") (together, collectively, the "GDPR"), (iii) the Swiss Federal Act on Data Protection, (iv) the UK Data Protection Act 2018, (v) the Privacy and Electronic Communications (EC Directive) Regulations 2003, and (vi) applicable U.S. State Privacy Laws, in each case, as updated, amended or replaced from time to time. The terms "Data Subject", "Personal Data", "Personal Data Breach", "processing", "processor", "controller", and "supervisory authority" shall have the meanings set forth in the GDPR.

1.8 "Data Privacy Framework" means, as applicable, the EU-U.S. Data Privacy Framework, the UK Extension to the EU-U.S. Data Privacy Framework, and/or the Swiss-U.S. Data Privacy Framework.

1.9 "EU SCCs" means, as applicable, the standard contractual clauses approved by the European Commission in Commission Decision 2021/914 dated 4 June 2021, for transfers of personal data to countries not otherwise recognized as offering an adequate level of protection for personal data by the European Commission (as amended and updated from time to time), as modified by Section 5.3 of this DPA.

1.10 "ex-EEA Transfer" means the transfer of Personal Data, which is processed in accordance with the GDPR, from the Data Exporter to the Data Importer (or its premises) outside the European Economic Area (the "EEA"), where such transfer is not governed by an adequacy decision made by the European Commission in accordance with the relevant provisions of the GDPR.

1.11 "ex-UK Transfer" means the transfer of Personal Data covered by Chapter V of the UK GDPR, which is processed in accordance with the UK GDPR and the Data Protection Act 2018, from the Data Exporter to the Data Importer (or its

premises) outside the United Kingdom (the "UK"), where such transfer is not governed by an adequacy decision made by the Secretary of State in accordance with the relevant provisions of the UK GDPR and the Data Protection Act 2018.

1.12 "Services" has the meaning set forth in the Agreement.

1.13 "Standard Contractual Clauses" means the EU SCCs and the UK SCCs.

1.14 "UK Addendum" has the meaning set forth in Exhibit D.

1.15 "UK SCCs" means, as applicable, the EU SCCs, as amended by the UK Addendum.

1.16 "U.S. State Privacy Laws" means any applicable U.S. state privacy, consumer data protection, or consumer health data privacy law, including the CCPA and other similar laws, in each case as amended or replaced from time to time.

2. Relationship of the Parties; Processing of Data

2.1 The parties acknowledge and agree that with regard to the processing of Personal Data, Customer may act either as a controller or processor and, except as expressly set forth in this DPA or the Agreement, Company is a processor. Customer shall, in its use of the Services, at all times process Personal Data, and provide instructions for the processing of Personal Data, in compliance with Data Protection Laws. Customer shall ensure that the processing of Personal Data in accordance with Customer's instructions will not cause Company to be in breach of the Data Protection Laws. Customer is solely responsible for the accuracy, quality, and legality of (i) the Personal Data provided to Company by or on behalf of Customer, (ii) the means by which Customer acquired any such Personal Data, and (iii) the instructions it provides to Company regarding the processing of such Personal Data. Customer shall not provide or make available to Company any Personal Data in violation of the Agreement or otherwise inappropriate for the nature of the Services, and shall indemnify Company from all claims and losses in connection therewith.

2.2 Company shall not process Personal Data (i) for purposes other than those set forth in the Agreement and/or Exhibit A, (ii) in a manner inconsistent with the terms and conditions set forth in this DPA or any other documented instructions provided by Customer, including with regard to transfers of Personal Data to a third country or an international organization, unless required to do so by a Supervisory Authority or applicable law to which Company is subject; in such a case, Company shall inform Customer of that legal requirement before processing, unless that law prohibits such information on important grounds of public interest, or (iii) in violation of Data Protection Laws. Customer hereby instructs Company to process Personal Data in accordance with the foregoing and as part of any processing initiated by Customer in its use of the Services.

2.3 The subject matter, nature, purpose, and duration of this processing, as well as the types of Personal Data collected and categories of Data Subjects, are described in Exhibit A to this DPA.

2.4 Company shall not use Customer Data, Customer Personal Data, prompts, outputs, uploaded content, or other Customer-specific information to train, fine-tune, improve, benchmark, or develop any artificial intelligence model, large language model, or other product or service, except solely as necessary to provide the Services to Customer.

2.5 Following completion of the Services, and in any event within thirty (30) days following termination or expiration of the Services, at Customer's choice, Company shall return or securely delete Customer's Personal Data, unless further storage of such Personal Data is required or authorized by applicable law. Such deletion shall include Customer Personal Data held by Company and its subprocessors. If return or destruction is impracticable or prohibited by law, rule or regulation, Company shall take measures to block such Personal Data from any further processing (except to the extent necessary for its continued hosting or processing required by law, rule or regulation) and shall continue to appropriately protect the Personal Data remaining in its possession, custody, or control. If Customer and Company have entered into Standard Contractual Clauses as described in Section 5 (Transfers of Personal Data), the parties agree that the certification of deletion of Personal Data that is described in Clause 8.1(d) and Clause 8.5 of the EU SCCs (as applicable) shall be provided by Company to Customer only upon Customer's request. Notwithstanding the foregoing, Company may retain Personal Data: (a) in backup systems for up to ninety (90) days following deletion from production, after which such data will be overwritten in the ordinary course; (b) as reasonably necessary to investigate or respond to security incidents; (c) as reasonably necessary to establish, exercise, or defend legal claims; and (d) in aggregated or de-identified form that does not identify Customer or any Data Subject. Personal Data retained under (a)-(c) will remain subject to the protections of this DPA and will be deleted promptly when the applicable purpose is fulfilled.

2.6 U.S. State Privacy Laws. To the extent Customer Personal Data is subject to any applicable U.S. State Privacy Laws, the parties agree that such processing shall be carried out in accordance with Exhibit E.

3. Confidentiality

Company shall ensure that any person it authorizes to process Personal Data has agreed to protect Personal Data in accordance with Company's confidentiality obligations in the Agreement. Customer agrees that Company may disclose

Personal Data to its advisers, auditors or other third parties as reasonably required in connection with the performance of its obligations under this DPA, the Agreement, or the provision of Services to Customer.

4. Authorized Subprocessors

4.1 Customer acknowledges and agrees that Company may (1) engage its Affiliates and Authorized Subprocessors to access and process Personal Data in connection with the Services and (2) from time to time engage additional third parties for the purpose of providing the Services, including without limitation the processing of Personal Data. By way of this DPA, Customer provides general written authorization to Company to engage subprocessors as necessary to perform the Services.

4.2 A list of Company's current Authorized Subprocessors (the "List") will be made available to Customer, either attached hereto, at a link provided to Customer, via email or through another means made available to Customer. Such List may be updated by Company from time to time. Company may provide a mechanism to subscribe to notifications of new Authorized Subprocessors and Customer agrees to subscribe to such notifications where available. At least thirty (30) days before enabling any third party other than existing Authorized Subprocessors to access or participate in the processing of Personal Data, Company will add such third party to the List and notify Customer via email. Customer may object to such an engagement by informing Company within thirty (30) days of receipt of the aforementioned notice, provided such objection is in writing and based on reasonable grounds relating to data protection. Customer acknowledges that certain subprocessors are essential to providing the Services and that objecting to the use of a subprocessor may prevent Company from offering the Services to Customer.

4.3 If Customer reasonably objects to an engagement in accordance with Section 4.2, and Company cannot provide a commercially reasonable alternative within a reasonable period of time, Customer may discontinue the use of the affected Service by providing written notice to Company. Discontinuation shall not relieve Customer of any fees owed to Company under the Agreement.

4.4 If Customer does not object to the engagement of a third party in accordance with Section 4.2 within thirty (30) days of notice by Company, that third party will be deemed an Authorized Subprocessor for the purposes of this DPA.

4.5 Company will enter into a written agreement with each Authorized Subprocessor imposing on the Authorized Subprocessor data protection obligations comparable to those imposed on Company under this DPA with respect to the protection of Personal Data. If an Authorized Subprocessor fails to fulfill its data protection obligations under such written agreement with Company, Company will remain liable to Customer for the performance of the Authorized Subprocessor's obligations under such agreement.

4.6 If Customer and Company have entered into Standard Contractual Clauses as described in Section 5 (Transfers of Personal Data), (i) the above authorizations will constitute Customer's prior written consent to the subcontracting by Company of the processing of Personal Data if such consent is required under the Standard Contractual Clauses, and (ii) the parties agree that copies of the agreements with Authorized Subprocessors that must be provided by Company to Customer pursuant to Clause 9(c) of the EU SCCs may have commercial information, or information unrelated to the Standard Contractual Clauses or their equivalent, removed by Company beforehand, and that such copies will be provided by Company only upon request by Customer.

5. Security of Personal Data

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, Company shall maintain appropriate technical and organizational measures to ensure a level of security appropriate to the risk of processing Personal Data. Exhibit C sets forth additional information about Company's technical and organizational security measures.

5.1 Transfers of Personal Data

The parties agree that Company may transfer Personal Data processed under this DPA outside the EEA, the UK, or Switzerland as necessary to provide the Services. Customer acknowledges that Company's primary processing operations take place in the United States, and that the transfer of Customer's Personal Data to the United States is necessary for the provision of the Services to Customer. If Company transfers Personal Data protected under this DPA to a jurisdiction for which the European Commission has not issued an adequacy decision, Company will ensure that appropriate safeguards have been implemented for the transfer of Personal Data in accordance with Data Protection Laws.

5.2 Ex-EEA Transfers

The parties agree that ex-EEA Transfers will be made pursuant to the EU SCCs, which are deemed entered into and incorporated into this DPA by reference and completed as set forth below. To the extent Company is certified to and relies upon the Data Privacy Framework for an applicable transfer, such transfer may also be made pursuant to the Data Privacy Framework.

5.2.1 Module One (Controller to Controller) of the EU SCCs apply when Company is processing Personal Data as a controller pursuant to Section 7 of this DPA.

5.2.2 Module Two (Controller to Processor) of the EU SCCs apply when Customer is a controller and Company is processing Personal Data for Customer as a processor pursuant to Section 2 of this DPA.

5.2.3 Module Three (Processor to Subprocessor) of the EU SCCs apply when Customer is a processor and Company is processing Personal Data on behalf of Customer as a subprocessor.

5.3 SCC Completion

5.3.1 The optional docking clause in Clause 7 does not apply.

5.3.2 In Clause 9, Option 2 (general written authorization) applies, and the minimum time period for prior notice of subprocessor changes shall be as set forth in Section 4.2 of this DPA.

5.3.3 In Clause 11, the optional language does not apply.

5.3.4 All square brackets in Clause 13 are hereby removed.

5.3.5 In Clause 17 (Option 1), the EU SCCs will be governed by Ireland law.

5.3.6 In Clause 18(b), disputes will be resolved before the courts of Ireland.

5.3.7 Exhibit B to this DPA contains the information required in Annex I and Annex III of the EU SCCs.

5.3.8 Exhibit C to this DPA contains the information required in Annex II of the EU SCCs.

5.3.9 By entering into this DPA, the parties are deemed to have signed the EU SCCs incorporated herein, including their Annexes.

5.4 Ex-UK Transfers

The parties agree that ex-UK Transfers will be made pursuant to the UK SCCs, which are deemed entered into and incorporated into this DPA by reference, and amended and completed in accordance with the UK Addendum incorporated herein as Exhibit D. To the extent Company is certified to and relies upon the Data Privacy Framework, including the UK Extension, for an applicable transfer, such transfer may also be made pursuant to the Data Privacy Framework.

5.5 Supplementary Measures

5.5.1 If, after the date of this DPA, the Data Importer receives any request from a law enforcement or government agency for Customer's Personal Data (a "Government Agency Request"), Company shall attempt to redirect the law enforcement or government agency to request that data directly from Customer. As part of this effort, Company may provide Customer's basic contact information to the government agency. If compelled to disclose Customer's Personal Data to a law enforcement or government agency, Company shall give Customer reasonable notice of the demand and cooperate to allow Customer to seek a protective order or other appropriate remedy unless Company is legally prohibited from doing so. Company shall not voluntarily disclose Personal Data to any law enforcement or government agency. Data Exporter and Data Importer shall, as soon as reasonably practicable, discuss and determine whether all or any transfers of Personal Data pursuant to this DPA should be suspended in light of such Government Agency Requests.

5.5.2 The Data Exporter and Data Importer will meet regularly to consider whether: (i) the protection afforded by the laws of the country of the Data Importer to data subjects whose Personal Data is being transferred is sufficient to provide broadly equivalent protection to that afforded in the EEA or the UK, whichever the case may be; (ii) additional measures are reasonably necessary to enable the transfer to be compliant with the Data Protection Laws; and (iii) it is still appropriate for Personal Data to be transferred to the relevant Data Importer, taking into account all relevant information available to the parties, together with guidance provided by supervisory authorities.

5.5.3 If Data Protection Laws require the Data Exporter to execute the Standard Contractual Clauses applicable to a particular transfer of Personal Data to a Data Importer as a separate agreement, the Data Importer shall, on request of the Data Exporter, promptly execute such Standard Contractual Clauses incorporating such amendments as may reasonably be required by the Data Exporter to reflect the applicable appendices and annexes, the details of the transfer, and the requirements of the relevant Data Protection Laws.

5.5.4 If either (i) any of the means of legitimizing transfers of Personal Data outside of the EEA or UK set forth in this DPA ceases to be valid or (ii) any supervisory authority requires transfers of Personal Data pursuant to those means to be suspended, then Data Importer may by notice to the Data Exporter, with effect from the date set out in such notice, amend or put in place alternative arrangements in respect of such transfers, as required by Data Protection Laws.

5.6 Rights of Data Subjects

Company shall, to the extent permitted by law, notify Customer upon receipt of a request by a Data Subject to exercise the Data Subject's right of access, rectification, erasure, data portability, restriction or cessation of processing, withdrawal of consent to processing, and/or objection to being subject to processing that constitutes automated decision-making (such requests individually and collectively, "Data Subject Requests"). If Company receives a Data Subject Request in relation to Customer's data, Company will advise the Data Subject to submit their request to Customer and Customer will be responsible for responding to such request, including, where necessary, by using the functionality of the Services. Customer is solely responsible for ensuring that Data Subject Requests for erasure, restriction or cessation of processing, or withdrawal of consent to processing of any Personal Data are communicated to Company, and, if applicable, for ensuring that a record of consent to processing is maintained with respect to each Data Subject.

5.7 Data Subject Request Assistance

Company shall, at the request of Customer, and taking into account the nature of the processing applicable to any Data Subject Request, apply appropriate technical and organizational measures to assist Customer in complying with Customer's obligation to respond to such Data Subject Request and/or in demonstrating such compliance, where possible, provided that (i) Customer is itself unable to respond without Company's assistance and (ii) Company is able to do so in accordance with all applicable laws, rules, and regulations. Customer shall be responsible to the extent legally permitted for any costs and expenses arising from any such assistance by Company.

6. Actions and Access Requests; Audits

6.1 Company shall, taking into account the nature of the processing and the information available to Company, provide Customer with reasonable cooperation and assistance where necessary for Customer to comply with its obligations under the Data Protection Laws to conduct a data protection impact assessment and/or to demonstrate such compliance, provided that Customer does not otherwise have access to the relevant information. Customer shall be responsible to the extent legally permitted for any costs and expenses arising from any such assistance by Company.

6.2 Company shall, taking into account the nature of the processing and the information available to Company, provide Customer with reasonable cooperation and assistance with respect to Customer's cooperation and/or prior consultation with any Supervisory Authority or regulatory agency, where necessary and where required by the Data Protection Laws. Customer shall be responsible to the extent legally permitted for any costs and expenses arising from any such assistance by Company.

6.3 Company shall maintain records sufficient to demonstrate its compliance with its obligations under this DPA, and retain such records for a period of three (3) years after the termination of the Agreement. Customer shall, with reasonable notice to Company, have the right to review, audit and copy such records at Company's offices during regular business hours.

6.4 Upon Customer's written request at reasonable intervals, and subject to reasonable confidentiality controls, Company shall either (i) make available for Customer's review copies of certifications or reports demonstrating Company's compliance with prevailing data security standards applicable to the processing of Customer's Personal Data, or (ii) if the provision of reports or certifications pursuant to (i) is not reasonably sufficient under Data Protection Laws, allow Customer's independent third party representative to conduct an audit or inspection of Company's data security infrastructure and procedures that is sufficient to demonstrate Company's compliance with its obligations under Data Protection Laws, provided that (a) Customer provides reasonable prior written notice of any such request for an audit and such inspection shall not be unreasonably disruptive to Company's business; (b) such audit shall only be performed during business hours and occur no more than once per calendar year; and (c) such audit shall be restricted to data relevant to Customer. Customer shall be responsible for the costs of any such audits or inspections, including without limitation a reimbursement to Company for any time expended for on-site audits. If Customer and Company have entered into Standard Contractual Clauses as described in Section 5 (Transfers of Personal Data), the parties agree that the audits described in Clause 8.9 of the EU SCCs shall be carried out in accordance with this Section 6.4.

6.5 Company shall immediately notify Customer if an instruction, in Company's opinion, infringes Data Protection Laws or an instruction of a Supervisory Authority.

6.6 In the event of a Personal Data Breach, Company shall, without undue delay, and in any event no later than seventy-two (72) hours after becoming aware of the Personal Data Breach, inform Customer of the Personal Data Breach and take such steps as Company in its sole discretion deems necessary and reasonable to remediate such violation (to the extent that remediation is within Company's reasonable control).

6.7 In the event of a Personal Data Breach, Company shall, taking into account the nature of the processing and the information available to Company, provide Customer with reasonable cooperation and assistance necessary for Customer to comply with its obligations under the Data Protection Laws with respect to notifying (i) the relevant Supervisory Authority or regulatory agency and (ii) Data Subjects affected by such Personal Data Breach without undue delay.

6.8 The obligations described in Sections 6.6 and 6.7 shall not apply in the event that a Personal Data Breach results from the actions or omissions of Customer. Company's obligation to report or respond to a Personal Data Breach under Sections 6.6 and 6.7 will not be construed as an acknowledgment by Company of any fault or liability with respect to the Personal Data Breach.

7. Company's Role as a Controller

The parties acknowledge and agree that with respect to Company Account Data and Company Usage Data, Company is an independent controller, not a joint controller with Customer. Company will process Company Account Data and Company Usage Data as a controller (i) to manage the relationship with Customer; (ii) to carry out Company's core business operations, such as accounting, audits, tax preparation and filing and compliance purposes; (iii) to monitor, investigate, prevent and detect fraud, security incidents and other misuse of the Services, and to prevent harm to Customer; (iv) for identity verification purposes; (v) to comply with legal or regulatory obligations applicable to the processing and retention of Personal Data to which Company is subject; and (vi) as otherwise permitted under Data Protection Laws and in accordance with this DPA and the Agreement. Company may also process Company Usage Data as an independent controller to provide, optimize, secure, and maintain the Services, to investigate and prevent fraud, security incidents, abuse, and misuse of the Services, and to comply with applicable legal or regulatory obligations, provided that Company Usage Data shall not include Customer content, prompts, outputs, uploaded documents, Confidential Information, Customer Personal Data, or other information that identifies Customer or Customer users. Any processing by Company as a controller shall be in accordance with Company's privacy policy set forth at <https://www.iubenda.com/privacy-policy/45263214>.

8. Conflict

In the event of any conflict or inconsistency among the following documents, the order of precedence will be: (1) the applicable terms in the Standard Contractual Clauses; (2) the terms of this DPA; (3) the Agreement; and (4) Company's privacy policy. Any claims brought in connection with this DPA will be subject to the terms and conditions, including, but not limited to, the exclusions and limitations set forth in the Agreement.

Exhibit A

Details of Processing

Nature and Purpose of Processing: Company will process Customer's Personal Data as necessary to provide the Services under the Agreement, for the purposes specified in the Agreement and this DPA, and in accordance with Customer's instructions as set forth in this DPA. The nature of processing includes, without limitation:

- Receiving data, including collection, accessing, retrieval, recording, and data entry
- Holding data, including storage, organization and structuring
- Using data, including analysis, consultation, testing, automated decision making and profiling
- Updating data, including correcting, adaptation, alteration, alignment and combination
- Protecting data, including restricting, encrypting, and security testing
- Sharing data, including disclosure, dissemination, allowing access or otherwise making available
- Returning data to the data exporter or data subject
- Erasing data, including destruction and deletion

Duration of Processing: Company will process Customer's Personal Data as long as required (i) to provide the Services to Customer under the Agreement; or (ii) by applicable law or regulation. Company Account Data and Company Usage Data will be processed and stored as set forth in Company's privacy policy.

Categories of Data Subjects: Customer end-users/customers

Categories of Personal Data: Company processes Personal Data contained in Company Account Data, Company Usage Data, and any Personal Data provided by Customer (including any Personal Data Customer collects from its end users and processes through its use of the Services) or collected by Company in order to provide the Services or as otherwise set forth in the Agreement or this DPA. Categories of Personal Data include name, location, email address, phone number, address, occupation, and title.

Sensitive Data or Special Categories of Data: None

Exhibit B

SCC Annex Information and Authorized Subprocessors

The following includes the information required by Annex I and Annex III of the EU SCCs, and Table 1, Annex 1A, and Annex 1B of the UK Addendum.

1. The Parties

Item	Data Exporter	Data Importer
Party	Customer	Poll the People, Inc. (dba: CustomGPT.ai)
Address	As designated by Customer in Customer's account or applicable Order Form	16192 Coastal Highway, Lewes, Delaware 19958
Contact details	As designated by Customer in Customer's account	CustomGPT Operations (ops@customgpt.ai)
Signature and date	By entering into the Agreement, Data Exporter is deemed to have signed these Standard Contractual Clauses incorporated herein, as of the Effective Date of the Agreement.	By entering into the Agreement, Data Importer is deemed to have signed these Standard Contractual Clauses incorporated herein, as of the Effective Date of the Agreement.
Role	The Data Exporter's role is set forth in Section 2 of this DPA.	The Data Importer's role is set forth in Section 2 of this DPA.

2. Description of the Transfer

Description	Details
Data Subjects	As described in Exhibit A of the DPA
Categories of Personal Data	As described in Exhibit A of the DPA
Special Category Personal Data (if applicable)	As described in Exhibit A of the DPA
Nature of the Processing	As described in Exhibit A of the DPA
Purposes of Processing	As described in Exhibit A of the DPA
Duration of Processing and Retention (or the criteria to determine such period)	As described in Exhibit A of the DPA
Frequency of the transfer	As necessary to perform the obligations and exercise the rights set forth in the Agreement and this DPA.
Recipients of Personal Data Transferred to the Data Importer	Company's list of Authorized Subprocessors is set forth below or otherwise made available in accordance with Section 4.2 of the DPA.

3. Competent Supervisory Authority

The supervisory authority shall be the supervisory authority of the Data Exporter, as determined in accordance with Clause 13 of the EU SCCs. The supervisory authority for the purposes of the UK Addendum shall be the UK Information Commissioner's Office.

4. List of Authorized Subprocessors

Company's current list of Authorized Subprocessors may be made available at a Trust Center, subprocessor page, by email, or through another means made available to Customer. As of the effective date of this template, the following Authorized Subprocessors are listed:

Authorized Subprocessor	Contact	Description of Processing	Processing Location
Amazon Web Services, Inc.	security@aws.amazon.com	Cloud hosting, infrastructure, storage, and content delivery services.	United States
OpenAI, Inc.	security@openai.com	Generative AI processing services used to provide the Services.	United States
Pinecone Systems, Inc.	security@pinecone.io	Vector database storage and retrieval services.	United States
Microsoft Azure	security@microsoft.com	Cloud hosting, infrastructure, storage, and content delivery services.	United States

Exhibit C

Description of the Technical and Organizational Security Measures implemented by the Data Importer

The following includes the information required by Annex II of the EU SCCs and Annex II of the UK Addendum.

Technical and Organizational Security Measure	Details
Measures of pseudonymisation and encryption of personal data	As outlined in https://customgpt.ai/security/
Measures for ensuring ongoing confidentiality, integrity, availability and resilience of processing systems and services	As outlined in https://customgpt.ai/security/
Measures for ensuring the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident	As outlined in https://customgpt.ai/security/
Processes for regularly testing, assessing and evaluating the effectiveness of technical and organizational measures in order to ensure the security of the processing	SOC-2 Type 2 and as outlined in https://customgpt.ai/security/
Measures for user identification and authorization	MFA and as outlined in https://customgpt.ai/security/
Measures for the protection of data during transmission	SOC-2 Type 2 and as outlined in https://customgpt.ai/security/
Measures for the protection of data during storage	SOC-2 Type 2 and as outlined in https://customgpt.ai/security/
Measures for ensuring physical security of locations at which personal data are processed	SOC-2 Type 2 and as outlined in https://customgpt.ai/security/
Measures for ensuring event logging	SOC-2 Type 2 and as outlined in https://customgpt.ai/security/
Measures for ensuring system configuration, including default configuration	SOC-2 Type 2 and as outlined in https://customgpt.ai/security/
Measures for internal IT and IT security governance and management	SOC-2 Type 2 and as outlined in https://customgpt.ai/security/
Measures for certification/assurance of processes and products	SOC-2 Type 2 and as outlined in https://customgpt.ai/security/
Measures for ensuring data minimisation	SOC-2 Type 2 and as outlined in https://customgpt.ai/security/
Measures for ensuring data quality	SOC-2 Type 2 and as outlined in https://customgpt.ai/security/
Measures for ensuring limited data retention	SOC-2 Type 2 and as outlined in https://customgpt.ai/security/
Measures for ensuring accountability	SOC-2 Type 2 and as outlined in https://customgpt.ai/security/
Measures for allowing data portability and ensuring erasure	SOC-2 Type 2 and as outlined in https://customgpt.ai/security/
Technical and organizational measures of subprocessors	Company enters into Data Processing Agreements with its Authorized Subprocessors with data protection obligations substantially similar to those contained in this DPA.

Exhibit D

UK Addendum

International Data Transfer Addendum to the EU Commission Standard Contractual Clauses

Part 1: Tables

Table 1: Parties

Item	Exporter	Importer
Start Date	This UK Addendum shall have the same effective date as the DPA.	This UK Addendum shall have the same effective date as the DPA.
Parties' Details	Customer	Company
Key Contact	See Exhibit B of this DPA	See Exhibit B of this DPA

Table 2: Selected SCCs, Modules and Selected Clauses

EU SCCs	The version of the Approved EU SCCs which this UK Addendum is appended to as defined in the DPA and completed by Sections 5.2 and 5.3 of the DPA.
----------------	--

Table 3: Appendix Information

"Appendix Information" means the information which must be provided for the selected modules as set out in the Appendix of the Approved EU SCCs (other than the Parties), and which for this UK Addendum is set out in:

Appendix Item	Location
Annex 1A: List of Parties	As per Table 1 above
Annex 1B: Description of Transfer	See Exhibit B of this DPA
Annex II: Technical and organisational measures including technical and organisational measures to ensure the security of the data	See Exhibit C of this DPA
Annex III: List of Sub processors (Modules 2 and 3 only)	See Exhibit B of this DPA

Table 4: Ending this UK Addendum when the Approved UK Addendum Changes

Ending this UK Addendum when the Approved UK Addendum changes	Selection
Importer	Yes
Exporter	Yes
Neither Party	No

Entering into this UK Addendum

1. Each party agrees to be bound by the terms and conditions set out in this UK Addendum, in exchange for the other party also agreeing to be bound by this UK Addendum.
2. Although Annex 1A and Clause 7 of the Approved EU SCCs require signature by the Parties, for the purpose of making ex-UK Transfers, the Parties may enter into this UK Addendum in any way that makes them legally binding on the Parties and allows data subjects to enforce their rights as set out in this UK Addendum. Entering into this UK Addendum will have the same effect as signing the Approved EU SCCs and any part of the Approved EU SCCs.

Interpretation of this UK Addendum

3. Where this UK Addendum uses terms that are defined in the Approved EU SCCs those terms shall have the same meaning as in the Approved EU SCCs. In addition, the following terms have the following meanings:

Term	Meaning
UK Addendum	This International Data Transfer Addendum incorporating the EU SCCs, attached to the DPA as Exhibit D.
EU SCCs	The version(s) of the Approved EU SCCs which this UK Addendum is appended to, as set out in Table 2, including the Appendix Information.
Appendix Information	As set out in Table 3.
Appropriate Safeguards	The standard of protection over the personal data and of data subjects' rights, which is required by UK Data Protection Laws when making an ex-UK Transfer relying on

	standard data protection clauses under Article 46(2)(d) UK GDPR.
Approved UK Addendum	The template Addendum issued by the ICO and laid before Parliament in accordance with s119A of the Data Protection Act 2018 on 2 February 2022, as may be revised under Section 18 of the UK Addendum.
Approved EU SCCs	The standard contractual clauses approved by the European Commission in Commission Decision 2021/914 dated 4 June 2021, for transfers of personal data to countries not otherwise recognized as offering an adequate level of protection for personal data by the European Commission, as amended and updated from time to time.
ICO	The Information Commissioner of the United Kingdom.
ex-UK Transfer	Has the same definition as set forth in the DPA.
UK	The United Kingdom of Great Britain and Northern Ireland.
UK Data Protection Laws	All laws relating to data protection, the processing of personal data, privacy and/or electronic communications in force from time to time in the UK, including the UK GDPR and the Data Protection Act 2018.
UK GDPR	Has the definition set forth in the DPA.

4. The UK Addendum must always be interpreted in a manner that is consistent with UK Data Protection Laws and so that it fulfils the Parties' obligation to provide the Appropriate Safeguards.
5. If the provisions included in the UK Addendum amend the Approved EU SCCs in any way which is not permitted under the Approved EU SCCs or the Approved UK Addendum, such amendment(s) will not be incorporated in the UK Addendum and the equivalent provision of the Approved EU SCCs will take their place.
6. If there is any inconsistency or conflict between UK Data Protection Laws and the UK Addendum, UK Data Protection Laws applies.
7. If the meaning of the UK Addendum is unclear or there is more than one meaning, the meaning which most closely aligns with UK Data Protection Laws applies.
8. Any references to legislation (or specific provisions of legislation) means that legislation (or specific provision) as it may change over time. This includes where that legislation (or specific provision) has been consolidated, re-enacted and/or replaced after the UK Addendum has been entered into.

Hierarchy

9. Although Clause 5 of the Approved EU SCCs sets out that the Approved EU SCCs prevail over all related agreements between the parties, the parties agree that, for ex-UK Transfers, the hierarchy in Section 10 below will prevail.
10. Where there is any inconsistency or conflict between the Approved UK Addendum and the EU SCCs (as applicable), the Approved UK Addendum overrides the EU SCCs, except where (and insofar as) the inconsistent or conflicting terms of the EU SCCs provides greater protection for data subjects, in which case those terms will override the Approved UK Addendum.
11. Where this UK Addendum incorporates EU SCCs which have been entered into to protect ex-EU Transfers subject to the GDPR, the parties acknowledge that nothing in the UK Addendum impacts those EU SCCs.

Incorporation and Changes to the EU SCCs

12. This UK Addendum incorporates the EU SCCs which are amended to the extent necessary so that: (a) together they operate for data transfers made by the data exporter to the data importer, to the extent that UK Data Protection Laws apply to the data exporter's processing when making that data transfer, and they provide Appropriate Safeguards for those data transfers; (b) Sections 9 to 11 above override Clause 5 (Hierarchy) of the EU SCCs; and (c) the UK Addendum (including the EU SCCs incorporated into it) is (1) governed by the laws of Northern Ireland and (2) any dispute arising from it is resolved by the courts of Northern Ireland.
13. Unless the parties have agreed alternative amendments which meet the requirements of Section 12 of this UK Addendum, the provisions of Section 15 of this UK Addendum will apply.
14. No amendments to the Approved EU SCCs other than to meet the requirements of Section 12 of this UK Addendum may be made.
15. The following amendments to the EU SCCs (for the purpose of Section 12 of this UK Addendum) are made: (a) References to the "Clauses" means this UK Addendum, incorporating the EU SCCs; (b) in Clause 2, delete the words "and, with respect to data transfers from controllers to processors and/or processors to processors, standard contractual clauses pursuant to Article 28(7) of Regulation (EU) 2016/679"; (c) Clause 6 is replaced with the description of transfers specified in Annex I.B where UK Data Protection Laws apply; (d) onward transfer adequacy references are replaced with the corresponding UK adequacy regulations language; (e) references to Regulation (EU) 2016/679 are replaced by UK Data

Protection Laws and equivalent provisions; (f) references to the European Union, Union, EU, EU Member State, Member State, and EU or Member State are replaced with the UK; (g) the competent supervisory authority is replaced with the Information Commissioner; (h) Clause 17 is replaced with governance by the laws of Northern Ireland; (i) Clause 18 is replaced with jurisdiction of the courts of Northern Ireland, with data subjects able to bring proceedings before the courts of any country in the UK; and (j) the footnotes to the Approved EU SCCs do not form part of the UK Addendum, except for footnotes 8, 9, 10 and 11.

Amendments to the UK Addendum

16. The parties may agree to change Clauses 17 and/or 18 of the EU SCCs to refer to the laws and/or courts of Scotland and Northern Ireland.

17. If the parties wish to change the format of the information included in Part 1: Tables of the Approved UK Addendum, they may do so by agreeing to the change in writing, provided that the change does not reduce the Appropriate Safeguards.

18. From time to time, the ICO may issue a revised Approved UK Addendum which makes reasonable and proportionate changes to the Approved UK Addendum, including correcting errors in the Approved UK Addendum, and/or reflects changes to UK Data Protection Laws. The revised Approved UK Addendum will specify the start date from which the changes are effective and whether the parties need to review this UK Addendum including the Appendix Information. This UK Addendum is automatically amended as set out in the revised Approved UK Addendum from the start date specified.

19. If the ICO issues a revised Approved UK Addendum under Section 18 of this UK Addendum, if a party will as a direct result of the changes have a substantial, disproportionate and demonstrable increase in its direct costs of performing its obligations under the UK Addendum and/or its risk under the UK Addendum, and in either case it has first taken reasonable steps to reduce those costs or risks so that it is not substantial and disproportionate, then that party may end this UK Addendum at the end of a reasonable notice period by providing written notice for that period to the other party before the start date of the revised Approved UK Addendum.

20. The parties do not need the consent of any third party to make changes to this UK Addendum, but any changes must be made in accordance with its terms.

Exhibit E

United States Privacy Law Exhibit

This United States Privacy Law Exhibit ("Exhibit") supplements the DPA and applies to the extent Customer Personal Data is subject to any applicable U.S. State Privacy Laws. Any terms not defined in this Exhibit shall have the meanings set forth in the DPA, the Agreement, or the applicable U.S. State Privacy Laws.

A. General U.S. State Privacy Law Terms

1. For purposes of this Exhibit, terms such as "Controller", "Processor", "Business", "Service Provider", "Contractor", "Consumer", "Personal Data", "Personal Information", "Sell", "Share", and "Processing" shall have the meanings given to them under the applicable U.S. State Privacy Laws.
2. Except with respect to Company Account Data and Company Usage Data, the parties acknowledge and agree that Customer is the controller, business, regulated entity, or equivalent role under applicable U.S. State Privacy Laws, and Company is the processor, service provider, contractor, or equivalent role under applicable U.S. State Privacy Laws, in each case to the extent such law applies.
3. Customer shall disclose Customer Personal Data to Company only for the limited and specified purposes described in Exhibit A to this DPA, the Agreement, and Customer's documented instructions.
4. Company shall process Customer Personal Data only for the limited and specified purposes described in Exhibit A to this DPA, the Agreement, and Customer's documented instructions, and as otherwise permitted by applicable U.S. State Privacy Laws.
5. Company shall not retain, use, disclose, or otherwise process Customer Personal Data outside of the direct business relationship between Company and Customer except as permitted by the Agreement, this DPA, Customer's documented instructions, or applicable U.S. State Privacy Laws.
6. Company shall not Sell or Share Customer Personal Data, as those terms are defined under the CCPA, and shall not process Customer Personal Data for targeted advertising or cross-context behavioral advertising except to the extent expressly instructed by Customer and permitted by applicable law.
7. Company shall not combine Customer Personal Data with personal data that Company receives from or on behalf of another person or collects from its own interaction with a Consumer, except as permitted by applicable U.S. State Privacy Laws.
8. Company shall comply with obligations applicable to processors, service providers, contractors, or equivalent roles under applicable U.S. State Privacy Laws, including by providing Customer Personal Data the level of privacy protection required by such laws.
9. Company shall notify Customer if Company makes a determination that it can no longer meet its obligations under applicable U.S. State Privacy Laws.
10. Company shall assist Customer in responding to Consumer rights requests as set forth in Section 5.7 of the DPA.
11. Company shall maintain the confidentiality of Customer Personal Data and require that each person processing such Customer Personal Data be subject to a duty of confidentiality with respect to such processing.
12. Company shall implement and maintain appropriate technical and organizational measures as described in Section 5 and Exhibit C of the DPA.
13. Upon Customer's written request, Company shall delete or return Customer Personal Data in accordance with Section 2.5 of the DPA, unless retention is required or authorized by law, this DPA, or the Agreement.
14. Company shall only engage a new subprocessor to assist Company in providing the Services to Customer under the Agreement in accordance with Section 4.2 of the DPA, including by providing notice and an opportunity to object as described therein, and by entering into a written contract with the subprocessor requiring the subprocessor to observe applicable requirements under applicable U.S. State Privacy Laws.
15. Upon Customer's written request at reasonable intervals, Company shall, as set forth in Sections 6.3 and 6.4 of the DPA, make available to Customer information in Company's possession that is reasonably necessary to demonstrate Company's compliance with its obligations under applicable U.S. State Privacy Laws and allow and cooperate with reasonable inspections or audits as required or permitted under such laws.
16. If Customer determines that Company is processing Customer Personal Data in an unauthorized manner, Customer may, taking into account the nature of Company's processing and the nature of the Customer Personal Data processed by Company on behalf of Customer, take commercially reasonable and appropriate steps to stop and remediate such unauthorized processing.

B. California-Specific Terms

1. For purposes of the CCPA, the parties acknowledge and agree that Company is a Service Provider and, as applicable, a Contractor, and is receiving Personal Information from Customer in order to provide the Services pursuant to the Agreement, which constitutes a Business Purpose.
2. Company shall not Sell or Share Personal Information provided by Customer under the Agreement.
3. Company shall not retain, use, or disclose Personal Information provided by Customer pursuant to the Agreement for any purpose, including a Commercial Purpose, other than as necessary for the specific purpose of performing the Services for Customer pursuant to the Agreement, as otherwise set forth in the Agreement or this DPA, or as permitted by the CCPA.
4. Company shall not retain, use, or disclose Personal Information provided by Customer pursuant to the Agreement outside of the direct business relationship between Company and Customer, except where and to the extent permitted by the CCPA.
5. Company will not combine Personal Information received from, or on behalf of, Customer with Personal Information that it receives from, or on behalf of, another party, or that it collects from its own interaction with the Consumer, except as permitted by the CCPA.
6. Company shall comply with all obligations applicable to Service Providers and Contractors under the CCPA, including by providing Personal Information provided by Customer under the Agreement the level of privacy protection required by the CCPA.

C. Washington-Specific Terms

1. For purposes of this Part C, the terms "Consumer Health Data," "Processor," "Regulated Entity," "Small Business," and "Process" or "Processing" have the meanings set forth in the Washington My Health My Data Act ("MHMDA").
2. Except with respect to Company Account Data and Company Usage Data (as defined in the DPA), the parties acknowledge and agree that Company is a Processor for purposes of the MHMDA (to the extent it applies).
3. The nature, purpose, and duration of Processing, as well as the types of Consumer Health Data and categories of Consumers, are described in Exhibit A to this DPA.
4. Company acknowledges that if it fails to adhere to Customer's instructions or processes Consumer Health Data outside the scope of the Agreement or this DPA, Company may be subject to the obligations of a Regulated Entity or a Small Business, as applicable, under the MHMDA.

D. Virginia-Specific Terms

1. In the event of a Personal Data Breach affecting Customer Personal Data subject to the Virginia Consumer Data Protection Act ("VCDPA"), Company shall, in addition to its obligations under Sections 6.6 and 6.7 of the DPA and Part A of this Exhibit, provide Customer with information sufficient to enable Customer to meet its obligations under Virginia's breach notification laws (Va. Code § 18.2-186.6).