Electronic Record of Contracts

This document was generated as a record of certain contracts created, accepted and stored electronically.

Summary of Contracts

This document contains the following contracts.

Title	Revision	ID
Data Processing Agreement (data IQ AG and OpenAI)	1	650dd840456b3e14f76eae21

Contract signed by:

data IQ AG

Signer ID: f0d8d6b8-717b-451f-9f91-a69ecb6d92ee
Email: stefan.oglesby@data-iq.ch

Date / Time: Sep 22, 2023 at 2:09 PM EDT
IP Address: 91.190.19.197
User Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/116.0.0.0 Safari/537.36

Completed by all parties on:
Sep 22, 2023 at 2:09 PM EDT

Ironclad

OpenAI Data Processing Addendum

This Data Processing Addendum ("**DPA**") governs OpenAI's processing of Customer Data (i) provided by Customer to OpenAI through OpenAI's API or any OpenAI services for businesses ("API **Services**") or (ii) pursuant to OpenAI's provision of the ChatGTPT Enterprise service for businesses (the "ChatGPT Enterprise Services") (for purposes of this DPA, the API Services and ChatGPT Enterprise Services are together the "Services") under the terms of the OpenAI Business Terms (located at openai.com/policies/business-terms), Enterprise Agreement, or other agreement between Customer and OpenAI governing Customer's use of the Services (the "**Agreement**") and is hereby incorporated into the Agreement. If and to the extent language in this DPA conflicts with the Agreement, the conflicting terms in this DPA shall control. Capitalized terms not defined in this DPA have the meaning set forth in the Agreement. For purposes of this DPA only, "Customer" includes any affiliate entity of Customer's that (a) has entered into an Order Form with OpenAI and that (b) directly or indirectly, through one or more intermediaries controls, is controlled by, or is under common control with Customer.

OpenAI and Customer each agree to comply with their respective obligations under applicable data privacy and data protection laws (collectively, "**Data Protection Laws**") in connection with the Services. Data Protection Laws may include, depending on the circumstances, Cal. Civ. Code §§ 1798.100 et seq., as amended by the California Privacy Rights Act of 2020 (the California Consumer Privacy Act) ("**CCPA**"), Colo. Rev. Stat. §§ 6-1-1301 et seq. (the Colorado Privacy Act) ("**CPA**"), Connecticut's Data Privacy Act ("**CTDPA"**), Utah Code Ann. §§ 13-61-101 et seq. (the Utah Consumer Privacy Act) ("**UCPA**"), VA Code Ann. §§ 59.1-575 et seq. (the Virginia Consumer Data Protection Act) ("**VCDPA**") (collectively "**U.S. Privacy Laws**"), and the United Kingdom and/orEuropean Union General Data Protection Regulation (Regulation (EU) 2016/679) (collectively the "**GDPR**"), and applicable subordinate legislation and regulations implementing those laws.

In connection with the Agreement, Customer is the person that determines the purposes and means for which Customer Data (as defined below) is processed (a "**Data Controller**"), whereas OpenAI processes Customer Data in accordance with the Data Controller's instructions and on behalf of the Data Controller (as a "**Data Processor**"). "Data Controller" and "Data Processor" also mean the equivalent concepts under Data Protection Laws. For purposes of the Agreement and this DPA, (i) "Personal Data" has the meaning assigned to the term "personal data" or "personal information" under applicable Data Protection Laws; and (ii)"**Customer Data**" means Personal Data that Customer provides to OpenAI that OpenAI processes on behalf of Customer to provide the Services. OpenAI will process Customer Data as Customer's Data Processor to provide or maintain the Services and for the purposes set forth in this DPA, the Agreement and/or in any other applicable agreements between Customer and OpenAI.

1. **Processing Requirements.** As a Data Processor, OpenAI agrees to:
    a. process Customer Data only (i) on Customer's behalf for the purpose of providing and supporting OpenAI's Services (including to provide insights, reporting, analytics and platform abuse, trust and safety monitoring); (ii) in compliance with the written instructions received from Customer; and (iii) in a manner that provides no less than the level of privacy protection required of it by Data Protection Laws;
    b. promptly inform Customer in writing if OpenAI cannot comply with the requirements of this DPA;
    c. not provide Customer with remuneration in exchange for Customer Data from Customer. The parties acknowledge and agree that Customer has not "sold" (as such term is defined by the CCPA) Customer Data to OpenAI;
    d. not "sell" (as such term is defined by U.S. Privacy Laws) or "share" (as such term is defined by the CCPA) Personal Data;
    e. inform Customer promptly if, in OpenAI's opinion, an instruction from Customer violates applicable Data Protection Laws;
    f. require (i) persons employed by it and (ii) other persons engaged to perform on OpenAI's behalf to be subject to a duty of confidentiality with respect to the Customer Data and to comply with the data protection obligations applicable to OpenAI under the Agreement and this DPA;

g. engage the organizations or persons listed at https://platform.openai.com/subprocessors to process Customer Data (each a "**Subprocessor**," and the list at the foregoing URL, the "**Subprocessor List**") to help OpenAI satisfy its obligations in accordance with this DPA or to delegate all or part of the processing activities to such Subprocessors. Customer hereby consents to the use of such Subprocessors. If Customer subscribes to email notifications as provided on the Subprocessor List website, then OpenAI will notify Customer of any changes OpenAI intends to make to the Subprocessor List at least 15 days before the changes take effect (which may be via email, a posting, or notification on an online portal for our services or other reasonable means). In the event that Customer does not wish to consent to the use of such additional Subprocessor, Customer may notify OpenAI that Customer does not consent within fifteen (15) days on reasonable grounds relating to the protection of Customer Data by following the instructions set forth in the Subprocessor List or contacting privacy@openai.com. In such case, OpenAI shall have the right to cure the objection through one of the following options: (i) OpenAI will cancel its plans to use the Subprocessor with regards to processing Customer Data or will offer an alternative to provide its Services or services without such Subprocessor; (ii) OpenAI will take the corrective steps requested by Customer in Customer objection notice and proceed to use the Subprocessor; (iii) OpenAI may cease to provide, or Customer may agree not to use whether temporarily or permanently, the particular aspect or feature of the OpenAI Services or services that would involve the use of such Subprocessor; or (iv) Customer may cease providing Customer Data to OpenAI for processing involving such Subprocessor. If none of the above options are commercially feasible, in OpenAI's reasonable judgment, and the objection(s) have not been resolved to the satisfaction of the parties within thirty (30) days of OpenAI's receipt of Customer's objection notice, then either party may terminate any subscriptions, order forms or usage regarding the Services that cannot be provided without the use of the new Subprocessor for cause and in such case, Customer will be refunded any pre-paid fees for the applicable subscriptions, order forms or usage to the extent they cover periods or terms following the date of such termination. Such termination right is Customer's sole and exclusive remedy if Customer objects to any new Subprocessor. OpenAI shall enter into contractual arrangements with each Subprocessor binding them to provide a comparable level of data protection and information security to that provided for herein. Subject to the limitations of liability included in the Agreement, OpenAI agrees to be liable for the acts and omissions of its Subprocessors to the same extent OpenAI would be liable under the terms of the DPA if it performed such acts or omissions itself;

h. upon reasonable request no more than once per year, provide Customer with OpenAI's privacy and security policies and other such information necessary to demonstrate compliance with the obligations set forth in this DPA and applicable Data Protection Laws;

i. where required by law and upon reasonable notice and appropriate confidentiality agreements, cooperate with assessments, audits, or other steps performed by or on behalf of Customer at Customer's sole expense and in a manner that is minimally disruptive to OpenAI's business that are necessary to confirm that OpenAI is processing Customer Data in a manner consistent with this DPA. Where permitted by law, OpenAI may instead make available to customer a summary of the results of a third-party audit or certification reports relevant to OpenAI's compliance with this DPA. Such results, and/or the results of any such assessments, audits, or other steps shall be the Confidential Information of OpenAI;

j. to the extent that Customer permits or instructs OpenAI to process Customer Data subject to U.S. Privacy Laws in a deidentified, anonymized, and/or aggregated form as part of the Services, OpenAI, OpenAI shall (i) adopt reasonable measures to prevent such deidentified data from being used to infer information about, or otherwise being linked to, a particular natural person or household; (ii) not attempt to reidentify the information, except that OpenAI may attempt to reidentify the information solely for the purpose of determining whether its deidentification processes comply with Data Protection Laws or are functioning as intended; and (iii) before sharing deidentified data with any other party, including Subprocessors, contractually obligate any such recipients to comply with the requirements of this provision;

k. where the Customer Data is subject to the CCPA, not (i) retain, use, disclose, or otherwise process Customer Data except as necessary for the business purposes specified in the Agreement or this DPA;

(ii) retain, use, disclose, or otherwise process Customer Data in any manner outside of the direct business relationship between OpenAI and Customer; or (iii) combine any Customer Data with Personal Data that OpenAI receives from or on behalf of any other third party or collects from OpenAI's own interactions with individuals, provided that OpenAI may so combine Customer Data for a purpose permitted under the CCPA if directed to do so by Customer or as otherwise permitted by the CCPA;

l. where required by law, grant Customer the rights to (i) take reasonable and appropriate steps to ensure that OpenAI uses Customer Data in a manner consistent with Data Protection Laws by exercising the audit provisions set forth in this DPA above; and (ii) stop and remediate unauthorized use of Customer Data, for example by requesting that OpenAI provide written confirmation that applicable Customer Data has been deleted.

2. **Notice to Customer.** OpenAI will inform Customer if OpenAI becomes aware of:
   a. any legally binding request for disclosure of Customer Data by a law enforcement authority, unless OpenAI is otherwise forbidden by law to inform Customer, for example to preserve the confidentiality of an investigation by law enforcement authorities;
   b. any notice, inquiry or investigation by an independent public authority established by a member state pursuant to Article 51 of the GDPR (a "**Supervisory Authority**") with respect to Customer Data; or
   c. any complaint or request (in particular, requests for access to, rectification or blocking of Customer Data) received directly from Customer's data subjects. OpenAI will not respond to any such request without Customer's prior written authorization.
3. **Assistance to Customer.** OpenAI will provide reasonable assistance to Customer regarding:
   a. information necessary, taking into account the nature of the processing, to respond to requests received pursuant to Data Protection Laws from Customer's data subjects in respect of access to or the rectification, erasure, restriction, portability, objection, blocking or deletion of Customer Data that OpenAI processes for Customer. In the event that a data subject sends such a request directly to OpenAI, OpenAI will promptly send such request to Customer;
   b. the investigation of any breach of OpenAI's security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or unauthorized access to Customer Data processed by OpenAI for Customer (a "**Personal Data Breach**"); and
   c. where appropriate, the preparation of data protection impact assessments with respect to the processing of Customer Data by OpenAI and, where necessary, carrying out consultations with any supervisory authority with jurisdiction over such processing.
4. **Required Processing.** If OpenAI is required by Data Protection Laws to process any Customer Data for a reason other than in connection with the Agreement, OpenAI will inform Customer of this requirement in advance of any such processing, unless legally prohibited.
5. **Security.** OpenAI will:
   a. maintain reasonable and appropriate organizational and technical security measures (including with respect to personnel, facilities, hardware and software, storage and networks, access controls, monitoring and logging, vulnerability and breach detection, incident response, and encryption) to protect against unauthorized or accidental access, loss, alteration, disclosure or destruction of Customer Data and to protect the rights of the subjects of that Customer Data;
   b. take appropriate steps to confirm that OpenAI personnel are protecting the security, privacy and confidentiality of Customer Data consistent with the requirements of this DPA; and
   c. notify Customer of any Personal Data Breach by OpenAI, its Subprocessors, or any other third parties acting on OpenAI's behalf without undue delay after OpenAI becomes aware of such Personal Data Breach.
6. **Obligations of Customer.**
   a. Customer represents, warrants and covenants that it has and shall maintain throughout the term all necessary rights, consents and authorizations to provide the Customer Data to OpenAI and to authorize OpenAI to use, disclose, retain and otherwise process Customer Data as contemplated by this DPA, the Agreement and/or other processing instructions provided to OpenAI.
   b. Customer shall comply with all applicable Data Protection Laws.

c. Customer shall reasonably cooperate with OpenAI to assist OpenAI in performing any of its obligations with regard to any requests from Customer's data subjects.
d. Without prejudice to OpenAI's security obligations in Section 5 of this DPA, Customer acknowledges and agrees that it, rather than OpenAI, is responsible for certain configurations and design decisions for the services and that Customer, and not OpenAI, is responsible for implementing those configurations and design decisions in a secure manner that complies with applicable Data Protection Laws.
e. Customer shall not provide Customer Data to OpenAI except through agreed mechanisms. For example, Customer shall not include Customer Data other than technical contact information, or in technical support tickets, transmit user Customer Data to OpenAI by email. Without limitation to the foregoing, Customer represents, warrants and covenants that it shall only transfer Customer Data to OpenAI using secure, reasonable and appropriate mechanisms, to the extent such mechanisms are within Customer's control.
f. Customer shall not take any action that would (i) render the provision of Customer Data to OpenAI a "sale" under U.S. Privacy Laws or a "share" under the CCPA (or equivalent concepts under U.S. Privacy Laws); or (ii) render OpenAI not a "service provider" under the CCPA or "processor" under U.S. Privacy Laws.

7. **Standard Contractual Clauses.**
   a. OpenAI will process Customer Data that originates in the European Economic Area in accordance with the standard contractual clauses adopted by the EU Commission on June 4, 2021 ("**EU SCCs**") which are deemed entered into (and incorporated into this DPA by this reference) and completed as follows:
      i. Module Two (Controller to Processor) of the EU SCCs apply when Customer is a controller and OpenAI is processing Customer Data as a processor.
      ii. Module Three (Processor to Sub-Processor) of the EU SCCs apply when Customer is a processor and OpenAI is processing Customer Data as a sub-processor.
   b. For each module of the EU SCCs, where applicable, the following applies:
      i. The optional docking clause in Clause 7 does not apply;
      ii. In Clause 9, Option 2 (general written authorization) applies, and the minimum time period for prior notice of sub-processor changes shall be as set forth in Section 1(g) of this DPA.
      iii. In Clause 11, the optional language does not apply;
      iv. All square brackets in Clause 13 are hereby removed;
      v. In Clause 17 (Option 1), the EU SCCs will be governed by the EU member state where the data exporter is located;
      vi. In Clause 18(b), disputes will be resolved before the courts of the EU member state where the data exporter is located;
      vii. Exhibit A to this DPA contains the information required in Annex I and Annex III of the EU SCCs;
      viii. Exhibit B to this DPA contains the information required in Annex II of the EU SCCs; and
   c. Customer Data originating from Switzerland shall be processed in accordance with the EU SCCs with the following amendments:
      i. "FDPIC" means the Swiss Federal Data Protection and Information Commissioner.
      ii. "Revised FADP" means the revised version of the FADP of 25 September 2020, which is scheduled to come into force on 1 January 2023.
      iii. The term "EU Member State" must not be interpreted in such a way as to exclude data subjects in Switzerland from the possibility for suing their rights in their place of habitual residence (Switzerland) in accordance with Clause 18(c).
      iv. The EU SCCs also protect the data of legal entities until the entry into force of the Revised FADP.
      v. The FDPIC shall act as the "competent supervisory authority" insofar as the relevant data transfer is governed by the FADP

d. With respect to Customer Data originating from the United Kingdom, the parties will comply with the terms of Part 2: 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 2 February 2022, as it is revised under Section 18 of those Mandatory Clauses (the "**UK Addendum**"). The parties also agree (i) that the information included in Part 1 of the UK Addendum is as set out in Annex I of Appendix A to this DPA and (ii) that either party may end the UK Addendum as set out in Section 19 of the UK Addendum.

8. **Term; Data Return and Deletion.** This DPA shall remain in effect as long as OpenAI carries out Customer Data processing operations on Customer's behalf or until the termination of the Agreement (and all Customer Data has been returned or deleted in accordance with this DPA). OpenAI will retain API Service Customer Data sent through the API for a maximum of thirty (30) days, after which it will be deleted, except where OpenAI is required to retain copies under applicable laws, in which case OpenAI will isolate and protect that Customer Data from any further processing except to the extent required by applicable laws. [OpenAI will retain ChatGPT Enterprise Service Customer Data during the term of the Agreement, unless otherwise stated in the Agreement or Order Form.] On the termination of the DPA, OpenAI will direct each Subprocessor to delete the Customer Data within thirty (30) days of the DPA's termination, unless prohibited by law. For clarity, OpenAI may continue to process information derived from Customer Data that has been deidentified, anonymized, and/or aggregated such that the data is no longer considered Personal Data under applicable Data Protection Laws and in a manner that does not identify individuals or Customer to improve OpenAI's systems and services.

OpenAI OpCo, LLC

Signature:

Sheila Dunning

Name: Sheila Dunning

Title: Authorized Signer

Date: 8/24/2023

data IQ AG

Orgnanization ID:org-WA5RxAl9oJdqjfOnURLDVDuZ

Name: Stefan Oglesby

Title: CEO

Date: September 22, 2023

Exhibit A

ANNEX I

A. LIST OF PARTIES

Data exporter(s): the Services customer identified on the applicable Services registration documents

Data importer(s):

Name: OpenAI, LLC

Address: 3180 18th St., San Francisco, CA 94110

Contact Person's name, position and contact details:

Sheila Dunning
Head of Commercial Legal
privacy@openai.com

Activities relevant to the data transferred under these Clauses: The performance of the services described in the agreement to which this is attached.

Signature and date: Sheila Dunning 8/24/2023

Role (controller/processor): Processor

B. DESCRIPTION OF TRANSFER

Categories of data subjects whose personal data is transferred

Users of data exporters applications.

Categories of personal data transferred

Name, contact information, demographic information, or other information provided by the user in unstructured data.

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 specialised 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 the user includes it unexpectedly in unstructured data.

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 described in the agreement to which this appendix is attached.

Purpose(s) of the data transfer and further processing

The performance of the services described in the agreement to which this appendix is attached.

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 described in the agreement to which this appendix is attached.

C. 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 exporter is established.

Exhibit B

ANNEX II

TECHNICAL AND ORGANISATIONAL MEASURES INCLUDING TECHNICAL AND ORGANISATIONAL MEASURES TO ENSURE THE SECURITY OF THE DATA

INTRODUCTION

OpenAI's mission is to deploy safe and responsible AI at scale for the benefit of all. In accordance with this mission, OpenAI maintains an information security program designed to safeguard its systems, data, and Customer Data. This Addendum describes the information security program and security standards that OpenAI maintains with respect to the Services and handling of data submitted by or on behalf of Customer the Services (the "Customer Data"). Capitalized terms not defined in this Annex II have the meanings given in the DPA or Agreement.

ChatGPT Enterprise is a new OpenAI Service and so certain technical or security measures below apply differently to ChatGPT Enterprise; in each case that difference is noted in *italicized* language. "ChatGPT Enterprise" is the version of OpenAI's AI-powered ChatGPT language model that is available to enterprises.

To learn more about OpenAI's technical and organizational security measures to protect Customer Data, see the OpenAI Security Portal at https://trust.openai.com/ (the "Security Portal"). The Security Measures below include the subset of the information available in the Security Portal which applies to this DPA.

SECURITY MEASURES

Corporate Identity, Authentication, and Authorization Controls. OpenAI maintains industry best practices for authenticating and authorizing internal employee and service access, including the following measures:

- OpenAI uses single sign-on (SSO) to authenticate to third-party services used in the delivery of the Services. Role Based Access Controls (RBAC) are used when provisioning internal access to the Services;
- Mandatory multi-factor authentication is used for authenticating to OpenAI's identity provider.
- Unique login identifiers are assigned to each user;
- Established review and approval processes for any access requests to services storing Customer Data;
- Periodic access audits designed to ensure access levels are appropriate for the roles each user performs;
- Established procedures for promptly revoking access rights upon employee separation;
- Established procedures for reporting and revoking compromised credentials such as passwords and API keys); and

- Established password reset procedures, including procedures designed to verify the identity of a user prior to a new, replacement, or temporary password.

Customer Identity, Authentication, and Authorization Controls. OpenAI maintains industry best practices for authenticating and authorizing customers to the Services, including the following measures:

- Use of a third-party identity access management service to manage Customer identity, meaning OpenAI does not store user-provided passwords on users' behalf; and
- Logically separating Customer Data by organization account using unique identifiers. Within an organization account, unique user accounts are supported.

Cloud Infrastructure and Network Security. OpenAI maintains industry 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.
- The Services are routinely audited for security vulnerabilities.
- Application secrets and service accounts are managed by a secrets management service;
- Network security policies and firewalls are configured for least-privilege access against a pre-established set of permissible traffic flows. Non-permitted traffic flows are blocked; and
- Services logs are monitored for security and availability.

System and Workstation Control. OpenAI maintains industry best practices for securing OpenAI's corporate systems, including laptops and on-premises infrastructure, including:

- Endpoint management of corporate workstations;
- Endpoint management of mobile devices;
- Automatic application of security configurations to workstations;
- Mandatory patch management; and
- Maintaining appropriate security logs.

Data Access Control. OpenAI maintains industry best practices for preventing authorized users from accessing data beyond their authorized access rights and for preventing the unauthorized input, reading, copying, removal, modification, or disclosure of data. Such measures include the following:

- Employee access to the Services follows the principle of least privilege. Only employees whose job function involves supporting the delivery of Services are credentialed to the Services environment; and
- Customer 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.

Disclosure Control. OpenAI maintains industry best practices for preventing the unauthorized access, alteration, or removal of data during transfer, and for securing and logging all transfers. Such measures include:

- Encryption of data at rest in production datastores using strong encryption algorithms;
- Encryption of data in transit;

- Audit trail for all data access requests for production datastores;
- Full-disk encryption required on all corporate workstations;
- Device management controls required on all corporate workstations;
- Restrictions on use of portable or removable media; and
- Customer Data can be deleted upon request.

Availability control. OpenAI maintains industry best practices for maintaining Services functionality through accidental or malicious intent, including:

- Ensuring that systems may be restored in the event of an interruption;
- Ensuring that systems are functioning and faults are reported; and
- Anti-malware and intrusion detection/prevention solutions implemented comprehensively across our environment

Segregation control. OpenAI maintains industry best practices for separate processing of data collected for different purposes, including:

- Logical segregation of Customer Data;
- Restriction of access to data stored for different purposes according to staff roles and responsibilities;
- Segregation of business information system functions; and
- Segregation of testing and production information system environments.

Risk Management. OpenAI maintains industry best practices for detecting and managing cybersecurity risks, including:

- Threat modeling to document and triage sources of security risk for prioritization and remediation;
- Penetration testing is conducted on the Services at least annually, and any remediation items identified are resolved as soon as possible on a timetable commensurate with the associated risk. Upon request, OpenAI will provide summary details of the tests performed and whether the identified issues have been resolved; *for clarity, the ChatGPT Enterprise Service was not included in past penetration testing and will be included in a penetration test by the end of 2023*;
- Annual engagements of a qualified, independent external auditor to conduct periodic reviews of OpenAI's security practices against recognized audit standards, including SOC 2 Type II certification audits. Upon reasonable request, OpenAI will provide summary details, *provided that for ChatGPT Enterprise, SOC 2 Type II audits will be initiated by the end of 2023, and OpenAI will share summary details when available*; and
- A vulnerability management program designed to ensure the prompt remediation of vulnerabilities affecting the Services.

Personnel. OpenAI maintains industry best practices for vetting, training, and managing personnel with respect to security matters, including:

- Background checks, where legally permissible, of employees with access to Customer Data or supporting other aspects of the Services;
- Annual security training for employees, and supplemental security training as appropriate.

Physical Access Control. OpenAI maintains industry best practices for preventing unauthorized physical access to OpenAI facilities, including:

- Physical barrier controls including locked doors and gates;
- 24-hour on-site security guard staffing;
- 24-hour video surveillance and alarm systems, including video surveillance of common areas and facility entrance and exit points;
- Access control systems requiring biometrics or photo-ID badge and PIN for entry to all OpenAI facilities by OpenAI personnel;
- Visitor identification,sign-in and escort protocols; and
- Logging of facility exits and entries.

Third Party Risk Management. OpenAI maintains industry best practices for managing third party security risks, including with respect to any subprocessor or subcontractor to whom OpenAI provides Customer Data, including the following measures:

- Written contracts designed to ensure that any agent agrees to maintain reasonable and appropriate safeguards to protect Customer Data; and
- Vendor Security Assessments: All third parties undergo a formal vendor assessment process maintained by OpenAI's Security team.

Security Incident Response. OpenAI maintains a security incident response plan for responding to and resolving events that compromise the confidentiality, availability, or integrity of the Services or Customer Data including the following:

- OpenAI aggregates system logs for security and general observability from a range of systems to facilitate detection and response; and
- If OpenAI becomes aware that a Personal Data Breach has occurred, OpenAI will notify Customer in accordance with the DPA.

Security Evaluations. OpenAI performs regular security and vulnerability testing to assess whether key controls are implemented properly and are effective as measured against industry security standards and its policies and procedures and to ensure continued compliance with obligations imposed by law, regulation, or contract with respect to the security of Customer Data as well as the maintenance and structure of OpenAI's information systems.