Data Processing Addendum

Effective February 26, 2025

A. Definitions

This Data Processing Addendum ("**DPA**") is incorporated into and forms part of the Agreement between Anthropic and the Customer for purchasing services from Anthropic and Anthropic that embodies the DPA and governs Customer's use of the Services (the "**Agreement**"), and applies to Anthropic's processing of Personal Data that is subject to Data Protection Laws and Regulations, defined in this DPA will have the meaning set forth in the Agreement. Notwithstanding any usual DPA limits from time to time on reasonable notice to Customer to the extent necessary to comply with Data Protection Laws and Regulations, Anthropic Laws, if there is any conflict between the terms of this DPA and the Agreement, the conflicting terms in this DPA will govern.

a. Definitions

1.1. "**Applicable Data Protection Laws**" means all applicable privacy or data protection laws and regulations relating to the processing of personal data, as may be amended or replaced from time to time.

1.2. "**Customer Personal Data**" means personal data submitted through the Services by or for Customer or a Customer Affiliate.

1.3. "**Customer Affiliate**" means an affiliate of Customer that (a) is permitted to use the Services pursuant to the Agreement between Anthropic and Customer, and (b) directly or indirectly controls, is controlled by, or is under common control with Customer. "Control", for purposes of this definition, means direct or indirect ownership or control of more than 50% of voting interests.

1.4. "**Customer Data**" means all data or other information submitted through the Services by or for Customer or a Customer Affiliate.

1.5. "**Data Subject Request**" means a request from a data subject to exercise rights under Applicable Data Protection Laws and Regulations (such as rights to rectify or erase, access, or delete their personal data).

1.6. "**GDPR**" means Regulation (EU) 2016/679.

1.7. "**Security Breach**" means a breach of Anthropic's security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or unauthorized access to, Customer Personal Data.

1.8. "**Standard Contractual Clauses**" or "**SCCs**" means Module Two Controller to Processor of the EU Standard Contractual Clauses and Module Three Processor to Controller Contractual Clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and the Council ("**EU Standard Contractual Clauses**"), the Commission Decision 2010/87/EU of June 2010, available at https://www.eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32010D0087&from=EN.

1.9. "**Subprocessor**" means an entity engaged by Anthropic to process Customer Personal Data.

1.10. "**UK Addendum**" means the International Data Transfer Addendum to the EU Commission Standard Contractual Clauses, issued by the Information Commissioner's Office, available at https://ico.org.uk/media/for-organisations/documents/4019539/international-data-transfer-addendum.pdf.

1.11. The terms "**personal data**", "**data subject**", "**processing**", "**controller**", and "**processor**" as used in this DPA have the meanings given by Applicable Data Protection Laws and Regulations, or if not defined thereunder, the GDPR.

1.12. The terms "**business**" and "**processor**" in Cal. Civ. Code § 1798.140 and "**service provider**", respectively, as recognized by Applicable Data Protection Laws.

B. Processing of Customer Data

2.1. Anthropic shall process Customer Personal Data on Customer's behalf and in accordance with Customer's documented instructions, Anthropic will comply with the respective obligations under Applicable Data Protection Laws in connection with the processing of Customer Personal Data.

2.2. Anthropic's obligations under Anthropic's Anthropic Laws and Regulations, Anthropic's Anthropic Laws and Regulations, Anthropic will comply with its respective obligations under Applicable Data Protection Laws in connection with the processing of Customer Personal Data.

2.3. Anthropic's processing activities in Customer's Anthropic Laws and Regulations, Anthropic's Anthropic Laws and Regulations, Anthropic will comply with its respective obligations under Applicable Data Protection Laws and Regulations, and in compliance with Customer's documented instructions (including as set out in the Agreement and this DPA).

2.4. Without limiting the foregoing, Anthropic will not:

2.4.1. "sell" or "share" Customer Personal Data, as defined by Applicable Data Protection Laws;

2.4.2. retain, use, or disclose Customer Personal Data outside of the direct business relationship and for any purpose other than for the business purposes specified in this DPA or Schedule 1 or as otherwise permitted by Applicable Data Protection Laws; and

2.4.3. except as otherwise permitted by Applicable Data Protection Laws, combine Customer Personal Data with personal data that Anthropic receives from or on behalf of another person or persons, or collects from its own interaction with the data subject.

2.5. As required under Applicable Data Protection Laws, Anthropic will promptly inform Customer if, in its opinion, an instruction from Customer relating to the processing obligations under this DPA, or which such Customer instructions may reasonably and appropriate steps in accordance with the Agreement to stop or remedy any unauthorized processing of Customer Personal Data.

2.6. Anthropic will promptly inform Customer if, in its opinion, an instruction from Customer relating to the processing of Customer Personal Data violates Applicable Data Protection Laws.

2.6. Anthropic will cooperate with and provide reasonable assistance to Customer, at Customer's reasonable request, in connection with Anthropic's assessment of the processing of Customer Personal Data by Anthropic, and (b) related consultation with supervisory authorities, either or both of which Anthropic reasonably considers to be required by Applicable Data Protection Laws.

2.7. Anthropic will ensure that each person it authorizes to process Customer Personal Data is subject to an appropriate duty of confidentiality.

C. Subprocessors

2.1. Customer grants Anthropic general authorization to engage the Subprocessors listed in Schedule 3, and any additional Subprocessors in accordance with Section 2.2 below.

2.2. Anthropic will: (a) enter into a contractual agreement with each Subprocessor that imposes on the Subprocessor obligations substantially as protective as Anthropic's obligations under this DPA to the extent applicable to the nature of the services provided by Subprocessor; and (b) remain liable to Customer for the acts and omissions of each Subprocessor to the extent that Anthropic is liable for its own, consistent with the limitation of liability provisions in the Agreement.

2.3. Anthropic will maintain a list, which it will update as additional Subprocessors (or Anthropic will provide Customer reasonable notice of the new Subprocessor prior to giving the Subprocessor access to Customer Personal Data, and (b) Customer may object to the addition of a Subprocessor, provided Customer objects to Anthropic's use of such Subprocessor for providing Anthropic with written notice of the objection within fifteen (15) days of the date of such notice, and Customer and Anthropic will work together in good faith to find a mutually acceptable resolution to address such objection raised by Customer. Anthropic and Anthropic will work together in good faith to find a mutually acceptable resolution to address any objection raised by Customer.

D. Data Subject Requests

3.1. Anthropic will forward to Customer promptly any Data Subject Request received by Anthropic relating to the Customer Personal Data and may refuse to do so if the request is directed to Customer or a Customer Affiliate.

3.2. Anthropic will, taking into account the nature of the processing, provide Customer with reasonable and timely assistance as necessary for Customer to enable Customer to comply with Applicable Data Protection Laws in respect to Data Subject Requests.

E. Security

4.1. Anthropic will comply with the data security obligations of Applicable Data Protection Laws and Regulations, and will implement and maintain appropriate technical and organizational data protection and security measures designed to ensure a level of security for the Customer Data (including the Customer Personal Data) appropriate to the risk, taking into account the matters set out in Schedule 2. Anthropic may update those measures from time to time, provided that such updates do not materially reduce the overall security of the Services.

4.2. The parties agree that the measures set out in Schedule 2 provide an appropriate level of security for the Customer Data (including the Customer Personal Data) taking into account the risks presented by the processing contemplated by the Agreement and this DPA.

F. Compliance and Audits

5.1. Anthropic is audited annually against leaves, established industry standards performed by external auditors. Upon Customer's written request, and subject to appropriate confidentiality obligations, Anthropic will make available to Customer and auditor all such reports or certifications applicable to the Services (e.g., SOC 2 report), to the extent available, or such other information reasonably necessary to demonstrate Anthropic's compliance with this DPA, such certifications are available for Customer's review at www.anthropic.com.

5.2. Upon Customer's written request, Anthropic will permit Customer, at Customer's expense, to audit Anthropic's applicable controls and compliance with this DPA (an "**Audit**"), provided such Audit is (a) conducted by Customer or a third party auditor mutually agreed upon by Customer and Anthropic, subject to confidentiality agreement with Anthropic, (b) Customer and Anthropic mutually agree on reasonable details of the Audit, including the start date, scope and duration of the Audit, and security and confidentiality controls applicable to the Audit and (c) whether Audit has already been conducted less than twelve (12) months prior, unless there are indications of non-compliance and/or is required by a Supervisory Authority or Customer's Data Protection Laws and Regulations or substantiated of Applicable Data Protection Laws.

5.3. Customer will pay any reasonably incurred costs and expenses incurred by Anthropic in connection with Customer's performance an Audit that is not required by a Supervisory Authority or Customer's Data Protection Laws and Regulations.

5.4. Customer may use the results of an Audit only for the purposes of meeting Customer's regulatory audit requirements and/or confirming compliance with the requirements of this DPA.

G. Security Breaches

6.1. Anthropic will notify Customer in writing without undue delay, but in any event within 48 hours, after becoming aware of any Security Breach, and will assist Customer to complying with Customer's obligations under Applicable Data Protection Laws and Regulations, taking into account the nature of processing and the information available to Anthropic. Anthropic's notification of or response to a Security Breach will not be construed as an acknowledgment by Anthropic of any fault or liability with respect to the Security Breach.

6.2. Upon becoming aware of a Security Breach, Anthropic will (a) investigate the Security Breach, and (b) provide timely information relating to the nature of the Security Breach, the personal data compromised, the identity of affected or approximate number of data subjects concerned and the categories and approximate number of Customer Personal Data records concerned, the likely consequences of the Security Breach, and the measures taken or proposed to be taken by Anthropic to address the Security Breach, including, where appropriate, measures to mitigate its possible adverse effects.

H. Deletion and Return

7.1. Upon Customer's written request after the date of termination or expiration of the Agreement, Anthropic will:

(i) or, if requested to do so by Customer within that period, return a copy of all Customer Data to its control or possession or provide a self-service functionality allowing Customer to do the same; or

(ii) delete all other copies of Customer Data (including Customer Personal Data) processed by Anthropic or any Subprocessors, except to the extent (i) Applicable Data Protection Laves or other applicable legal or regulatory requirements applicable to Anthropic or any Subprocessor permit or require Anthropic or Anthropic's successor to retain a dispute between the parties, or (iii) the retention of the Customer Data is necessary to continue hosted use of the Services.

I. Standard Contractual Clauses

8.1. Anthropic will comply with the obligations of Applicable Data Protection Laws, the terms of the SCCs Module Two (controller to processor) and Module Three (processor to processor), as completed as described in Schedule 3 of this DPA, and will provide Customer with the relevant information and the documents necessary for the parties.

8.2. To the extent required by Applicable Data Protection Laves, the jurisdiction specific addenda to the SCCs set out in Schedule 3 are also incorporated into the SCCs, and Anthropic will comply with the obligations therein.

8.3. To the extent that there is any conflict between the terms of this DPA, the Agreement, and the terms of the SCCs, the terms of the following documents will prevail (in order of precedence): (i) the SCCs; (ii) this DPA; and (iii) the Agreement.

8.4. Anthropic will provide Customer reasonable support to enable Customer to perform any impact assessments or prior consultations required by Applicable Data Protection Laves. Anthropic will, upon Customer's request, provide information to Customer which is reasonably necessary for Customer to demonstrate its compliance with its obligations under Applicable Data Protection Laws.

Schedule 1 - Details of Processing and Transfers

A. List of Parties

Anthropic is a provider of the personnelle to this DPA. With regard to any transfers of Customer Personal Data falling within the scope of Applicable Data Protection Laves, additional information regarding the data exporter and data importer is set out below.

1.1. **Data Exporter**: The data exporter is the Customer and the Customer Affiliate (if any) that enters into an Agreement with Anthropic. The data exporter's contact person's name, position and contact details are set out in the Agreement. The data protection officer's name and contact details (and if relevant, the representative in the European Union) are set out in the Agreement or will be disclosed to Anthropic upon request.

1.2. **Data Importer**: The data importer is the Anthropic entity that executes the Agreement. The data importer's contact person's name, position and contact details are set out in the Agreement or will be disclosed to Customer upon request.

B. Description of Processing

B.1. **Categories of data subjects**: Determined by Customer in accordance with the Agreement.

B.2. **Categories of personal data**: Determined by the Customer in accordance with the Agreement.

B.3. **Special categories of personal data (if applicable)**: None.

B.4. **Duration and Frequency of the processing**: The processing is performed on a continuous basis for the duration of the Agreement and is determined by Customer's configuration of the Services.

B.5. **Nature and purpose of the processing**: Performing the Services on behalf of Customer which involves processing (including collection, storage, organization and structuring) of personal data as part of a natural language processing service provided by the Services, and any other Services Anthropic is undertaking to provide, security, and testing of the Services (including to identify and repair errors that impair existing intended functionality).

B.6. **Purpose(s) of the data transfer and further processing**: To provide the Services to Customer pursuant to the Agreement and as may be further agreed by the parties in writing from time to time.

B.7. **Storage Limitation**: The duration is the term of the Agreement.

B.8. **Subprocessors (where applicable)**: Subject to the security set out in the provisions of the Services listed in Schedule 3.

C. Competent Supervisory Authority

Identify the competent supervisory authority/authorities in accordance with clause 13 of the SCCs:

Where the data exporter is established in an EU Member State: The supervisory authority of the country in which the data exporter established is the competent authority.

Where the data exporter is not established in an EU Member State, but falls within the extra-territorial scope of the GDPR, and has appointed an EU representative: EU will have jurisdiction's supervisory authority in the one of the Member States in which the representative is established.

Where the data exporter is not established in an EU Member State, but falls within the extra-territorial scope of the GDPR, without however having to appoint an EU representative: Anthropic's supervisory authority in the one of the Member States in which the representative is established.

Where the data exporter is not established in an EU Member State, but falls within the extra-territorial scope of the GDPR, without however having to appoint an EU representative: Anthropic's supervisory authority in the one of the Member States in which the representative is established.

Schedule 2 - Technical and Organizational Measures

Anthropic has implemented and will maintain technical and organizational measures designed in accordance with industry-standard practices to protect the security, confidentiality, and integrity of the Customer Data, as set out below. Anthropic may update or modify these measures from time to time provided that such updates will not materially diminish the overall security of the Customer Data during the term of the Agreement. Anthropic's current certifications and/or audit reports are available on request at https://trust.anthropic.com.

A. Security Program and Policies

1.1. Anthropic maintains organizational management and dedicated staff responsible for the development, implementation, and maintenance of Anthropic's information security program. Anthropic has a qualified security team of sufficient resources commensurate with the size, and complexity of its operations.

1.2. Anthropic's operational procedures and controls define physical, technical, and administrative safeguards that provide for the configuration, monitoring and maintenance of technology and information systems that process Customer Data according to prescribed internal and auto-protect standards.

1.3. Anthropic's change management procedures and tracking mechanisms are designed to test, approve, and monitor all changes to Anthropic's technology and information assets that process Customer Data.

1.4. Anthropic's business resiliency and continuity plan and procedures are designed to maintain Customer Data availability and to avoid any recovery from emergency situations or disasters.

1.5. Anthropic's network security controls provide for appropriate network traffic filtering, segmentation of networks, and other event correlation procedures designed to prevent systems from intrusion and limit the scope of any successful attack.

1.6. Anthropic maintains a clear policy of internal security policies that are communicated and distributed to all personnel, including policies covering:

• Information Security
• Personnel Security
• Asset Management
• Data Management
• Risk Management
• Access Control
• Secure Development
• Operational Security
• Physical Security
• Incident Response
• Business Continuity and Disaster Recovery
• Cryptography

B. Access Controls

2.1. All Anthropic personnel are assigned unique identifiers for interacting with systems managing Customer Data.

2.2. All default systems embedded on changed by Anthropic prior to a system's use in production capacity.

2.3. Anthropic maintains a least privileged access approach to system access, using RBAC (Role Based Access Control), by restricting Anthropic personnel to only the information and resources that are necessary for their job function.

2.4. All accounts systems processing Customer Data are protected by Multi-Factor Authentication (MFA).

2.5. MFA via Anthropic's Okta IDP is enforced for all systems with access, or that store or maintain, Customer Data.

2.6. Anthropic utilizes Content Secure Access to prevent unauthorized devices from accessing sensitive information, including Customer Data.

2.7. Anthropic maintains strong password requirements (including:

2.8. a minimum of 16 characters;

2.9. changing of initial passwords; and

2.1. the prevention of password re-use.

2.2. Anthropic prohibits the sharing or transmission of passwords through unsecured channels or methods.

2.3. Anthropic reviews privileged access systems managing Customer Data on a regular basis to ensure performance access remains appropriate for job functions on a business needs.

2.4. All access with privileged access to Customer Data have all access revoked promptly following termination of employment.

C. Personnel Management

3.1. All personnel engaged by Anthropic are properly trained and obligated to comply with Anthropic's security policies, and are subject to a binding, with respect to the confidentiality and security of the Customer Data.

3.2. Anthropic employees, at hire and annually thereafter, complete security awareness, HIPAA, and other training including confidentiality and data security. These trainings provide information regarding relevant threats and vulnerabilities, including, but not limited to, phishing, social engineering, handling, control of personal data/sensitive, and mobile/portable identification and reporting.

3.3. As part of pre-employment, all candidates complete a rigorous interview process, undergo background checks, and sign confidentiality agreements.

3.4. Anthropic's employee terminations are managed by a formal process without undue delay and in accordance with standard industry practices.

D. Audits and Certifications

4.1. Anthropic defines audit and risk assessment procedures for the purposes of periodically reviewing and assessing risk to Anthropic's organization, IT systems and data, (b) monitoring and maintaining compliance with Anthropic's policies and procedures, and (c) reporting the condition of its information security and compliance to internal senior management.

4.2. Anthropic's information security program is assessed annually by independent third party auditors. Anthropic's current certifications are made available to Anthropic's customers.

4.3. To request access to any of our reports and certifications, please go to https://trust.anthropic.com.

E. Encryption Standards

Anthropic utilizes industry-standard encryption methods for protection of Customer Data, including a minimum of AES 256 for data at rest, and TLS 1.2+ for data in transit over public networks.

F. Endpoint Protection

Anthropic's endpoint protection tools, and cloud enterprise (where applicable), are installed on all Anthropic-owned laptops and engineer's systems that include, but are not limited to, (a) anti-virus and anti-malware protections, (b) active real-time system monitoring, and (c) alerting to internal security teams.

G. Vulnerability Management

5.1. Anthropic's vulnerability assessment, patch management, threat protection technologies, and scheduled monitoring procedures are designed to identify, assess, mitigate, and remediate, on a periodic basis, security vulnerabilities on all machines (e.g., Anthropic utilizes a multi-faceted approach to vulnerability management, including: automated code vulnerability scanning; automated dependency vulnerability scanning; automated container image scanning; active endpoint detection and response; outsourced pen testing; and ongoing analysis).

5.2. Anthropic engages qualified external assessors for the completion of annual penetration testing of systems that process Customer Data in Anthropic's production environment. Anthropic's vulnerability management, threat protection, and identified vulnerabilities are addressed as part of Anthropic's vulnerability management program. Upon request, Anthropic will make available to Customer a summary of its most recent penetration testing results.

5.3. Anthropic applies a remediation timeline based on risk level and is aligned with industry accepted timelines.

H. Data Management

6.1. Customer Data within Anthropic is logically separated such that no customer's data is accessible by/to/to any other customer without authorization. Customer Data associated with a specific customer is easily identifiable. Further, Anthropic's production environment is logically separated from its corporate/separate environments processing Customer Data from its internal, from development and testing environments, and from other workspaces.

I. Logging, Monitoring, and Incident Response

1.1. Anthropic's incident management procedures are designed to allow Anthropic to investigate, respond to, mitigate, and notify of cyber events. Anthropic's technology and infrastructure assets that process Customer Data are configured to generate security logs and alerts.

1.2. Anthropic maintains a centralized SIEM (security information and event management) SOAR (security orchestration, automation, and response) tool.

1.3. Anthropic logs employee access and actions within Anthropic's systems, inclusive of those storing or maintaining Customer Data.

1.4. System audit or event logging and related monitoring procedures are used to proactively record user access and system activity for routine security and compliance activities for review.

1.5. Security-related logs are retained for appropriate timeframes to aid in the investigation of security incidents.

J. Third Party Vendors

Anthropic maintains a third party information security risk management program, which evaluates the extension of periodic risk assessments to enhance the security posture of Anthropic's third party vendors.

Schedule 3 - International Data Transfers

A. EU SCCs

1.1. Elections for the purposes of Module Two and Module Three of the Standard Contractual Clauses:

1.2. Clause 7 (Docking clause) - does not apply.

1.3. Clause 11 (Redress) - optional wording does not apply.

1.4. Clause 17 (Governing Law) - Option 1 will apply and the governing law will be the law of the Republic of Ireland.

1.5. Clause 18(b) (Choice of forum and jurisdiction) - the applicable courts of Ireland will be the forum and jurisdiction of choice.

1.6. For the purpose of Annex I of the Standard Contractual Clauses, Part A of Schedule 3 contains the specifications regarding the parties, Part B of Schedule 3 contains the description of transfer for Module Two and Module Three, and Part C of Schedule 3 contains the competent supervisory authority.

1.7. For the purpose of Annex II of the Standard Contractual Clauses, Schedule 2 contains the technical and organizational measures.

1.8. Additional elections for the purposes of Module Two and Module Three of the Standard Contractual Clauses:

1.9. Clause 9 (Use of subprocessors) – Option 2 (General written authorization) will apply, and the time periods as specified in Section C.2. of this DPA.

1.10. For the purpose of Annex III of the Standard Contractual Clauses, the list of Subprocessors to be specified pursuant to Section C.2. of this DPA, Section C.2. of this DPA. The Subprocessor's contact persons name, position and contact details will be provided by Anthropic upon request.

B. UK Addendum

1.1. The UK Addendum will apply to the processing of Customer Personal Data that is subject to the UK GDPR or both the UK GDPR and the GDPR. For the purposes of this UK Addendum:

"**Approved Addendum**" means the template addendum, version B.1.0 issued by the Information Commissioner's Office and laid before Parliament in accordance with Section 119A of the Data Protection Act 2018 on 2 February 2022, as it may be revised according to Section 18 of the Mandatory Clauses;

"**Approved EU SCCs**" means the SCCs pursuant to GDPR of the European Parliament and the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, 5/4 of the European Union (General Data Protection Regulation) ("GDPR") and Commission Implementing Decision (EU) 2021/914 of 4 June 2021;

"**Mandatory Clauses**" means "**Part 2: Mandatory Clauses**" of the Approved Addendum.

1.2. With respect to any transfers of Customer Personal Data falling within the scope of the UK GDPR (the "Restricted Transfers") the parties to Anthropic's Data Processing Addendum hereby:

1.2.1. to the extent necessary under Applicable Data Protection Laws, the Standard Contractual Clauses (the "Standard Contractual Clauses") in the Agreement, as amended by the Approved Addendum, shall be deemed to be the Standard Contractual Clauses for the Restricted Transfers;

1.2.2. to the extent necessary under Applicable Data Protection Laves, the Standard Contractual Clauses in the Agreement, as amended by the Approved Addendum, shall be deemed to be the Standard Contractual Clauses for the Restricted Transfers; and

1.2.3. the Approved Addendum, in the form attached to Schedule 3 of this DPA, shall be deemed to be duly and effectively completed and executed by the parties.

3 will be incorporated into and form part of this DPA;

B.1.b. for the purposes of Table 1 of Part 1 of the Approved Addendum, the parties' details are as set out in Part A of Schedule 1;

B.1.c. for the purposes of Table 2 of Part 1 of the Approved Addendum, the version of the Approved EU SCCs as set out in the EU SCCs of this Schedule 3 including the Appendix Information are the selected SCCs; and

B.1.d. for the purposes of Table 4 of Part 1 of the Approved Addendum, Anthropic (as data importer) may end the Approved Addendum.

C. Swiss Addendum

This Swiss Addendum will apply to any processing of Customer Personal Data that is subject to Swiss Data Protection Laws (as defined below) or to both Swiss Data Protection Laws and the GDPR.

C.1. Interpretation of this Addendum

C.1.a. Where this Addendum uses terms that are defined in the Standard Contractual Clauses, those terms will have the same meaning as in the Standard Contractual Clauses. In addition, the following terms have the following meanings:

C.1.a.i. This **"Addendum"** means this Addendum to the Clauses.

C.1.a.ii. **"Clauses"** means the Standard Contractual Clauses as further specified in this Schedule.

C.1.a.iii. **"Swiss Data Protection Laws"** means The Swiss Federal Act on Data Protection of 19 June 1992 and the Swiss Ordinance to the Swiss Federal Act on Data Protection of 14 June 1993, and any new or revised version of these laws that may enter into force from time to time.

C.1.b. This Addendum will be read and interpreted in the light of the provisions of Swiss Data Protection Laws, and so that if fulfills the intention for it to provide the appropriate safeguards as required by Article 46 GDPR and/or Article 6(2)(a) of the Swiss Data Protection Laws, as the case may be.

C.1.c. This Addendum will not be interpreted in a way that conflicts with rights and obligations provided for in Swiss Data Protection Laws.

C.1.d. 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 this Addendum has been entered into.

C.2. HierarchyIn the event of a conflict or inconsistency between this Addendum and the provisions of the Clauses or other related agreements between the parties, existing at the time this Addendum is agreed or entered into thereafter, the provisions which provide the most protection to data subjects will prevail.

C.3. Incorporation of the Clauses

C.3.a. In relation to any processing of personal data subject to Swiss Data Protection Laws or to both Swiss Data Protection Laws and the GDPR, this Addendum amends the DPA the Standard Contractual Clauses to the extent necessary so they operate:

C.3.a.i. for transfers made by the data exporter to the data importer, to the extent that Swiss Data Protection Laws or Swiss Data Protection Laws and the GDPR apply to the data exporter's processing when making that transfer; and

C.3.a.ii. to provide appropriate safeguards for the transfers in accordance with Article 46 of the GDPR and/or Article 6(2)(a) of the Swiss Data Protection Laws, as the case may be.

C.3.b. To the extent that any processing of personal data is exclusively subject to Swiss Data Protection Laws, the amendments to the DPA including the SCCs, as further specified in this Schedule and as required by Section 3(a) of this Swiss Addendum, include (without limitation):

C.3.b.i. References to the **"Clauses"** or the **"SCCs"** mean this Swiss Addendum as it amends the SCCs.

C.3.b.ii. Clause 6 Description of the transfer(s) is replaced with: "The details of the transfer(s), and in particular the categories of personal data that are transferred and the purpose(s) for which they are transferred, are those specified in Schedule 1 of this DPA where Swiss Data Protection Laws apply to the data exporter's processing when making that transfer."

C.3.b.iii. References to **"Regulation (EU) 2016/679"** or **"that Regulation"** or **"GDPR"** are replaced by **"Swiss Data Protection Laws"** and references to specific Article(s) of **"Regulation (EU) 2016/679"** or **"GDPR"** are replaced with the equivalent Article or Section of Swiss Data Protection Laws to the extent applicable.

C.3.b.iv. References to Regulation (EU) 2018/1725 are removed.

C.3.b.v. References to the **"European Union"**, **"Union"**, **"EU"** and **"EU Member State"** are all replaced with **"Switzerland"**.

C.3.b.vi. Clause 13(a) and Part C of Annex I are not used; the **"competent supervisory authority"** is the Federal Data Protection and Information Commissioner (the **"FDPIC"**) insofar as the transfers are governed by Swiss Data Protection Laws;

C.3.b.vii. Clause 17 is replaced to state: "These Clauses are governed by the laws of Switzerland insofar as the transfers are governed by Swiss Data Protection Laws".

C.3.b.viii. Clause 18 is replaced to state: "Any dispute arising from these Clauses relating to Swiss Data Protection Laws will be resolved by the courts of Switzerland. A data subject may also bring legal proceedings against the data exporter and/or data importer before the courts of Switzerland in which he/she has his/her habitual residence. The parties agree to submit themselves to the jurisdiction of such courts."

Until the entry into force of the revised Swiss Data Protection Laws, the Clauses will also protect the personal data of legal entities and legal entities will receive the same protection under the Clauses as natural persons.

To the extent that any processing of personal data is subject to both Swiss Data Protection Laws and the GDPR, the DPA (including the Clauses as further specified in this Schedule) will apply (i) as is and (ii) additionally, to the extent that a transfer is subject to Swiss Data Protection Laws, as amended by Sections 1 and 3 of this Swiss Addendum, with the sole exception that Clause 17 of the SCCs will not be replaced as stipulated under Section 3(b)(vii) of this Swiss Addendum.

Customer warrants that it and/or Customer Affiliates have made any notifications to the FDPIC which are required under Swiss Data Protection Laws.

Schedule 4 - Subprocessors

Anthropic's list of subprocessors is available at https://www.anthropic.com/subprocessors.

Products

Claude
Claude Code
Claude Code Enterprise
Claude Cowork
Claude Security
Claude for Chrome
Claude for Slack
Claude for Microsoft 365
Skills
Max plan
Team plan
Enterprise plan
Download app
Pricing
Log in to Claude

Models

Mythos preview
Opus
Sonnet
Haiku

Solutions

AI agents
Code modernization
Coding
Customer support
Education
Financial services
Government
Healthcare
Life sciences
Nonprofits
Security

Claude Platform

Overview
Developer docs
Pricing
Marketplace
Regional compliance
Claude on AWS
Google Cloud's Vertex AI
Microsoft Foundry
Console login

Resources

Blog
Claude partner network
Community
Connectors
Courses
Customer stories
Engineering at Anthropic
Events
Inside Claude Code
Inside Claude Cowork
Inside Claude Enterprise
Inside Claude Security
Plugins
Powered by Claude
Service partners
Startups program
Tutorials
Use cases

Help and security

Availability
Status
Support center

Company

Anthropic
Careers
Economic Futures
Research
News
Claude's Constitution
Responsible Scaling Policy
Security and compliance
Transparency

Terms and policies

Privacy choices
Privacy policy
Consumer health data privacy policy
Responsible disclosure policy
Terms of service: Commercial
Terms of service: Consumer
Usage policy

© 2026 Anthropic PBC