Data Processing Addendum

Anthropic PBC

Archivierte Kopie · Quelle: anthropic.com/legal/data-processing-addendum · Effective Date laut Original: February 24, 2025 · Abgerufen und archiviert am: 2026-08-10

This Data Processing Addendum ("DPA") is incorporated into and forms part of the Anthropic Commercial Terms of Service or other agreement between Customer and Anthropic that references this DPA and governs Customer's use of the Services (the "Agreement"), and applies to Anthropic's processing of Customer Data (defined below). Capitalized terms used but not otherwise defined in this DPA will have the meaning set forth in the Agreement. Anthropic may amend this DPA from time to time on reasonable notice to Customer to the extent such changes are required due to changes in Applicable Data Protection 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

A.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 from time to time.

A.2. "Customer Personal Data" means personal data submitted through the Services by or for Customer or a Customer Affiliate.

A.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 the subject entity. "Control," for purposes of this definition, means direct or indirect ownership or control of more than 50% of voting interests.

A.4. "Customer Data" means all data or other information submitted through the Services by or for Customer or a Customer Affiliate.

A.5. "Data Subject Request" means a request from a data subject to exercise their personal data-related rights under Applicable Data Protection Laws, such as rights to access, correct, or delete their personal data.

A.6. "GDPR" means Regulation (EU) 2016/679.

A.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.

A.8. "Standard Contractual Clauses" or "SCCs" means Module Two (controller to processor) or Module Three (processor to processor) of the Standard Contractual Clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and the Council approved by European Commission Implementing Decision (EU) 2021/914 of 4 June 2021.

A.9. "Subprocessor" means an entity engaged by Anthropic to process Customer Personal Data.

A.10. "UK Addendum" means the International Data Transfer Addendum to the SCCs, issued by the Information Commissioner under S119A(1) Data Protection Act 2018.

A.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 or, absent any such meaning or law, by GDPR.

A.12. The terms "controller" and "processor" include "business", and "service provider", respectively, as required by Applicable Data Protection Laws.

B. Processing of Customer Data

B.1. With respect to Customer Personal Data, Customer is the controller and Anthropic is Customer's processor. Each party will comply with its respective obligations under Applicable Data Protection Laws in connection with the Services and the Customer Personal Data.

B.2. Unless required by applicable law to which Anthropic is subject, Anthropic will only process Customer Personal Data to provide or maintain the Services, and in compliance with Customer's documented instructions (including as set out in the Agreement and this DPA).

B.3. Without limiting the foregoing, Anthropic will not: (a) "sell" or "share" Customer Personal Data, as defined by Applicable Data Protection Laws; (b) 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 Part B of Schedule 1 or as otherwise permitted by Applicable Data Protection Laws; and (c) 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.

B.4. As required under Applicable Data Protection Laws, Anthropic will promptly inform Customer if it makes a determination that it can no longer comply with its processing obligations under this DPA, in which case Customer may take reasonable and appropriate steps in accordance with the Agreement to stop or remediate any unauthorized processing of Customer Personal Data.

B.5. 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 Law.

B.6. Anthropic will cooperate with and provide reasonable assistance to Customer for: (a) Customer's performance of any data protection impact assessment of the processing of Customer Personal Data by Anthropic, and (b) related consultation with supervisory authorities.

B.7. Anthropic will ensure that each person it authorizes to process Customer Personal Data is subject to an appropriate duty of confidentiality.

C. Subprocessors

C.1. Customer grants Anthropic general authorization to engage the Subprocessors listed in Schedule 4, and any additional Subprocessors in accordance with Section C.3.

C.2. Anthropic will: (a) enter into a contractual agreement with each Subprocessor imposing data protection obligations that are substantially as protective as Anthropic's obligations under this DPA; and (b) remain liable to Customer for each Subprocessors' acts and omissions related to this DPA to the extent Anthropic is liable for its own.

C.3. In the event that Anthropic wishes to appoint an additional Subprocessor: (a) Anthropic will provide Customer reasonable notice of the new Subprocessor prior to giving the Subprocessor access to Customer Personal Data; and (b) Customer may, on the basis of reasonable data privacy or data security concerns, object to Anthropic's use of such Subprocessor by providing Anthropic with written notice of the objection within fifteen (15) days of the date of such notice, or Customer is deemed to consent to the new Subprocessor.

D. Data Subject Requests

D.1. Anthropic will forward to Customer promptly any Data Subject Request received by Anthropic relating to the Customer Personal Data and may advise the Data Subject to submit their request directly to Customer.

D.2. Anthropic will, taking into account the nature of the processing, provide Customer with reasonable and timely assistance as necessary for Customer to fulfill its obligation under Applicable Data Protection Laws to respond to Data Subject Requests.

E. Security

E.1. Anthropic will comply with the data security obligations of Applicable Data Protection Laws, and will implement and maintain reasonable and appropriate technical and organizational data protection and security measures designed to ensure a level of security for the Customer Data appropriate to the risk of the relevant processing, as summarized in Schedule 2.

E.2. The parties agree that the measures set out in Schedule 2 provide an appropriate level of security for the Customer Data, accounting for the risks presented by the processing outlined in the Agreement and this DPA.

F. Compliance and Audits

F.1. Anthropic is audited annually against known, established industry standards performed by external auditors. Upon Customer's written request, Anthropic will provide Customer with such audit reports or certificates applicable to the Services (e.g., SOC 2 report), to the extent available. Anthropic's current certifications are available for Customer's review at trust.anthropic.com.

F.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, provided such Audit is (a) conducted by Customer or a designated third-party auditor with an executed confidentiality agreement, (b) mutually agreed in scope and timing, and (c) not conducted less than twelve (12) months after a prior similar Audit, unless required by law or due to indications of non-compliance.

F.3. Customer will pay any reasonably incurred costs and expenses incurred by Anthropic in the event Customer performs an Audit that is not required by law or in response to a Security Breach.

F.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 this DPA.

G. Security Breaches

G.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 in complying with Customer's obligations by reasonably cooperating with Customer's investigation.

G.2. Upon becoming aware of a Security Breach, Anthropic will (a) investigate the Security Breach, and (b) provide timely information relating to its nature, likely consequences, and mitigation measures taken or proposed.

H. Deletion and Return

H.1. Within thirty (30) days of the date of termination or expiration of the Agreement, Anthropic will: (a) if requested, return a copy of all Customer Data or provide self-service functionality to do the same; and (b) delete all copies of Customer Data processed by Anthropic or any Subprocessors, except where retention is required by law, necessary to resolve a dispute, or necessary to combat harmful use of the Services.

I. Standard Contractual Clauses

I.1–I.4. The parties agree that, to the extent required by Applicable Data Protection Laws, the SCCs Module Two (controller to processor) and/or Module Three (processor to processor), as completed in Schedule 3, are incorporated by reference. Jurisdiction-specific addenda in Schedule 3 are likewise incorporated. In case of conflict, precedence is: (i) the SCCs; (ii) this DPA; (iii) the Agreement. Anthropic will provide reasonable support for Customer's transfer impact assessments.

Schedule 1 – Details of Processing and Transfers

A. List of Parties. Data Exporter: Customer and/or Customer Affiliates exporting Customer Personal Data subject to GDPR. Data Importer: the Anthropic entity that executed the Agreement.

B. Description of Processing. Categories of data subjects and personal data: determined by Customer. Special categories: none. Duration: continuous for the term of the Agreement. Subject matter: performing the Services (natural language / machine-learning tool processing), quality/security/integrity maintenance, debugging. Purpose: to provide the Services pursuant to the Agreement. Storage limitation: the term of the Agreement. Subprocessors: as set out in Schedule 4.

C. Competent Supervisory Authority. Where the data exporter is established in an EU Member State: the supervisory authority of that Member State. Otherwise, per Art. 3(2) GDPR territorial scope rules, typically the supervisory authority of Ireland.

Schedule 2 – Technical and Organizational Measures (Summary)

• A. Security Program and Policies – dedicated security team; documented policies covering information security, personnel security, asset management, data management, risk management, access control, secure development, operational security, physical security, incident response, business continuity/disaster recovery, cryptography.

• B. Access Controls – unique identifiers, least-privilege RBAC, MFA enforced for all systems processing Customer Data, SSO via primary IDP, Context Aware Access, strong password policy (minimum 16 characters), prompt revocation on termination.

• C. Personnel Management – trained and bound personnel, annual security/HIPAA training, background checks, confidentiality agreements, prompt access removal on termination.

• D. Audits and Certifications – annual third-party assessment; reports available via trust.anthropic.com.

• E. Encryption Standards – minimum AES-256 at rest, TLS 1.2+ in transit.

• F. Endpoint Protection – EDR on all workstations and cloud endpoints (anti-virus/anti-malware, real-time monitoring, alerting).

• G. Vulnerability Management – automated code/artifact scanning, manual and automated code review, annual third-party penetration testing (summary available on request).

• H. Data Management – logical separation of Customer Data per customer; network segmentation from internet, dev/test environments, and office workspaces.

• I. Logging, Monitoring, and Incident Response – centralized SIEM/SOAR, employee access logging, proactive detection/escalation, annually tested incident response procedures.

• J. Third Party Vendors – periodic risk assessments of Anthropic's own subprocessors.

Schedule 3 – International Data Transfers (Summary)

EU SCCs: Clause 7 (Docking) does not apply. Clause 17 (Governing Law): Republic of Ireland. Clause 18 (Forum/Jurisdiction): Republic of Ireland. Clause 9 (Subprocessors): Option 2, General written authorization, 15-day objection period per Section C.3. Additional UK Addendum and Swiss Addendum apply where the respective national data protection laws are engaged, adapting governing law and supervisory authority references accordingly (ICO for UK; FDPIC for Switzerland).

Schedule 4 – Subprocessors

Anthropic's current list of subprocessors is published and maintained at: anthropic.com/subprocessors (nicht Teil dieses archivierten Auszugs, da dynamisch aktualisiert; gesondert abzurufen und zu dokumentieren).