Data Processing Addendum for Anthropic Services

This Data Processing Addendum ("**DPA**") applies to Anthropic PBC, a Public Benefit Corporation ("**Anthropic**") and its processing of Personal Data in relation to the provision of Anthropic's Services to the Customer (as specified in the applicable Anthropic Services Agreement (the "**Agreement**")). Unless otherwise expressly stated in the Agreement, this DPA shall be effective and remain in force for the full term of the Agreement. Anthropic and the Customer each may be referred to herein as a "Party" or collectively as the "Parties."

1. DEFINITIONS

"**Customer Affiliate**" means an affiliate of Customer who is a beneficiary to the Agreement.

"**Applicable Data Protection Laws**" means all applicable laws, rules, regulations, and governmental requirements relating to the privacy, confidentiality, or security of Personal Data, as they may be amended or otherwise updated from time to time.

"**Controller**" will have the following meaning (as applicable): (a) the meaning given to "controller" under Applicable Data Protection Laws; or (b) the meaning given to "business" under Applicable Data Protection Laws.

"**Covered Data**" means Personal Data shared by Customer or a Customer Affiliate in relation to the provision of the Services.

"**Data Subject**" means a natural person whose Personal Data is part of the Covered Data.

"**Data Subject Requests**" means a request from a Data Subject to exercise their rights under Applicable Data Protection Laws.

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

"**Personal Data**" means any data or information that: (a) is linked or reasonably linkable to an identified or identifiable natural person; or (b) is otherwise "personal data," "personal information," "personally identifiable information," or similarly defined data or information under Applicable Data Protection Laws.

"**Processing**" means any operation or set of operations which is performed on Personal Data or on sets of Personal Data, whether or not by automated means. "**Process**", "**Processes**" and "**Processed**" will be interpreted accordingly.

"**Processor**" will have the following meaning (as applicable): (a) the meaning given to "processor" under Applicable Data Protection Laws; or (b) the meaning given to "service provider" under Applicable Data Protection Laws.

"**Security Incident**" means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or unauthorized access to (including unauthorized internal access to), Covered Data.

"**Services**" means the services to be provided by Anthropic pursuant to the Agreement.

"**Standard Contractual Clauses**" or "**SCCs**" means Module Two (*controller to processor*) and/or Module Three (*processor to processor*) of the Standard Contractual Clauses annexed to Commission Implementing Decision (EU) 2021/914.

"**Sub-processor**" means an entity appointed by Anthropic, as a Processor, to Process Covered Data on its behalf.

"**UK GDPR**" has the meaning given under the Data Protection Act 2018 (UK).

2. GENERAL

2.1 This DPA is incorporated into and forms an integral part of the Agreement. If there is any conflict between this DPA and the Agreement relating to the Processing of Covered Data, this DPA shall govern. Customer acknowledges and agrees that Anthropic may amend this DPA from time to time on reasonable notice to Customer where such changes are required because of changes in Applicable Data Protection Laws.

2.2 Clauses 3 to 9 of this DPA apply to the extent Anthropic acts as a Processor on behalf of Customer with respect to the Covered Data.

3. DETAILS OF DATA PROCESSING

3.1 The details of the Processing of Covered Data (such as subject matter, duration, nature, and purpose of the Processing, categories of Personal Data and Data Subjects) are described in the Agreement and in Part B of Schedule 1 to this DPA.

3.2 Anthropic will only Process Covered Data in accordance with Applicable Data Protection Laws and on the documented instructions of Customer (including as set out in the Agreement and this DPA), unless required to do otherwise by applicable law to which Anthropic is subject, in which case Anthropic will, unless prohibited by applicable law, inform Customer of such legal requirement before Processing. Without limiting the foregoing, Anthropic is prohibited from:

(a) selling Covered Data or otherwise making Covered Data available to any third party for monetary or other valuable consideration;

(b) sharing Covered Data with any third party for cross-context behavioural advertising;

(c) retaining, using, or disclosing Covered 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

(d) except as otherwise permitted by Applicable Data Protection Laws, combining Covered 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.

3.3 To the extent that any of the instructions provided by Customer to Anthropic in accordance with clause 3.2 require Processing of Covered Data in a manner that falls outside the scope of the Services, Anthropic may:

(a) notify Customer that such instructions fall outside the scope of Services under the Agreement and not carry out such instructions, or at Anthropic's election, make the performance of any such instructions subject to the payment by Customer of any costs and expenses incurred by Customer or such additional charges as Customer may reasonably determine; or

(b) immediately terminate the Agreement and the Services.

3.4 Anthropic will promptly inform Customer if, in its opinion, an instruction from Customer relating to the Processing of Covered Data infringes Applicable Data Protection Law.

3.5 Customer hereby authorises and instructs Anthropic to Process Covered Data anywhere that Anthropic or its Sub-processors maintain facilities.

3.6 Anthropic will, at the request of Customer, provide assistance that is reasonable necessary for Customer to conduct and document any data protection assessments required under Applicable Data Protection Laws.

3.7 Customer will have the right to take reasonable and appropriate steps to ensure that Anthropic uses Covered Data in a manner consistent with Customer's obligations under Applicable Data Protection Laws.

3.8 Anthropic will ensure that each person authorised to process Covered Data is subject to a duty of confidentiality.

3.9 Customer acknowledges that Anthropic's Services are not designed, intended, or provided for the purpose of making predictions regarding any Data Subject, determining creditworthiness, or any other manner of automated decision-making regarding Data Subject(s) to which the Covered Data relates.

3.10 Anthropic may charge Customer, and Customer will reimburse Anthropic, for any assistance provided by Anthropic to Customer in relation to this DPA, including with respect to any TIAs or consultation with any supervisory authority of Customer.

4. SUB-PROCESSORS

4.1 Customer grants Anthropic the general authorisation to engage the Sub-processors listed in Schedule 4, and any additional Sub-processors in accordance with clause 4.3.

4.2 Anthropic will: (i) enter into a written agreement with each Sub-processor imposing data protection obligations that are substantively no less protective of Covered Data than Anthropic's obligations under this DPA; and (ii) remain liable for each Sub-processor's compliance with the obligations under this DPA.

4.3 In the event that Anthropic wishes to appoint an additional Sub-processor: (a) Anthropic will provide Customer reasonable notice; and (b) Customer may, on the basis of reasonable data privacy and data security concerns, object to Anthropic's use of such Sub-processor by providing Anthropic with written notice of the objection within ten (10) days of the date of such notice, otherwise the additional Sub-processor shall be deemed approved. In the event Customer objects to Anthropic's use of a new Sub-processor, Customer and Anthropic will work together in good faith to find a mutually acceptable resolution to address any objections raised by Customer.

5. DATA SUBJECT RIGHTS REQUESTS

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

5.2 Anthropic will, taking into account the nature of the Processing of Covered Data, provide Customer with reasonable assistance as necessary for Customer to fulfil its obligation under Applicable Data Protection Laws to respond to Data Subject Requests.

6. SECURITY

6.1 Accounting for the state of the art, costs of implementation and the nature, scope and context and purposes of the relevant Processing, as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, Anthropic will implement and maintain reasonable and appropriate technical and organizational data protection and security measures designed to ensure a level of security for the Covered Data appropriate to the risk of the relevant Processing.

6.2 The Parties agree that the measures set out in Schedule 2 provide an appropriate level of security for the Covered Data, accounting for the risks presented by the Processing outlined in the Agreement and this DPA.

7. AUDITS AND RECORDS

7.1 Upon request, Anthropic will make available to Customer information reasonably necessary to demonstrate compliance with this DPA.

7.2 To the extent required by Applicable Data Protection Legislation, Anthropic will permit Customer (or a suitably qualified, independent third-party auditor which is not a competitor of Anthropic) to audit Anthropic's compliance with this DPA no more than once per calendar year on at least thirty (30) days' written notice to Anthropic (an "**Audit**"), provided that Customer (or Customer's third-party auditor, as applicable):

(a) may only conduct an Audit during Anthropic's normal business hours;

(b) will conduct the Audit in a manner that does not disrupt Anthropic's business;

(c) enters into a confidentiality agreement reasonably acceptable to Anthropic prior to conducting the Audit;

(d) pays any reasonably incurred costs and expenses incurred by Anthropic in the event of an Audit;

(e) ensures that its personnel comply with any policies and procedures notified by Anthropic to Customer when attending Anthropic's premises;

(f) submits, as part of the written notice provided by Customer to Anthropic, a detailed proposed audit plan which is agreed by Anthropic (an "**Audit Plan**"); and

(g) conducts the Audit in compliance with the final agreed Audit Plan.

7.3 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 the DPA. Nothing in this clause 7 will require Anthropic to breach any duties of confidentiality it owes to third parties.

8. SECURITY INCIDENTS

8.1 Anthropic will notify Customer in writing without undue delay after becoming aware of any Security Incident. Anthropic will, to the extent reasonably necessary, cooperate with Customer's investigation of the Security Incident. Anthropic's notification of, or response to, a Security Incident will not be construed as an acknowledgement by Anthropic of any fault or liability with respect to the Security Incident.

9. DELETION AND RETURN

9.1 Anthropic will, in any event, within thirty (30) days of the date of termination or expiry of the Agreement (a) if requested to do so by Customer within that period, return a copy of all Covered Data or provide a self-service functionality allowing Customer to do the same; and (b) delete all other copies of Covered Data Processed by Anthropic or any Sub-processors.

10. STANDARD CONTRACTUAL CLAUSES

10.1 The Parties agree that, to the extent required by Applicable Data Protection Laws, the terms of the Standard Contractual Clauses Module 1 (Controller to Controller), Module Two (Controller to Processor) and/or Module Three (Processor to Processor), each as further specified in Schedule 3 of this DPA, are hereby incorporated by reference and will be deemed to have been executed by the Parties.

10.2 To the extent required by Applicable Data Protection Laws, the jurisdiction-specific addenda to the Standard Contractual Clauses set out in Schedule 3 are also incorporated herein by reference and will be deemed to have been executed by the Parties.

10.3 To the extent that there is any conflict between the terms of this DPA and the terms of the Standard Contractual Clauses, the Standard Contractual Clauses shall govern.

10.4 Anthropic will provide Customer reasonable support to enable Customer's compliance with the requirements imposed on international transfers of Covered Data. Anthropic will, upon Customer's request and at Customer's cost, provide information to Customer which is reasonably necessary for Customer to complete a transfer impact assessment ("TIA") to the extent required under Applicable Data Protection Laws.

SCHEDULE 1
DETAILS OF PROCESSING AND TRANSFERS

PART A – List of Parties

The Parties are set out in the preamble to this DPA. With regard to any transfers of Covered Data falling within the scope of Applicable Data Protection Laws, additional information regarding the data exporter and data importer is set out below.

1. Data Exporter

The data exporter is: Customer and/or Customer Affiliates exporting Covered Data to which the GDPR applies.

The data exporter's contact person's name, position and contact details as well as (if appointed) the data protection officer's name and contact details and (if relevant) the representative's contact details are included in the Agreement or will be disclosed to Anthropic upon request.

2. Data Importer

The data importer is: Anthropic PBC, 548 Market Street, PMB 90375, San Francisco, CA 94104, United States.

The data importer's contact person and contact details are included in the Agreement or will be disclosed to Customer upon request.

PART B – Description of Processing

3. **Categories of Data Subjects -** Determined by Customer (in accordance with the Agreement).

4. **Categories of Personal Data -** Determined by the Customer (in accordance with the Agreement).

5. **Special categories of Personal Data (if applicable) -** None.

6. **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.

7. **Subject matter and nature of the Processing -** Performing the Services on behalf of Anthropic which involves Processing (including collection, storage, organisation and structuring) of Personal Data as part of a natural language-based, machine-learning tool, as further described in the Agreement; undertaking activities to verify or maintain the quality of the Services; debugging to identify and repair errors that impair existing intended functionality; helping to ensure security and integrity of the Services.

8. **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 upon by Customer and Anthropic.

9. **Storage Limitation -** The duration is the term of the Agreement.

10. **Sub-processor (if applicable) -** To provide Processing system capability to Anthropic (as described in Schedule 4) to provide the Services described in the Agreement.

PART C – Competent Supervisory Authority

Identify the competent supervisory authority/ies 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 territorial scope of application of the GDPR in accordance with its Article 3(2) and has appointed a representative pursuant to Article 27(1) of the GDPR*: The competent supervisory authority is the one of the Member State in which the representative is established.*

Where the data exporter is not established in an EU Member State, but falls within the territorial scope of application of the GDPR in accordance with its Article 3(2) without, however, having to appoint a representative pursuant to Article 27(2) of the GDPR*: The competent supervisory authority is the supervisory authority of Ireland.*

SCHEDULE 2
TECHNICAL AND ORGANIZATIONAL MEASURES

Anthropic has implemented the following technical and organizational measures (including any relevant certifications) to ensure an appropriate level of security, accounting for the nature, scope, context, and purpose of the processing, as well as the risks for the rights and freedoms of natural persons:

1. Organizational management and dedicated staff responsible for the development, implementation, and maintenance of Anthropic's information security program.

2. Audit and risk assessment procedures for the purposes of periodic review and assessment of risks to Anthropic's organization, monitoring and maintaining compliance with Anthropic's policies and procedures, and reporting the condition of its information security and compliance to internal senior management.

3. Utilization of commercially available and industry standard encryption technologies for Covered Data that is:

    a. being transmitted by Anthropic over public networks (i.e., the Internet) or when transmitted wirelessly; or

    b. at rest or stored on portable or removable media (i.e., laptop computers, CD/DVD, USB drives, back-up tapes).

4. Data security controls which include at a minimum, but may not be limited to, logical segregation of data, logical access controls designed to manage electronic access to data and system functionality based on authority levels and job functions, (e.g., granting access on a need-to-know and least privilege basis, use of unique IDs and passwords for all users, periodic review, and revoking/changing access promptly when employment terminates or changes in job functions occur).

5. Password controls designed to manage and control password strength, expiration and usage including prohibiting users from sharing passwords and requiring that Anthropic's passwords that are assigned to its employees; controls include appropriate password security requirements, and specific time and use limitations for passwords.

6. System audit or event logging and related monitoring procedures to proactively record user access and system activity for routine review.

7. Physical and environmental security of data center, server room facilities and other areas containing Covered Data designed to: (i) protect information assets from unauthorized physical access, (ii) manage, monitor, and log movement of persons into and out of Anthropic facilities, and (iii) guard against environmental hazards such as heat, fire, and water damage.

8. Operational procedures and controls to provide for configuration, monitoring and maintenance of technology and information systems according to prescribed internal and adopted industry standards, including secure disposal of systems and media to render all information or data contained therein as undecipherable or unrecoverable prior to final disposal or release from Anthropic's possession.

9. Change management procedures and tracking mechanisms designed to test, approve, and monitor all changes to Anthropic's technology and information assets.

10. Incident / problem management procedures design to allow Anthropic to investigate, respond to, mitigate, and notify of events related to Anthropic's technology and information assets.

11. Network security controls that provide for the use of firewall systems and other traffic and event correlation procedures designed to protect systems from intrusion and limit the scope of any successful attack.

12. Vulnerability assessment, patch management and threat protection technologies and scheduled monitoring procedures designed to identify, assess, mitigate, and protect against identified security threats, viruses, and other malicious code.

13. Business resiliency/continuity plan and procedures designed to maintain service and/or recovery from foreseeable emergency situations or disasters.

SCHEDULE 3
INTERNATIONAL TRANSFERS

1. EU SCCS

Elections for the purposes of Module 1, Module Two and Module Three of the Standard Contractual Clauses:

1.1 Clause 7 (Docking clause) – does not apply.

1.2 Clause 11 (Redress) – optional wording does not apply.

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

1.4 Clause 18 (Choice of forum and jurisdiction) – the applicable choice of forum and jurisdiction will be the Republic of Ireland.

1.5 For the purpose of Annex I of the Standard Contractual Clauses, Part A of Schedule 1 contains the specifications regarding the parties, Part B of Schedule 1 contains the description of transfer for Module Two and Module Three, and Part B of Schedule 1 contains the description of transfer for Module 1 except that the purpose, nature and subject matter of the processing shall be as set out in clause 2.3, and Part C of Schedule 1 contains the competent supervisory authority.

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

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

1.7 Clause 9 (Use of sub-processors) – Option 2 (General written authorization) will apply, and the time period is as specified in clause 4.3 of the DPA.

1.8 For the purpose Annex III of the Standard Contractual Clauses, the list of Sub-processors are set out in Schedule 4 or as otherwise determined by clause 4.3 of the DPA. The Sub-processor's contact person's name, position and contact details will be provided by Anthropic upon request.

2. UK ADDENDUM

This UK Addendum will apply to any Processing of Covered Data that is subject to the UK GDPR or both the UK GDPR and the GDPR.

2.1 For the purposes of this Paragraph 2:

"Approved Addendum" means the template addendum, version B.1.0 issued by the UK Information Commissioner under S119A(1) Data Protection Act 2018 and laid before the UK Parliament on 2 February 2022, as it may be revised according to Section 18 of the Mandatory Clauses.

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

2.2 With respect to any transfers of Covered Data falling within the scope of the UK GDPR from Customer (as data exporter) to Anthropic (as data importer):

(a) to the extent necessary under Applicable Data Protection Law, the Approved Addendum as further specified in this section 2 of this Schedule 3 will be incorporated into and form part of this DPA;

(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;

(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 section 1 of this Schedule 3 including the Appendix Information are the selected SCCs; and

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

3. SWISS ADDENDUM

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

3.1 Interpretation of this Addendum

(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:

This Addendum	This Addendum to the Clauses
Clauses	The Standard Contractual Clauses as further specified in this Schedule
Swiss Data Protection Laws	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.

(b) This Addendum will be read and interpreted in the light of the provisions of Swiss Data Protection Laws, and so that if fulfils 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) This Addendum will not be interpreted in a way that conflicts with rights and obligations provided for in Swiss Data Protection Laws.

(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.

3.2 Hierarchy

In 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.

3.3 Incorporation of the Clauses

(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:

(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

(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.

(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 clause 3.1 of this Swiss Addendum, include (without limitation):

(i) References to the "Clauses" or the "SCCs" mean this Swiss Addendum as it amends the SCCs.

(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."

(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 extent applicable.

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

(v) References to the "European Union", "Union", "EU" and "EU Member State" are all replaced with "Switzerland".

(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;

(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".

(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 Personal Data of legal entities and legal entities will receive the same protection under the Clauses as natural persons.

3.4 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 clauses 3.1 and 3.3 of this Swiss Addendum, with the sole exception that Clause 17 of the SCCs will not be replaced as stipulated under clause 3.3(b)(vii) of this Swiss Addendum.

3.5 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
SUB-PROCESSORS

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