Data Processing Agreement (DPA) of Connect AI

Version: June 2025

Introduction

This Data Processing Agreement (the "DPA") constitutes an integral part of the Agreement between Connect AI and the Customer (the "Agreement") and specifies the obligations of the Parties with regard to the requirements of the Swiss Data Protection Act (FADP) and the EU General Data Protection Regulation (GDPR). In this regard, it supplements the contractual arrangements resulting from the Agreement.

This DPA only applies if and to the extent that (i) the Customer is the controller or processor within the scope of the FADP and/or the GDPR and (ii) the Customer involves Connect AI under the Agreement as a processor or sub-processor for the processing of personal data covered by the scope of the FADP and/or the GDPR.

This DPA shall remain in effect as long as Connect AI processes personal data on behalf of the Customer.

1. Definitions

The terms "controller", "processor", "personal data" and "processing" shall have the meaning given to these terms in the FADP and the GDPR (together the "Regulation").

"Data Privacy Laws" means all applicable legislation regarding the protection of personal data, including the Regulation, local laws and/or EU legislation and the decisions, advice and recommendations of the competent Supervisory Authority.

”Supervisory Authority” means the or those supervisory authority(ies) with the power to conduct supervision of the processing of personal data under the Data Privacy Laws. At the effective date of the Agreement and with respect to Switzerland, the Federal Data Protection and Information Commissioner (FDPIC) is such an authority.

2. Processing of personal data

The Parties agree that the Customer is considered the controller and Connect AI is the processor under the Regulation.

Connect AI shall process personal data in accordance with the instructions set out in the Agreement. The Customer reserves the right to provide amended or supplemented instructions to Connect AI. Connect AI shall comply with these instructions, provided that they are technically feasible and objectively reasonable for Connect AI within the scope of the services agreed upon under the Agreement (the "Services"). If such instructions result in Connect AI incurring additional costs or lead to a change in the scope of Services, the agreed contract change procedure shall apply. Connect AI shall inform the Customer promptly if it is of the opinion that an instruction contravenes the Data Privacy Laws. Connect AI may in this case defer implementing the respective instruction until it has been confirmed or amended by the Customer.

The Parties undertake to process personal data under this DPA in compliance with the Data Privacy Laws. The Parties shall refrain from any form of action that may cause the other Party to violate such Data Privacy Laws.

The Parties shall actively collaborate in order to fulfil their reporting and/or filing obligations and, where appropriate, obtain the necessary authorizations from the competent Supervisory Authority. Connect AI may, where appropriate given the effort required, demand an adequate remuneration for supporting the Customer in this regard. The Customer shall, where appropriate, inform all individuals whose personal data is subject to data processing.

3. Connect AI's obligations

Connect AI shall cooperate with the Customer with regard to the processing of personal data, the handling of requests from data subjects for the exercise of their rights, the compilation of any impact assessment, and in general reasonably assist the Customer to comply with its obligations under the Data Privacy Laws. Connect AI undertakes to provide the Customer with all relevant and necessary information that the Customer needs in order to fulfill its obligations as controller or processor. Connect AI may, where appropriate given the effort required, demand an adequate remuneration for supporting the Customer in the aforementioned regard.

Connect AI warrants:

- to only process personal data in accordance with the Customer's documented instructions and only to the extent necessary to fulfill its obligations under the Agreement (in particular for the provision of the Services) and never process personal data for any other purposes,
- that every person having access to and/or processing personal data under this DPA is bound by confidentiality obligations and has received the necessary information for the processing of the personal data,
- to notify the Customer if a data subject directly contacts Connect AI to exercise his/her rights under the Regulation (e.g. the right to information, to rectify, to delete and/or to object to the processing of personal data). Connect AI shall share the request in question with the Customer as soon as Connect AI becomes aware of such request,
- in the event that an authority, data subject or other third party requests information from Connect AI regarding the processing of personal data under this DPA, Connect AI must refer to the Customer as soon as possible. Connect AI may only disclose personal data or information regarding the processing of personal data in accordance with the Customer's instructions or if Connect AI is required to disclose the relevant information according to law, regulation, court or other authority's decision or stock exchange regulation,
- to keep records of all of categories of processing performed on behalf of the Customer in accordance with the Regulation,
- to inform the Customer if any contacts are initiated by the Supervisory Authority regarding the processing of personal data,
- to immediately notify the Customer if any change may impact the processing of personal data under the DPA,
- to immediately inform the Customer if, according to Connect AI's opinion, an instruction constitutes a breach of Data Privacy Laws or is technically not feasible.

4. Technical and organisational measures

Connect AI shall implement appropriate technical and organisational measures to ensure that all personal data processed under this DPA is appropriately protected, given their nature and the risks entailed by the processing. The measures implemented to ensure the protection of personal data shall, at a minimum, comply with what is stated in Attachment 2 (Technical and organisational measures).

In the event that Connect AI wishes to replace or amend the technical or organisational measures for the protection of personal data, the new or amended measures shall achieve an equivalent or higher level of confidentiality and protection.

5. Sub-processors

Connect AI may not engage any sub-processors without the Customer's prior consent. With regard to the sub-processors listed in Attachment 3 (Sub-processors), the Customer's consent shall be deemed granted at the date the Agreement (and thereby this DPA) comes into force. Connect AI must inform the Customer in advance if, after the Agreement (and thereby this DPA) has come into force, it engages new sub-processors or replaces existing sub-processors. If there is good cause under Data Privacy Laws, the Customer may, within a period of 30 days upon receipt of Connect AI's information, provide a written objection against the engagement of a new or the replacement of an existing sub-processor. If there is good cause under Data Privacy Laws, and where the Parties cannot agree on an amicable solution, the Customer shall be granted a termination right in relation to the Service affected thereby. Attachment 3 (Sub-processors) shall be kept updated accordingly.

Personal data may only be processed by such sub-processor on the condition that Connect AI has entered into a written agreement with the sub-processor in which the sub-processor is imposed equivalent obligations as Connect AI is imposed to by the Customer under this DPA and in which the sub-processor warrants to take appropriate technical and organisational measures in such way that the processing of personal data is in accordance with applicable Data Privacy Laws.

The Customer has the right to obtain from Connect AI a copy of the relevant agreement with the sub-processors, or, if confidentiality obligations prevent Connect AI from disclosing the full agreement, a description of its essential elements, including a description of the obligations related to the processing of personal data.

Connect AI is responsible for the services provided by the sub-processor, unless otherwise agreed between the Parties. In case that a sub-processor fails to comply with its obligations with regard to the protection of personal data, Connect AI shall be liable to the Customer for the performance of the sub-processor's undertakings.

6. Transfers to third countries

Connect AI undertakes to ensure that all processing of personal data is performed in Switzerland, a member state of the European Economic Area and/or in a country recognized as providing an adequate level of protection by the European Commission.

Accordingly, Connect AI shall ensure that no personal data is disclosed, transmitted or made available to third parties or sub-processors in a country outside Switzerland, the European Economic Area and/or to a country where, according to the European Commission, there is no adequate level of protection.

Provided that Connect AI has obtained the Customer's prior consent and only to the extent required to fulfil the obligations under the Agreement and this DPA, Connect AI is entitled to transfer personal data outside Switzerland, the European Economic Area or outside a country recognized as providing

an adequate level of protection by the European Commission, however only in the cases where the Connect AI has entered into such agreement with the relevant sub-processor as referred to in the decision of the European Commission dated 4 June 2021 regarding standard contractual terms for the transfer of personal data to processors established in third countries including any updates thereto (the "Standard Terms") and Connect AI warrants that the engaged sub-processors in third countries comply with the Standard Terms.

7. Deletion and return of personal data

At the termination of the Agreement, and in accordance with the Customer's instructions, Connect AI undertakes to delete/anonymise or return to the Customer all personal data, subject to mandatory Data Privacy Laws or other applicable mandatory laws preventing or permitting (in case of overriding legitimate interests) Connect AI from completely or partially deleting/anonymising or returning the personal data. Where possible and feasible, Connect AI shall anonymize or pseudo-anonymize such retained personal data depending on the nature of the legal obligations applicable and Connect AI hereby guarantees that the confidentiality of such personal data will be maintained.

This section shall survive the termination or the expiry of the Agreement (and thereby this DPA) for any reason whatsoever.

8. Audit

Where provided by applicable mandatory Data Privacy Laws, the Customer has the right to perform audits and inspections to ensure Connect AI's compliance with its obligations under this DPA. The principle of proportionality shall be adhered to in all cases in such audits and inspections and reasonable account must be taken of the legitimate interests of Connect AI (namely to confidentiality). Unless otherwise provided, the Customer shall be responsible for all costs of such audits and inspections (including documented internal costs incurred by Connect AI in cooperating in the audit or inspection).

9. Liability

Notwithstanding any limitation of liability in the Agreement, each Party is responsible for its processing of personal data in accordance with this DPA and applicable Data Privacy Laws and shall compensate the other Party for any loss or damage due to claims from third parties or administrative fines resulting from, arising out of or directly relating to any breach by such first-mentioned Party of this DPA or applicable Data Privacy Laws.

However, except for claims to which, according to the Regulation, no limitation applies, either Party's total aggregate liability arising in connection with this DPA shall be limited in accordance with the relevant provisions in the Agreement.

10. Personal data breach

Connect AI shall without undue delay notify the Customer when Connect AI becomes aware of a personal data breach leading to or which is at risk of leading to, accidental or illegal destruction, loss or alteration or unauthorized disclosure or access to personal data.

Connect AI shall remedy the breaches/failures as soon as possible and minimize the negative impact of such breaches/failures on the data subjects. Further, Connect AI undertakes to adopt the measures required to remedy the breaches/failures in the protection of personal data to prevent similar incidents from occurring in the future.

Connect AI shall inform the Customer in text form and provide a description of the personal data breach and its consequences, the measures implemented to remedy the breaches/failures and minimize the consequences for the data subjects, and the measures adopted to prevent similar incidents in the future. If possible, Connect AI shall indicate the number of data subjects that has been impacted by the personal data breach.

Connect AI is aware that any breach of Data Privacy Laws may impose obligations on the Customer, including the obligation to notify the data subjects and the Supervisory Authorities of the personal data breach. Connect AI undertakes to cooperate with the Customer and to assist the Customer in fulfilling such obligations.

Attachment 1 – Description of the data processing

Version: June 2025

This Attachment 1 describes the data processing performed by Connect AI under the Data Processing Agreement (DPA) within the scope of the Agreement.

1. Details of Connect AI

1.1. Contact details of Connect AI (responsible recipient of instructions):

Connect AI Group GmbH
Lagerstrasse 93
8004 Zürich
Switzerland

E-mail: info@connectai.ch

1.2. Contact details of Connect AI's data protection officer:

Connect AI Group GmbH
Matthias Zwingli
Lagerstrasse 93
8004 Zürich
Switzerland

E-mail: privacy@connectai.ch

1.1. Contact details of Connect AI's data protection representative within the European Union that can be contacted by supervisory authorities and data subjects for all questions relating to EU data protection law:

VGS Datenschutzpartner UG
Am Kaiserkai 69
20457 Hamburg
Germany

E-mail: info@datenschutzpartner.eu

2. Data processing

2.1. General

Within the scope of the Agreement, the Customer provides Connect AI, at its own discretion and on its behalf, with personal data and/or confidential data for processing purposes.

2.2. Purpose of the processing

The personal data entrusted to Connect AI by the Customer and the personal data arising therefrom shall be processed exclusively for the purpose of and related to fulfilling the Agreement.

2.3. Duration of the processing

Connect AI generally processes the personal data for the term of the Agreement. After the end of the Agreement, the personal data will be transferred to the Customer within 90 days (if requested by the Customer) and subsequently deleted from Connect AI’s systems or anonymized. Connect AI may

retain certain personal data if this required based on statutory retention obligations or if a further retention of certain personal data is necessary for the legitimate interests pursued by Connect AI (e.g. for evidence purposes).

Communication content (see section 2.5. below) is processed for a maximum of 12 months in order to recognize seasonal effects and long-tail questions and to continuously improve the quality of the service. After this period, the data is automatically deleted or anonymised. An earlier deletion can be requested by the Customer or the Customer's users via e-mail.

2.4. Data subjects

Connect AI processes personal data related to:

- Internal or external employees of the Customer
- Internal or external employees of the Customer's customers

2.5. Categories of personal data

Connect AI may process the following categories of personal data:

- Private and professional contact and identification data as well as (work) organisation data (e.g. surname, first name, gender, address, e-mail address, telephone number, mobile phone number, company, work area, department, cost centre, personnel numbers/personal identifiers, responsibilities, functions, attendance (yes/no), etc.).
- Image and/or sound recordings (e.g. audio, video, photos)
- Contract data (e.g. products purchased, (financial) services, date of purchase agreement, purchase price, special equipment, guarantees, etc.)
- IT usage data (e.g. user ID, roles, network connection data (e.g. IP address, MAC address, IMEI, network edge data), authorisations, login times, computer name, etc.)
- Communication content (chat prompts, natural-language queries and assistant responses) which may include, depending on the content entered by the Customer or the Customer's users, personal data requiring special protection (e.g. racial and ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data, biometric data uniquely identifying a natural person, social assistance measures, health data or data concerning sex life or sexual orientation, and data relating to criminal offences or the suspicion thereof) and/or personal data that is subject to a special statutory secrecy obligation (e.g., official, bank client secrecy, professional secrecy)

2.6. Special statutory secrecy obligations

Subject to section 2.5. above (see "Communication content"), Connect AI does not process any personal data that is subject to a special statutory secrecy obligation.

3. Place of data processing

3.1. Place of processing of personal data

The personal data is processed in or accessed from the following countries:

- Switzerland
- EU/EEA
- UK

- US

3.2. Guarantees in the case of data processing outside of the EU/EEA

When processing personal data outside of the EU/EEA, Switzerland and the UK, including countries without adequate level of data protection, Connect AI ensures adequate data protection by entering into data transfer agreements with the relevant recipients which include the necessary privacy safeguards. These agreements include contracts that have been approved, issued, or recognized by the European Commission and the Federal Data Protection and Information Commissioner, known as standard contractual clauses (SCC). Such contractual arrangements can partially offset weaker or absent legal protection but may not fully eliminate all risks (such as foreign government access). In exceptional cases, transmission to countries without adequate level of protection may also be permissible for other reasons, such as based on consent, in connection with foreign legal proceedings, or when the transmission is necessary for the execution of the Agreement.

3.3. Disclosure of personal data to sub-processors (e.g. group companies, suppliers)

The third parties listed in Attachment 3 (Sub-processors) have access to and process personal data as sub-processors or personal data is transferred to these third parties.

4. Notification of personal data breaches

Connect AI will without undue delay notify the Customer when Connect AI becomes aware of a personal data breach leading to or which is at risk of leading to, accidental or illegal destruction, loss or alteration or unauthorized disclosure or access to personal data. The notification will be via e-mail to the known representatives of the Customer.

Connect AI will provide the Customer with a description of the personal data breach and its consequences, the measures implemented to remedy the breaches/failures and minimize the consequences for the data subjects, and the measures adopted to prevent similar incidents in the future. If possible, Connect AI will indicate the number of data subjects that has been impacted by the personal data breach.

Attachment 2 – Technical and organisational measures (TOM)

Version: June 2025

This Attachment 2 describes the technical and organisational measures which are implemented by Connect AI under the Data Processing Agreement (DPA) within the scope of the Agreement to protect the personal data processed and to ensure data security appropriate to the risk (Art. 8 FADP and Art. 3 Data Protection Ordinance/DPO and Art. 32 (1) GDPR).

The technical and organisational measures are subject to technical progress and constant further development. Alternative or additional measures may be implemented, provided that the agreed level of protection is not reduced.

This Attachment 2 is limited to the description of the technical and organisational measures that Connect AI itself has taken. Connect AI has contractually obligated its sub-processors (see Attachment 3) to take appropriate technical and organisational measures. The description of these technical and organisational measures can be found in the corresponding documentation of the sub-processors. Upon request, Connect AI will provide corresponding detailed information.

1. Entry control (*Zutrittskontrolle*)

Measures suitable for preventing unauthorised persons from entering facilities in which personal data are processed (processing facilities).

Technical measures	**Organisational measures**
Manual locking system (key)	Key regulation / list
Security locks	Accompanying visitors
Locking system with code lock	Careful selection of cleaning staff

2. Access control (*Zugangskontrolle*)

Measures suitable for preventing the use of data processing systems (e.g. computers) by unauthorised persons.

Technical measures	**Organisational measures**
Login with passwords (e.g. user name and password)	Manage user permissions
Login with biometric data	Creating user profiles
Anti-Virus Software Clients	Password policy ("secure password")
Firewall (incl. regular updating)	General guideline "Data protection and security"
Mobile Device Management	Mobile Device Policy
VPN for remote access	
Encryption smartphones	
Automatic locking mechanisms (e.g. desktop lock)	

Encryption of notebooks / tablet	
Two-factor authentication	

3. Access control (*Zugriffskontrolle*)

Measures suitable for limiting the access of persons authorised to use a data processing system exclusively to the pesonal data subject to their access authorisation and for preventing the reading, copying, modification or removal of personal data by unauthorised persons (including unauthorised input into the memory and unauthorised viewing, inspection, modification or deletion of personal data stored):

Technical measures	**Organisational measures**
Access logging	Authorisation concept
Standard authorisation profiles on a "need to know" basis	Minimum number of administrators
	Management of user rights through administrators
	Periodic check of the assigned authorisations
	Standard process for authorisation allocation
	Clean-Desk/Clean-Screen Policy

4. Transfer and transmission control

Measures suitable for preventing the unauthorised reading, copying, modification or removal of personal data during electronic transmission or during its transport (incl. by means of data carriers), as well as measures for checking and determining to which entities a transmission of personal data using data transmission equipment is intended or takes place.

Technical measures
E-mail encryption
Use of Virtual Private Networks (VPN)
Logging of accesses and retrievals
Provision via encrypted connections such as sftp, https

5. Input control

Measures suitable to enable the verification and determination of whether, by whom and when which pesonal data have been entered, modified or removed in data processing systems.

Technical measures	**Organisational measures**
Technical logging of the entry, modification and deletion/anonymisation of data	Overview of which programmes can be used to enter, change or delete which data

Manual or automated control of the logs	Traceability of entry, modification and deletion/anonymisation of data through individual user names (not user groups)
Document management	

6. Order control

Measures suitable to ensure that the processing of personal data by third parties (sub-processors) only takes place in accordance with the Customer's instructions.

Organisational measures
Prior review of the security measures taken by the sub-procesor and their documentation (e.g. ISO certification, ISMS)
Careful selection of the relevant sub-processor (with regard to data protection and data security), prior review of the security measures implemented by the sub-processor, and assignment of the relevant responsibilities
Conclusion of the necessary data processing agreement with the sub-processor (incl. in the form of the EU standard contractual clauses, if required)
Right of the Customer to issue written instructions to the sub-processor
Obligation of the sub-processor's employees to data protection (incl. data secrecy)
Agreement on effective rights of control and follow-up (e.g. audits) vis-à-vis the sub-processor
Regulation on the involvement of further sub-processors
Agreement on the deletion or return of data after completion of the contractual relationship
In case of longer cooperation: Ongoing review of the sub-processor and its level of protection

7. Availability control

Measures suitable to protect the personal data against accidental or deliberate destruction or loss.

Technical measures	**Organisational measures**
Virus protection (incl. regular updating)	Backup & recovery concept (online/offline, on-site/off-site)
Firewall (incl. regular updating)	Multi-level backup concept with encrypted outsourcing of backups to a backup data centre
	Standard processes in the event of employee turnover/leaving
	Checking the backup process

8. Separability

Measures suitable to ensure the separate processing of personal data collected for different purposes.

Technical measures	Organisational measures
Separation of productive and test environment	Control via authorisation concept
Multi-client capability of relevant applications	Setting database rights

9. Review, assessment and evaluation

Establishment of procedures to regularly review, assess and evaluate the effectiveness of the technical and organisational measures to ensure the security of processing.

Data protection management:

Technical measures	Organisational measures
Documented security concept	Employee training in the area of data protection and security
Checking the effectiveness of the technical protective measures (at least once a year)	Regular sensitisation of employees (at least once a year)
	Internal / external Information Security Officer (ISO)
	Internal / external Data Protection Officer and Data Protection Representative (EU) as per Attachment 1 (Description of the data processing)
	Formalised process for handling requests from data subjects
	Commitment of employees to confidentiality and data protection (incl. data secrecy)
	Compliance with the information requirements pursuant to Art. 13 and 14 GDPR

Incident response management:

Technical measures	Organisational measures
Firewall (incl. regular updating)	Documented process for the detection and reporting of security incidents / data mishaps (also with regard to the obligation to report to the supervisory authority)
Spam filter (incl. regular updating)	Documented procedure for dealing with security incidents
Virus protection (incl. regular updating)	Involvement of DPO and ISO in security incidents and data breaches

	Documentation of security incidents and data breakdowns e.g. via ticket system
	Formal process and responsibilities for follow-up on security incidents and data breaches

Data protection-friendly default settings (Privacy by Design / Privacy by Default):

Technical measures	**Organisational measures**
No collection of more personal data than necessary for the respective purpose	Definition of the role for Privacy by Design / Privacy by Default in projects

Attachment 3 – Sub-processors

Version: June 2025

This Attachment 3 lists the sub-processors engaged by Connect AI. The engagement of new sub-processors and the replacement of existing sub-processors shall be governed by the provisions of the Data Processing Agreement (DPA).

Sub-processor (company name, address)	**Service**	**Location of stored data (if applicable)**	**Personal data processed**	**Guarantee under EU-GDPR and further remarks**
Google Cloud Platform Google Belgium NV/SA, Avenue Louise 326, 1050 Brussels, BE	Cloud hosting & storage, AI-based natural language processing	EU/EEA	All personal data processed under the Agreement, system logs, metadata	Data Processing Agreement incl. EU Standard Contractual Clauses, ISO 27001, SOC 2
OpenAI Ireland Ltd. / OpenAI Inc. * 3 Dublin Landings, North Wall Quay, Dublin 1, IE	GPT-API LLM inference	EU / US	Chat prompts, outputs, metadata	Data Processing Agreement incl. EU Standard Contractual Clauses, SCC Module 3, SOC 2
Pinecone Systems, Inc., 228 Hamilton Avenue, Palo Alto, CA 94301, USA	Vector database	EU/EEA	High-dimensional data vectors derived from personal data	Data Processing Agreement incl. EU Standard Contractual Clauses, SOC 2
Freihandlabor GmbH Bremgartnerstr. 18, 8003 Zürich, CH	Multi-LLM routing & vector DB	CH / EU	Prompts, embeddings	Data Processing Agreement, no third-country transfer
n8n GmbH, Novalisstr. 10, 10115 Berlin, Germany	Workflow-Automation services	EU/Deutschland	Conversational data and related metadata	Data Processing Agreement including EU Standard Contractual Clauses
Zappr.AI LTD, 41 Devonshire Street, Ground Floor, London W1G 7AJ, UK	AI platform services	EU/EEA, UK	User identifiers, system usage data	Data Processing Agreement incl. EU Standard Contractual Clauses

* Connect AI is in the process of migrating to the fully EU-hosted version of OpenAI, and both EU- and US-based data centres may currently be in operation.