

Data Processing Agreement

This Data Processing Agreement (“DPA”) governs how 4Degrees processes your firm’s data when you connect 4Degrees to an external AI client through the **4Degrees AI Connector**. It sets out, in one place: the roles of each party, the categories of data processed, the sub-processors engaged, the commitment that your data is not used to train AI models, the security measures in place, breach notification, international transfers, retention, audit rights, and how data-subject rights are handled.

■ Effective June 19, 2026 · Version 1.0

DOWNLOAD

A PDF copy of this agreement is available for your records: [Download the DPA \(PDF\)](#).

1. Parties & scope

This DPA is entered into between **4Degrees, Inc.** (“4Degrees”, “we”, “us”) and the customer organization whose authorized administrator enables the 4Degrees AI Connector (“Customer”, “you”, “your firm”). It governs the processing of Customer data through the connector and supplements, but does not replace, the master agreement between you and 4Degrees governing your overall use of the platform.

This DPA covers the **4Degrees AI Connector** — the Model Context Protocol (MCP) server hosted at <https://mcp.4degrees.ai/mcp> that lets AI assistants such as Anthropic’s Claude and OpenAI’s ChatGPT query and, with explicit per-user consent, modify your 4Degrees data on your behalf. Where this DPA and the master agreement conflict on the subject of data processing, this DPA controls for the connector.

2. Roles of the parties

KEY CLAUSE

With respect to data processed through the connector, your firm is the **data controller** and 4Degrees acts as a **data processor**, processing data only on your documented instructions.

Your firm determines the purposes and means of processing the personal data in your 4Degrees account and is the **controller**. 4Degrees processes that data on your behalf and is a **processor**. The AI client you connect (Claude, ChatGPT, or another MCP client) is an independent controller of the conversation that occurs inside that client and is governed by that vendor's own terms; 4Degrees is not a party to your relationship with the AI vendor.

4Degrees processes connector data only on your documented instructions, which include enabling the connector, the queries your authorized users make through it, and the configuration you set in your workspace. 4Degrees will not process connector data for any other purpose.

3. Subject matter, duration & purpose

Subject matter. Processing of Customer CRM data to answer your authorized users' questions and to perform a fixed, enumerated set of write operations that those users explicitly request through their AI assistant.

Duration. For as long as the connector is enabled in your workspace. Processing of connector requests ceases when an administrator disables the AI Connector feature, which immediately invalidates every token issued to your organization.

Nature & purpose. Reads return data your seat is already permitted to view; writes are limited to the enumerated operations listed in our [connector privacy policy](#), are permission-scoped, and are auditable.

4. Categories of data & data subjects

The connector processes the following categories of Customer data (see Annex A for the authoritative list):

- Contacts — name, title, company, email, phone, location, tags, custom fields, relationship-strength signals.
- Companies — name, domain, location, employee count, deal count, custom fields.
- Deals — name, pipeline, stage, owner, value, associated contacts, tags, custom fields.
- Interaction *metadata* — subject, sender / recipient names, date, and type (email / meeting / note).
- Custom-field and pipeline definitions, team membership, portfolio dashboards, and introduction paths.

Data subjects are the contacts, companies, and teammates represented in your 4Degrees account.

KEY CLAUSE

Encrypted email and meeting **bodies are never returned** to any AI assistant — only metadata is queryable. Passwords, API keys, billing data, admin settings, and any data outside your firm's permission scope are never exposed.

5. No AI model training

KEY CLAUSE

Neither Anthropic (per Anthropic's Connector Terms) nor OpenAI (per the OpenAI Apps SDK terms) trains its models on data returned by third-party connectors. 4Degrees does not share connector data with any other third party, and does not use connector data to train any model.

The data the connector returns to your AI assistant is not used by the AI vendor to train its models, and 4Degrees does not use it to train any model or share it with any third party beyond the AI vendor

you have connected. This commitment applies to all Customer data processed through the connector.

6. Sub-processors

The Customer authorizes 4Degrees to engage the sub-processors listed in Annex B to process Customer data in connection with the connector. Each sub-processor is bound by a written agreement imposing data-protection obligations no less protective than those in this DPA, and 4Degrees remains responsible for each sub-processor's performance of its obligations.

4Degrees maintains the current list of sub-processors in Annex B. 4Degrees will give the Customer at least **thirty (30) days'** prior notice before adding or replacing a sub-processor that processes Customer data, by updating Annex B and notifying the Customer's designated administrator. If the Customer has a reasonable, data-protection-based objection to a new sub-processor, the Customer may raise it with 4Degrees during the notice period; the parties will work in good faith to resolve the objection, and if it cannot be resolved the Customer may suspend or terminate use of the connector with respect to the affected processing.

The AI vendor you connect (Anthropic or OpenAI) processes connector data as an **independent controller** under its own terms, not as a 4Degrees sub-processor.

7. Security measures

4Degrees maintains technical and organizational measures appropriate to the risk, including those set out in Annex C and summarized below:

- **Encryption in transit.** TLS 1.2 or higher on every network leg — the AI assistant to the connector, and the connector to the 4Degrees database inside a private virtual private cloud (VPC).
- **Encryption at rest.** Customer CRM data is encrypted at rest in Google Cloud SQL with Google-managed keys. Stored bot/connector credentials are additionally encrypted with a dedicated application key. Email and meeting bodies are independently

encrypted with per-tenant keys and are never exposed through the connector.

- **Permission-scoped access.** Every read and write enforces the same permission cascade as the 4Degrees web app; the connector cannot access a record your seat cannot see.
- **Least-data logging.** The connector does not store the text of your AI conversation, the arguments passed to it, or the CRM data it returns. It records only request metadata (numeric user/org identifiers, the endpoint called, success/failure, a one-way hash of the token reference, and a timestamp) for audit and reliability.
- **Consent-gated writes.** Writes require explicit per-user consent, are limited to a fixed enumerated set, perform no deletes, no bulk operations, no cross-tenant writes, and no background/autonomous actions.
- **Immediate revocation.** Tokens can be revoked from the AI client, from 4Degrees account settings, or organization-wide by an administrator; revocation is effective on the next request.

4Degrees holds a **SOC 2 Type II** attestation covering its platform; the connector operates within that existing control scope and does not introduce regulated data flows beyond it. A copy of the current SOC 2 report and 4Degrees' Security Policy is available to customers under NDA on request to security@4degrees.ai.

8. Confidentiality

4Degrees ensures that personnel authorized to process Customer data are bound by appropriate obligations of confidentiality.

9. Data-subject rights & assistance

Taking into account the nature of the processing, 4Degrees assists the Customer by appropriate technical and organizational measures, insofar as possible, to fulfill the Customer's obligation to respond to requests to exercise data-subject rights. Because connector access mirrors your existing 4Degrees permissions, data subject records remain manageable through the 4Degrees web app.

10. Personal-data breach notification

4Degrees will notify the Customer without undue delay, and in any event within **seventy-two (72) hours** of becoming aware of a personal-data breach affecting Customer data processed through the connector. The notification will, to the extent known and as information becomes available, describe:

- the nature of the breach, including the categories and approximate number of data subjects and records concerned;
- the likely consequences of the breach;
- the measures taken or proposed to address the breach and mitigate its effects; and
- a contact point at 4Degrees from whom further information can be obtained.

4Degrees will cooperate with the Customer and take reasonable steps as directed by the Customer to assist in the investigation, mitigation, and remediation of the breach. Notification of a breach is not an acknowledgement by 4Degrees of fault or liability.

11. Retention, return & deletion

The connector itself does not retain conversation text, request arguments, or returned CRM data. The only connector-specific data retained is request metadata (as described in section 7), kept for audit and reliability under the standard 4Degrees database backup, retention, and deletion policies described in our [master Privacy Policy](#).

On termination or expiry of the connector engagement — which takes effect immediately when an administrator disables the AI Connector feature, invalidating every token issued to the organization — 4Degrees will, at the Customer's election, delete or return the connector request metadata, and delete existing copies within **ninety (90) days**, except where retention is required by applicable law (in which case 4Degrees will continue to protect that data and limit further processing to the extent of the legal

requirement). Customer CRM data itself is governed by the deletion terms of the master agreement and the master Privacy Policy.

12. International transfers

4Degrees hosts each customer's environment on Google Cloud Platform in a defined region. Customer environments are provisioned in either the **United States** or the **Kingdom of Saudi Arabia** region; your environment's region is the one assigned to your firm at provisioning and is available from your account team on request. Customer CRM data is processed and stored within that region; 4Degrees does not move Customer CRM data between regions in the ordinary course of operating the connector.

Where processing of personal data nonetheless involves a transfer across borders — for example, support or administrative access by 4Degrees personnel, or the connected AI vendor's own processing as an independent controller — 4Degrees relies on an appropriate transfer mechanism recognized under applicable data-protection law, including the European Commission's Standard Contractual Clauses (and the UK International Data Transfer Addendum where applicable), supplemented by the technical measures in section 7. The connected AI vendor's cross-border processing is governed by that vendor's own terms and transfer mechanisms.

13. Audit & records

Every successful write through the connector is recorded in your 4Degrees activity feed — who initiated it, the action type, the target resource, the timestamp, and, where applicable, the prior value of the changed field. Your administrator can review this audit log at any time.

4Degrees makes available to the Customer the information reasonably necessary to demonstrate compliance with this DPA, including its current SOC 2 Type II report and a summary of its technical and organizational measures (Annex C), provided under NDA on request. Where the Customer reasonably requires further information to satisfy a regulatory audit obligation that cannot be met by those materials, the parties will agree in advance on the

scope, timing, and reasonable cost of any additional audit, conducted no more than once per twelve-month period (absent a regulator requirement or a confirmed breach), during business hours, and subject to confidentiality and to not unreasonably disrupting 4Degrees' operations or the security of other customers' data.

14. Liability & governing terms

This DPA forms part of, and is subject to, the master agreement between the Customer and 4Degrees. Each party's liability arising out of or related to this DPA, whether in contract, tort, or under any other theory of liability, is subject to the limitations and exclusions of liability set out in the master agreement, and any reference in the master agreement to the liability of a party means the aggregate liability of that party under the master agreement and this DPA together.

This DPA is governed by, and construed in accordance with, the governing law and exclusive jurisdiction stated in the master agreement, without regard to its conflict-of-laws provisions. If the master agreement does not state a governing law, this DPA is governed by the laws of the State of Delaware, United States. In the event of a conflict between this DPA and the master agreement on the subject of the processing of personal data, this DPA prevails. If any provision of this DPA is held invalid or unenforceable, the remainder remains in full force and effect.

15. Contact

Data-protection and DPA questions: privacy@4degrees.ai.

Security disclosures: security@4degrees.ai.

General support: support@4degrees.ai.

Annex A — Categories of personal data

The data categories enumerated in section 4 above, as exposed by the connector's `discover`, `query`, and `compare` tools and modified by the consented `execute_action` writes.

Annex B — Sub-processors

The sub-processors 4Degrees engages to deliver the connector:

Sub-processor	Purpose	Processing location
Google Cloud Platform (Google LLC)	Cloud hosting, application compute (Cloud Run), and database (Cloud SQL) for the connector and the 4Degrees platform.	United States or Kingdom of Saudi Arabia (per the Customer’s assigned region)
Functional Software, Inc. (Sentry)	Application error and performance monitoring. Receives operational diagnostics and request metadata, not CRM record content.	United States

The connected AI vendor — **Anthropic, PBC** (Claude) or **OpenAI, L.L.C.** (ChatGPT), depending on which client the Customer connects — processes connector data as an **independent controller** under its own terms, and is not a 4Degrees sub-processor. Per those vendors’ terms, neither trains its models on data returned by third-party connectors.

Annex C — Technical & organizational measures

The security measures enumerated in section 7 above.