

Dataceen Data Processing Agreement

This Data Processing Agreement ("DPA") sets out how Dataceen processes personal data on behalf of its customers, as article 28 of the GDPR requires. It forms part of the agreement under which the customer uses Dataceen (the "Terms"), and applies automatically when the customer accepts the Terms; no separate signature is needed. A customer who wants a countersigned copy can ask at info@dataceen.com.

Parties

- **The customer** ("Controller"): the organisation or person that has accepted the Terms.
- **Dataceen** ("Processor"): Dataceen AB, organisation number 559529-9016, Engelbrektsgatan 9, 411 27 Göteborg, Sweden.

Effective date: the date the customer accepts the Terms, or 18 October 2026 for customers who accepted earlier versions.

1. Definitions

Terms such as *personal data*, *processing*, *controller*, *processor*, *data subject*, *personal data breach* and *supervisory authority* have the meaning given in the GDPR (Regulation (EU) 2016/679).

- **Customer Personal Data:** personal data in customer content or system data that Dataceen processes on the Controller's behalf.
- **Customer content:** sources, models, scopes, rules, instructions, generated code and applications the Controller submits to or creates with Dataceen.
- **System data:** the records held in a system published from the Controller's models, and the data its applications and users send to it, including example data.
- **Subprocessor:** a third party Dataceen engages to process Customer Personal Data.
- **Data protection law:** the GDPR, the Swedish Data Protection Act (2018:218), the UK GDPR and the Swiss Federal Act on Data Protection, as far as each applies.

2. Roles, scope and instructions

2.1 The Controller determines the purposes and means of processing Customer Personal Data. Dataceen processes it only as the Controller's processor, and only as described in Annex 1.

2.2 Dataceen processes Customer Personal Data only on the Controller's documented instructions. The Terms, this DPA, and the Controller's configuration and use of Dataceen (the models it builds, the scopes it publishes, the applications and agents it connects, the storage it chooses) are the Controller's complete instructions. Further instructions must be in writing and consistent with the Terms.

2.3 Dataceen may process Customer Personal Data otherwise only where Union or Member State law requires it. Dataceen then informs the Controller before processing, unless that law prohibits it.

2.4 Dataceen tells the Controller without delay if, in its opinion, an instruction infringes data protection law.

2.5 The Controller is responsible for the lawfulness of the processing it instructs: having a legal basis, giving notice to data subjects, and not putting special categories of personal data into Dataceen unless its own legal basis covers it.

2.6 Dataceen does not use Customer Personal Data to train AI models, for advertising, or for any purpose of its own. Account data about the Controller's users is processed by Dataceen as a controller under its Privacy Policy at dataceen.com/legal/privacy, not under this DPA.

2.7 When the Controller chooses storage it runs itself, system data is stored there and not by Dataceen; Dataceen processes it only while serving requests to the Controller's systems.

3. Confidentiality and security

3.1 Dataceen ensures that everyone it authorises to process Customer Personal Data is bound by confidentiality, by contract or by law, and has access only as far as their task requires.

3.2 Dataceen implements the technical and organisational measures in Annex 2, which meet article 32 of the GDPR. Dataceen may update them, provided the overall level of protection does not decrease.

3.3 Dataceen staff access the content of a Controller's models or systems only to provide support the Controller has asked for, to investigate a security incident, or where the law requires it.

4. Subprocessors

4.1 The Controller gives Dataceen general authorisation to engage subprocessors. The current list is in Annex 3 and at dataceen.com/legal/subprocessors.

4.2 Dataceen gives at least 30 days' notice before adding or replacing a subprocessor, by updating that page and emailing the Controller's account owner. The Controller may object on reasonable data protection grounds within that period. If the parties cannot resolve the objection, the Controller may terminate the affected part of the service and receive a refund of prepaid, unused credits for it.

4.3 Dataceen imposes on each subprocessor, by written contract, data protection obligations that are no less protective than this DPA. Dataceen remains fully liable to the Controller for each subprocessor's performance.

4.3a If an existing subprocessor changes its terms in a way that affects how Customer Personal Data is retained, used or located, Dataceen tells the Controller before the change takes effect where Dataceen has notice of it, and in any case without undue delay, and the Controller may object as in 4.2. Dataceen does not opt in to any subprocessor programme that uses Customer Personal Data for model training or improvement.

4.4 Services the Controller connects itself are not subprocessors of Dataceen: the AI host the Controller uses (such as Claude or Cursor), a GitHub account the Controller invites or transfers a repository to, and storage the Controller runs. Their own terms govern them.

5. Assistance

5.1 Data subject requests. Dataceen gives the Controller the means to find, export, correct and delete records in its systems through Studio, the API and the MCP tools. If a data subject contacts Dataceen directly about Customer Personal Data, Dataceen forwards the request to the Controller without undue delay and does not answer it itself, except to say it has been forwarded.

5.2 Security, impact assessments and consultation. Taking into account the nature of the processing and the information available to it, Dataceen assists the Controller in meeting its obligations under articles 32 to 36 of the GDPR, including data protection impact assessments and prior consultation with a supervisory authority.

5.3 Assistance beyond what Studio and the documentation provide may be charged at Dataceen's then-current hourly rate, unless it results from Dataceen's breach of this DPA.

6. Personal data breaches

6.1 Dataceen notifies the Controller without undue delay, and in any case within 48 hours, after becoming aware of a personal data breach affecting Customer Personal Data.

6.2 The notice describes, as far as then known: the nature of the breach, the categories and approximate number of data subjects and records concerned, the likely consequences, the measures taken or proposed, and a contact point. Dataceen supplements the notice as more becomes known.

6.3 Dataceen takes reasonable steps to contain the breach and limit its effects, and cooperates with the Controller's own notification to the supervisory authority and to data subjects. Notification by Dataceen is not an admission of fault.

7. International transfers

7.1 Dataceen stores Dataceen-hosted system data in the EU, in Sweden and Belgium. Dataceen transfers Customer Personal Data outside the EEA only to the subprocessors in Annex 3, and only with a transfer mechanism recognised by data protection law: an adequacy decision (including the EU-US Data Privacy Framework for certified recipients) or the Standard Contractual Clauses (Decision (EU) 2021/914, module 3, processor to processor), with transfer impact assessments where needed.

7.2 For Customer Personal Data subject to UK law, the UK International Data Transfer Addendum applies; for Swiss law, the Standard Contractual Clauses with the Swiss amendments apply.

7.3 The Controller may ask for a copy of the safeguards for any transfer, with commercially sensitive terms removed.

8. Audits and information

8.1 Dataceen makes available to the Controller the information needed to demonstrate compliance with article 28 of the GDPR: this DPA, the measures in Annex 2, the subprocessor list, and on request any security certifications or third-party audit reports Dataceen holds.

8.2 Where that information is not sufficient, or a supervisory authority requires it, the Controller may audit Dataceen, itself or through an independent auditor bound by confidentiality. The Controller gives at least 30 days' written notice, audits no more than once in any 12 months except after a personal data breach, and bears its own costs. Audits take place during business hours and must not compromise other customers' data or Dataceen's security.

8.3 Every call to a published system is recorded with its caller, time, scope and outcome, but not the content returned; records are kept 90 days, and Dataceen provides the Controller with the records for its own systems on request.

9. Return and deletion

9.1 Until the service ends, the Controller can export its system data through the API and its generated code through its repository, or take over the repository entirely.

9.2 When the service ends, Dataceen deletes Customer Personal Data within 30 days, unless the Controller asks within that period for it to be returned in a machine-readable format. Deleted data may remain in database snapshots for up to 3 months after deletion; snapshots are used only to restore the service and are not accessed otherwise.

9.3 Dataceen may keep Customer Personal Data longer only where Union or Member State law requires it, and then only for that purpose, under this DPA's protections.

9.4 On request, Dataceen confirms deletion in writing.

10. General terms

10.1 **Term.** This DPA applies for as long as Dataceen processes Customer Personal Data for the Controller, and its obligations on deletion and confidentiality survive the end of the Terms.

10.2 **Liability.** Each party's liability under this DPA is subject to the limitations in the Terms, except where data protection law does not allow them to be limited. The limitation in the Terms applies to claims under this DPA, including regulatory fines and claims by data subjects, to the extent the law allows.

10.3 **Precedence.** If this DPA conflicts with the Terms, this DPA prevails for the processing of Customer Personal Data. If it conflicts with the Standard Contractual Clauses, the clauses prevail.

10.4 **Changes.** Dataceen may update this DPA to reflect changes in law or in the service, with at least 30 days' notice, provided the protection of Customer Personal Data does not decrease.

10.5 Governing law and disputes. This DPA is governed by Swedish law. Disputes are settled by the Gothenburg District Court (Göteborgs tingsrätt) as first instance, except where the Standard Contractual Clauses require otherwise.

Annex 1 — Details of the processing

Item	Description
Subject matter	Providing Dataceen to the Controller: drafting models from its sources, publishing and hosting systems, generating example data, code and applications, and keeping repositories
Duration	The term of the Terms, plus the deletion period in section 9
Nature of processing	Storage, retrieval, search, structuring, transformation into generated systems, transmission to the Controller's applications and agents, AI processing of sources, logging, deletion
Purpose	Operating the systems the Controller builds, as the Controller instructs
Categories of data subjects	Determined by the Controller. Typically its customers, employees, contractors, suppliers and the users of its applications, and people named in sources it adds
Categories of personal data	Determined by the Controller. Typically names, contact details, addresses, identifiers, records of orders, assets, work orders, invoices and similar business records, and usage logs of its systems
Special categories	None expected. The Controller must not submit them unless its own legal basis covers it and it has told Dataceen in writing
Frequency	Continuous, for as long as the Controller's systems run
Retention	As configured by the Controller; deleted as section 9 describes
Location	Dataceen-hosted data in the EU (Sweden and Belgium); storage the Controller runs, where it chooses; transfers per section 7

Annex 2 — Technical and organisational measures

Area	Measure
Access control	Every person, application and agent signs in through an identity provider (Microsoft Entra External ID or the Controller's directory). Access is granted per scope, defined in the model, down to entity, operation, property and row
Tenant separation	Each published model has its own database, named after the system, domain and model; no two customers' system data share a database. Search indexes are separated per system
Encryption	TLS for all data in transit; encryption at rest for Dataceen-hosted storage and backups
Logging	Every call to a published system is recorded with caller, time, scope and outcome, not the content returned; kept 90 days; provided to the Controller on request
Staff access	Least privilege. Multi-factor authentication is required for all administrative access to the platform's cloud, database, search, source-code and identity consoles. Administrative access is reviewed quarterly, and access that is no longer needed is removed; access of people who leave is removed the same day
Infrastructure	Hosted on Microsoft Azure (Sweden Central) on Kubernetes, with databases in MongoDB Atlas (AWS Stockholm) and search indexes in Elastic Cloud (Google Cloud, Belgium); hosted customer applications are isolated by network policy; platform secrets are held in Kubernetes Secrets with access restricted to the platform's own services, and data-protection keys are stored encrypted in the database
Development	Code review before release;

Area	Measure
Availability	dependencies monitored for known vulnerabilities Database snapshots in MongoDB Atlas: every 6 hours kept 7 days, daily kept 7 days, weekly kept 4 weeks, monthly kept 3 months; snapshots are used only to restore the service; restore tested twice a year, and the search index rebuild verified at the same time
Incident response	A documented process for detecting, containing and notifying personal data breaches (section 6)
Subprocessors	Assessed before engagement and bound by written data protection terms (section 4)
People	Staff bound by confidentiality and trained in data protection

Annex 3 — Subprocessors

The current list is kept at dataceen.com/legal/subprocessors; as of the effective date it is:

Subprocessor	Purpose	Customer Personal Data involved	Location	Transfer mechanism
Microsoft Azure	Hosting of Studio, MCP servers, systems and applications	All	EU (Sweden Central)	n/a within EU
MongoDB Atlas (MongoDB, Inc.)	Databases of Dataceen-hosted systems	All system data	EU (AWS Stockholm)	n/a within EU
Elastic Cloud (Elasticsearch B.V.)	Search indexes of Dataceen-hosted systems	System data in the search index	EU (Google Cloud, Belgium)	n/a within EU
Microsoft (Entra External ID)	Sign-in for the Controller's	Identities of users of the Controller's	EU (Microsoft EU)	n/a within EU; DPF and SCCs under

Subprocessor	Purpose	Customer Personal Data involved	Location	Transfer mechanism
	users and applications	systems	datacenters)	Microsoft's DPA for any support access from outside the EU
Anthropic (Claude API)	Drafting models from sources, generating example data and applications	Personal data contained in sources and instructions	US	SCCs (modules 2 and 3), UK Addendum and Swiss Addendum in Anthropic's DPA
GitHub	Private repositories holding generated code	Personal data contained in generated code or example data, if any	US	SCCs in GitHub's Data Protection Agreement

Providers that process only Dataceen's own account data (payment, email, website analytics) are listed in the Privacy Policy and are not subprocessors under this DPA.