Data Processing Agreement

How Cravit B.V., as processor, handles personal data when providing the Cravit Gateway: what is processed, where, by whom, for how long, and what happens in case of a breach.

Version 1.0 — November 2026. Part of the Agreement with Cravit B.V., Breda, the Netherlands (KvK 20099850). It prevails over the other parts of the Agreement for the processing of personal data.

1. Parties and subject

1. This Data Processing Agreement ("DPA") is part of the Agreement between Cravit B.V., Breda, the Netherlands, KvK 20099850 ("Cravit", the processor) and the Customer (the controller) for the Cravit Gateway (the "Service"), as defined in the Terms of Use.
2. It sets out the terms under which Cravit processes personal data on behalf of the Customer when providing the Service, as required by article 28 of the General Data Protection Regulation (GDPR).
3. Capitalised terms have the meaning given in the Terms of Use or in the GDPR.

2. Scope of the processing

1. Cravit processes personal data only for the purposes described in the Annex: forwarding requests between the Customer's AI Application and the Customer's Odoo Environment, and keeping the Audit Log.
2. Customer Data retrieved from Odoo passes through the Service to the AI Application and is not stored by Cravit, except for the Audit Log metadata described in the Annex.
3. The processing by the AI Provider is outside the scope of this DPA. The Customer contracts with the AI Provider directly (Terms of Use, article 6).

3. Instructions

1. Cravit processes personal data only on documented instructions from the Customer. The Agreement, the configuration the Customer's administrators make in the admin console and the requests Users send through the Service constitute those instructions.
2. Cravit informs the Customer if, in its opinion, an instruction infringes the GDPR or other data protection law.
3. Cravit does not use personal data for its own purposes, does not sell it and does not use it to train AI models.

4. Confidentiality

Cravit ensures that persons authorised to process the personal data are bound by confidentiality and have access only to the extent needed to operate and support the Service.

5. Security

1. Cravit implements appropriate technical and organisational measures as described in the Terms of Use, article 11, and in the Annex, within an ISO 27001-certified information security management

system.

2. Cravit may update the measures provided the level of protection does not decrease.

6. Sub-processors

1. The Customer gives general authorisation for the sub-processors listed in the Annex.
2. Cravit informs the Customer at least 30 days before adding or replacing a sub-processor. The Customer may object on reasonable grounds within that period; if no solution is found, the Customer may terminate the Agreement as of the date the change takes effect.
3. Cravit imposes data protection obligations on each sub-processor that are no less protective than those in this DPA and remains responsible for their performance.

7. Transfers outside the EEA

1. The Service is hosted and the Audit Log is stored in Google Cloud regions within the European Union.
2. Where a sub-processor is part of a group established outside the EEA, transfers are covered by the European Commission's Standard Contractual Clauses as included in that sub-processor's data processing terms (for Google Cloud: the Cloud Data Processing Addendum).
3. Data sent by the Customer's Users to an AI Application is transferred by the Customer to the AI Provider under the Customer's own agreement with that provider, and falls outside this article.

8. Data breaches

1. Cravit notifies the Customer of a personal data breach affecting Customer Data without undue delay and in any case within 48 hours of discovery, to the administrators' email addresses registered in the admin console.
2. The notification contains, as far as known: the nature of the breach, the categories and approximate number of data subjects and records, the likely consequences and the measures taken or proposed. Information may be provided in phases.
3. The Customer is responsible for notifying the supervisory authority and the data subjects where required; Cravit provides reasonable assistance.

9. Data subjects' rights and assistance

1. Because Cravit does not store Customer Data from Odoo, requests from data subjects are handled by the Customer in its Odoo Environment. Cravit assists with requests that concern the Audit Log (the Customer can view and export it in the admin console).
2. Cravit assists the Customer, where reasonably needed and taking into account the nature of the processing, with security, breach notification and data protection impact assessments. Cravit may charge its applicable rates for assistance that goes beyond what the Service itself provides.

10. Audits

1. Cravit makes available the information needed to demonstrate compliance with this DPA, including its ISO 27001 certificate and, on request, summaries of relevant audit reports of its sub-processors.

2. Where that information is insufficient, the Customer may, once per year and on 30 days' notice, have an audit performed by an independent auditor bound by confidentiality, during office hours and without disrupting the Service. Each party bears its own costs.

11. End of the processing

1. When the Agreement ends, Cravit revokes all Access Keys. On request within 30 days the Customer receives an export of the Audit Log.
2. Cravit deletes the Customer's data, including the Audit Log and stored credentials, within 60 days after the end of the Agreement, unless the law requires longer retention.

12. Liability and precedence

1. The limitation of liability in the Terms of Use applies to this DPA.
2. In case of conflict between this DPA and the other parts of the Agreement, this DPA prevails for the processing of personal data.
3. Dutch law applies; disputes are submitted to the court competent under the Terms of Use.

Annex – Details of the processing

Item	Content for the Service
Purpose	Forwarding requests between the AI Application and the Customer's Odoo Environment; keeping the Audit Log; operating the Customer's account (administrators, Users, billing contact).
Categories of data subjects	The Customer's administrators and Users; persons whose data is in the Customer's Odoo (customers, suppliers, employees, contacts).
Categories of personal data	Name, email address and user id of administrators and Users (account, Audit Log); the Odoo login and API key of each User (stored encrypted); all personal data in Odoo that a User retrieves or changes (transit only, not stored).
Audit Log	Per request: User, time, function used, Odoo model and record ids, result. No prompt or response content.
Retention	Audit Log: term of the Agreement and at least 12 months thereafter, deleted within 60 days after the end of the Agreement. Other Customer Data: not stored.
Sub-processors	Google Cloud EMEA Limited, Dublin, Ireland — hosting, storage and logging (Cloud Run, Firestore, Cloud Logging), EU regions. Google LLC as email delivery provider for the Service's notification mails (Google Workspace, EU data region where offered).
Location	European Union (Google Cloud, region europe-west1, Belgium, with logging and storage configured in EU regions).

Data breach notification	Within 48 hours of discovery.
Security measures	ISO 27001 ISMS; TLS for all connections; encrypted storage of keys and credentials; per-User access limited to the User's own Odoo rights; confirmation before every change in Odoo; IP allow-lists and two-factor authentication for the admin console; audit logging; least-privilege access for Cravit staff.
Expressly out of scope	Processing by the AI Provider; the Customer contracts with that party directly.