Sinsou Data Processing Agreement

For Integration Management on Alumio, for customers with their own Alumio licence.

Data Processing Agreement

Parties

- The customer named in the Quote, hereinafter "Controller"
- Sinsou B.V., KvK 86851314, Hoenderkamp 20, 7812 VZ Emmen, hereinafter "Processor"

Article 1. Subject and definitions

1.1 This data processing agreement belongs to the Agreement. Processor processes personal data only to provide the services in the Agreement, as described per service in Annex 1.

1.2 If this data processing agreement and the Agreement conflict, this data processing agreement prevails on matters of personal data, except for liability, which follows Article 12.1.

1.3 In this data processing agreement:

a. **Agreement** means the Quote as accepted by Controller, with any addendum, any service level agreement and Processor's General Terms and Conditions;

b. **Connected Systems** means Controller's systems and the third-party services Controller procures itself, such as webshop, ERP, PIM, WMS and integration platform, which Processor connects to on Controller's instruction;

c. **Service Environments** means the systems and environments listed per service in Annex 1;

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

Article 2. Instructions

2.1 Processor processes personal data only on Controller's documented instructions and for the purpose Controller has set. The Agreement and Annex 1 are those instructions. Processor does not use the data for its own purposes and does not disclose it to third parties, unless Controller instructs it or the law requires it. In the latter case Processor informs Controller in advance, unless the law prohibits this.

2.2 If Processor considers an instruction to breach the GDPR or other law, Processor notifies Controller immediately.

Article 3. Confidentiality

3.1 Processor and everyone working under its authority, including contractors, are bound in writing to keep the personal data confidential. Only persons who need the data for the service get access.

Article 4. Security

4.1 Processor takes appropriate technical and organisational measures to secure the personal data, as described per service in Annex 3. Processor may change these measures as long as the level of security does not decrease.

Article 5. Sub-processors

5.1 Controller gives general authorisation for the sub-processors in Annex 2 for the service it uses.

5.2 Processor notifies Controller by email at least 30 days before adding or replacing a sub-processor. Controller may object on reasonable grounds within that period. If the parties cannot resolve the objection, Controller may terminate the affected part of the Agreement. If a sub-processor in Annex 2 changes its own sub-processors, Processor passes that notice on to Controller within five working days after receiving it; Controller may object within the period the sub-processor gives Processor, and for the rest 5.2 applies.

5.3 Processor imposes on each sub-processor in writing the same obligations as in this data processing agreement. Processor remains responsible to Controller for the sub-processor's performance, within the limitation in Article 12.1.

5.4 The suppliers of the Connected Systems are not sub-processors of Processor. This includes an integration platform that Controller licenses itself, such as Alumio. Controller contracts with those suppliers directly.

5.5 Where Processor itself procures a platform or environment in which Controller's personal data is processed, its supplier is a sub-processor and is listed in Annex 2.

Article 6. Retention

6.1 Processor keeps personal data no longer than the periods stated in Annex 1 for the service concerned.

6.2 Error messages, alerts and incident records that Processor writes itself contain no personal data beyond the record identifier the Agreement provides for, such as an internal record ID. This does not apply to content Controller supplies itself, such as in a ticket, email or chat.

6.3 Controller may instruct different periods in writing.

Article 7. Location and transfers

7.1 Processor and its sub-processors store the personal data within the European Economic Area (EEA), unless Annex 2 states otherwise for a sub-processor. Where a sub-processor can store the data outside the EEA, or access or process it from a country outside the EEA, Annex 2 says so, with the basis for that transfer.

7.2 Sending data to and retrieving data from the Connected Systems happens on Controller's instruction. Where Controller is established outside the EEA, or a Connected System is located outside the EEA, Controller is responsible for that transfer being lawful.

7.3 Processor does not transfer personal data outside the EEA other than under 7.1 and 7.2, unless Controller agrees in writing in advance and appropriate safeguards are in place.

Article 8. Personal data breaches

8.1 If Processor discovers a security incident in which Controller's personal data may have been lost or altered, or accessed by unauthorised persons, Processor notifies Controller by phone and email without undue delay and in any case within 24 hours of discovery, with what is known at that point about the nature, scope, data affected and measures taken. Processor supplements the notification as more becomes known.

8.2 Processor carries out the instructions that follow from the investigation and helps Controller with any notification to the supervisory authority or data subjects. Controller decides on that notification.

Article 9. Assistance

9.1 Processor helps Controller with data subject requests (Articles 15 to 22 GDPR), with a data protection impact assessment and with questions from a supervisory authority, as far as they concern Processor's processing. Work outside the normal service is charged at the hourly rate in the Agreement.

Article 10. Audit

10.1 Processor makes available all information needed to demonstrate that it complies with this data processing agreement.

10.2 Controller may have compliance checked at most once per calendar year, with at least 30 days' written notice. These limits do not apply within 12 months after a personal data breach affecting Controller's personal data, or where a supervisory authority asks for the check.

10.3 A check starts with documentation: Processor's answers to a questionnaire from Controller, Annex 3 and any certifications or third-party reports. If these do not sufficiently demonstrate compliance, or an exception in 10.2 applies, Controller may have an inspection carried out. An inspection takes place during Office Hours, does not disrupt the service more than necessary and is limited to the processing for Controller.

10.4 The check is carried out by Controller or by an independent auditor who is bound by confidentiality and is not a competitor of Processor.

10.5 Controller bears the costs of the check, including Processor's time at the hourly rate in the Agreement. If the check shows that Processor does not comply with this data processing agreement on a material point, Processor bears its own costs. Processor remedies shortcomings within a reasonable period.

Article 11. End

11.1 This data processing agreement runs for as long as Processor processes personal data for Controller.

11.2 By the end date of the Agreement at the latest, Controller states in writing whether it wants data returned, as far as the Agreement provides for this. Processor then deletes, within 30 days after the end date, all personal data it holds for Controller, including the items listed in Annex 1 for the service concerned, and revokes or deletes its accounts and credentials for the Connected Systems. Backups expire as set out in Annex 1.

11.3 Processor confirms the deletion in writing. This does not apply to data Processor is required by law to keep.

Article 12. Liability

12.1 Processor's liability under this data processing agreement is subject to the limitation of liability that applies to the Agreement. This data processing agreement contains no separate or different limitation.

Article 13. Conclusion

13.1 This data processing agreement applies once Controller accepts a Quote that refers to it, or once it becomes applicable through the change procedure in the General Terms and Conditions. On request the parties also sign it separately.

13.2 Where the parties have previously signed a different data processing agreement, that agreement continues to apply instead of this one, unless the parties agree otherwise in writing.

13.3 This data processing agreement is drawn up in Dutch and English. If they differ, the version in the language of the Quote prevails.

Annex 1. Processing description

This Annex describes the processing for Integration Management on Alumio: Processor builds, monitors and supports Integrations in Controller's own Alumio environment. The fields marked "per customer" are filled in from section B of the delivery document. A new Integration is recorded in its delivery document and thereby supplements this Annex, without a new data processing agreement, as long as it stays within the data subjects and categories of this Annex and carries no special categories of personal data; otherwise the parties record the addition in writing before Processor starts that processing, in the Quote or at the latest in the signed delivery document.

Service	Building, monitoring and supporting Integrations in Controller's own Alumio environment, under the Quote and, if agreed, the SLA Integration Management (Alumio)
Purpose	Exchanging data between Controller's Connected Systems; diagnosing and repairing Integrations
Service Environments	Controller's Alumio environment, through named Sinsou accounts; the Connected Systems Sinsou has access to; Sinsou's support records; Sinsou's automated monitoring tools (SLA article 3.1), which read whether Alumio is reachable, whether data flows through the Integrations and whether Integrations perform differently from normal: metric information only, no payloads; hosted for Sinsou by Hetzner Online GmbH in Germany; the Sinsou portal (portal.sinsou.app), in production and test, which reads data from Controller's Alumio environment with a Sinsou staff member's rights for Sinsou's assistant (in the portal and in Slack) and for Sinsou's AI agents, and which, for those AI agents only, also sends read requests to the Connected Systems through Alumio's HTTP clients (Annex 2); hosted for Sinsou by Hetzner Online GmbH in Germany (Annex 2)
Data subjects	Controller's customers (B2C and B2B contacts); Controller's staff whose names appear in system accounts or support contact; Controller's suppliers (contact persons), where a route carries them
Categories of data	Per customer, from the routes in the delivery document. Typical for order routes: name, delivery and billing address, phone, email, customer ID, order contents and amounts
Special categories	Not expected: the routes carry e-commerce data only. If a route does carry them, the introduction to this Annex applies

Processing operations	Configuring, testing, viewing logs and payloads in Alumio, troubleshooting, resubmitting, exchanging incident details with Alumio B.V. on Controller's behalf, having questions about task data and logs answered by an AI service in Annex 2, and having an AI service in Annex 2 automatically make documentation, overviews and a classification from the configuration of Integrations
Where the data is	In Controller's own Alumio environment and Connected Systems. Sinsou keeps no copy of payloads as part of the service, apart from the items below
Retention by Sinsou	Copies of test data and production samples outside Alumio (exports, files, mailbox): deleted within 30 days after acceptance in the delivery document, or after the incident they were needed for is closed. This applies to deliveries accepted after this data processing agreement has become applicable. Support records: no personal data (article 6.2). Monitoring tools: metric information only, no personal data; no retention period applies. Sinsou portal: conversations with Sinsou's assistant, in the portal and in Slack (questions, answers, tool calls and their results, so retrieved task data too): kept until Sinsou deletes them; an automatic deletion period follows. Sinsou deletes them where Controller instructs it in writing (article 6.3). The answers the assistant posts in Slack stay in Slack under the retention setting of Sinsou's Slack workspace: 30 days for the assistant's conversations, set per conversation. Sinsou sets that period on each conversation before the assistant answers in it (Annex 2, Slack)
Retention in Alumio	Set by Controller under its own Alumio Licence. Not Sinsou's responsibility
Deletion at the end (article 11)	Revoke Sinsou's accounts in Alumio and the Connected Systems; delete local copies; confirm in writing. Data in Controller's Alumio environment stays with Controller
Duration	Term of the Agreement plus the deletion period in article 11

Annex 2. Sub-processors

Not listed on purpose: the suppliers of the Connected Systems (article 5.4), including Alumio: Controller holds its own Alumio licence.

Sub-processor	Service	Data	Storage location	Access from outside the EEA
Microsoft Ireland Operations Ltd (Microsoft 365)	Email, files and Teams for support and project work, including channels Controller shares with Sinsou	Order details customers send by mail or in a shared channel; test files	EU (tenant region EU; Microsoft's EU Data Boundary)	Limited, as documented by Microsoft (EU Data Boundary transfers). Basis: the 2021 standard contractual clauses (SCCs) in Microsoft's data processing agreement (Products and Services DPA)
awork GmbH, Hamburg	Project and incident records. Only a sub-processor if records carry personal data; aim for none. awork's AI functions are not used	Only an internal reference (article 6.2)	Germany (Microsoft Azure, Frankfurt and Berlin; awork DPA V05)	Limited: support chat via Intercom (USA), only when a Sinsou user shares content with awork support; stored data stays in Germany.
Slack Technologies Limited, Dublin (Slack Pro)	Channels Controller shares with Sinsou: messages and files in that channel. The answers Sinsou's assistant gives Sinsou staff. Salesforce's data processing addendum for Slack concluded	What Controller's staff post in a shared channel; this can include order data or data of a customer of Controller (article 6.2). Names and email addresses of the channel's members. In the assistant's answers: excerpts of task data, such as names, email addresses and order numbers of Controller's customers	United States (Amazon Web Services): Sinsou is on Slack Pro, and Slack offers storage in the EEA (data residency) only on Business+ and Enterprise. In a shared channel (Slack Connect) each organisation keeps its own messages in its own region	Yes: storage in the United States. Basis: Salesforce's data processing addendum for Slack (Revision August 2026), with the Salesforce Processor BCR and the standard contractual clauses (SCCs), Module Two and Three

Sub-processor	Service	Data	Storage location	Access from outside the EEA
Anthropic Ireland, Limited (Claude Team and Claude API)	The AI agents Sinsou staff work with: technical questions, incident diagnosis and support correspondence, with read access to Sinsou's mailbox and files and, through the Sinsou portal's connection for AI agents, read-only access to Controller's Alumio environment and, through Alumio's HTTP clients, to Controller's Connected Systems. In use under Anthropic's Commercial Terms (17 June 2025) and Anthropic's data processing addendum. Under those terms Anthropic does not train models on this data. No personal accounts (Free, Pro, Max) for customer data	Configuration of Integrations (routes, incoming and outgoing connections and transformers), with the names and web addresses of the Connected Systems, without credentials; it can contain names and email addresses of Controller's staff. Data from the Alumio environment (configuration, tasks, task payloads and task logs, reports, routes and the queue) and whatever a Connected System of Controller returns to a read request, such as orders and customers, with credentials masked (Annex 3, item 10); these can contain the names, addresses, email addresses and phone numbers of Controller's customers. In support correspondence: data from an email	Not guaranteed in the EEA: Anthropic states no storage location	Yes: Anthropic's data processing addendum (24 February 2025) incorporates the standard contractual clauses (SCCs), Module Two and Three

Sub-processor	Service	Data	Storage location	Access from outside the EEA
HostYourAI B.V., Groningen	The language model behind Sinsou's assistant (Sinsei), in the Sinsou portal and in Slack. Answers Sinsou staff's questions about Integrations using data the portal retrieves from Controller's Alumio environment (routes, configuration, tasks, task logs, route runs and their logs) and the data the portal itself keeps on Controller, and automatically makes documentation, overviews and a classification from the configuration of Integrations. HostYourAI does not train models on this data (its DPA, 4.11). No third-party models through a customer's own key. Data processing agreement with HostYourAI concluded on 5 November 2026; EU only is enabled on every Sinsou API key	Task payloads and task logs as Alumio returns them, with credentials masked (Annex 3, item 10) and every string cut at 4,000 characters; no other fields are removed, so the names, addresses, email addresses and phone numbers of Controller's customers can be in them. Configuration of Integrations without credentials, with the names and web addresses of the Connected Systems; it can contain names and email addresses of Controller's staff. The documentation, overviews and classification are made from that configuration: text Controller's staff type, such as names of systems and routes, in which a staff member's name can stand; no personal data of customers. HostYourAI does not keep prompts and responses; Sinsou keeps the conversations itself in the portal (Annex 1). Technical metadata (IP address, time, model, token	Platform and database: Amsterdam (UpCloud). Prompts and responses are used only while being processed, by providers established in the EU that process in the EU (HostYourAI's Sovereignty Mode). Which provider handles a request depends on the model. HostYourAI's own sub-processors are on its sub-processor list	No, for prompts, responses and metadata, as long as Sinsou sends no data of Controller to HostYourAI's support; that support runs through Proton AG (Switzerland) and Mailgun (United States)

Sub-processor	Service	Data	Storage location	Access from outside the EEA
		count), kept as in HostYourAI's data processing agreement		
Hetzner Online GmbH, Gunzenhausen, Germany	Hosting of the Sinsou portal and its database, in production and test. Data processing agreement with Hetzner concluded on 23 October 2026 (version 1.2 of 16 February 2026); all portal servers are under that Hetzner account	Conversations with Sinsou's assistant (questions, answers, tool calls and their results), kept as in Annex 1; these can contain task data with the names, addresses, email addresses and phone numbers of Controller's customers. The data the portal keeps on Controller	Germany: test, production and the current portal	No. All portal servers are in Germany, and with a server location in the EU Hetzner processes the data only in the EU (Hetzner's data processing agreement, Appendix 3)
Laravel Holdings Inc., New York, United States (Laravel Forge)	Server management (Laravel Forge) for the servers of the Sinsou portal and its database: access to those servers and their configuration, including access credentials. Laravel's data processing agreement (1 October 2026) applies through the Forge terms	Through that access Laravel can reach the data on those servers, as in the Hetzner row for the portal above	United States (Forge). The servers themselves are in Germany (Hetzner, above). Laravel's own sub-processors are on its sub-processor list	Yes: Laravel can access the servers from the United States. Basis: the standard contractual clauses (2021) in Laravel's data processing agreement; Laravel is also certified under the EU-US Data Privacy Framework

Sinsou's monitoring tools (Annex 1) are not listed: they read metric information only, no personal data.

Annex 3. Security measures

Processor takes at least the following measures (article 4.1). **The measures hold from the start of processing:** Processor sets up an environment this way before any of Controller's personal data is processed in it.

#	Measure
1	Named personal accounts for every Sinsou user in customer systems; no shared logins
2	MFA on Microsoft 365, awork and every customer system that offers it
3	Access removed immediately when someone leaves or no longer works on the customer
4	Confidentiality signed by everyone with access, including contractors
5	Laptops with disk encryption, screen lock and current updates
6	Credentials stored in a password manager (1Password), not in mail or documents
7	Sinsou puts no personal data in tickets, alerts or chat; content Controller supplies itself is outside this (article 6.2), and so are incident diagnosis and support correspondence with an AI service in Annex 2, data that AI services in Annex 2 read through the Sinsou portal, and the answers Sinsou's assistant gives Sinsou staff in Slack (Annex 2, Slack)
8	Test data and samples deleted after acceptance (Annex 1)
9	Configuration sent to an AI service in Annex 2 contains no credentials; documentation is made without sample records
10	From the go-live of the new Sinsou portal, the portal masks credentials (secret-named keys, Bearer and Basic headers, JWTs, PEM blocks, URL passwords and secret query parameters) before task data or logs go to an AI service, and cuts every string at 4,000 characters. Incident snapshots never go to an AI service
11	Sinsou's assistant answers in Slack only in direct messages and in channels whose members are all active Sinsou portal administrators, and posts only its answer there, never raw task data or logs
12	Sinsou gets administrator rights in Controller's Alumio environment where the work needs them. Controller keeps administrator rights itself and can withdraw Sinsou's access at any time
13	Payloads viewed in Alumio, not exported, unless needed for a specific incident