# Sinsou Data Processing Agreement

For the Managed Integration Service.

## 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 error text that a Connected System returns and Pulse keeps as a log (Annex 1), or 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 the Managed Integration Service: Processor runs Integrations on infrastructure Sinsou operates, with the order portal Pulse for Controller. 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 | Running Integrations on infrastructure Sinsou operates, with an order portal for Controller (Pulse: Sinsou Pulse, pulse.sinsou.app, as defined in Addendum 1.9), under the Addendum Managed Integration Service |
| Purpose | Exchanging data between Controller's Connected Systems; monitoring, troubleshooting and resubmitting |
| Service Environments | The Runtime Environment (UAT and production, database; the software is currently n8n), currently on a separate server for each Controller, hosted for Sinsou by the provider in Annex 2; Pulse, one instance for all Sinsou customers, with the separation in Annex 3; Sinsou's support records |
| Data subjects | Controller's customers (B2C and B2B contacts); Controller's staff with Pulse accounts or named system credentials; Controller's suppliers (contact persons), where a route carries them |
| Categories of data | Per customer, from the routes in the delivery document. Typical for Shopify order routes, per Shopify's Order object: name, delivery and billing address, email, phone, customer ID, order lines and amounts, payment status, shipment and tracking data, refund data, free text in order notes. Pulse users: name, email, login data |
| Special categories | None expected; if a route does carry them, the introduction to this Annex applies. Free text in order notes can contain anything, which is one reason full payloads are kept short |
| Processing operations | Receiving, transforming, temporarily storing, forwarding, logging, troubleshooting, resubmitting |

| | |
|---|---|
| Retention | a. full execution data, including order contents: 30 days; b. order index in Pulse (order number, ERP number, route, status, timestamps and the error message Sinsou writes, without personal data: article 6.2, Addendum 1.10), without name, address or contact details; Controller can still link these identifiers to a person, so they are pseudonymised data, not anonymous data: 12 months, longer or shorter on Controller's written instruction (article 6.3); logs in Pulse: Sinsou writes Pulse's log messages without personal data, but error text that a Connected System returns can contain personal data (article 6.2); kept 12 months, or shorter where Controller instructs this in writing (article 6.3); c. backups: 7 days, then overwritten; d. local copies of test data and production samples outside the Runtime Environment (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 |
| Deletion at the end (article 11) | The Runtime Environment including all execution data; Controller's data in Pulse; the Pulse accounts; all credentials for the Connected Systems; after any order index export under Addendum 8.3 |
| 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).

| Sub-processor | Service | Data | Storage location | Access from outside the EEA |
|---|---|---|---|---|
| Hetzner Online GmbH, Gunzenhausen, Germany (Hetzner Cloud) | Hosting of the Runtime Environment and database, currently one server per customer | All data in Annex 1 | Germany (Hetzner Cloud, location DE: Falkenstein or Nuremberg); all servers in Germany | No. Processing takes place exclusively in the EU or the EEA (Hetzner's data processing agreement, § 3(1)); with a server location in the EU the data is processed only in the EU, and technical and customer support take place in the EU (Appendix 3 to that agreement) |
| Hetzner Online GmbH (Hetzner Cloud backup option) | Backups, kept 7 days | All data in Annex 1 | Germany | No, as above |
| Hetzner Online GmbH (Hetzner Cloud) | Hosting of Pulse (pulse.sinsou.app), one instance for all customers | Order index (pseudonymised) and logs, as in Annex 1; Pulse accounts | Germany | No, as above |
| 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 and answers). The data the portal keeps on Controller: the name of the organisation, and names and email addresses of Controller's portal users and invoice contacts | 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) |

| Sub-processor | Service | Data | Storage location | Access from outside the EEA |
|---|---|---|---|---|
| Laravel Holdings Inc., New York, United States (Laravel Forge) | Server management (Laravel Forge) for the servers of the Sinsou portal and its database, and of Pulse (pulse.sinsou.app): 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 rows for the portal and Pulse 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 |
| 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. |

| Sub-processor | Service | Data | Storage location | Access from outside the EEA |
|---|---|---|---|---|
| Slack Technologies Limited, Dublin (Slack Pro) | Channels Controller shares with Sinsou: messages and files in that channel. 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 | 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 |
| Anthropic Ireland, Limited (Claude Team and Claude API) | AI assistant for technical questions, for documentation Sinsou makes from the configuration of Integrations, for incident diagnosis and for support correspondence. 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 without credentials; it can contain names and email addresses of Controller's staff. In incident diagnosis and support correspondence, data from a failed record or an email can come along, such as the name, address or email of a customer of Controller | 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. Answers Sinsou staff's questions using the data the portal itself keeps on Controller. 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 | The data the portal keeps on Controller: the name of the organisation, and names and email addresses of Controller's portal users and invoice contacts. Questions Sinsou staff type. HostYourAI does not keep prompts and responses; Sinsou keeps the conversations itself in the portal. Technical metadata (IP address, time, model, token count), kept as in HostYourAI's data processing agreement | 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) |

n8n GmbH, the publisher of the software Sinsou currently uses, is not listed: Sinsou runs that software itself, and with diagnostics switched off no customer data goes to n8n GmbH (Annex 3, item 20). Slack is listed for channels Controller shares with Sinsou; Sinsou's own alerts in Slack carry trends only, no personal data (article 6.2).

## 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.

The Runtime Environment currently runs on n8n, which is why the measures below name n8n and its settings. If Processor replaces that software under Addendum 6.3, each measure applies to the replacement software with an equivalent setting, and the level of security does not decrease (article 4.1). The parties agree now that, if Processor replaces that software under Addendum 6.3, Processor updates Annex 1 and this Annex to describe the replacement software and its settings, within the limits of this paragraph, and that the updated annexes bind the parties from the date of the replacement without a separate signature. Processor sends the updated annexes to Controller with the notice under Addendum 6.3. If the replacement involves a new supplier that processes personal data, article 5.2 applies. If the replacement lowers the level of security, article 5.2 applies as if a sub-processor were replaced.

| # | 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 the AI service in Annex 2 |
| 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 | Logical separation between customers: Controller's workflows, credentials and execution data are kept separate from those of other customers, currently one n8n instance per customer (UAT and production) with no shared database |
| 11 | Hosting in the EEA |
| 12 | Runtime Environment database and backups encrypted at rest |
| 13 | All traffic over TLS (Runtime Environment, webhooks, Pulse) |
| 14 | Credentials in the Runtime Environment encrypted with an instance-specific key (currently n8n's `N8N_ENCRYPTION_KEY`), stored outside the server |
| 15 | Runtime Environment editor not reachable from the public internet, or behind VPN or IP allow-list; only webhooks exposed |

| # | Measure |
|---|---|
| 16 | MFA on server access, hosting console and the Runtime Environment owner account |
| 17 | Only named Sinsou staff have access to the Runtime Environment and the servers |
| 18 | Pulse: personal accounts per customer user, MFA, each customer sees only its own data |
| 19 | Execution data pruning set to the Annex 1 period |
| 20 | Software diagnostics switched off (currently n8n: `N8N_DIAGNOSTICS_ENABLED=false`) |
| 21 | Security updates for the Runtime Environment software and the server's operating system installed within 7 days of release if the publisher rates them critical, otherwise within 30 days (same period as Addendum 5.3) |
| 22 | Daily backups, restore tested monthly |

Separation between customers in Pulse (item 18). One instance of Pulse serves all Sinsou customers. Customers are kept apart by permission scoping in the application: a user sees only the data of the customer the user belongs to, and can act only on that data, such as with the re-run action in Addendum 4.3, once Sinsou enables it.