Verwerkersovereenkomst Sinsou

Voor de Beheerde Integratiedienst.

Verwerkersovereenkomst

Partijen

- De klant genoemd in de Offerte, hierna "Verantwoordelijke"
- Sinsou B.V., KvK 86851314, Hoenderkamp 20, 7812 VZ Emmen, hierna "Verwerker"

Artikel 1. Onderwerp en definities

1.1 Deze verwerkersovereenkomst hoort bij de Overeenkomst. Verwerker verwerkt persoonsgegevens uitsluitend om de diensten in de Overeenkomst te leveren, zoals per dienst beschreven in Bijlage 1.

1.2 Bij strijd tussen deze verwerkersovereenkomst en de Overeenkomst gaat deze verwerkersovereenkomst voor op het gebied van persoonsgegevens, behalve voor aansprakelijkheid: daarvoor geldt artikel 12.1.

1.3 In deze verwerkersovereenkomst betekent:

a. **Overeenkomst**: de door Verantwoordelijke geaccepteerde Offerte, met een eventueel addendum, een eventuele service level agreement en de Algemene Voorwaarden van Verwerker;

b. **Gekoppelde Systemen**: de systemen van Verantwoordelijke en de diensten van derden die Verantwoordelijke zelf afneemt, zoals webshop, ERP, PIM, WMS en integratieplatform, waarmee Verwerker op instructie van Verantwoordelijke verbinding maakt;

c. **Dienstomgevingen**: de systemen en omgevingen die in Bijlage 1 per dienst staan;

d. **AVG**: Verordening (EU) 2016/679.

Artikel 2. Instructies

2.1 Verwerker verwerkt persoonsgegevens alleen op schriftelijke instructie van Verantwoordelijke, voor het doel dat Verantwoordelijke heeft vastgesteld. De Overeenkomst en Bijlage 1 gelden als die instructie. Verwerker gebruikt de gegevens niet voor eigen doeleinden en verstrekt ze niet aan derden, tenzij Verantwoordelijke dat opdraagt of de wet het vereist. In dat laatste geval informeert Verwerker Verantwoordelijke vooraf, tenzij de wet dat verbiedt.

2.2 Is een instructie naar het oordeel van Verwerker in strijd met de AVG of ander recht, dan meldt Verwerker dat direct.

Artikel 3. Geheimhouding

3.1 Verwerker en iedereen die onder zijn gezag werkt, inclusief ingehuurde krachten, zijn schriftelijk verplicht de persoonsgegevens geheim te houden. Alleen personen die de gegevens nodig hebben voor de dienst krijgen toegang.

Artikel 4. Beveiliging

4.1 Verwerker neemt passende technische en organisatorische maatregelen om de persoonsgegevens te beveiligen, zoals per dienst beschreven in Bijlage 3. Verwerker mag de maatregelen aanpassen, zolang het beveiligingsniveau niet daalt.

Artikel 5. Subverwerkers

5.1 Verantwoordelijke geeft algemene toestemming voor de subverwerkers in Bijlage 2 voor de dienst die hij afneemt.

5.2 Verwerker meldt een nieuwe of vervangende subverwerker ten minste 30 dagen vooraf per e-mail. Verantwoordelijke kan binnen die termijn op redelijke gronden bezwaar maken. Komen partijen er niet uit, dan kan Verantwoordelijke het betreffende deel van de Overeenkomst opzeggen. Wijzigt een subverwerker uit Bijlage 2 zijn eigen subverwerkers, dan geeft Verwerker die melding binnen vijf werkdagen na ontvangst door aan Verantwoordelijke; Verantwoordelijke kan bezwaar maken binnen de termijn die de subverwerker aan Verwerker geeft, en voor het overige geldt 5.2.

5.3 Verwerker legt aan iedere subverwerker schriftelijk dezelfde verplichtingen op als in deze verwerkersovereenkomst. Verwerker blijft tegenover Verantwoordelijke verantwoordelijk voor de nakoming door de subverwerker, binnen de beperking van artikel 12.1.

5.4 De leveranciers van de Gekoppelde Systemen zijn geen subverwerkers van Verwerker. Dat geldt ook voor een integratieplatform waarvoor Verantwoordelijke zelf een licentie heeft, zoals Alumio. Verantwoordelijke contracteert die leveranciers zelf.

5.5 Neemt Verwerker zelf een platform of omgeving af waarin de persoonsgegevens van Verantwoordelijke worden verwerkt, dan is de leverancier daarvan een subverwerker en staat die in Bijlage 2.

Artikel 6. Bewaartermijnen

6.1 Verwerker bewaart persoonsgegevens niet langer dan de termijnen die in Bijlage 1 voor de betreffende dienst staan.

6.2 Foutmeldingen, waarschuwingen en de vastlegging van incidenten die Verwerker zelf opstelt, bevatten geen persoonsgegevens, behalve de recordaanduiding waarin de Overeenkomst voorziet, zoals een intern record-ID. Dit geldt niet voor foutteksten die een Gekoppeld Systeem teruggeeft en die Pulse als log bewaart (Bijlage 1), en niet voor inhoud die Verantwoordelijke zelf aanlevert, zoals in een ticket, e-mail of chat.

6.3 Verantwoordelijke kan schriftelijk andere termijnen opdragen.

Artikel 7. Locatie en doorgifte

7.1 Verwerker en zijn subverwerkers slaan de persoonsgegevens op binnen de Europese Economische Ruimte (EER), tenzij Bijlage 2 bij een subverwerker anders vermeldt. Kan een subverwerker de gegevens buiten de EER opslaan, of vanuit een land buiten de EER inzien of verwerken, dan staat dat in Bijlage 2, met de grondslag voor die doorgifte.

7.2 Het versturen van gegevens naar en ophalen van gegevens uit de Gekoppelde Systemen gebeurt op instructie van Verantwoordelijke. Is Verantwoordelijke gevestigd buiten de EER, of staat een Gekoppeld Systeem buiten de EER, dan is Verantwoordelijke ervoor verantwoordelijk dat die doorgifte rechtmatig is.

7.3 Verwerker geeft geen persoonsgegevens door buiten de EER anders dan in 7.1 en 7.2, tenzij Verantwoordelijke daar vooraf schriftelijk mee instemt en er passende waarborgen zijn.

Artikel 8. Datalekken

8.1 Ontdekt Verwerker een beveiligingsincident waarbij persoonsgegevens van Verantwoordelijke mogelijk verloren of gewijzigd zijn, of door onbevoegden ingezien, dan meldt Verwerker dit zonder onredelijke vertraging en in ieder geval binnen 24 uur na ontdekking telefonisch en per e-mail aan Verantwoordelijke, met wat op dat moment bekend is over aard, omvang, betrokken gegevens en genomen maatregelen. Verwerker vult de melding aan zodra er meer bekend is.

8.2 Verwerker voert de instructies uit die volgen uit het onderzoek van het incident en helpt Verantwoordelijke bij een melding aan de toezichthouder of betrokkenen. Verantwoordelijke beslist over die melding.

Artikel 9. Bijstand

9.1 Verwerker helpt Verantwoordelijke bij verzoeken van betrokkenen (artikelen 15 tot en met 22 AVG), bij een gegevensbeschermingseffectbeoordeling en bij vragen van een toezichthouder, voor zover dat de verwerking door Verwerker betreft. Werk dat buiten de normale dienst valt, rekent Verwerker af tegen het uurtarief in de Overeenkomst.

Artikel 10. Audit

10.1 Verwerker stelt alle informatie beschikbaar die nodig is om aan te tonen dat hij deze verwerkersovereenkomst naleeft.

10.2 Verantwoordelijke kan de naleving ten hoogste eenmaal per kalenderjaar laten controleren, met een schriftelijke aankondiging van ten minste 30 dagen. Deze beperkingen gelden niet binnen 12 maanden na een datalek waarbij persoonsgegevens van Verantwoordelijke zijn betrokken, en niet als een toezichthouder om de controle vraagt.

10.3 Een controle begint met documentatie: de antwoorden van Verwerker op een vragenlijst van Verantwoordelijke, Bijlage 3 en eventuele certificeringen of rapporten van derden. Blijkt de naleving daaruit niet voldoende, of geldt een uitzondering uit 10.2, dan mag Verantwoordelijke een inspectie laten uitvoeren. Een inspectie vindt plaats tijdens Kantooruren, verstoort de dienstverlening niet onnodig en beperkt zich tot de verwerking voor Verantwoordelijke.

10.4 De controle wordt uitgevoerd door Verantwoordelijke of een onafhankelijke auditor die geheimhouding heeft toegezegd en geen concurrent van Verwerker is.

10.5 Verantwoordelijke draagt de kosten van de controle, inclusief de tijd van Verwerker tegen het uurtarief in de Overeenkomst. Blijkt dat Verwerker deze verwerkersovereenkomst op een wezenlijk punt niet naleeft, dan draagt Verwerker zijn eigen kosten. Verwerker herstelt tekortkomingen binnen een redelijke termijn.

Artikel 11. Einde

11.1 Deze verwerkersovereenkomst loopt zolang Verwerker persoonsgegevens voor Verantwoordelijke verwerkt.

11.2 Uiterlijk op de einddatum van de Overeenkomst laat Verantwoordelijke schriftelijk weten of hij gegevens terug wil, voor zover de Overeenkomst daarin voorziet. Daarna verwijdert Verwerker binnen 30 dagen na de einddatum alle persoonsgegevens die hij voor Verantwoordelijke bewaart, inclusief de onderdelen die in Bijlage 1 voor de betreffende dienst staan, en trekt hij zijn accounts en inloggegevens voor de Gekoppelde Systemen in of verwijdert hij die. Back-ups vervallen volgens Bijlage 1.

11.3 Verwerker bevestigt de verwijdering schriftelijk. Dit geldt niet voor gegevens die Verwerker wettelijk moet bewaren.

Artikel 12. Aansprakelijkheid

12.1 Voor de aansprakelijkheid van Verwerker onder deze verwerkersovereenkomst geldt de beperking van aansprakelijkheid die op de Overeenkomst van toepassing is. Deze verwerkersovereenkomst bevat geen eigen of afwijkende beperking.

Artikel 13. Totstandkoming

13.1 Deze verwerkersovereenkomst geldt zodra Verantwoordelijke een Offerte accepteert die ernaar verwijst, of zodra zij van toepassing wordt via de wijzigingsregeling in de Algemene Voorwaarden. Op verzoek ondertekenen partijen haar ook afzonderlijk.

13.2 Hebben partijen eerder een andere verwerkersovereenkomst ondertekend, dan blijft die gelden in plaats van deze, tenzij partijen schriftelijk anders afspreken.

13.3 Deze verwerkersovereenkomst is opgesteld in het Nederlands en het Engels. Bij verschil gaat de versie in de taal van de Offerte voor.

Bijlage 1. Beschrijving van de verwerking

Deze Bijlage beschrijft de verwerking bij de Beheerde Integratiedienst: Verwerker voert Integraties uit op infrastructuur die Sinsou beheert, met het orderportaal Pulse voor Verantwoordelijke. De velden met "per klant" worden ingevuld vanuit onderdeel B van het opleverdocument. Een nieuwe Integratie wordt vastgelegd in het opleverdocument van die Integratie en vult daarmee deze Bijlage aan, zonder nieuwe verwerkersovereenkomst, zolang zij binnen de betrokkenen en categorieën van deze Bijlage blijft en geen bijzondere categorieën van persoonsgegevens bevat; anders leggen partijen de aanvulling schriftelijk vast voordat Verwerker met die verwerking begint, in de Offerte of uiterlijk in het ondertekende opleverdocument.

Dienst	Uitvoeren van Integraties op infrastructuur die Sinsou beheert, met een orderportaal voor Verantwoordelijke (Pulse: Sinsou Pulse, pulse.sinsou.app, zoals omschreven in artikel 1.9 van het Addendum), onder het Addendum Beheerde Integratiedienst
Doel	Uitwisselen van gegevens tussen de Gekoppelde Systemen van Verantwoordelijke; bewaken, storingen oplossen en opnieuw aanbieden
Dienstomgevingen	De Uitvoeringsomgeving (UAT en productie, database; de software is op dit moment n8n), op dit moment op een eigen server per Verantwoordelijke, voor Sinsou gehost door de aanbieder in Bijlage 2; Pulse, één instantie voor alle klanten van Sinsou, met de scheiding in Bijlage 3; de supportregistratie van Sinsou
Betrokkenen	Klanten van Verantwoordelijke (B2C- en B2B-contactpersonen); medewerkers van Verantwoordelijke met een Pulse-account of systeeminloggegevens op naam; leveranciers van Verantwoordelijke (contactpersonen), als een route die bevat
Categorieën gegevens	Per klant, uit de routes in het opleverdocument. Gebruikelijk voor Shopify-orderroutes, volgens het Order-object van Shopify: naam, aflever- en factuuradres, e-mail, telefoon, klant-ID, orderregels en bedragen, betaalstatus, verzend- en trackinggegevens, terugbetalingsgegevens, vrije tekst in ordernotities. Pulse-gebruikers: naam, e-mail, inloggegevens
Bijzondere categorieën	Niet verwacht; bevat een route ze toch, dan geldt de inleiding van deze Bijlage. Vrije tekst in ordernotities kan van alles bevatten; dat is een van de redenen dat volledige payloads kort worden bewaard
Verwerkingen	Ontvangen, omzetten, tijdelijk opslaan, doorsturen, loggen, storingen oplossen, opnieuw aanbieden

Bewaartermijn	a. volledige uitvoeringsgegevens, inclusief orderinhoud: 30 dagen; b. orderindex in Pulse (ordernummer, ERP-nummer, route, status, tijdstempels en de foutmelding die Sinsou schrijft, zonder persoonsgegevens: artikel 6.2, Addendum 1.10), zonder naam, adres of contactgegevens; Verantwoordelijke kan deze kenmerken wel tot een persoon herleiden, dus het zijn gepseudonimiseerde gegevens, geen anonieme: 12 maanden, langer of korter op schriftelijke instructie van Verantwoordelijke (artikel 6.3); logs in Pulse: Sinsou stelt de logberichten van Pulse op zonder persoonsgegevens, maar een fouttekst die een Gekoppeld Systeem teruggeeft, kan persoonsgegevens bevatten (artikel 6.2); bewaard 12 maanden, of korter als Verantwoordelijke dat schriftelijk opdraagt (artikel 6.3); c. back-ups: 7 dagen, daarna overschreven; d. lokale kopieën van testdata en productievoorbeelden buiten de Uitvoeringsomgeving (exports, bestanden, mailbox): verwijderd binnen 30 dagen na acceptatie in het opleverdocument, of nadat het incident waarvoor ze nodig waren is gesloten; dit geldt voor opleveringen die worden geaccepteerd nadat deze verwerkersovereenkomst van toepassing is geworden
Verwijdering bij einde (artikel 11)	De Uitvoeringsomgeving inclusief alle uitvoeringsgegevens; de gegevens van Verantwoordelijke in Pulse; de Pulse-accounts; alle inloggegevens voor de Gekoppelde Systemen; na een eventuele export van de orderindex onder Addendum 8.3
Duur	Looptijd van de Overeenkomst plus de verwijderingstermijn in artikel 11

Bijlage 2. Subverwerkers

Bewust niet opgenomen: de leveranciers van de Gekoppelde Systemen (artikel 5.4).

Subverwerker	Dienst	Gegevens	Opslaglocatie	Toegang van buiten de EER
Hetzner Online GmbH, Gunzenhausen, Duitsland (Hetzner Cloud)	Hosting van de Uitvoeringsomgeving en database, op dit moment een eigen server per klant	Alle gegevens in Bijlage 1	Duitsland (Hetzner Cloud, locatie DE: Falkenstein of Neurenberg); alle servers in Duitsland	Nee. De verwerking vindt uitsluitend plaats in de EU of de EER (verwerkersovereenkomst van Hetzner, § 3 lid 1); bij een serverlocatie in de EU worden de gegevens alleen in de EU verwerkt, en technische en klantensupport vinden in de EU plaats (bijlage 3 van die verwerkersovereenkomst)
Hetzner Online GmbH (back-upoptie van Hetzner Cloud)	Back-ups, 7 dagen bewaard	Alle gegevens in Bijlage 1	Duitsland	Nee, zoals hierboven
Hetzner Online GmbH (Hetzner Cloud)	Hosting van Pulse (pulse.sinsou.app), één instantie voor alle klanten	Orderindex (gepseudonimiseerd) en logs, zoals in Bijlage 1; Pulse-accounts	Duitsland	Nee, zoals hierboven
Hetzner Online GmbH, Gunzenhausen, Duitsland	Hosting van het Sinsou-portaal en zijn database, in productie en test. Verwerkersovereenkomst met Hetzner gesloten op 23 oktober 2026 (versie 1.2 van 16 februari 2026); alle portalservers staan onder dat Hetzner-account	Gesprekken met de assistent van Sinsou (vragen en antwoorden). De gegevens die het portaal over Verantwoordelijke bijhoudt: de naam van de organisatie, en namen en e-mailadressen van portalgebruikers en factuurcontactpersonen van Verantwoordelijke	Duitsland: test, productie en het huidige portaal	Nee. Alle portalservers staan in Duitsland, en bij een serverlocatie in de EU verwerkt Hetzner de gegevens alleen in de EU (verwerkersovereenkomst van Hetzner, Appendix 3)

Subverwerker	Dienst	Gegevens	Opslaglocatie	Toegang van buiten de EER
Laravel Holdings Inc., New York, Verenigde Staten (Laravel Forge)	Serverbeheer (Laravel Forge) voor de servers van het Sinsou-portaal en zijn database, en van Pulse (pulse.sinsou.app): toegang tot die servers en hun configuratie, inclusief toegangsgegevens. De verwerkersovereenkomst van Laravel (1 oktober 2026) geldt via de voorwaarden van Forge	Via die toegang kan Laravel bij de gegevens op die servers, zoals in de Hetzner-rijen voor het portaal en Pulse hierboven	Verenigde Staten (Forge). De servers zelf staan in Duitsland (Hetzner, hierboven). De eigen subverwerkers van Laravel staan in haar lijst van subverwerkers	Ja: Laravel kan de servers vanuit de Verenigde Staten benaderen. Grondslag: de standaardcontractbepalingen (2021) in de verwerkersovereenkomst van Laravel; Laravel is daarnaast gecertificeerd onder het EU-VS Data Privacy Framework
Microsoft Ireland Operations Ltd (Microsoft 365)	E-mail, bestanden en Teams voor support- en projectwerk, ook kanalen die Verantwoordelijke met Sinsou deelt	Ordergegevens die klanten per mail of in een gedeeld kanaal sturen; testbestanden	EU (tenantregio EU; EU Data Boundary van Microsoft)	Beperkt, zoals door Microsoft gedocumenteerd (doorgiften onder de EU Data Boundary). Grondslag: de standaardcontractbepalingen (SCC) van 2021 in de verwerkersovereenkomst van Microsoft (Products and Services DPA)
awork GmbH, Hamburg	Project- en incidentregistratie. Alleen subverwerker als de registratie persoonsgegevens bevat; streven is geen. De AI-functies van awork worden niet gebruikt	Alleen een interne referentie (artikel 6.2)	Duitsland (Microsoft Azure, Frankfurt en Berlijn; verwerkersovereenkomst van awork, V05)	Beperkt: supportchat via Intercom (VS), alleen als een Sinsou-gebruiker inhoud deelt met de support van awork; opgeslagen gegevens blijven in Duitsland.

Subverwerker	Dienst	Gegevens	Opslaglocatie	Toegang van buiten de EER
Slack Technologies Limited, Dublin (Slack Pro)	Kanalen die Verantwoordelijke met Sinsou deelt: berichten en bestanden in dat kanaal. Verwerkersovereenkomst van Salesforce voor Slack gesloten	Wat medewerkers van Verantwoordelijke in een gedeeld kanaal plaatsen; dat kan ordergegevens of gegevens van een klant van Verantwoordelijke bevatten (artikel 6.2). Namen en e-mailadressen van de leden van het kanaal	Verenigde Staten (Amazon Web Services): Sinsou heeft Slack Pro, en opslag in de EER (dataresidentie) biedt Slack alleen op Business+ en Enterprise. In een gedeeld kanaal (Slack Connect) bewaart elke organisatie haar eigen berichten in haar eigen regio	Ja: opslag in de Verenigde Staten. Grondslag: de verwerkersovereenkomst van Salesforce voor Slack (revisie augustus 2026), met de Processor BCR van Salesforce en de standaardcontractbepalingen (SCC), module 2 en 3
Anthropic Ireland, Limited (Claude Team en Claude API)	AI-assistent voor technische vragen, voor documentatie die Sinsou maakt uit de configuratie van Integraties, voor storingsonderzoek en voor supportcorrespondentie. In gebruik onder de commerciële voorwaarden van Anthropic (17 juni 2025) en de verwerkersovereenkomst van Anthropic. Volgens die voorwaarden traint Anthropic geen modellen op deze gegevens. Geen privéaccounts (Free, Pro, Max) voor klantgegevens	Configuratie van Integraties zonder inloggegevens; daarin kunnen namen en e-mailadressen van medewerkers van Verantwoordelijke staan. Bij storingsonderzoek en supportcorrespondentie kunnen gegevens uit een mislukt record of een e-mail meekomen, zoals naam, adres of e-mail van een klant van Verantwoordelijke	Niet in de EER gegarandeerd: Anthropic noemt geen opslaglocatie	Ja: de verwerkersovereenkomst van Anthropic (24 februari 2025) neemt de standaardcontractbepalingen (SCC) op, module 2 en 3

Subverwerker	Dienst	Gegevens	Opslaglocatie	Toegang van buiten de EER
HostYourAI B.V., Groningen	Het taalmodel achter de assistent van Sinsou (Sinsei) in het Sinsou-portaal. Beantwoordt vragen van Sinsou-medewerkers met de gegevens die het portaal zelf over Verantwoordelijke bijhoudt. HostYourAI traint geen modellen op deze gegevens (haar verwerkersovereenkomst, 4.11). Geen modellen van derden via een eigen sleutel. Verwerkersovereenkomst met HostYourAI gesloten op 5 november 2026; de instelling EU only staat aan op elke API-sleutel van Sinsou	De gegevens die het portaal over Verantwoordelijke bijhoudt: de naam van de organisatie, en namen en e-mailadressen van portalgebruikers en factuurcontactpersonen van Verantwoordelijke. Vragen die Sinsou-medewerkers typen. HostYourAI bewaart prompts en antwoorden niet; Sinsou bewaart de gesprekken zelf in het portaal. Technische metadata (IP-adres, tijdstip, model, aantal tokens), bewaard zoals in de verwerkersovereenkomst van HostYourAI	Platform en database: Amsterdam (UpCloud). Prompts en antwoorden worden alleen tijdens de verwerking gebruikt, bij aanbieders die in de EU gevestigd zijn en in de EU verwerken (Sovereignty Mode van HostYourAI). Welke aanbieder een verzoek verwerkt, hangt af van het model. De eigen subverwerkers van HostYourAI staan in haar lijst van subverwerkers	Nee, voor prompts, antwoorden en metadata, zolang Sinsou geen gegevens van Verantwoordelijke naar de support van HostYourAI stuurt; die support loopt via Proton AG (Zwitserland) en Mailgun (Verenigde Staten)

n8n GmbH, de uitgever van de software die Sinsou op dit moment gebruikt, staat er niet in: Sinsou draait die software zelf, en met diagnostics uitgeschakeld gaan er geen klantgegevens naar n8n GmbH (Bijlage 3, punt 20). Slack staat er in voor kanalen die Verantwoordelijke met Sinsou deelt; de meldingen van Sinsou zelf in Slack bevatten alleen trends, geen persoonsgegevens (artikel 6.2).

Bijlage 3. Beveiligingsmaatregelen

Verwerker neemt ten minste de volgende maatregelen (artikel 4.1). **De maatregelen gelden vanaf de start van de verwerking:** Verwerker richt een omgeving zo in voordat er persoonsgegevens van Verantwoordelijke in worden verwerkt.

De Uitvoeringsomgeving draait op dit moment op n8n; daarom noemen de maatregelen hieronder n8n en de instellingen daarvan. Vervangt Verwerker die software op grond van artikel 6.3 van het Addendum, dan geldt elke maatregel voor de vervangende software met een gelijkwaardige instelling, en daalt het beveiligingsniveau niet (artikel 4.1). Partijen komen nu overeen dat, als Verwerker die software op grond van artikel 6.3 van het Addendum vervangt, Verwerker Bijlage 1 en deze Bijlage aanpast aan de vervangende software en haar instellingen, binnen de grenzen van deze alinea, en dat de aangepaste bijlagen partijen binden vanaf de datum van de vervanging zonder afzonderlijke ondertekening. Verwerker stuurt de aangepaste bijlagen aan Verantwoordelijke met de kennisgeving op grond van artikel 6.3 van het Addendum. Is bij de vervanging een nieuwe leverancier betrokken die persoonsgegevens verwerkt, dan geldt artikel 5.2. Verlaagt de vervanging het beveiligingsniveau, dan geldt artikel 5.2 alsof een subverwerker wordt vervangen.

#	Maatregel
1	Persoonlijke accounts voor elke Sinsou-gebruiker in klantsystemen; geen gedeelde logins
2	MFA op Microsoft 365, awork en elk klantsysteem dat het aanbiedt
3	Toegang direct ingetrokken als iemand vertrekt of niet meer voor de klant werkt
4	Geheimhouding getekend door iedereen met toegang, inclusief ingehuurde krachten
5	Laptops met schijfversleuteling, schermvergrendeling en actuele updates
6	Inloggegevens opgeslagen in een wachtwoordmanager (1Password), niet in mail of documenten
7	Sinsou zet geen persoonsgegevens in tickets, meldingen of chat; inhoud die Verantwoordelijke zelf aanlevert valt hierbuiten (artikel 6.2), en ook storingsonderzoek en supportcorrespondentie met de AI-dienst in Bijlage 2
8	Testdata en voorbeelden verwijderd na acceptatie (Bijlage 1)
9	Configuratie die naar een AI-dienst in Bijlage 2 gaat, bevat geen inloggegevens; documentatie wordt gemaakt zonder voorbeeldrecords
10	Logische scheiding tussen klanten: de workflows, inloggegevens en uitvoeringsgegevens van Verantwoordelijke staan los van die van andere klanten; op dit moment één n8n-instantie per klant (UAT en productie), zonder gedeelde database
11	Hosting in de EER
12	Database van de Uitvoeringsomgeving en back-ups versleuteld opgeslagen
13	Al het verkeer via TLS (Uitvoeringsomgeving, webhooks, Pulse)

#	Maatregel
14	Inloggegevens in de Uitvoeringsomgeving versleuteld met een instantie-specifieke sleutel (op dit moment de `N8N_ENCRYPTION_KEY` van n8n), buiten de server bewaard
15	Editor van de Uitvoeringsomgeving niet bereikbaar vanaf het openbare internet, of achter VPN of IP-allowlist; alleen webhooks open
16	MFA op servertoegang, hostingconsole en het owneraccount van de Uitvoeringsomgeving
17	Alleen genoemde Sinsou-medewerkers hebben toegang tot de Uitvoeringsomgeving en de servers
18	Pulse: persoonlijke accounts per gebruiker van de klant, MFA, elke klant ziet alleen zijn eigen gegevens
19	Opschonen van uitvoeringsgegevens ingesteld op de termijn in Bijlage 1
20	Diagnostics van de software uitgeschakeld (op dit moment n8n: `N8N_DIAGNOSTICS_ENABLED=false`)
21	Beveiligingsupdates van de software van de Uitvoeringsomgeving en van het besturingssysteem van de server geïnstalleerd binnen 7 dagen na uitgifte als de uitgever ze als kritiek aanmerkt, en anders binnen 30 dagen (zelfde termijn als Addendum 5.3)
22	Dagelijkse back-ups, herstel maandelijks getest

Scheiding tussen klanten in Pulse (punt 18). Eén instantie van Pulse bedient alle klanten van Sinsou. Klanten worden van elkaar gescheiden door permissie-scoping in de applicatie: een gebruiker ziet alleen de gegevens van de klant waartoe hij behoort, en kan alleen op die gegevens handelen, zoals met de actie voor herverwerking uit artikel 4.3 van het Addendum, zodra Sinsou die inschakelt.