



NLdigital

# Verwerkersovereenkomst

Versie: 1.0 maart 2026

*NLdigital versie maart 2025*

## Deel 1: Data Pro Statement

Dit Data Pro Statement vormt samen met de Algemene voorwaarden de verwerkersovereenkomst voor het product of de dienst van het bedrijf dat dit Data Pro Statement heeft opgesteld.

### Algemene informatie

1. Dit Data Pro Statement is opgesteld door de volgende data processor (verwerker):  
Clara Intelligence B.V.

Voor vragen over dit Data Pro Statement of dataprotectie kan contact opgenomen worden met: Stefan Knecht via [support@zoef.ai](mailto:support@zoef.ai)

2. Dit Data Pro Statement geldt vanaf 1 januari 2026

Dit Data Pro Statement en de daarin omschreven beveiligingsmaatregelen passen wij regelmatig aan om ten aanzien van dataprotectie steeds voorbereid en actueel te blijven. Wij houden u op de hoogte van nieuwe versies per e-mail.

3. Dit Data Pro Statement is van toepassing op de volgende producten en diensten van data processor

Zoef

4. **Omschrijving product(en)/dienst(en)**

Zoef is een AI-platform (SaaS) waarmee teams binnen organisaties slimmer kunnen werken met behulp van kunstmatige intelligentie.

Bij dit product/deze dienst is rekening gehouden met de verwerking van bijzondere persoonsgegevens, of gegevens betreffende strafrechtelijke veroordelingen en strafbare feiten of door de overheid uitgegeven persoonsnummers.

5. **Beeoogd gebruik**

**Product/dienst is ontworpen en ingericht om er de volgende soort gegevens mee te verwerken:**

Accountgegevens: naam, e-mailadres, organisatienaam

Gebruiksgegevens: inlogmomenten, gebruikte functies en interacties binnen de applicatie

Content en documenten: bestanden, teksten, prompts en andere informatie die gebruikers uploaden of invoeren. De inhoud hiervan wordt bepaald door de opdrachtgever en kan persoonsgegevens bevatten, afhankelijk van het gebruik.

Technische gegevens: IP-adres, browsertype, apparaat informatie en loggegevens

Communicatie: berichten via e-mail of supportkanalen

6. **Privacy by design/privacy by default**

Dataminimalisatie: Er worden alleen die persoonsgegevens verzameld die noodzakelijk zijn voor het leveren van de dienst. Voor het aanmaken van een account zijn uitsluitend een naam en e-mailadres vereist.

Encryptie: Alle gegevens worden versleuteld opgeslagen (encryption at rest) en versleuteld verzonden (TLS/SSL in transit). Wachtwoorden worden gehashed opgeslagen.

EU-only verwerking: Alle verwerking van klantdata vindt uitsluitend plaats binnen de EU/EER. Sub-processors en AI-modelproviders worden uitsluitend geselecteerd op configuraties binnen de EU/EER.

Geen training op klantdata: AI-modelproviders worden uitsluitend geselecteerd op configuraties waarbij klantdata niet wordt gebruikt voor training of (her)training van AI-modellen.

Klant heeft regie over eigen data: Klanten uploaden zelf hun documenten en gegevens en kunnen deze wijzigen en verwijderen. De verwerker zal gegevens alleen inzien op verzoek van de klant, bijvoorbeeld als dat nodig is om een support vraag te beantwoorden.

Privacyvriendelijke standaardinstellingen: Er worden geen tracking cookies geplaatst voor advertentiedoeleinden. De meest privacy vriendelijke instellingen zijn standaard geactiveerd.

Toegangsbeperking: Alleen geautoriseerde medewerkers van Clara Intelligence hebben toegang tot persoonsgegevens, en uitsluitend voor zover noodzakelijk voor het leveren van de dienst.

7. **Data processor gebruikt de Standaardclausules voor verwerkingen, welke onderdeel zijn van de Algemene Voorwaarden die als bijlage bij de Overeenkomst te vinden zijn.**
8. **Data processor verwerkt de persoonsgegevens van zijn opdrachtgevers binnen de EU/EER.**
9. **Data processor maakt gebruik van de volgende sub-processors:**

| Sub-processor | Dienst                | Server Locatie |
|---------------|-----------------------|----------------|
| Leafcloud     | Server hosting        | Nederland      |
| Microsoft     | AI-modellen           | Zweden         |
| Google        | AI-modellen           | België         |
| Mistral       | AI-modellen           | EU             |
| Nebius        | AI-modellen           | Finland        |
| Lettermint    | Transactionele e-mail | EU             |

10. **Data processor ondersteunt opdrachtgever op de volgende manier bij verzoeken van betrokkenen:**

Wanneer een betrokkene (bijvoorbeeld een medewerker van opdrachtgever) een verzoek indient op grond van de AVG — zoals een verzoek tot inzage, rectificatie, verwijdering, beperking of dataportabiliteit — verwijst data processor dit verzoek door naar de opdrachtgever, aangezien de opdrachtgever verwerkingsverantwoordelijke is.

Data processor ondersteunt opdrachtgever bij het afhandelen van dergelijke verzoeken op de volgende manieren:

- a. Inzage: Op verzoek van opdrachtgever kan data processor een overzicht verstrekken van de persoonsgegevens die voor de betreffende betrokkene worden verwerkt, inclusief accountgegevens, gebruiksgegevens en eventueel opgeslagen content.
- b. Rectificatie: Accountgegevens (zoals naam en e-mailadres) kunnen door de gebruiker zelf worden aangepast in de applicatie. Waar dit niet mogelijk is, voert data processor correcties door op verzoek van opdrachtgever.
- c. Verwijdering: Op verzoek van opdrachtgever kan data processor het account van een betrokkene en de daaraan gekoppelde persoonsgegevens verwijderen. Opdrachtgever kan ook zelf content en documenten verwijderen binnen de applicatie.

- d. Beperking van verwerking: Op verzoek van opdrachtgever kan data processor de verwerking van gegevens van een specifieke betrokkene beperken, bijvoorbeeld door een account te deactiveren.
- e. Dataportabiliteit: Op verzoek van opdrachtgever kan data processor de persoonsgegevens van een betrokkene exporteren in een gangbaar formaat (zoals JSON of CSV).

Data processor reageert binnen een redelijke termijn, en uiterlijk binnen 10 werkdagen, op verzoeken van opdrachtgever tot ondersteuning bij betrokkenen verzoeken.

**11. Data processor zal op de volgende wijze medewerking verlenen aan Data Protection Impact Assessments (DPIA):**

Indien opdrachtgever op grond van artikel 35 AVG verplicht is een DPIA uit te voeren voor verwerkingen die (mede) door data processor worden uitgevoerd, zal data processor na een daartoe redelijk gedaan verzoek zijn medewerking verlenen. Deze medewerking omvat:

- a. Het verstrekken van informatie over de wijze waarop persoonsgegevens worden verwerkt binnen het product, waaronder de technische en organisatorische beveiligingsmaatregelen, de inzet van sub-processors en de locatie van dataverwerking.
- b. Het beantwoorden van gerichte vragen van opdrachtgever of diens functionaris voor gegevensbescherming (FG/DPO) over het product en de verwerking.
- c. Het beschikbaar stellen van relevante documentatie, zoals dit Data Pro Statement, het privacybeleid en eventuele auditrapportages of certificeringen.

**12. Na beëindiging van de Overeenkomst met een opdrachtgever verwijdert data processor de persoonsgegevens die hij voor opdrachtgever verwerkt in principe binnen 3 maanden op zodanige wijze dat deze niet langer kunnen worden gebruikt en niet langer toegankelijk zijn (render inaccessible).**

**13. Retourneren van persoonsgegevens na beëindiging van de Overeenkomst**

Er worden geen persoonsgegevens geretourneerd, alle persoonsgegevens worden binnen 3 maanden verwijderd.

## Beveiligingsbeleid

**14. Data processor heeft de volgende beveiligingsmaatregelen genomen ter beveiliging van zijn product of dienst:**

**Versleuteling**

- a. Alle persoonsgegevens worden versleuteld opgeslagen (encryption at rest, AES-256).
- b. Alle gegevensoverdracht vindt versleuteld plaats via TLS 1.2 of hoger (encryption in transit).
- c. Enkel inloggen via SSO is mogelijk.

**Pseudonimisering**

Persoonsgegevens worden niet standaard gepseudonimiseerd, omdat het product is ontworpen om gebruikers op naam te identificeren voor accountbeheer en toegangscontrole.

**Vertrouwelijkheid**

- a. Alleen geautoriseerde medewerkers van Clara Intelligence B.V. hebben toegang tot persoonsgegevens, uitsluitend voor zover noodzakelijk voor het leveren van de dienst (need-to-know-principe).
- b. Medewerkers zijn gebonden aan geheimhoudingsverplichtingen.
- c. Authenticatie en autorisatie worden afgedwongen op applicatie- en infrastructuurniveau. SSO-integratie (Azure AD, Google Workspace) is beschikbaar voor opdrachtgevers.
- d. Rollen- en rechtenbeheer stelt opdrachtgevers in staat om per team te bepalen wie toegang heeft tot welke projecten, documenten en modellen.

**Integriteit**

- a. Alle wijzigingen en toegang worden gelogd (audit-logging).
- b. Periodieke updates van software en afhankelijkheden.

#### Beschikbaarheid en veerkracht

- a. Hosting vindt plaats bij Leafcloud B.V. in Nederlandse datacenters.
- b. Automatische back-ups met beveiligde opslag.
- c. Disaster recovery procedures zijn ingericht om bij een incident de beschikbaarheid van en toegang tot persoonsgegevens tijdig te herstellen.
- d. Systemen worden gemonitord op beschikbaarheid en prestaties.

#### AI-modelbeleid

- a. AI-modelproviders worden uitsluitend geselecteerd op configuraties binnen de EU/EER.
- b. Klantdata wordt niet gebruikt voor training of hertraining van AI-modellen.
- c. Modelproviders bewaren geen klantdata na verwerking, behoudens tijdelijke opslag voor abuse monitoring en veiligheidscontroles.

#### 15. **Data processor heeft zich geconformeerd aan een Information Security Management System (ISMS), geborgd in/via:**

- a. ISO 27001
- b. NEN 7510, NEN 7512, NEN 7513 (voor zorg)

Dit ISMS wordt op dit moment opgebouwd en wordt naar verwachting in het 3e kwartaal van 2026 volledig in gebruik genomen.

#### 16. **Data processor heeft de volgende verificaties en certificeringen:**

Nog geen relevante verificatie en certificeringen op dit moment. Data processor is in traject voor ISO 27001 en NEN 7510 certificering met een verwachte afronding van dit traject voor het einde van 2026.

### **Datalekkenprotocol**

#### 17. **In geval er toch iets mis gaat, hanteert data processor het volgende datalekkenprotocol om ervoor te zorgen dat opdrachtgever op de hoogte is van incidenten:**

Data processor stelt opdrachtgever zonder onredelijke vertraging op de hoogte van het datalek.

De melding bevat tenminste de volgende informatie:

- a. Een beschrijving van de aard van het datalek, inclusief — voor zover bekend — de categorieën en het geschatte aantal getroffen betrokkenen en persoonsgegevensrecords.
- b. De naam en contactgegevens van het aanspreekpunt bij data processor.
- c. Een beschrijving van de waarschijnlijke gevolgen van het datalek.
- d. Een beschrijving van de maatregelen die zijn genomen of worden voorgesteld om het datalek aan te pakken en de gevolgen te beperken.

De melding wordt gedaan per e-mail aan het door opdrachtgever opgegeven contactadres. Indien noodzakelijk vanwege de urgentie wordt opdrachtgever eerst telefonisch geïnformeerd, gevolgd door een schriftelijke bevestiging.

Data processor verleent volledige medewerking aan opdrachtgever bij het onderzoeken van het incident en bij het voldoen aan eventuele meldplichten van opdrachtgever bij de Autoriteit Persoonsgegevens en/of betrokkenen.

Na afhandeling van het incident evalueert data processor het voorval en neemt waar nodig aanvullende maatregelen om herhaling te voorkomen. Opdrachtgever wordt geïnformeerd over de uitkomsten van deze evaluatie.

Alle datalekken worden geregistreerd in een intern datalekkenregister, inclusief de aard van het incident, de gevolgen, de genomen maatregelen en de communicatie met opdrachtgever.