LUCIDON
Helder over jouw data

Veilig en autonoom werken in de cloud met LUCIDON.

Verwerkersovereenkomst

De klant van Lucidon, hierna te noemen "Verantwoordelijke" (Opdrachtgever),

en

Lucidon b.v., gevestigd te **Amsterdam**, ingeschreven bij de Kamer van Koophandel onder nummer **98532839**, hierna te noemen: "Verwerker" (Dienstverlener),

gezamenlijk te noemen: "Partijen".

Overwegingen

1. Verantwoordelijke heeft met Verwerker een raamovereenkomst gesloten voor het leveren van cloud- en IT-diensten.
2. Verwerker verwerkt daarbij namens Verantwoordelijke persoonsgegevens in de zin van de Algemene Verordening Gegevensbescherming (AVG, EU 2016/679).
3. Partijen willen met deze Verwerkersovereenkomst vastleggen hoe met persoonsgegevens wordt omgegaan, zodat verwerking veilig, transparant en in overeenstemming met de AVG plaatsvindt.
4. Deze overeenkomst vormt een integraal onderdeel van de overeenkomst tussen Partijen.
5. Lucidonlevert diensten die gericht zijn op autonoom en veilig databeheer, binnen de Europese Economische Ruimte (EER).

Deze Verwerkersovereenkomst is onderdeel van alle gesloten contracten met de Opdrachtgever. De Verwerkersovereenkomst (AVG) is van toepassing op persoonsgegevens. Bij strijdigheid geldt de rangorde: (1) De gesloten overeenkomsten, (2) de Service Level Overeenkomst, (3) de Verwerkersovereenkomst, en (4) de ICT leveringsvoorwaarden.

1. Doel en aard van de verwerking

1.1 Verantwoordelijke bepaalt het doel en de middelen van de verwerking. Verwerker verwerkt persoonsgegevens uitsluitend voor het uitvoeren van de overeengekomen diensten zoals beschreven in **Bijlage A**.

1.2 Verwerker zal persoonsgegevens nooit voor eigen doeleinden gebruiken of aan derden verstrekken, tenzij dit wettelijk verplicht is.

1.3 Sub-verwerkers mogen alleen worden ingeschakeld met voorafgaande schriftelijke toestemming van Verantwoordelijke. In Bijlage 1 is aangegeven welke sub-verwerkers zijn toegestaan (bijv. hostingpartners binnen de EER).

1.4 Verwerker garandeert dat sub-verwerkers minstens hetzelfde beveiligings- en vertrouwelijkheidsniveau hanteren als Lucidon zelf.

1.5 Verwerker verleent ondersteuning bij het nakomen van verplichtingen uit artikelen 32 t/m 36 AVG (beveiliging, datalekken, DPIA's, samenwerking met toezichthouders).

1.6 Alle gegevensverwerking vindt plaats binnen de EER. Verwerking buiten de EER is alleen toegestaan na schriftelijke toestemming van Verantwoordelijke.
1.7 Verwerker maakt informatie over beveiligingsmaatregelen en audits op verzoek inzichtelijk. Eventuele audits worden in overleg gepland; kosten daarvan zijn voor rekening van Verantwoordelijke.
1.8 Verantwoordelijke waarborgt dat de verwerking rechtmatig is en vrijwaart Verwerker voor aanspraken van derden die daaruit voortvloeien.

2. Beveiliging van gegevens

2.1 Verwerker treft passende technische en organisatorische maatregelen om persoonsgegevens te beschermen tegen verlies, ongeoorloofde toegang en onrechtmatige verwerking, conform artikel 32 AVG.
2.2 Deze maatregelen omvatten onder meer:

- encryptie in rust en tijdens transport,
- strikte toegangsbeveiliging met tweefactorauthenticatie,
- scheiding van klantdata per tenant,
- logging en periodieke controle van toegangsrechten,
- back-up en herstelprocedures binnen de EER.

Een overzicht staat in **Bijlage B**.

2.3 Indien aanvullende maatregelen noodzakelijk blijken door gewijzigde wet- of regelgeving, zal Verwerker dit tijdig melden. Eventuele meerkosten worden in overleg overeengekomen.

3. Datalekken

3.1 Onder een datalek wordt verstaan: een inbreuk op de beveiliging die leidt tot verlies, vernietiging of ongeoorloofde verstrekking van persoonsgegevens.
3.2 Verwerker meldt elk datalek onverwijld aan Verantwoordelijke, uiterlijk binnen 24 uur na ontdekking, met minimaal de volgende informatie:

- aard en oorzaak van het incident,
- categorieën betrokkenen en gegevens,
- omvang en mogelijke gevolgen,
- genomen of voorgenomen maatregelen,
- contactpersoon bij LUCIDON.

3.3 Verantwoordelijke beslist over melding aan de Autoriteit Persoonsgegevens en/of betrokkenen.
3.4 Verwerker werkt volledig mee aan onderzoek en communicatie over het incident.
3.5 Beide Partijen behandelen informatie over datalekken vertrouwelijk.

4. Geheimhouding

4.1 Alle persoonsgegevens en aanverwante informatie zijn vertrouwelijk.
4.2 Verwerker waarborgt dat medewerkers en derden die toegang hebben tot persoonsgegevens gebonden zijn aan een geheimhoudingsplicht.
4.3 Deze verplichting blijft bestaan na beëindiging van de overeenkomst.

5. Duur en beëindiging

5.1 Deze overeenkomst geldt zolang Verwerker diensten uitvoert voor Verantwoordelijke.

5.2 Na beëindiging van de diensten zal Verwerker, naar keuze van Verantwoordelijke:

- alle persoonsgegevens veilig verwijderen, of
- terugleveren aan Verantwoordelijke in een gangbaar formaat.

5.3 Kopieën of back-ups worden verwijderd tenzij wettelijke bewaarplicht geldt.

6. Wijzigingen

6.1 Indien wet- of regelgeving wijzigt of aanvullende eisen stelt, zullen Partijen deze overeenkomst aanpassen om te blijven voldoen aan de AVG.

7. Toepasselijk recht

7.1 Op deze overeenkomst is Nederlands recht van toepassing. Geschillen worden voorgelegd aan de bevoegde rechter in het arrondissement Amsterdam.

8. Overdracht

8.1 Geen van beide Partijen mag rechten of verplichtingen uit deze overeenkomst overdragen aan derden zonder schriftelijke toestemming van de andere partij.

9. Bijlagen

Bijlage A: Omschrijving van de verwerking, categorieën gegevens en sub-verwerkers

Bijlage B: Beveiligingsmaatregelen

Bijlage A

1. Doel van de verwerking

Verwerker (LUCIDON) verwerkt persoonsgegevens uitsluitend ten behoeve van de uitvoering van de getekende offerte.

2. Aard en categorieën van persoonsgegevens

De volgende categorieën van persoonsgegevens kunnen worden verwerkt:

Categorie	Voorbeelden	Bijzonderheden
Identificatiegegevens	Naam, e-mailadres, gebruikersnaam, IP-adres	Nodig voor toegang en authenticatie
Organisatiegegevens	Functie, afdeling, organisatie, tenant-ID	Voor gebruikersbeheer
Contactgegevens	Telefoonnummer, zakelijke adresgegevens	Voor communicatie en support
Gebruik- en loggegevens	Inlogmomenten, sessies, bestandsnamen (geen inhoud)	Voor audit- en beveiligingsdoeleinden
Optioneel / door klant opgeslagen gegevens	Documenten, agenda-items, notities, bestanden	Inhoud onder exclusieve controle van Verantwoordelijke

Opmerking: Lucidonheeft geen inzicht in de inhoud van opgeslagen bestanden. Alleen metadata (zoals bestandsnamen of logregistraties) kunnen in uitzonderlijke gevallen zichtbaar zijn voor technische ondersteuning.

4. Duur van de verwerking

De persoonsgegevens worden verwerkt zolang de klantovereenkomst actief is en tot maximaal 30 dagen na beëindiging, tenzij anders overeengekomen.

5. Locatie van verwerking

Alle gegevens worden verwerkt uitsluitend binnen de Europese Economische Ruimte (EER).
Standaardlocaties:

Datacenters van Hetzner Online GmbH (Duitsland / Finland)

6. Sub-verwerkers

Lucidonmaakt gebruik van zorgvuldig geselecteerde sub-verwerkers voor specifieke onderdelen.

Sub-verwerker	Locatie	Doel van verwerking	AVG-conformiteit / verwerkersovereenkomst
Hetzner Online GmbH	Duitsland / Finland	Hosting en opslag van data	ja

Verantwoordelijke geeft hierbij toestemming voor bovengenoemde sub-verwerkers, mits deze voldoen aan de vereisten van artikel 28 AVG.

7. Contactgegevens voor privacyzaken

LucidonB.V. – Privacy & Security Desk
E-mail: privacy@lucidon.nl

Bijlage B

Lucidontreft structurele maatregelen om persoonsgegevens te beschermen tegen verlies, wijziging, onbevoegde toegang of enige andere vorm van onrechtmatige verwerking.

Onderstaande tabel geeft een overzicht van de genomen maatregelen.

Categorie maatregel	Beschrijving	Status / Opmerking
Toegangsbeveiliging	Authenticatie via beveiligde inlog (2FA), sterkte wachtwoordbeleid, sessietijdlimieten.	Mogelijk
Encryptie	Alle data wordt versleuteld tijdens transport (TLS 1.3)	Actief
Datacenterbeveiliging	ISO 27001-gecertificeerde datacenters binnen de EU (Hetzner).	Actief
Logging & monitoring	Systeem- en toegangslogs worden bewaard en gemonitord.	Actief
Scheiding van data	Logische scheiding per tenant / klantomgeving.	Actief
Back-up & herstel	Dagelijkse back-ups, versleuteld opgeslagen binnen de EER; hersteltests op aanvraag.	Actief
Patching & updates	Regelmatige beveiligingsupdates voor OS, containers en Nextcloud-instances.	Actief
Incidentrespons	Interne meldprocedure, inclusief escalatie naar Verantwoordelijke binnen 24 uur bij incident.	Actief
Medewerkers Security awereness	Regelmatig overleg over privacy, beveiliging en incidentbeheer.	Actief
Privacy	Minimale dataverwerking, standaard versleutelde communicatie, opt-in functionaliteiten.	Actief
Beoordeling door klant	Verantwoordelijke mag jaarlijks een audit of security review uitvoeren (op verzoek).	Actief