ombra

Verwerkersovereenkomst

Laatst bijgewerkt op 19 oktober 2026
ombra · Abeliaerf 37, 4125 WH Hoef en Haag, Nederland · KVK 88959945 · btw NL004674188B20

Jij bent verantwoordelijk voor de gegevens van je cliënten. ombra verwerkt ze alleen voor jou. Hier staat hoe.

Wie wat doet

Deze verwerkersovereenkomst hoort bij de algemene voorwaarden van ombra. Je sluit haar wanneer je de voorwaarden aanvaardt. Ze volgt artikel 28 van de AVG en artikel 9 van de Belgische wet van 30 juli 2018 over de bescherming van persoonsgegevens.

Jij, de psycholoog, therapeut of praktijk met een account, bent **verwerkingsverantwoordelijke**: je bepaalt waarom en hoe de gegevens van je cliënten worden verwerkt. ombra, gevestigd op Abeliaerf 37, 4125 WH Hoef en Haag, Nederland (KVK 88959945), is **verwerker**: we verwerken ze alleen voor jou. Wil je een ondertekend exemplaar, mail dan support@ombracare.com.

Berichten over deze overeenkomst, zoals een melding van een datalek, sturen we naar het e-mailadres van je account. Moeten we iemand anders verwittigen, bijvoorbeeld je functionaris voor gegevensbescherming, laat het ons dan weten via privacy@ombracare.com.

1. Onderwerp en duur

ombra verwerkt persoonsgegevens voor jou om ombra te kunnen leveren, zoals bijlage A beschrijft. Gezondheidsgegevens horen daar uitdrukkelijk bij. Deze overeenkomst loopt zolang je ombra gebruikt, en daarna tot we je gegevens hebben teruggegeven en verwijderd (artikel 12).

2. Alleen in jouw opdracht

We verwerken je gegevens alleen op jouw instructies. Die staan in deze overeenkomst en de voorwaarden, en je geeft ze door ombra te gebruiken: wat je invoert, instelt, koppelt, exporteert of verwijdert. Een andere instructie spreek je schriftelijk met ons af, via privacy@ombracare.com.

Verplicht de wet ons tot iets anders, dan laten we je dat vooraf weten, tenzij die wet dat verbiedt. Vinden we dat een instructie ingaat tegen de privacywetgeving, dan zeggen we je dat meteen.

Schenden we deze overeenkomst ernstig, dan kun je ons vragen de verwerking meteen te stoppen. Je gegevens meenemen kan dan nog altijd.

3. Geen eigen gebruik

We gebruiken je gegevens niet voor onszelf. We verkopen ze niet, gebruiken ze niet voor reclame of onderzoek, maken er geen profielen mee, voegen ze niet samen met die van andere praktijken, sturen ze niet naar AI-diensten en trainen er geen AI-modellen mee (geen AI op je dossiers).

We geven je gegevens aan niemand anders, tenzij jij dat vraagt of de wet ons ertoe verplicht. Moeten we iets afgeven, dan laten we je dat vooraf weten, tenzij de wet dat verbiedt.

Het rijksregisternummer of BSN gebruiken we alleen om je cliënt in jouw dossier te herkennen, nooit als ons eigen kenmerk of voor iets anders. Technische gegevens zonder inhoud, zoals tijden en foutcodes, gebruiken we om ombra te laten werken en te verbeteren.

4. Geheimhouding

Iedereen die voor ombra bij je gegevens kan, heeft een schriftelijke geheimhoudingsplicht, ook nadat dat werk stopt. Bijlage D zegt wie bij gezondheidsgegevens kan, en waarom. Die lijst houden we bij en geven we aan de Gegevensbeschermingsautoriteit als die erom vraagt.

5. Beveiliging

We nemen passende technische en organisatorische maatregelen om je gegevens te beschermen (artikel 32 AVG), afgestemd op de gevoeligheid van gezondheidsgegevens. Ze staan in bijlage B. We houden ze bij met de stand van de techniek. Vervangen we een maatregel, dan door een die minstens even goed beschermt.

6. Toegang door ombra

Niemand van ombra heeft vaste toegang tot de inhoud van je werkruimte. Een beheerder komt alleen bij je gegevens via een tijdelijke beheerrol, en alleen:

- als jij ons daarom vraagt, bijvoorbeeld om je te helpen;
- om een storing op te lossen of een beveiligingsincident te onderzoeken;
- als de wet ons ertoe verplicht.

We leggen telkens vast wie, wanneer en waarom. Daarnaast hebben noodaccounts blijvende rechten, alleen voor als al het andere faalt; ook dat gebruik leggen we vast. Op je verzoek vertellen we je of en wanneer een beheerder bij je gegevens kwam.

7. Subverwerkers

Je geeft ons toestemming om de subverwerkers in bijlage C in te schakelen. We leggen hun minstens dezelfde plichten op als in deze overeenkomst, en we blijven tegenover jou verantwoordelijk voor hun werk.

Over een nieuwe of andere subverwerker mailen we je minstens 30 dagen voordat die aan de slag gaat, met wat die doet, met welke gegevens en waar. Je hoeft je daarvoor nergens in te schrijven. Heb je een gegronde reden voor bezwaar, laat het ons dan binnen die termijn weten. Vinden we samen geen oplossing, dan mag je kosteloos opzeggen, en betalen we terug wat je vooruitbetaalde.

8. Gegevens buiten de EU

Je gegevens staan in de Europese Unie, zoals bijlage C beschrijft. Gaan ze toch naar een land buiten de Europese Economische Ruimte, bijvoorbeeld voor ondersteuning door Microsoft, dan alleen binnen jouw instructies en met de waarborgen die de AVG vraagt, zoals een adequaatheidsbesluit of de standaardcontractbepalingen van de Europese Commissie.

Een kopie van die waarborgen krijg je op verzoek. Kunnen we de bescherming niet meer bieden, dan stoppen we die doorgifte. Hoe we omgaan met verzoeken van overheden, lees je bij Beveiliging.

9. Hulp bij de rechten van je cliënten

Je cliënten hebben rechten op hun gegevens, en jij hebt plichten als zorgverlener: in België onder de Wet patiëntenrechten en de Kwaliteitswet, in Nederland onder de WGBO. ombra helpt je die na te komen:

- Je drukt een dossieroverzicht af of bewaart het als pdf, voor inzage of een kopie.
- Je verbetert of vult gegevens aan. Notities houden al hun versies bij.
- ombra legt vast wie een dossier opent of wijzigt. Dat logboek zit in je export, zodat je een cliënt kunt vertellen wie het dossier opende. Zoeken en het overzicht op Vandaag staan er per werkruimte in, nog niet per dossier (het logboek).
- Na de bewaartermijn verwijder je een dossier definitief.

Moet een aanmelding of inschrijving weg, bijvoorbeeld omdat iemand erom vraagt, mail dan support@ombracare.com: dan verwijderen wij ze voor je. Krijgen wij zelf een vraag van een cliënt over diens gegevens, dan sturen we die zonder onnodige vertraging naar je door. We beantwoorden haar niet zelf, en geven niets vrij zonder jouw instructie of een wettelijke plicht.

10. Datalekken

Ontdekken we een inbreuk op de beveiliging die jouw gegevens raakt, dan melden we je dat zonder onnodige vertraging. We wachten niet tot ons onderzoek klaar is. We mailen het adres van je account, met wat we op dat moment weten:

- wat er gebeurde, en wanneer;
- welke gegevens het raakt, en hoeveel cliënten en dossiers ongeveer;
- de waarschijnlijke gevolgen;
- wat we doen om het op te lossen en de schade te beperken;
- wie je kunt bereiken voor meer informatie.

Weten we nog niet alles, dan vullen we aan zodra we meer weten. Een datalek bij een subverwerker geven we op dezelfde manier aan je door. Jij beslist of je het meldt aan de toezichthouder, binnen de 72 uur die de wet daarvoor geeft, en aan je cliënten: in België is dat de Gegevensbeschermingsautoriteit, in Nederland de Autoriteit Persoonsgegevens. We helpen je daarbij. Van elk incident houden we een register bij.

11. Hulp bij een DPIA

Maak je een gegevensbeschermingseffectbeoordeling (DPIA), of moet je de toezichthouder vooraf raadplegen? Dan geven we je kosteloos wat je over ombra nodig hebt: deze overeenkomst, de beveiligingsmaatregelen, de subverwerkers en antwoorden op je vragen.

12. Bewaren, teruggeven en verwijderen

Zolang je ombra gebruikt, verwijderen we geen dossiergegevens op eigen initiatief. Jij beslist wat weg mag. In België vraagt de Kwaliteitswet een dossier minstens 30 en hoogstens 50 jaar na het laatste contact te bewaren. ombra laat je een dossier pas verwijderen als die 30 jaar voorbij zijn, en toont je onder Instellingen → Gegevens welke dossiers zover zijn. Wanneer je het daarna verwijdert, beslis jij.

In Nederland vraagt de WGBO in de regel 20 jaar, en kan een cliënt je vragen het dossier te vernietigen. Moet een dossier eerder weg dan ombra toelaat, mail dan privacy@ombracare.com vanaf het e-mailadres van je account: tot ombra dat zelf kan, verwijderen wij het voor je.

Stop je met ombra, dan kies jij: we geven alles terug en verwijderen daarna, of we verwijderen zonder teruggave. Standaard geven we eerst alles terug, zoals artikel 12 van de voorwaarden zegt:

1. Je downloadt je volledige export.
2. Je hebt 30 dagen om nog te downloaden of je account te heropenen.
3. Daarna verwijderen we alles van je werkruimte, ook het logboek. Uit de databaseback-ups verdwijnt het binnen 35 dagen. Eerdere versies van documenten ruimen we op als ze ouder zijn dan 35 dagen; daarna zijn ze nog 35 dagen terug te halen. Zetten we in die tijd een back-up terug, dan verwijderen we het opnieuw.

Heb je je gegevens al veilig en wil je geen nieuwe export? Mail dan privacy@ombracare.com vanaf het e-mailadres van je account, dan verwijderen we zonder teruggave. Voor die route hoef je geen nieuwe export te downloaden. Je kunt je keuze wijzigen tot de verwijdering begint. Je eigen wettelijke bewaarplicht blijft gelden.

Een kopie van het logboek met alleen kenmerken, zonder namen of inhoud, bewaren we 365 dagen voor de beveiliging. Teruggeven kost niets. Op verzoek bevestigen we de verwijdering schriftelijk. Moet de wet ons iets langer laten bewaren, dan zeggen we je wat en waarom, en gebruiken we het voor niets anders.

13. Informatie en audits

We geven je kosteloos alle informatie die je nodig hebt om te laten zien dat deze afspraken worden nagekomen: deze overeenkomst, de beveiligingsmaatregelen en antwoorden op je vragenlijsten.

Wil je een audit, door jezelf of door een onafhankelijke deskundige met geheimhoudingsplicht? Laat het ons minstens tien werkdagen vooraf weten, dan spreken we samen af wanneer en hoe, op een werkdag en zo dat de gegevens van andere klanten veilig blijven. Je draagt de kosten van je eigen audit; onze eigen tijd rekenen we niet aan. Blijkt dat we deze overeenkomst niet nakomen, dan herstellen we dat zo snel mogelijk, op onze kosten. Vraagt een toezichthouder een onderzoek, dan werken we mee.

14. Aansprakelijkheid

Voor deze overeenkomst geldt de aansprakelijkheid uit artikel 13 van de voorwaarden. Die doet niets af aan de rechten van je cliënten onder artikel 82 van de AVG.

15. Wijzigingen en voorrang

We wijzigen deze overeenkomst zoals artikel 16 van de voorwaarden zegt: met een goede reden, minstens 30 dagen vooraf, en pas als je de nieuwe versie aanvaardt. Verandert de wet, dan passen we haar daaraan aan. Gaat het over persoonsgegevens, dan gaat deze overeenkomst voor op de voorwaarden.

Deze plichten blijven gelden zolang we gegevens voor je bewaren. Je kunt deze overeenkomst als pdf downloaden, bewaren of afdrukken als deel van je afspraken met ombra.

Deze overeenkomst is opgesteld in het Nederlands. Er bestaat ook een Engelse vertaling; verschillen de twee, dan gaat de Nederlandse tekst voor.

Bijlage A. De verwerking

Waarvoor

ombra leveren: dossiers voeren, notities en documenten bewaren, afspraken plannen, aanmeldingen en een wachtlijst beheren, groepen en hun inschrijvingen bijhouden, formulieren en een boekingspagina publiceren, agenda en mail koppelen, mail versturen in jouw naam, en alles exporteren.

Wat ombra ermee doet

Gegevens ontvangen, bewaren, ordenen, tonen, versleutelen, in jouw naam versturen, exporteren en verwijderen.

Over wie

- je cliënten, ook minderjarigen, en hun vertegenwoordigers;
- aanmelders en mensen die een afspraak boeken;
- groepsdeelnemers en wie zich voor een groep inschrijft;
- mensen die in een dossier staan, zoals verwijzers, huisartsen, contactpersonen en naasten;
- collega's met wie je een aanmeldruimte of groep deelt;
- mensen in je gekoppelde agenda en mailbox.

Welke gegevens

- **Identiteit en contact**: naam, geboortedatum, adres, e-mailadressen, telefoon, taal, voornaamwoorden en het rijksregisternummer of BSN.
- **Zorgadministratie**: ziekenfonds of zorgverzekeraar, verwijzer, huisarts, contactpersoon bij nood, zorgvorm, tarief en betaalstatus.
- **Gezondheid**: hulpvraag, doelen, sessienotities met al hun versies, huiswerk, documenten, groepsnotities en aanwezigheid.
- **Aanmeldingen en boekingen**: wat iemand invult in je aanmeld- of inschrijfformulier, met de vragen en de privacytekst van dat moment. Bij een boeking: naam, contactgegevens, bericht en het gekozen moment.
- **Agenda en mail**: afspraken met hun deelnemers uit je gekoppelde agenda; welke mails gelezen, beantwoord of afgehandeld zijn; je concepten; van elke verstuurde mail een vingerafdruk en de status. De inhoud van je mail haalt ombra live op en bewaart die niet.

- **Logboek**: wie wanneer welk dossier opende of wijzigde.

Bijzondere gegevens

Gezondheidsgegevens (artikel 9 AVG) en een nationaal identificatienummer, het rijksregisternummer of BSN (artikel 87 AVG). Andere bijzondere gegevens leg je alleen vast als je zorg ze nodig heeft.

Hoe lang

Zolang je ombra gebruikt, en daarna zoals artikel 12 zegt.

Bijlage B. Beveiligingsmaatregelen

- **Opslag in de EU**: Microsoft Azure in Ierland (Microsoft Azure North Europe), met een kopie van de back-ups van de database in Nederland (Microsoft Azure West Europe).
- **Versleuteling**: alle verbindingen (TLS 1.2 of nieuwer) en alle opslag (AES-256). Documenten, mailconcepten, notities bij groepssessies en de sleutels van koppelingen versleutelt ombra er zelf nog eens bij (AES-256-GCM), met de sleutel in een aparte sleutelkluis.
- **Scheiding**: de database schermt elke werkruimte af van de andere. Collega's zien alleen wat jij met hen deelt, zoals een gedeelde aanmeldruimte of een groep.
- **Inloggen**: met een wachtwoord, via Google of Microsoft, met een eenmalige code per e-mail of met een toegangssleutel (passkey) die op het apparaat om gezicht, vingerafdruk of pincode vraagt. Op een apparaat waarop de laatste 90 dagen niet met een code uit de mail, Google, Microsoft of een toegangssleutel is ingelogd, vraagt ombra na het wachtwoord ook een code uit de mail. Wachtwoorden bewaren we alleen als onleesbare hash. Een authenticator als extra slot; dan vragen gevoelige stappen een nieuwe code, en volstaat een toegangssleutel als beide sloten. Inlogsessies lopen af na 30 minuten zonder activiteit en na hoogstens 12 uur.
- **Logboek**: wie een dossier opent, wijzigt of exporteert, zonder inhoud; zoeken en Vandaag per werkruimte. Een export van een volledig account geeft ons een melding.
- **Documenten**: een malwarescan voor iemand een upload kan openen.
- **Netwerk**: de database en de opslag zijn niet bereikbaar vanaf het internet. Uitgaand verkeer gaat alleen naar Microsoft en Google. Een firewall voor webapplicaties staat voor de app.
- **Back-ups en herstel**: een reservekopie van de database in een tweede datacenter neemt automatisch over; doorlopende back-ups van 35 dagen, met een kopie in een tweede regio; documenten verspreid over meerdere datacenters, met hun eerdere versies. Doel: hoogstens 15 minuten aan wijzigingen kwijt na een fout, een uur na het verlies van een hele regio, en binnen 4 uur weer werkend. Elk kwartaal een hersteloefening.
- **Beheer**: geen gewone, vaste toegang tot gegevens, een tijdelijke beheerrol met een tweede stap bij het inloggen en een vastgelegde reden, noodaccounts alleen voor als al het andere faalt, een geheimhoudingsplicht, elk kwartaal een controle van wie welke rechten heeft, toegang ingetrokken op de dag dat iemand stopt, en versleutelde werkcomputers.
- **Ontwikkeling**: gescheiden omgevingen, met alleen verzonnen gegevens buiten de echte app; elke wijziging nagelezen en automatisch getest, met een beveiligingsscan; onderdelen automatisch gecontroleerd op bekende kwetsbaarheden; de maatregelen minstens één keer per jaar nagelopen.

Meer uitleg staat bij Beveiliging.

Bijlage C. Subverwerkers

Subverwerker	Waarvoor	Waar
Microsoft Ireland Operations Ltd. (Microsoft Azure)	Hosting van ombra: de app, de database, documenten, sleutels en logboeken, de malwarescan van uploads en de beveiligde toegang (Azure Front Door met firewall).	Ierland (Microsoft Azure North Europe), met een kopie van de back-ups van de database in Nederland (Microsoft Azure West Europe). Verbindingen komen binnen op het dichtstbijzijnde knooppunt van Microsoft.

De volledige lijst, met de diensten die ombra voor zijn eigen werk gebruikt en de koppelingen die je zelf maakt, staat bij Subverwerkers.

Bijlage D. Wie toegang heeft

Wie bij de gezondheidsgegevens van je cliënten kan, met welke rol, en wat hen tot geheimhouding verplicht (artikel 9 van de wet van 30 juli 2018).

Wie	Rol	Gebonden door
Jij, en wie jij toegang geeft	Zorg en praktijkadministratie. Collega's zien alleen wat jij met hen deelt: leden van een gedeelde aanmeldruimte de aanmeldingen in die ruimte, groepstherapeuten hun groep.	Jouw beroepsgeheim, en wat jij met hen afspreekt.
Beheerders van ombra	Technisch beheer: een storing oplossen, een beveiligingsincident onderzoeken of je helpen als je daarom vraagt. Alleen via een tijdelijke beheerrol, of in nood via een noodaccount, en we leggen vast wie, wanneer en waarom.	Een schriftelijke geheimhoudingsplicht.
Medewerkers van Microsoft	Beheer van de datacenters en de clouddiensten. Geen gewone toegang tot de inhoud.	De verwerkersovereenkomst van Microsoft en hun geheimhoudingsplicht.