

Verwerkersovereenkomst (AVG art. 28) — Nara · versie 2, 12 oktober 2026

Status: VOORSTEL ter juridische toetsing en ondertekening · opgesteld 2026-10-12 · weerspiegelt de code op d3427b8 (PROD) · vervangt het concept van 2026-08-04 (dat blijft leesbaar in de git-historie).

Toelichting van de opsteller — lees dit vóór je het stuk verstuurt

Wat dit is. Een volledige verwerkersovereenkomst naar art. 28 AVG en de Uitvoeringswet AVG, geschreven voor een vrijgevestigde GGZ-praktijk (de Praktijk) die Nara gebruikt om sessies op te nemen, verslagen, behandelplannen en onderzoeksanalyses voor te bereiden en het dossier te raadplegen. De tekst volgt de opbouw die de Autoriteit Persoonsgegevens en de NVvM in hun modelovereenkomsten hanteren, met de acht verplichte elementen van art. 28(3) elk in een eigen artikel, en met bijlagen die de feiten dragen (verwerkingen, subverwerkers, bewaartermijnen, beveiliging). De bijlagen zijn geschreven op wat de code **vandaag aantoonbaar doet**; waar een belofte verder zou gaan dan de code, staat dat in deze toelichting en niet in het contract.

Ik ben geen advocaat. Dit stuk is opgesteld met de zorg van een jurist die het dossier kent, maar het is niet door een advocaat met zorg- en AVG-praktijk gezien. Laat het nakijken vóór ondertekening; de punten waar een advocaat het eerst naar zal kijken staan hieronder onder "Risico's".

Wat is veranderd ten opzichte van het concept van 04-08

1. **De verwerker is een onderneming.** Rick heeft op 12-10 besloten tussen het "ja" van de eerste praktijk en de start een eenmanszaak in te schrijven en de overeenkomst daaruit te sluiten. Art. 1 is daarop geschreven (handelsnaam Nara, KvK-nummer in te vullen). Zie Risico 1 over aansprakelijkheid.
2. **Microsoft bewaart geen prompts meer.** De uitzondering *Modified Abuse Monitoring* is op 16-09-2026 toegekend (Application 3836663): geen opslag van prompts en completions, geen menselijke beoordeling. Het "30-dagenvenster" uit het oude §12 is weg; de portal-verificatie staat nog op de invullijst.
3. **Twee nieuwe verwerkingen** sinds 04-08: de **onderzoeksanalyse** (upload van het verslag van een psychodiagnostisch medewerker, 12-10) en de **gebruiksmetrie** (tokens per modelaanroep gekoppeld aan opname- en verslag-id, ADR-0049, 12-10). Beide staan in Bijlage 1; de metrie is in art. 3 lid 4 uitdrukkelijk als geïnstrueerde verwerking ondergebracht, zodat art. 28(10) niet in beeld komt.
4. **Regio's en diensten zijn concreet:** Azure Speech en Blob in Sweden Central, Azure OpenAI als resource in Sweden Central met verwerking in de EU-datazone, Railway compute EU West. Wat nog niet in de portal is nagemeten staat als zodanig op de invullijst, niet als feit in het contract.
5. **Bewaartermijnen zijn geactualiseerd** naar wat de code doet, inclusief de bronfragmenten die na goedkeuring bij het verslag blijven (dat stond in v1 te rooskleurig) en het onderzoeksverslag.
6. **Het hoofdstuk "openstaande punten" is uit het contract gehaald.** Een contract is geen takenlijst. Wat de Praktijk moet weten vóór ze tekent, staat in art. 16 (transparantie bij ondertekening) in drie zinnen; de rest staat hieronder en in `actielijst-rick.md`.
7. **Nieuw:** toegang door Nara tot inhoud alleen via een door de Praktijk geautoriseerde, tijdgebonden en gelogde ondersteuningssessie (art. 8 lid 3, naar ADR-0003); afgeleide geheimhouding onder het medisch beroepsgeheim (art. 10); de operationele start-eis dat de praktijk in de gecertificeerde modus van de applicatie draait (art. 4 lid 5); een aansprakelijkheidsartikel dat naar de hoofdovereenkomst verwijst met de verdeling van art. 82 AVG (art. 13).

Risico's die een advocaat als eerste zal zien

1. **Eenmanszaak = onbeperkte persoonlijke aansprakelijkheid.** Alles wat uit art. 82 AVG of uit een datalek voortvloeit raakt Ricks privévermogen. Mitigatie: een beroeps- en bedrijfsaansprakelijkheids- verzekering met cyberdekking vóór de eerste echte sessie, en een aansprakelijkheidsplafond in de hoofdovereenkomst (gebruikelijk: het jaarbedrag van de vergoeding, met uitzondering van opzet en grove schuld). Een BV op termijn is de structurele oplossing; dat is geen vereiste voor deze start.
2. **De hoofdovereenkomst bestaat nog niet.** Een verwerkersovereenkomst hangt aan een dienstverlenings-overeenkomst (duur, vergoeding, beëindiging, aansprakelijkheid). Art. 13 en 14 verwijzen ernaar. Voor een proefperiode volstaat een korte dienstverleningsovereenkomst van één pagina; zonder die pagina mist de verwerkersovereenkomst zijn anker.
3. **Gebruiksmetrick (art. 3 lid 4).** De koppeling van tokentellingen aan opname- en verslag-id is gepseudonimiseerd en inhoudsvrij, maar dient Nara's bedrijfsvoering. Daarom staat hij als geïnstrueerde verwerking in het contract, met het verbod om er iets anders mee te doen dan factureren, capaciteit beheren en misbruik opsporen, en met de ontkoppeling bij wissen. Zo blijft Nara verwerker en niet (mede)verantwoordelijke voor dat stukje (art. 28(10)). Dit is ook de regel die in het verwerkingsregister (ropa.md) moet komen; die staat er nog niet.
4. **Wat de code nog niet doet, belooft het contract niet.** Twee plekken waar v1 of de website méér zei dan de code: (a) er is **geen export van een hele cliënt in één handeling**, alleen per verslag; (b) er is **geen tweestapsverificatie** bij het inloggen. Beide staan op de bouwlijst; ze horen niet in het contract tot ze er zijn. (De 30-dagenregel voor het onderzoeksverslag is op 12-10 gebouwd, Rule D in de opschoonronde, en staat daarom wél in Bijlage 3.) De website (meetnara.nl) zegt op deze punten nog meer dan de code; dat moet gelijkgetrokken worden vóór de Praktijk beide naast elkaar legt.
5. **Back-ups.** Verwijdering uit de live-omgeving werkt niet onmiddellijk door in back-ups van de subverwerkers. Art. 9 lid 5 regelt dat eerlijk (back-ups vallen binnen de retentie van de subverwerker en worden niet gelezen), maar de termijn moet van Railway en Microsoft worden overgenomen; invullijst.
6. **NEN 7510.** Het contract zegt "ingericht naar NEN 7510 en NEN 7513, niet gecertificeerd". Dat is de enige verdedigbare formulering; "conform" of "gecertificeerd" zou misleidend zijn.
7. **WGBO en beroepsgeheim.** Nara is geen hulpverlener en geen "hulp persoon" in de zin van art. 7:457 lid 2 BW; de geheimhouding is contractueel en afgeleid (art. 10). De informatieplicht richting de cliënt en het vastleggen van de toestemming voor de opname blijven bij de Praktijk; Nara legt alleen vast dát en wanneer er toestemming is (art. 4).

Invullijst voor Rick (elk `[...]` in het contract)

#	Waar	Wat
1	art. 1	Naam, handelsnaam, KvK-nummer, adres en e-mail van de eenmanszaak; privacycontact
2	art. 1	Gegevens van de Praktijk (rechtsvorm, KvK, BIG-nummer behandelaar, privacycontact)
3	art. 14	Verwijzing naar de dienstverleningsovereenkomst en haar datum
4	art. 15	Bevoegde rechtbank (voorstel: Rechtbank Overijssel, Zwolle)
5	Bijlage 2	Microsoft: bevestig dat het Microsoft Products and Services DPA geldt voor de tenant; portal-bewijs dat abuse monitoring uit staat (instructielink in de mail van 16-09)
6	Bijlage 2	Railway: DPA accepteren (railway.app/legal/dpa), databaseregio

		en volume-versleuteling nameten, back-upretentie overnemen
7	Bijlage 2	Azure Blob en OpenAI: regio in de portal nameten (de code toetst de opgegeven waarde, niet de werkelijke)
8	Bijlage 3	Back-upretentie Railway en Microsoft invullen
9	art. 16	Datum van ondertekening en de drie transparantiezinnen controleren op die datum

Checklist vóór ondertekening

- ☐ Eenmanszaak ingeschreven; KvK-nummer in art. 1.
- ☐ Dienstverleningsovereenkomst (één pagina volstaat) getekend of gelijktijdig getekend.
- ☐ Verzekering (BAV met cyberdekking) afgesloten of aantoonbaar aangevraagd.
- ☐ Invulijst 5 t/m 8 gedaan; register dpa-subverwerkersregister.md en ropa.md bijgewerkt (gebruiksmetriek erin).
- ☐ De tenant van de Praktijk in de gecertificeerde modus van de applicatie gezet (art. 4 lid 5).
- ☐ Juridische nakijkronde gedaan; opmerkingen verwerkt.
- ☐ Website gelijkgetrokken met Bijlage 3 en 4 (geen beloften die de code niet doet).

VERWERKERSOVEREENKOMST

Artikel 1 — Partijen

De Praktijk (verwerkingsverantwoordelijke, art. 4 onder 7 AVG)	[naam praktijk], [rechtsvorm], KvK [nummer], gevestigd te [adres], vertegenwoordigd door [naam behandelaar], BIG [nummer]. Contactpersoon gegevensbescherming: [naam, e-mail].
Nara (verwerker, art. 4 onder 8 AVG)	[voorletters en achternaam], handelend onder de naam Nara, eenmanszaak, KvK [nummer], gevestigd te [adres]. Contactpersoon gegevensbescherming en meldpunt incidenten: [naam, e-mail, telefoon].

Partijen worden hierna gezamenlijk "Partijen" genoemd.

Artikel 2 — Onderwerp, aard en doel van de verwerking (art. 28(3) AVG)

- Onderwerp.** Nara stelt de Praktijk een webapplicatie ter beschikking waarmee de behandelaar behandel sessies opneemt, een conceptverslag laat opstellen uit de opname, een behandelplan en een analyse van een psychodiagnostisch onderzoek laat voorbereiden, en per cliënt terugvindt wat er in eerdere sessies is vastgelegd (hierna: "de Dienst").
- Aard.** Opnemen, transcriberen, in fragmenten knippen, gestructureerd uitlezen, genereren van concepttekst, ordenen en tellen, opslaan, tonen, exporteren, verwijderen; alsmede het bijhouden van een logboek van handelingen en van het gebruik van de Dienst.
- Doel.** Uitsluitend het ondersteunen van de dossiervoering en behandelvoorbereiding van de Praktijk. Nara gebruikt de persoonsgegevens niet voor eigen doeleinden, niet voor productonderzoek en niet voor het trainen of verbeteren van modellen, niet van eigen modellen en niet van die van subverwerkers.
- De grens die Nara zichzelf oplegt en die contractueel geldt.** Nara ordent en hervindt wat de behandelaar en de cliënt hebben voortgebracht; Nara voelt geen klinisch oordeel. Nara genereert geen diagnoses, geen ernst- of risico-inschattingen, geen behandeladviezen en geen uitspraken over voor- of achteruitgang. Elke door Nara gegenereerde zin draagt een verwijzing naar het bronfragment; tekst zonder bron wordt niet getoond. Alle gegenereerde tekst is concept en komt uitsluitend in het dossier na een uitdrukkelijke goedkeuring door de behandelaar.
- Categorieën betrokkenen:** cliënten van de Praktijk; personen over wie een cliënt of een onderzoeker in een sessie of verslag spreekt (naasten, informanten bij een heteroanamnese); behandelaren en medewerkers van de Praktijk.

6. Categorieën persoonsgegevens:

Categorie	Voorbeelden
Identificerende gegevens cliënt	naam, geboortedatum, voornaamwoord, initialen, startdatum traject
Bijzondere persoonsgegevens, gezondheid (art. 9 AVG)	audio-opname van de sessie, transcript, bronfragmenten, verslagtekst, behandelplan, behandeldoelen, verbatim uitspraken van de cliënt, het geüploade onderzoeksverslag van een psychodiagnostisch medewerker en de daaruit opgestelde analyse
Gegevens van derden in het dossier	wat een cliënt over naasten zegt; informatie van een informant in een heteroanamnese
Toestemmingsgegevens	wel of geen toestemming, reikwijdte, tijdstip, intrekking
Gegevens behandelaar	naam, e-mail, BIG- en AGB-nummer, registratietype,

	handelingen in de applicatie
Gebruiksgegevens	token tellingen per modelaanroep, gekoppeld aan opname- en verslag-id (geen cliënt-id, geen tekst)

7. **Duur.** Deze overeenkomst geldt zolang de Dienst wordt geleverd. De artikelen 9 (teruggave en verwijdering), 10 (geheimhouding) en 13 (aansprakelijkheid) blijven na beëindiging van kracht.

Artikel 3 — Instructies (art. 28(3)(a))

1. Nara verwerkt persoonsgegevens uitsluitend op gedocumenteerde instructie van de Praktijk. Deze overeenkomst met haar bijlagen, de dienstverleningsovereenkomst en het normale gebruik van de applicatie door een geautoriseerde behandelaar gelden als die instructie.
2. Nara stelt de Praktijk onverwijld in kennis wanneer een instructie naar haar oordeel in strijd is met de AVG of andere toepasselijke wetgeving.
3. Nara verwerkt niet buiten instructie, behoudens een verplichting krachtens Unierecht of Nederlands recht; in dat geval stelt Nara de Praktijk vooraf in kennis, tenzij die wet dat verbiedt.
4. **Gebruiksmetriek.** De Praktijk instrueert Nara om per modelaanroep het tokengebruik vast te leggen, gekoppeld aan het opname- en verslag-id, uitsluitend voor (a) de berekening van de kosten van de Dienst per verslag, (b) capaciteitsbeheer en (c) het opsporen van misbruik. Nara legt daarbij geen cliënt-id en geen inhoud vast, koppelt de ids los zodra een cliënt wordt gewist (artikel 9 lid 3) en gebruikt de gegevens voor geen ander doel. Geaggregeerde totalen zonder enig id zijn geen persoonsgegevens en mag Nara voor haar bedrijfsvoering gebruiken.
5. **Wat Nara niet doet.** Nara koppelt de persoonsgegevens niet aan gegevens van andere praktijken, gebruikt ze niet voor profilering van behandelaren of cliënten, en maakt ze niet toegankelijk voor enige andere partij dan de in Bijlage 2 genoemde subverwerkers.

Artikel 4 — Toestemming, informatieplicht en de start van de verwerking

1. **Geen opname zonder vastgelegde toestemming.** De applicatie weigert het starten van een opname en het verwerken van een onderzoeksverslag wanneer voor die cliënt geen actieve toestemming is vastgelegd. Deze grendel faalt in de veilige richting.
2. **Het verkrijgen van de toestemming en het informeren van de cliënt zijn taken van de Praktijk** (art. 13 en 14 AVG; art. 7:448 BW). Nara legt vast dát er toestemming is, met welke reikwijdte en wanneer; Nara toetst niet of het gesprek met de cliënt inhoudelijk is gevoerd.
3. **Intrekking werkt door.** Trekt een cliënt de toestemming in, dan verwijdert Nara de audio en het transcript van de betrokken opnames bij de eerstvolgende opschoning en in elk geval binnen 7 dagen. Reeds goedgekeurde verslagtekst blijft bestaan tot de Praktijk om verwijdering verzoekt; die tekst is op dat moment onderdeel van het dossier van de Praktijk.
4. **Derden in het dossier.** Gegevens over naasten en informanten verwerkt Nara uitsluitend als onderdeel van het dossier van de cliënt en op dezelfde voet; de Praktijk is verantwoordelijk voor de rechtmatigheid van het opnemen van die gegevens in het dossier.
5. **Start.** Nara zet de omgeving van de Praktijk pas in de modus waarin gegevens van echte cliënten verwerkt kunnen worden ("gecertificeerde modus" van de applicatie) nadat deze overeenkomst door beide Partijen is ondertekend. Tot dat moment accepteert de applicatie uitsluitend fictieve cliënten.

Artikel 5 — Rechten van betrokkenen (art. 28(3)(e))

1. Nara verleent de Praktijk bijstand bij verzoeken van betrokkenen, voor zover dat gezien de aard van de verwerking mogelijk is:

Recht	Wat Nara levert
Inzage (art. 15)	De Praktijk kan alle gegevens van een cliënt in de applicatie inzien en per verslag exporteren
Rectificatie (art. 16)	Alle door Nara gegenereerde tekst is door de behandelaar bewerkbaar; feitelijke onjuistheden in gegenereerde tekst worden door de behandelaar gecorrigeerd vóór goedkeuring
Verwijdering (art. 17)	Eén handeling verwijdert de gegevens van een cliënt uit alle onderdelen van de Dienst (artikel 9 lid 3)
Beperking (art. 18)	Archivering van een cliënt; tijdens archivering wordt niets verwerkt en niets gegenereerd
Overdraagbaarheid (art. 20)	Export van goedgekeurde verslagen, plannen en analyses als leesbare tekst, per stuk
Bezwaar (art. 21)	De beoordeling ligt bij de Praktijk; Nara voert uit wat de Praktijk beslist

2. Nara reageert op een verzoek van de Praktijk binnen 5 werkdagen, zodat de Praktijk de termijn van art. 12(3) AVG kan halen.
3. Wendt een betrokkene zich rechtstreeks tot Nara, dan verwijst Nara door naar de Praktijk en stelt de Praktijk onverwijld in kennis. Nara beantwoordt zo'n verzoek niet zelfstandig.

Artikel 6 — Beveiliging (art. 28(3)(c) en art. 32)

1. Nara treft passende technische en organisatorische maatregelen, rekening houdend met de stand van de techniek, de kosten en het risico van de verwerking van bijzondere persoonsgegevens over gezondheid. De maatregelen staan in Bijlage 4 en worden beschreven in het beheersmaatregelenregister van Nara.
2. **Normenkader.** De Dienst is ingericht naar NEN 7510 (informatiebeveiliging in de zorg) en NEN 7513 (logging). Nara is niet gecertificeerd en doet daarover geen andere uitspraak dan deze.
3. **Wijzigingen.** Nara verlaagt het beveiligingsniveau niet zonder voorafgaande schriftelijke instemming van de Praktijk. Verhogingen meldt Nara in de actualisering van Bijlage 4.
4. **Personen onder Nara's gezag.** Iedereen die namens Nara toegang heeft tot persoonsgegevens is schriftelijk tot geheimhouding verplicht (art. 28(3)(b)) en heeft alleen de toegang die voor de taak nodig is. Op de datum van ondertekening is dat uitsluitend de ondernemer zelf.

Artikel 7 — Subverwerkers (art. 28(2) en 28(4))

1. De Praktijk verleent Nara algemene schriftelijke toestemming voor het inschakelen van de in Bijlage 2 genoemde subverwerkers.
2. Nara stelt de Praktijk ten minste 30 dagen vooraf schriftelijk in kennis van een voorgenomen toevoeging of vervanging. De Praktijk kan binnen die termijn gemotiveerd bezwaar maken. Leidt overleg niet tot een oplossing, dan mag de Praktijk de dienstverleningsovereenkomst met onmiddellijke ingang en zonder kosten beëindigen; artikel 9 is dan van toepassing.
3. Nara legt elke subverwerker bij schriftelijke overeenkomst dezelfde verplichtingen op als in deze overeenkomst, in het bijzonder passende waarborgen naar art. 32 AVG, en blijft jegens de Praktijk volledig aansprakelijk voor het nakomen van die verplichtingen door de subverwerker.

4. **Diensten die uitdrukkelijk geen cliëntgegevens verwerken.** Nara gebruikt voor haar oefen- en demonstratieomgeving diensten buiten de EER (Bijlage 2, deel B). Die omgeving bevat uitsluitend fictief materiaal. De scheiding is in de programmatuur afgedwongen en wordt bij elke wijziging geautomatiseerd gecontroleerd; een verwijzing vanuit die omgeving naar cliëntgegevens laat de bouw van de programmatuur falen. Deze diensten zijn geen subverwerkers in de zin van deze overeenkomst.

Artikel 8 — Locatie van de verwerking, doorgifte en toegang

1. **Alle verwerking van persoonsgegevens vindt plaats binnen de Europese Economische Ruimte.** De applicatie start niet wanneer een geconfigureerde dienst een ontbrekende of niet-EER-regio heeft.
2. Nara geeft geen persoonsgegevens door naar een land buiten de EER en schakelt daarvoor geen subverwerker in, behoudens voorafgaande schriftelijke toestemming van de Praktijk en een geldig doorgiftemechanisme in de zin van hoofdstuk V AVG. Voor zover een subverwerker in Bijlage 2 behoort tot een concern met vestigingen buiten de EER, geldt de contractuele vastlegging van die subverwerker dat de verwerking voor Nara binnen de EER plaatsvindt (Bijlage 2).
3. **Toegang door Nara tot inhoud.** De beheeromgeving van Nara toont geen cliëntinhoud. Toegang van Nara tot inhoud van de Praktijk vindt uitsluitend plaats binnen een door de Praktijk in de applicatie geautoriseerde ondersteuningssessie, die in tijd beperkt is, door de Praktijk kan worden ingetrokken en in het logboek wordt vastgelegd. Buiten zo'n sessie heeft Nara geen leesrecht op inhoud.

Artikel 9 — Bewaren, teruggave en verwijdering (art. 28(3)(g))

1. **Nara is niet het dossier van de Praktijk.** De Dienst is een werkplek waar een verslag ontstaat; het medisch dossier en de bewaarplicht van art. 7:454 BW (twintig jaar) liggen bij het dossiersysteem van de Praktijk. De Praktijk draagt er zorg voor dat goedgekeurde stukken daarheen worden overgebracht.
2. **Bewaartermijnen binnen de Dienst** staan in Bijlage 3. Nara bewaart niet langer dan daar vermeld.
3. **Verwijdering van een cliënt** gebeurt op verzoek van de Praktijk in één handeling in de applicatie. Daarbij worden alle opnames, transcripten, fragmenten, verslagen, plannen, analyses, geüploade documenten, toestemmingsrecords en afspraken van die cliënt verwijderd, en worden de opname- en verslag-ids in de gebruiksmetrick losgekoppeld. Er blijft één anonieme plaatshouder zonder persoonsgegevens over, zodat het logboek consistent blijft.
4. **Bij het einde van de overeenkomst** exporteert de Praktijk wat zij wil behouden; Nara verleent daarbij bijstand. Nara verwijdert alle persoonsgegevens van de Praktijk binnen 30 dagen na beëindiging en bevestigt dat schriftelijk, tenzij Unierecht of Nederlands recht opslag voorschrijft.
5. **Logboek en back-ups.** Het logboek (artikel 11 lid 4) blijft bestaan; het bevat identificatie- nummers en handelingen, nooit inhoud. Back-ups van subverwerkers worden niet gelezen en vallen binnen de retentietermijn van die subverwerker (Bijlage 3); binnen die termijn verdwijnen de gegevens ook daaruit.

Artikel 10 — Geheimhouding en beroepsgeheim

1. Nara houdt alles geheim wat zij in het kader van deze overeenkomst over cliënten, naasten en behandelaren verneemt, en legt dezelfde verplichting op aan personen onder haar gezag en aan subverwerkers. Deze verplichting blijft na afloop van de overeenkomst bestaan.
2. Nara erkent dat de gegevens vallen onder het medisch beroepsgeheim van de behandelaar (art. 7:457 BW en art. 88 Wet BIG) en dat op Nara een daarvan afgeleide geheimhoudingsplicht rust. Nara verstrekt

geen gegevens aan derden, ook niet op verzoek van een overheidsinstantie, zonder de Praktijk vooraf in de gelegenheid te stellen zich daartegen te verzetten, tenzij de wet dat verbiedt.

3. Nara rapporteert niet aan derden over het gebruik van de Dienst door de Praktijk, anders dan in geaggregeerde vorm zonder enig herleidbaar gegeven.

Artikel 11 — Inbreuken, bijstand en logboek (art. 28(3)(f), art. 32 t/m 36)

1. **Melding.** Nara stelt de Praktijk onverwijld en uiterlijk binnen 24 uur na ontdekking in kennis van een inbreuk in verband met persoonsgegevens, via het contactpunt in artikel 1. De melding bevat ten minste: de aard van de inbreuk, de categorieën en het aantal betrokkenen en gegevens, de waarschijnlijke gevolgen, de getroffen en voorgenomen maatregelen en een contactpersoon. Is niet alles direct bekend, dan meldt Nara wat bekend is en vult aan.
2. **De melding aan de Autoriteit Persoonsgegevens (art. 33) en aan betrokkenen (art. 34) doet de Praktijk.** Nara verleent daarbij alle redelijke bijstand en meldt niet zelfstandig, tenzij de Praktijk dat schriftelijk opdraagt.
3. **Bijstand.** Nara verleent de Praktijk bijstand bij het uitvoeren van een gegevensbeschermings-effectbeoordeling (art. 35) en een voorafgaande raadpleging (art. 36), door de relevante documentatie van de Dienst ter beschikking te stellen en vragen binnen 10 werkdagen te beantwoorden.
4. **Logboek.** Nara legt elke raadpleging en elke wijziging van cliëntgegevens, elke generatie en elke goedkeuring vast in een logboek waaraan alleen kan worden toegevoegd en dat per praktijk in een hash-keten is gezekerd (NEN 7513). De Praktijk kan het logboek van haar eigen omgeving opvragen. Het logboek bevat geen inhoud.
5. De volledige incidentprocedure van Nara, met rollen en escalatie, staat in `incident-procedure.md` en wordt op verzoek verstrekt.

Artikel 12 — Verantwoording en audit (art. 28(3)(h))

1. Nara stelt de Praktijk alle informatie ter beschikking die nodig is om de nakoming van art. 28 AVG aan te tonen, waaronder het beheersmaatregelenregister, het subverwerkersregister, het bewaarbeleid en de incidentprocedure.
2. De Praktijk, of een door haar aangewezen en tot geheimhouding verplichte auditor, mag ten hoogste eenmaal per kalenderjaar een audit uitvoeren, na aankondiging van ten minste 15 werkdagen en binnen kantooruren. Na een inbreuk of een geconstateerde tekortkoming geldt die beperking niet.
3. Nara mag voor een audit redelijke kosten in rekening brengen bij meer dan één audit per jaar, tenzij de aanleiding een inbreuk of een tekortkoming aan de zijde van Nara is.
4. Nara werkt mee aan onderzoeken van de Autoriteit Persoonsgegevens die de Praktijk betreffen.

Artikel 13 — Aansprakelijkheid

1. Elke Partij is jegens de andere aansprakelijk voor schade die voortvloeit uit een toerekenbare tekortkoming in de nakoming van deze overeenkomst of uit een overtreding van de AVG die aan haar is toe te rekenen, met inachtneming van de verdeling van art. 82 AVG.
2. Voor de omvang van de aansprakelijkheid en eventuele beperkingen daarvan geldt de dienstverleningsovereenkomst. Een beperking geldt niet voor opzet of bewuste roekeloosheid en niet voor zover de wet een beperking uitsluit.

3. Een door een toezichthouder opgelegde boete draagt de Partij aan wie de overtreding is toe te rekenen.

Artikel 14 — Duur, beëindiging en samenhang

1. Deze overeenkomst treedt in werking op de datum van ondertekening door beide Partijen en is onlosmakelijk verbonden met de dienstverleningsovereenkomst van [datum]. Bij strijdigheid gaat deze verwerkersovereenkomst voor, voor zover het de verwerking van persoonsgegevens betreft.
2. Beëindiging van de dienstverleningsovereenkomst beëindigt deze overeenkomst, onverminderd de bepalingen die naar hun aard voortduren.
3. Wijzigingen van deze overeenkomst zijn alleen geldig indien schriftelijk en door beide Partijen ondertekend. Bijlagen 2, 3 en 4 kunnen door Nara worden geactualiseerd volgens de procedure van artikel 7 lid 2 (subverwerkers) en artikel 6 lid 3 (beveiliging); een actualisering die de verplichtingen van Nara verzwakt kan zonder instemming.

Artikel 15 — Toepasselijk recht en geschillen

1. Op deze overeenkomst is Nederlands recht van toepassing.
2. Geschillen worden voorgelegd aan de bevoegde rechter van de Rechtbank [Overijssel, locatie Zwolle], nadat Partijen hebben getracht het geschil in onderling overleg op te lossen.

Artikel 16 — Transparantie bij ondertekening

Op de datum van ondertekening verklaart Nara aan de Praktijk het volgende, zodat de Praktijk weet wat er op dat moment nog niet is:

1. Nara is niet gecertificeerd voor NEN 7510 of ISO 27001; de Dienst is naar die normen ingericht.
2. De Dienst biedt op de datum van ondertekening geen tweestapsverificatie bij het inloggen; de Praktijk draagt zorg voor sterke, unieke wachtwoorden en het afsluiten van sessies op gedeelde apparaten.
3. De Praktijk behoort tot de eerste praktijken die gegevens van echte cliënten in de Dienst verwerkt; tot die datum is de Dienst met fictieve dossiers ontwikkeld en getest.

Ondertekening

De Praktijk	Nara
Naam:	Naam:
Functie:	Ondernemer
Plaats en datum:	Plaats en datum:
Handtekening:	Handtekening:

Bijlage 1 — Overzicht van verwerkingen

#	Verwerking	Gegevens	Grondslag Praktijk	Wat Nara doet	Wat Nara niet doet
1	Opname en transcriptie van een sessie	audio, transcript	art. 9(2)(h) jo. 6(1)(b), WGB0; toestemming voor de opname (art. 7:448 BW)	opname versleuteld opslaan, transcriberen bij Azure Speech, audio direct na transcriptie verwijderen	audio bewaren, audio terugluisterbaar maken
2	Conceptverslag	transcriptfragmenten, verslagtekst	idem	fragmenten uitlezen, concepttekst genereren met bron per zin, goedkeuring door behandelaar, transcript verwijderen bij goedkeuring	zelfstandig in het dossier schrijven, oordelen, samenvatten zonder bron
3	Behandelplan	fragmenten uit goedgekeurde intakeverslagen, plantekst	idem	navertellen uit de intake, voorstellen tonen naast het veld, oordeelsvelden leeg laten	diagnose, classificatie, prognose, crisisbeleid voorstellen
4	Dossier en briefing	goedgekeurde verslagen	idem	terughalen en tellen wat er in verslagen staat, met bron; signalen op frequentie en recentheid	duiding van beloop, ernst of richting
5	Analyse psychodiagnostisch onderzoek (12-10-2026)	geüpload onderzoeksverslag (PDF/Word), fragmenten met pagina, analyse	idem	document in fragmenten knippen op de kopjes van de onderzoeker, navertellen met pagina als bron, resultaten per onderzoeksvraag ordenen zoals het verslag dat doet, oordeelsvelden leeg laten	integratief beeld, antwoord op een onderzoeksvraag, classificatie of advies schrijven
6	Agenda en afspraken	datum, tijd, cliënt	art. 6(1)(b)	tonen en plannen	inhoud
7	Toestemmingsregistratie	wel/geen toestemming, reikwijdte, tijdstip	art. 7(1) (verantwoording)	vastleggen, intrekking doorvoeren	de toestemming zelf verkrijgen
8	Gebruiksmetrik (12-10-2026)	tokenellingen per modelaanroep, opname- en verslag-id, stap, modelversie, duur	art. 6(1)(b) (uitvoering van de Dienst, artikel 3 lid 4)	per verslag de kosten berekenen; ids loskoppelen bij wissen	cliënt-id of tekst vastleggen; ander gebruik
9	Logboek	wie, wat, wanneer, op welk id	art. 6(1)(c) jo. NEN 7513	toevoegen, hash-keten, op verzoek verstrekken	inhoud vastleggen, verwijderen
10	Account behandelaar	naam, e-mail,	art. 6(1)(b)	authenticatie,	delen met derden

		BIG/AGB, wachtwoordhash		scheiding per praktijk	
--	--	----------------------------	--	---------------------------	--

Buiten deze overeenkomst (geen cliëntgegevens, uitgeschakeld of fictief): de oefen- en trainingsomgeving, de therapeut-evaluatie (uit sinds 10-09-2026) en de intervisiefunctie (uit). Wordt een van deze functies voor de Praktijk ingeschakeld, dan wordt Bijlage 1 vooraf aangevuld.

Bijlage 2 — Subverwerkers

Deel A — subverwerkers van cliëntgegevens (binnen de EER)

Subverwerker	Entiteit	Dienst	Gegevens	Locatie	Overeenkomst en waarborgen
Microsoft Azure OpenAI	Microsoft Ireland Operations Ltd.	taalmodel voor concepttekst, ordening en tellingen	transcriptfragmenten, verslagtekst, fragmenten van het onderzoeksverslag	resource in Sweden Central; verwerking in de EU-datazone (Data Zone Standard, EU)	Microsoft Products and Services Data Protection Addendum [bevestiging tenant: invulijst 5]; geen training op klantgegevens; Modified Abuse Monitoring toegekend 16-09-2026 (Application 3836663): geen opslag van prompts en antwoorden, geen menselijke beoordeling
Microsoft Azure Speech	Microsoft Ireland Operations Ltd.	spraak naar tekst	audio	Sweden Central	idem DPA; content logging uitgeschakeld [bevestiging: invulijst 5]
Microsoft Azure Blob Storage	Microsoft Ireland Operations Ltd.	tijdelijke opslag van audio en van geüploade onderzoeksverslagen	audio, documenten	Sweden Central [portal-verificatie: invulijst 7]	idem DPA; privé-container; versleuteling in rust (AES-256)
Railway	Railway Corp.	hosting van de applicatie en de database	alle gegevens van de Dienst	compute EU West; database [regio: invulijst 6]	Railway Data Processing Addendum [acceptatie: invulijst 6]; versleuteling van opslag [invulijst 6]; back-upretentie [Bijlage 3]

Deel B — diensten die uitdrukkelijk geen cliëntgegevens verwerken (artikel 7 lid 4)

Dienst	Entiteit	Gebruik	Waarom geen subverwerker
Anthropic	Anthropic PBC (VS)	taalmodel voor de oefen- en demonstratieomgeving	uitsluitend fictief materiaal; de programmatuur weigert elke koppeling met cliëntgegevens (geautomatiseerd gecontroleerd bij elke wijziging)
ElevenLabs	ElevenLabs Inc. (VS)	spraaksynthese in de oefenomgeving	idem

Geen enkele andere partij heeft toegang tot persoonsgegevens van de Praktijk. Broncodebeheer en de bouwomgeving (GitHub) bevatten geen persoonsgegevens.

Bijlage 3 — Bewaartermijnen binnen de Dienst

Gegeven	Bewaartermijn	Mechanisme
Audio-opname	verwijderd direct na succesvolle transcriptie; een gemiste verwijdering wordt door een opschoonronde alsnog uitgevoerd	inline verwijdering + opschoonronde
Transcript	verwijderd bij goedkeuring van het verslag	inline verwijdering
Bronfragmenten (de stukjes transcript waar het verslag naar verwijst)	zolang het verslag bestaat; zij zijn de bronplicht van elke zin	gekoppeld aan het verslag
Conceptverslag dat nooit wordt goedgekeurd	zolang de cliënt bestaat, of tot verwijdering door de behandelaar	handeling behandelaar
Goedgekeurde verslagen, behandelplannen, analyses	zolang de cliënt in de Dienst bestaat, of tot verwijdering (artikel 9 lid 3); het bewaren voor de WGB0-termijn gebeurt in het dossiersysteem van de Praktijk	wissen in één handeling
Geüploade onderzoeksverslagen (PDF/Word), het bestand zelf	30 dagen na het vastleggen van de analyse; een niet-vastgelegde analyse houdt het bestand tot verwijdering	opschoonronde (Rule D), gelogd zonder inhoud
Fragmenten en citaten uit het onderzoeksverslag (de bronplicht van de analyse)	zolang de analyse bestaat; bij wissen van de cliënt verwijderd	wissen in één handeling
Toestemmingsrecords	zolang de cliënt bestaat; bij wissen verwijderd	wissen in één handeling
Afspraken (agenda)	zolang de cliënt bestaat	wissen in één handeling
Gebruiksmetrik	tokentellingen blijven als praktijk totaal; opname- en verslag-id worden bij het wissen van de cliënt losgekoppeld	automatisch bij wissen
Logboek	wordt niet verwijderd; bevat geen inhoud; bij wissen van een cliënt verwijst het naar een anonieme plaatshouder	hash-keten
Account behandelaar	tot beëindiging van de overeenkomst, daarna 30 dagen	artikel 9 lid 4
Back-ups bij subverwerkers	Railway: [retentie invullen]; Microsoft: [retentie invullen]; worden niet gelezen; verwijdering werkt binnen de retentietermijn door	beleid subwerker

Bijlage 4 — Technische en organisatorische maatregelen

Gebied	Maatregel
Scheiding per praktijk	elk verzoek is gebonden aan een ingelogde behandelaar en aan één praktijk; elke leesroute filtert op praktijk; een verwijzing naar een andere praktijk wordt niet gevonden; in de database is elke cliëntgebonden tabel met een samengestelde sleutel aan de cliënt én de praktijk gebonden; een geautomatiseerde test bewaakt dat elke route met een id op deze scheiding is getoetst
Residency	de applicatie weigert te starten wanneer een geconfigureerde dienst een ontbrekende of niet-EER-regio heeft; de modelpoort weigert elke aanbieder die niet in de EU staat voor cliëntgegevens
Versleuteling in transport	TLS op alle verbindingen; HSTS
Versleuteling in rust	opslag bij de subverwerkers is versleuteld (AES-256); [bevestiging databasevolume: invullijst 6]
Authenticatie	wachtwoordhash (scrypt); sessiecookie alleen via HTTPS, niet door scripts leesbaar, same-site strikt; geen tweestapsverificatie (artikel 16)
Dataminimalisatie vóór het taalmodel	burgerservicenummers, e-mailadressen, telefoonnummers en data worden gemaskeerd vóór aanbidding aan het taalmodel; audio en transcript worden zo kort mogelijk bewaard (Bijlage 3)
Geen oordeel, altijd bron	een verbodsjijst van oordelende termen op elke gegenereerde tekst; een zin zonder bronverwijzing wordt niet getoond; goedkeuring is de enige schrijfactie naar het dossier
Logboek	NEN 7513: elke raadpleging en wijziging van cliëntgegevens, elke generatie en goedkeuring; alleen toevoegen; hash-keten per praktijk; geen inhoud
Toegang door Nara	beheeromgeving zonder cliëntinhoud; inhoud alleen in een door de Praktijk geautoriseerde, tijdgebonden en gelogde ondersteuningssessie
Scheiding oefenomgeving	aparte gegevenslaag; een koppeling met cliëntgegevens laat de bouw falen; geautomatiseerd gecontroleerd bij elke wijziging
Wijzigingsbeheer	elke wijziging gaat door geautomatiseerde typecontrole, grenscontroles en testen vóór uitrol; uitrol naar productie uitsluitend na een geslaagde controle op exact die versie; de draaiende versie is op elk moment opvraagbaar
Kwetsbaarhedenbeheer	wekelijkse geautomatiseerde scans op code, geheimen en de draaiende applicatie; afhankelijkheden worden bewaakt
Incidentbeheer	procedure met triage binnen 2 uur, melding aan de Praktijk binnen 24 uur, intern incidentregister
Wissen	Art. 17 in één handeling, idempotent, inclusief opslag bij subverwerkers (audio, documenten)