Verwerkersovereenkomst

Versie 2026-11, geldig vanaf 4 november 2026.

Partijen

De verwerkingsverantwoordelijke: de praktijk die zich inschrijft in Horalena, met de gegevens die ze bij de inschrijving en in Instellingen opgeeft, hierna "de Praktijk". De persoon die de overeenkomst aanvaardt, verklaart bevoegd te zijn om de Praktijk te binden. Is de Praktijk een groepspraktijk, een kring of een ziekenhuisdienst, dan aanvaardt die persoon voor die groep en haar leden.

De verwerker: Nena Consult BV, ondernemingsnummer 1010.714.363, Parkwijk 31, 9810 Nazareth-De Pinte, RPR Gent, afdeling Gent, uitbater van Horalena, hierna "Nena Consult".

Artikel 1. Voorwerp en rollen

1.1 Nena Consult levert de Praktijk de software Horalena als onlinedienst. Daarbij verwerkt Nena Consult persoonsgegevens in opdracht van de Praktijk. De Praktijk is voor die gegevens de verwerkingsverantwoordelijke, Nena Consult de verwerker.

1.2 Deze overeenkomst geldt voor alle persoonsgegevens die de Praktijk, haar gebruikers, haar patiënten en de leden van haar wachtrollen in Horalena invoeren of laten verwerken, zoals beschreven in Bijlage A.

1.3 Voor een beperkte reeks gegevens is Nena Consult zelf verwerkingsverantwoordelijke: de gegevens van het account en de contactpersonen van de Praktijk voor de inschrijving, de facturatie en de communicatie over de dienst, de feedback die een gebruiker geeft, de bezoeken aan de productsite en de gegevens van de publieke demo. Die verwerkingen vallen buiten deze overeenkomst en staan in de privacyverklaring van Nena Consult.

Artikel 2. Instructies van de Praktijk

2.1 Nena Consult verwerkt de gegevens enkel op schriftelijke instructie van de Praktijk. Die instructies zijn: deze overeenkomst, de gebruiksvoorwaarden, en wat de gebruikers van de Praktijk in Horalena instellen of doen.

2.2 Is Nena Consult wettelijk verplicht om gegevens toch te verwerken of mee te delen, dan meldt ze dat vooraf aan de Praktijk, tenzij de wet die melding verbiedt.

2.3 Vindt Nena Consult dat een instructie de AVG of een andere regel over gegevensbescherming schendt, dan meldt ze dat meteen aan de Praktijk.

2.4 Nena Consult gebruikt de gegevens niet voor eigen doeleinden, verkoopt ze niet, en geeft ze niet door aan de zorggidsen die zij uitbaat. Ze mag er wel tellingen zonder patiëntgegevens uit maken (aantallen per praktijk), enkel om de dienst te beheren, te factureren en misbruik te herkennen.

Artikel 3. Vertrouwelijkheid

3.1 Nena Consult laat enkel personen aan de gegevens die dat voor de dienst nodig hebben en die aan een geheimhoudingsplicht gebonden zijn. Ze weet dat de gegevens onder het beroepsgeheim van de zorgverlener kunnen vallen, en behandelt ze daarnaar.

3.2 Vandaag is dat enkel de bestuurder van Nena Consult. Komt er personeel of een andere dienstverlener bij, dan wordt die lijst bijgewerkt en ter beschikking gehouden van de Praktijk en de Gegevensbeschermingsautoriteit.

3.3 De beheerschermen van Nena Consult tonen geen patiëntgegevens. Nena Consult heeft wel technische toegang tot de server, de databank en de sleutels. Die toegang gebruikt ze enkel als dat nodig is om de dienst te laten werken of op verzoek van de Praktijk. Kijkt ze daarbij gegevens van een Praktijk in, dan meldt ze dat achteraf aan de beheerders.

3.4 Nena Consult gebruikt bij de ontwikkeling en het beheer softwarehulpmiddelen, ook AI-assistenten. Die lezen

geen patiëntgegevens: op de server voeren ze enkel technische opdrachten uit, zoals uitrollen, versies nakijken en tellen. Moet iemand echte gegevens inkijken, dan doet de bestuurder dat zelf, zonder die hulpmiddelen.

Artikel 4. Beveiliging

4.1 Nena Consult neemt de technische en organisatorische maatregelen uit Bijlage B.

4.2 Nena Consult mag die maatregelen aanpassen als het beschermingsniveau niet daalt.

4.3 De Praktijk is verantwoordelijk voor wat aan haar kant gebeurt: wie ze toegang geeft en welke rol, het tijdig intrekken van een account, de beveiliging van haar eigen toestellen, en wat ze met een export doet.

4.4 Er is nog geen onafhankelijke beveiligingstest gebeurd en er is geen certificering. Bijlage B zegt wat er wel en niet is, zodat de Praktijk zelf kan beoordelen of dat voor haar volstaat.

Artikel 5. Subverwerkers

5.1 De Praktijk geeft Nena Consult een algemene toestemming om de subverwerkers uit Bijlage C in te schakelen.

5.2 Nena Consult meldt een nieuwe of vervangende subverwerker minstens 30 dagen vooraf per mail aan de beheerders van de Praktijk. De Praktijk kan binnen die termijn gemotiveerd bezwaar maken. Komen partijen er niet uit, dan kan de Praktijk het abonnement beëindigen, met terugbetaling van het deel dat nog niet verstreken is.

5.3 Nena Consult legt elke subverwerker in wezen dezelfde gegevensbeschermingsverplichtingen op als in deze overeenkomst, en blijft tegenover de Praktijk aansprakelijk voor die subverwerker.

Artikel 6. Doorgifte buiten de Europese Economische Ruimte

6.1 De server, de databank en de back-ups staan binnen de Europese Unie. Nena Consult geeft de gegevens niet door buiten de Europese Economische Ruimte, tenzij op instructie van de Praktijk of met de waarborgen van hoofdstuk V AVG.

6.2 Mails van Horalena lopen via Google Workspace. Google is een Amerikaans bedrijf en kan die berichten ook buiten de Europese Economische Ruimte verwerken. Daarvoor geldt de verwerkersregeling van Google, met de waarborgen van hoofdstuk V AVG. Zo'n mail bevat nooit een diagnose of verslag, wel de praktijk, het moment en de zorgverlener (Bijlage C).

Artikel 7. Bijstand bij de rechten van betrokkenen

7.1 Vragen van patiënten beantwoordt de Praktijk zelf. Krijgt Nena Consult zo'n vraag, dan stuurt ze die door zonder er zelf op te antwoorden.

7.2 Horalena geeft de Praktijk hiervoor de volgende middelen: een export per patiënt, een volledige kopie voor de patiënt, een export van alle gegevens van de praktijk, een pagina "wie opende mijn dossier", en aanpassen en doorhalen in het dossier.

7.3 Wat de Praktijk niet zelf kan, zoals een patiënt wissen die geen dossier heeft, doet Nena Consult op schriftelijk verzoek binnen 10 werkdagen. Vraagt een verzoek ongewoon veel werk, dan kan daarvoor een vergoeding gelden, na akkoord vooraf.

Artikel 8. Bijstand bij beveiliging, datalekken en DPIA

8.1 Stelt Nena Consult een inbreuk op de beveiliging van de gegevens vast, dan meldt ze dat zonder onredelijke vertraging en uiterlijk binnen 48 uur per mail aan de beheerders van de Praktijk, met wat op dat moment bekend is: de aard, de betrokken gegevens en personen voor zover gekend, de gevolgen en de genomen maatregelen.

8.2 De Praktijk beslist of ze de Gegevensbeschermingsautoriteit en de betrokkenen verwittigt (artikels 33 en 34 AVG).

8.3 Nena Consult helpt de Praktijk met informatie bij een gegevensbeschermingseffectbeoordeling en een voorafgaande raadpleging van de Gegevensbeschermingsautoriteit, en bij het nakomen van de artikels 32 tot en met 36 AVG, rekening houdend met de informatie waarover ze beschikt.

Artikel 9. Audit

9.1 Nena Consult bezorgt de Praktijk op verzoek de informatie die nodig is om na te gaan of deze overeenkomst nageleefd wordt.

9.2 De Praktijk kan hoogstens één keer per jaar, na een schriftelijke melding van minstens 30 dagen, een audit uitvoeren of laten uitvoeren door een deskundige die ze aanstelt en die aan geheimhouding gebonden is. Een audit raakt nooit de gegevens van een andere praktijk. De kosten zijn voor de Praktijk.

9.3 Is er een aanwijzing van een ernstige tekortkoming of een vraag van een toezichthouder, dan geldt de beperking in de tijd niet.

Artikel 10. Duur en einde

10.1 Deze overeenkomst geldt zolang Nena Consult gegevens verwerkt voor de Praktijk.

10.2 De overeenkomst kan niet beëindigd worden zolang er gegevens van de Praktijk bij Nena Consult staan, tenzij op de manier van artikel 11.

Artikel 11. Gegevens na het einde van de dienst

11.1 Na het einde van het abonnement blijven de gegevens bewaard en kan de Praktijk blijven aanmelden, inkijken en exporteren, zonder kosten, tenzij artikel 11.4 of 11.5 geldt. Nena Consult blijft voor die bewaring verwerker.

11.2 De Praktijk kiest zelf wanneer haar gegevens gewist worden. Op schriftelijk verzoek van een beheerder wist Nena Consult binnen 30 dagen de gegevens van de Praktijk uit de actieve databank. Uit de back-ups verdwijnen ze volgens het bewaarbeleid, dus hoogstens 12 maanden later. Nena Consult bevestigt het wissen schriftelijk. Wat ze wettelijk moet bewaren, zoals facturen aan de Praktijk, blijft staan.

11.3 De Praktijk maakt vóór dat verzoek zelf een volledige export, en regelt de verdere bewaring, overdracht of vernietiging van haar dossiers volgens de regels voor haar beroep. De wettelijke bewaartermijn van het patiëntendossier ligt bij de zorgverlener, niet bij Nena Consult.

11.4 Stopt Nena Consult met Horalena, dan geldt artikel 10.3 van de gebruiksvoorwaarden: minstens 12 maanden vooraf een bericht, zodat de Praktijk haar gegevens kan meenemen. Daarna wist Nena Consult de gegevens.

11.5 Beëindigt Nena Consult de overeenkomst met een Praktijk (artikel 10.1 of 10.2 van de gebruiksvoorwaarden), dan kan de Praktijk nog minstens 90 dagen na het einde aanmelden, inkijken en exporteren. Nena Consult wist de gegevens pas daarna, en pas nadat ze de beheerders minstens twee keer per mail verwittigde, de laatste keer minstens 30 dagen vooraf.

Artikel 12. Aansprakelijkheid

12.1 Elke partij is aansprakelijk zoals artikel 82 AVG bepaalt. De beperkingen uit de gebruiksvoorwaarden gelden ook voor deze overeenkomst, behalve tegenover betrokkenen en voor zover de wet dat niet toelaat.

Artikel 13. Wijzigingen

13.1 Nena Consult kan deze overeenkomst om een geldige reden wijzigen met een nieuwe versie. Ze meldt een nieuwe versie minstens 30 dagen vooraf aan de beheerders, tenzij de wet of een dringende beveiligingsreden een kortere termijn oplegt. Een nieuwe versie verlaagt het beschermingsniveau niet. De beheerder aanvaardt ze in Horalena. Elke aanvaarding wordt bewaard met versie, datum en gebruiker. Is de Praktijk niet akkoord, dan geldt

artikel 18.2 van de gebruiksvoorwaarden.

Artikel 14. Toepasselijk recht

14.1 Op deze overeenkomst is het Belgisch recht van toepassing. Geschillen behoren tot de bevoegdheid van de ondernemingsrechtbank Gent, afdeling Gent.

Bijlage A. Beschrijving van de verwerking

Doel. Het leveren van praktijksoftware aan zorgverleners: agenda, online boeken, wachtlijst, herinneringen, patiëntenbestand, dossier, RIZIV-administratie, rekeningen en betalingen, praktijksite, patiëntenportaal, oproepen en wachtrol, voor zover in de formule van de Praktijk.

Aard. Bewaren, ordenen, raadplegen, tonen, aanpassen, versturen van berichten in opdracht, exporteren.

Duur. Zolang de overeenkomst loopt, en daarna volgens artikel 11 en Bijlage D.

Betrokkenen. Patiënten, hun ouders, vertegenwoordigers en contactpersonen; betalers van een rekening; bezoekers die een bericht sturen of boeken via de site van de Praktijk; gebruikers van de Praktijk (zorgverleners, onthaal, beheerders); leden van een wachtrol, ook van buiten de Praktijk; voorschrijvers en andere zorgverleners die in een dossier genoemd worden; stagiairs. De Praktijk kan haar boekhouder een link geven naar een map met ontvangsten.

Soort gegevens	Voorbeelden	Bijzondere categorie?
Identificatie en contact	naam, geboortedatum, geslacht, adres, e-mailadres, telefoon, taal, contactpersoon	nee, maar in deze context vaak onthullend
Rijksregisternummer	INSZ, en velden van de eID (kaartnummer, geldigheid, nationaliteit), nooit de foto	apart wettelijk kader
Afspraken	moment, zorgverlener, soort, reden van het bezoek als de Praktijk die vraagt, aanwezigheid, wachtlijst	gezondheid (afleidbaar)
Dossier	notities, verslagen, bilans, bijlagen, vragenlijsten, toestemmingen, oefenprogramma's, tandschema, Katz-evaluaties, wonden, zwangerschap, medicatie, labo, vaccinaties, wilsverklaringen	gezondheid
Administratie	voorschriften, diagnose op een voorschrift, RIZIV-verstrekkingen, getuigschriften, akkoorden, ziekenfonds, statuut	gezondheid
Financieel	rekeningen, betalingen, betaalverzoeken, bankbewegingen (naam, rekeningnummer, mededeling)	deels afleidbaar
Berichten	portaalberichten, contactformulier, inhoud van mails en sms'en	kan gezondheid bevatten
Gebruikers	naam, e-mail, rol, RIZIV-nummer, tweestapgegevens, eHealth-certificaat en het INSZ daarin	nee
Wachtrol	naam, contact, beurten, verhinderingen, gewerkte uren	nee
Technisch	IP-adres als gesleutelde code in het auditlog, tijdelijke bezoekerscode voor statistieken, webserverlogs (IP-adres, tijdstip, pagina, browser)	nee

Bijlage B. Technische en organisatorische maatregelen

Scheiding tussen praktijken

Alle praktijken staan in één databank, logisch gescheiden: praktijkgebonden gegevens krijgen automatisch een filter op de praktijk, en zonder praktijkcontext geeft een vraag niets terug.

Toegang

- Tweestapsverificatie is verplicht voor elke gebruiker van de Praktijk.
- Wachtwoorden van minstens 12 tekens met hoofdletters, kleine letters en cijfers, bewaard als bcrypt-hash, met een controle op gelekte wachtwoorden.
- Hoogstens 5 aanmeldpogingen per minuut per adres en IP, en 30 per IP. Versleutelde sessies, cookie enkel over https, einde na 240 minuten. Er is geen functie om aangemeld te blijven.
- Rollen: enkel een zorgverlener opent het dossier, nooit het onthaal. Instellingen enkel de beheerder.
- Patiënten hebben geen wachtwoord: ze krijgen een link per mail waarvan enkel de hash bewaard wordt, 30 minuten geldig, of 7 dagen in een mail die meldt dat er iets klaarstaat. De sessie stopt na 30 minuten stilte en duurt hoogstens 12 uur. Wie hetzelfde e-mailadres heeft bij een praktijk, valt onder dezelfde aanmelding (bedoeld voor een gezin).
- Leden van een wachtrol hebben geen account maar een persoonlijke link.
- Het beheerscherm van Nena Consult vraagt tweestap en toont tellingen en geen patiëntgegevens. Wat Nena Consult daar wijzigt, staat in het auditlog. Toegang tot de server kan enkel met een SSH-sleutel, en staat niet in het auditlog van de app.

Versleuteling

- Onderweg: https met HSTS.
- In de databank, per veld, met AES-256: onder meer titel en inhoud van het dossier, rijksregisternummer, inhoud van berichten, contactformulier, taken, dagnotities, inhoud van rekeningen, naam en rekening uit bankafschriften.
- Niet versleuteld per veld, wel beveiligd door de toegang tot de databank: naam, geboortedatum, geslacht, e-mail, telefoon en adres van de patiënt, de reden van het bezoek, ontvanger en onderwerp van een bericht, moment en zorgverlener van een afspraak.
- Dossierbijlagen staan versleuteld op schijf, buiten de webroot. Het eHealth-certificaat staat versleuteld met een eigen sleutel per praktijk.
- De sleutel van de app staat op dezelfde server als de databank. De versleuteling per veld beschermt dus tegen wie enkel de databank of een kopie daarvan heeft, niet tegen wie de hele server of de beheerder heeft.

Auditlog

Via de app kan een regel niet gewijzigd of gewist worden. Het openen van een fiche, een dossier of een bijlage wordt gelogd, het IP-adres enkel als gesleutelde code. De patiënt ziet in het portaal wie zijn dossier opende, met naam en functie: de laatste 200 regels, zonder de regels over afspraken, reeksen, wachtlijst en herinneringen. Een agenda of patiëntenlijst openen wordt niet per patiënt gelogd.

Back-up en herstel

- Elke nacht een versleutelde back-up van de databank en de privébestanden (AES-256-GCM, een eigen sleutel per archief). Elke zondag wordt de nieuwste volledig ontsleuteld en nagerekend.
- Bewaarbeleid: de nieuwste van elk van de laatste 14 dagen, 8 weken en 12 maanden.
- De archieven staan op dezelfde server. Nena Consult haalt er geregeld een versleutelde kopie van af naar een eigen toestel. Herstellen op een lege installatie is geoefend. Herstellen op een echte nieuwe server is nog niet geoefend, dus de duur van een echte uitval is niet gemeten.

Bewaking en webbeveiliging

Elk uur een controle van planner, back-up, schijfruimte, wachtrij en databank, met een mail aan Nena Consult bij een probleem. Een Content-Security-Policy met enkel eigen bronnen, en aangemelde pagina's komen niet in de

cache van de browser. Een eID-foto wordt nooit bewaard.

Berichten

Mails en sms'en gaan via een eigen wachtrij; de inhoud staat versleuteld en wordt na 30 dagen gewist. Een sms bevat de praktijk, het moment en een korte link, nooit de reden of het beroep. Een afspraakmail bevat de praktijk, het moment, de zorgverlener, de plaats en de informatie die de Praktijk toevoegde, geen diagnose of verslag. Een oproep bevat de tekst die de Praktijk schreef.

Wat er (nog) niet is

Dit staat hier zodat niemand het leest als een belofte.

- Een onafhankelijke beveiligingstest. Wel een interne ronde op 2 en 3 november 2026, waarvan de ernstige fouten opgelost zijn. Dat is geen onafhankelijke test.
- Een certificering, zoals ISO 27001.
- Een sleutelkluis (KMS).
- Een tweede datacenter voor de back-ups.
- Een logboek van toegang op de server door de beheerder dat de Praktijk kan inkijken. Daarvoor geldt artikel 3.3.
- Een functionaris voor gegevensbescherming: er is er geen aangeduid. Vragen gaan naar team@horalena.be.

Bijlage C. Subverwerkers

Partij	Wat ze doet	Welke gegevens	Waar
Combell NV, Skaldenstraat 121, 9042 Gent (Managed VPS)	hosting van de server, de databank, de bestanden en de back-ups	alles wat in Horalena staat, versleuteld of niet	Europese Unie. De IP-adressen staan op naam van TransIP B.V. (Leiden, Nederland). Het exacte datacenter vult Nena Consult hier aan zodra de hoster het bevestigt.
Google Workspace	verzendt de mails van de app	ontvanger, onderwerp met de naam van de praktijk, inhoud van de mail (moment, zorgverlener, plaats, links, de tekst van een oproep)	Google is een Amerikaans bedrijf; zie artikel 6.2
Brevo (Sendinblue SAS, Parijs)	verzendt sms'en, enkel voor wie de sms-dienst van Horalena gebruikt	telefoonnummer en inhoud van de sms	Frankrijk

Gebruikt een Praktijk haar eigen Brevo-account, dan is Brevo haar eigen verwerker en geeft Horalena de opdracht enkel door. Cloudflare beheert enkel de DNS van horalena.be, zonder proxy: het verkeer loopt er niet door, en het is dus geen subverwerker. eHealth, MyCareNet en Recip-e krijgen vandaag niets (simulator); later zijn ze ontvangers op instructie van de zorgverlener, geen subverwerkers.

Bijlage D. Bewaartermijnen

Gegeven	Termijn	Wat er gebeurt
Patiëntendossier, ook versies en doorgehaalde items	geen automatische termijn; de bewaarplicht van 30 tot 50 jaar ligt bij de zorgverlener	nooit vanzelf gewist; zie artikel 11
Patiëntfiche, afspraken, verstrekkingen, getuigschriften, rekeningen en betalingen, auditlog	geen automatische termijn	blijven staan tot de Praktijk laat wissen (artikel 11)

Gegeven	Termijn	Wat er gebeurt
Inhoud van mails en sms'en	30 dagen	inhoud gewist; ontvanger, onderwerp, soort en tijdstip blijven
Bericht via het contactformulier van de site	12 maanden	gewist
Opgestuurd importbestand, bankafschrift	24 uur	bestand gewist; wat ingelezen werd, blijft
Export van een hele praktijk	72 uur, of vroeger met "Nu wissen"	bestand en sleutel gewist
Aanmeldlink van het portaal	30 dagen na het verlopen	gewist
MyCareNet en Recip-e: verzoek en antwoord	90 dagen	inhoud gewist; samenvatting en referentie blijven
Online patiënt die nooit bevestigde	30 dagen	identiteit geanonimiseerd
Wachtlijst	2 dagen zonder bevestiging, anders 90 dagen	vervalt; de rij blijft tot de Praktijk laat wissen
Bezoekersstatistieken van de site	ruwe metingen hoogstens 3 dagen, dagtellers 24 maanden	gewist
Webserverlogs	hoogstens 90 dagen	gewist
Logboek van de app	14 dagen	gewist
Back-ups	14 dagen, 8 weken, 12 maanden	wat in de databank gewist is, staat er hoogstens 12 maanden later ook daar niet meer in