



# Aansluiting op gezamenlijke dienst door zorgaanbieders t.b.v. pseudonimisering van persoonsgegevens binnen de Wkz

Versie 1.0, 29 april 2026

Zorgaanbieders lezen in dit document welke gezamenlijke pseudonimiseringsdienst beschikbaar is en hoe zij hier gebruik van kunnen maken.

## Achtergrond en uitgangspunten

De Wet kwaliteitsregistraties zorg (Wkz) verplicht zorgaanbieders om de persoonsgegevens die zij aanleveren aan kwaliteitsregistraties voorafgaand aan de verstrekking te pseudonimiseren. De Data-governancecommissie (DGC) heeft besloten om het veld te ondersteunen door het faciliteren van een gezamenlijke pseudonimiseringsdienst waar zorgaanbieders en registratiehouders gebruik van kunnen maken. De kern van deze dienst is dat er gebruik wordt gemaakt van één Trusted Third Party (TTP) die volgens een uniforme methode de pseudonimisatie voor zorgaanbieders uitvoert.

Centrale regie op de uitgifte van pseudonimiserings sleutels is zo goed als onvermijdelijk omdat:

1. Patiënten gevolgd moeten kunnen worden over meerdere zorgaanbieders heen.
2. Gegevens uit externe bronnen gekoppeld moeten kunnen worden.

Een gezamenlijke, centrale dienst garandeert consistente, unieke pseudoniemen die koppeling mogelijk maken zonder dat herleidbaarheid naar de persoon ontstaat.

## Uitvoerder van de pseudonimiseringsdienst

De DGC heeft [ZorgTTP](#) de opdracht gegeven voor het uitvoeren van de gezamenlijke pseudonimiseringsdienst. ZorgTTP is een bekende pseudonimiseringsdienstverlener binnen de zorg. ZorgTTP voldoet als organisatie én met het gehanteerde pseudonimiseringsproces als enige TTP aan het programma van eisen dat in opdracht van de DGC is opgesteld en met relevante veldpartijen is afgestemd. Wilt u dit onderzoek raadplegen dan kunt u contact opnemen met de servicedesk van het SSC-DG via [info@ssc-dg.nl](mailto:info@ssc-dg.nl). De DGC houdt toezicht op de dienstverlening van ZorgTTP.

Zorgaanbieders en registratiehouders kunnen kosteloos gebruikmaken van de gezamenlijke pseudonimiseringsdienst. In het document *Inrichting en financiering pseudonimisering van persoonsgegevens binnen de Wkz* leest u in meer detail waarom gekozen is voor een gezamenlijke, centrale dienst en wat onder de financiering valt (in relatie tot de inrichting bij zorgaanbieders). U vindt het document op [deze pagina](#), onder het kopje *Documentatie*. De notitie die nu voor u ligt heeft een meer praktisch karakter: we leggen uit hoe u kunt aansluiten op de TTP en hoe de dienst werkt.

## Geen verplichting, maar in de praktijk nauwelijks een alternatief

Er is geen wettelijke verplichting om gebruik te maken van de gezamenlijke dienst. Zorgaanbieders zijn in beginsel vrij in de keuze van hun pseudonimiseringsoplossing. In de praktijk is er echter nauwelijks een werkbaar alternatief, om de volgende redenen:

- **Juridisch:** Artikel 4 lid 5 AVG vereist dat de sleutel, waarmee re-identificatie mogelijk is, apart wordt bewaard van de gepseudonimiseerde data. Intern sleutelbeheer biedt daarmee nauwelijks juridische meerwaarde ten opzichte van onversleutelde verwerking.
- **Technisch:** Koppelbare pseudoniemen vereisen dat alle zorgaanbieders exact dezelfde methode, invoernormalisatie, sleutels en hetzelfde algoritme hanteren. Experts raden unaniem het gebruik van meerdere TTP's af vanwege de technische en organisatorische complexiteit.
- **Financieel:** De gezamenlijke dienst wordt gefinancierd via Zorgverzekeraars Nederland (ZN) en is voor deelnemende instellingen kosteloos voor alle verwerkingen die onder de Wkz vallen. Een eigen oplossing brengt substantieel hogere inrichtings-, beheer- en auditkosten met zich mee.
- **Uitzondering:** De gezamenlijke dienst is niet van toepassing wanneer een registratiehouder géén koppelingen met externe bronnen aangaat én er geen sprake is van longitudinale opvolging over een keten van zorgaanbieders. In alle overige situaties is aansluiting noodzakelijk.

Op basis van bovenstaande redenen wordt aansluiting op de gezamenlijke pseudonimiseringsdienst sterk aangeraden door de NVZ en UMCNL.

## Aansluiten bij ZorgTTP

### Voor wie is een gezamenlijke pseudonimiseringsdienst van toepassing?

In principe is de gezamenlijke pseudonimiseringsdienst van toepassing op alle zorgaanbieders en registratiehouders. De enige uitzondering geldt voor registratiehouders die geen koppelingen met externe bronnen aangaan én waarbij geen sprake is van longitudinale opvolging van patiënten over een keten van zorgaanbieders, evenals voor zorgaanbieders die uitsluitend gegevens leveren aan een kwaliteitsregistratie zonder dergelijke koppelingen en opvolging. In dit geval hoeven er geen direct herleidbare persoonsgegevens te worden verstuurd en is gebruik van de gezamenlijke pseudonimiseringsdienst niet nodig. De meeste zorgaanbieders zullen echter gegevens leveren aan een registratiehouder die wil koppelen met een externe bron of patiënten wil volgen over meerdere zorgaanbieders heen. Aansluiting op de gezamenlijke pseudonimiseringsdienst is in dit geval sterk aan te raden om te kunnen voldoen aan de eisen van de wet.

Een overzicht van kwaliteitsregistraties die gereed zijn om gepseudonimiseerde data conform de gezamenlijke dienst te ontvangen vindt u op [deze pagina](#) in het document *Overzicht kwaliteitsregistraties voor zorgaanbieders* onder het kopje *Handige documentatie en bronnen*. NB: De betreffende kolom in dit overzicht wordt actief zodra de eerste registratie is aangesloten op de dienst.

Twijfelt u of de gezamenlijke pseudonimiseringsdienst van toepassing is op uw organisatie? Neem dan contact op met de servicedesk van het SSC-DG via [info@ssc-dg.nl](mailto:info@ssc-dg.nl).

## Aanmelden bij ZorgTTP en starten met de implementatie

Zorgaanbieders kunnen zich vanaf 1 mei 2026 aanmelden bij ZorgTTP. Na aanmelding ontvangt u de starterskit met aanmeldformulier, technische documentatie voor beide technieken en de standaardovereenkomsten die nodig zijn voor aansluiting.

Op hoofdlijnen doorloopt u de volgende stappen:

1. **Neem contact op** via [advies@zorgttp.nl](mailto:advies@zorgttp.nl).
2. **Ontvang de starterskit** met aanmeldformulier, technische documentatie voor beide technieken en standaardovereenkomsten.
3. **Stel intern een projectgroep samen en maak een keuze voor de te gebruiken techniek(en)**. Zie de paragrafen hieronder voor meer informatie.
4. **Doorloop het implementatietraject** met ondersteuning van ZorgTTP. Implementatieondersteuning is inbegrepen in de dienstverlening voor alle instellingen.
5. **Sluit de benodigde overeenkomsten af** en start met het pseudonimiseren van uw eerste aanlevering.

## Wanneer starten?

Nu de gezamenlijke pseudonimiseringsdienst actief is, adviseren wij om direct in actie te komen. De gewijzigde Wkkgz is per 1 januari 2026 in werking getreden en de eerste kwaliteitsregistraties zijn inmiddels opgenomen in het [Register voor Kwaliteitsregistraties](#) van Zorginstituut Nederland. Voor deze kwaliteitsregistraties geldt een aanleververplichting. Het Register wordt doorlopend bijgewerkt zodra er nieuwe besluiten zijn genomen; naar verwachting wordt over het merendeel van de kwaliteitsregistraties in de periode maart-juni een besluit genomen door het Zorginstituut. Zorgaanbieders die niet tijdig zijn aangesloten op de gezamenlijke pseudonimiseringsdienst, lopen het risico niet te voldoen aan de technische vereisten voor gegevensaanlevering. Dit kan gevolgen hebben voor de continuïteit van hun deelname aan de betreffende kwaliteitsregistraties.

## Samenstelling projectgroep

Het aansluittraject raakt meerdere disciplines binnen de instelling. Wij adviseren een multidisciplinaire projectgroep samen te stellen met in ieder geval de volgende expertise:

- **Manager kwaliteit** — overzicht op registratieverplichtingen en aanleverprocessen.
- **Functionaris Gegevensbescherming (FG) en/of Privacy Officer** — beoordeling van verwerkingsovereenkomsten en AVG-conformiteit.
- **ICT-technicus / informatiearchitect** — keuze en implementatie van de techniek, epd-koppeling en data-extractie.
- **Jurist** — beoordeling van de standaardovereenkomsten van ZorgTTP en afstemming met eventuele dataverwerkers.
- **Data-analist / BI-medewerker** — inrichten van extractie- en voorverwerkingsprocessen (ETL).

Alle deelnemende instellingen kunnen gebruikmaken van de implementatieondersteuning van ZorgTTP. Deze ondersteuning is inbegrepen in de dienstverlening en geldt ook voor ZBC's en kleinere instellingen.

## Pseudonimiseren via de technieken van ZorgTTP

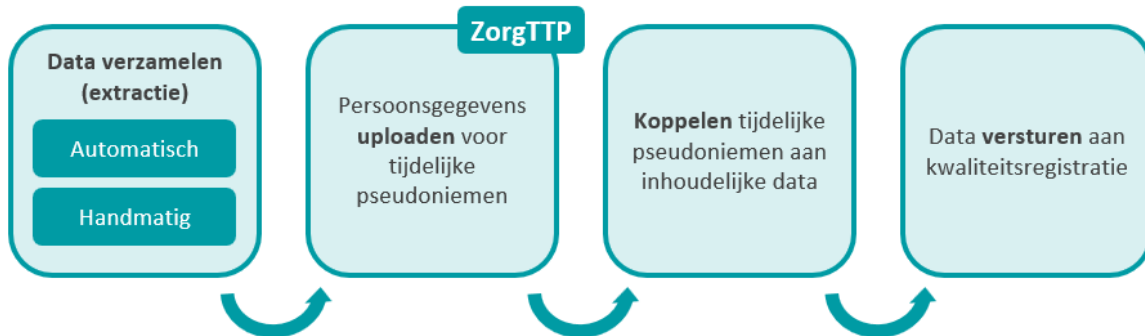
ZorgTTP stelt twee technieken beschikbaar voor het pseudonimiseren van persoonsgegevens binnen de eisen van de Wkz. Beide leveren identieke pseudoniemen op en zijn volledig koppelbaar over zorgaanbieders heen. Ze kunnen naast elkaar worden ingezet binnen dezelfde instelling.

1. Een **webgebaseerde techniek**, waarbij de zorgaanbieder tijdelijke pseudoniemen bij ZorgTTP ophaalt alvorens de gegevensset inclusief tijdelijke pseudoniemen naar de registratiehouder te sturen. De registratiehouder haalt de definitieve pseudoniemen vervolgens op via de webgebaseerde techniek van ZorgTTP. De stap van tijdelijke naar definitieve pseudoniemen is noodzakelijk zodat geen enkele partij over zowel de ongepseudonimiseerde als de gepseudonimiseerde gegevens beschikt.
2. Een **lokale techniek (lokale cliënt)**, waarbij de zorgaanbieder de gegevensset via de Privacy Verzend Module (PVM) naar ZorgTTP verzendt. ZorgTTP stelt de gegevensset na pseudonisatie beschikbaar aan de betreffende registratiehouder om te downloaden.

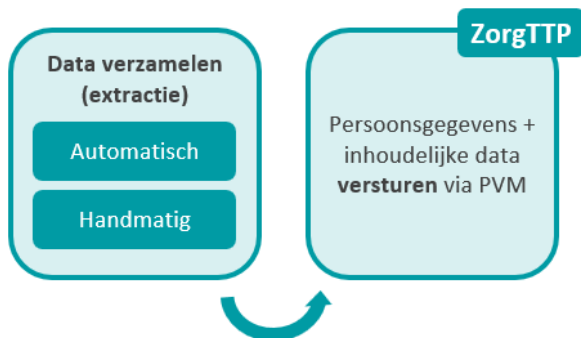
Kenmerk	Webgebaseerde techniek	Lokale techniek (PVM)
<b>Werkwijze</b>	Zorgaanbieder haalt tijdelijke pseudoniemen op via webportaal of API. Dataset met tijdelijke pseudoniemen gaat naar registratiehouder. Registratiehouder haalt definitieve pseudoniemen op bij ZorgTTP.	Zorgaanbieder verzendt dataset via de Privacy Verzend Module (PVM) naar ZorgTTP. ZorgTTP stelt de gepseudonimiseerde dataset beschikbaar aan de registratiehouder.
<b>Technische vereisten</b>	Internetverbinding; toegang tot ZorgTTP-webportaal of API-integratie in het epd/extractieproces.	Installatie van PVM-softwareclient op lokale infrastructuur van de zorgaanbieder.
<b>Meest geschikt voor</b>	Hoge mate van procesautomatisering; directe koppeling vanuit epd of BI-omgeving; FHIR-aanlevering.	Batchverwerking zonder API-koppeling; omgevingen met strikte firewallrestricties op uitgaand verkeer.
<b>Combineerbaar</b>	Ja — beide technieken kunnen naast elkaar worden ingezet binnen dezelfde instelling.	
<b>Pseudoniemen</b>	Identiek aan lokale techniek. Volledige koppelbaarheid over zorgaanbieders heen gewaarborgd.	Identiek aan webgebaseerde techniek. Volledige koppelbaarheid over zorgaanbieders heen gewaarborgd.

Zorgaanbieders kunnen kiezen om één of beide technieken in gebruik te nemen binnen de instelling. In Figuur 1 staat een schematische weergave van de verschillende stappen die zorgaanbieders bij beide technieken moeten uitvoeren. In de starterskit van ZorgTTP vinden zorgaanbieders meer informatie over de verschillende technieken. Meld u aan via [advies@zorgtpp.nl](mailto:advies@zorgtpp.nl) en ontvang de starterskit, met daarin een aanmeldformulier, technische documentatie voor beide technieken en verschillende overeenkomsten die benodigd zijn voor het aansluiten op de gezamenlijke pseudonimiseringsdienst.

### Stappen bij webservice gezamenlijke pseudonimiseringsdienst



### Stappen bij lokale client gezamenlijke pseudonimiseringsdienst



Figuur 1. Schematische weergave van de stappen per techniek van ZorgTTP die een zorgaanbieder neemt om data gepseudonimiseerd aan te leveren.

## Data-extractie: waar zit pseudonimisering in het proces?

Pseudonimisering vindt altijd plaats nadat de gegevens zijn verzameld en vóórdat ze worden verstuurd naar de registratiehouder. De keuze van extractiemethode staat los van de pseudonimiseringstechniek, maar heeft wel invloed op de praktische inrichting. Er zijn verschillende extractiemethoden om gegevens uit het epd van de zorgaanbieder te verkrijgen.

### Automatische extractie (voorkeur)

Het uitgangspunt voor gegevensverwerking is **éénmalig vastleggen, meervoudig gebruik**. Automatische extractie verdient daarom de voorkeur. Handmatige extractie heeft als nadelen dat het extra administratieve lasten met zich meebrengt, er een verhoogd risico op fouten bestaat en dat er discrepanties kunnen ontstaan tussen de brondata en de registratiedata.

- **Script via BI-/ETL-afdeling:** Een data-analist (BI-afdeling, ETL) schrijft een script voor de benodigde extractie dat op het gewenste moment gedraaid kan worden. Deze methode levert een batchbestand op.
- **Aanlevermodule van de epd-leverancier:** Een extractie wordt verkregen via een module in het epd. In dit geval spreken we van een uitbestede dienst.
- **FHIR-aanlevering:** Gestructureerde gegevensuitwisseling via het HL7 FHIR-protocol.

## Handmatige extractie (mogelijk, maar minder gewenst)

Hoewel handmatige extractie niet de voorkeur heeft blijft deze vorm van data verzamelen wel mogelijk.

- **Formulier of survey:** Een zorgmedewerker vult per geval een formulier of survey in. In een aantal gevallen worden deze surveys aangeboden door een dataverwerker die de invoer verwerkt tot een batchbestand. In dat geval spreken we van een uitbestede dienst.
- **Handmatig verzamelbestand:** Een zorgmedewerker typt de benodigde gegevens over in een verzamelbestand (bijvoorbeeld Excel). Dit levert een batchbestand op.

## Uitbestede dienst

Als een van deze extractiemethoden een *uitbestede dienst* is werkt de zorgaanbieder met een dataverwerker. Hiervoor dienen de juiste overeenkomsten afgesloten te zijn, waarbij ook is vastgelegd hoe de gegevens via de centrale pseudonimiseringsdienst bij de kwaliteitsregistratie aankomen. De zorgaanbieder kiest de gewenste methode van extractie. Extractiemethoden zijn onderdeel van het bestaande proces rondom de kwaliteitsregistraties en vallen daarom niet onder de financiering voor pseudonimiseren (zie het document *Inrichting en financiering pseudonimisering van persoonsgegevens binnen de Wkz* op [deze pagina](#)).

**Let op!** Als de dataverwerker van de zorgaanbieder dezelfde organisatie is als de dataverwerker van de kwaliteitsregistratie, is het mogelijk dat één partij zowel de persoonsgegevens als de definitieve pseudoniemen in handen krijgt. Dit is uitsluitend toegestaan wanneer een strikte organisatorische scheiding (Chinese muur) is aangebracht en persoonsgegevens zo snel mogelijk worden verwijderd.

## Contact en extra informatie

Op de website van het SSC-DG is alle informatie over de gezamenlijke pseudonimiseringsdienst gebundeld op [deze pagina](#); hier vindt u onder andere een FAQ waarin specifieke situaties rondom de gezamenlijke pseudonimiseringsdienst zijn uitgewerkt en informatie over informatiebijeentkomsten. Deze webpagina wordt regelmatig bijgewerkt.

Voor nadere informatie kunt u, afhankelijk van uw vraag, contact opnemen met ZorgTTP of het SSC-DG.

<b>ZorgTTP</b> Aanmelding, aansluiting en implementatieondersteuning  <a href="mailto:advies@zorgttp.nl">advies@zorgttp.nl</a>   <a href="http://www.zorgttp.nl">www.zorgttp.nl</a>	<b>SSC-DG (namens de DGC)</b> Programma van Eisen en governance  <a href="mailto:info@ssc-dg.nl">info@ssc-dg.nl</a>   <a href="#">Informatiepagina pseudonimisering</a>
--	--

Wij wensen u veel succes met de aansluiting.