de Nederlandse ggz

Handreiking gegevensuitwisseling met samenwerkingspartners buiten de zorg

dirkzwager legal & tax

Samen zijn we de Nederlandse ggz.

Colofon

Auteurs: de eerste versie van deze Handreiking is in opdracht van de Nederlandse ggz opgesteld door mr. dr. L.A.P Arends, mr. M.J. Roetert Steenbruggen-Hulshof, mr. M.M.A. Janssen en mr. R.H. Burm (Dirkzwager N.V.) samen met de juridisch adviseurs van de Nederlandse ggz.

Overname van teksten uit deze publicatie is toegestaan onder vermelding van de volledige bronvermelding: de Nederlandse ggz, ‘Handreiking gegevensuitwisseling met samenwerkingspartners buiten de zorg’, de Nederlandse ggz 2025.

Inhoudsopgave

Deel I: Inleiding 5

1.1 Waarom deze Handreiking 5

1.2 Voor wie is deze Handreiking bedoeld? 5

1.3 Leeswijzer 6

Deel II: Algemeen deel 6

2.1 Inleiding 6

2.1.1 AVG en UAVG 6

2.1.2 Beroepsgeheim 6

2.2 (U)AVG: algemeen kader voor de verwerking van persoonsgegevens 6

2.2.1 Toepassingsbereik (U)AVG 7

2.2.2 De (gezamenlijke) verwerkingsverantwoordelijke en de verwerker 7

2.2.3 Gewone persoonsgegevens en bijzondere typen persoonsgegevens 8

2.2.4 Beginselen 9

2.2.5 (Verwerkings-)grondslagen (U)AVG en uitzonderingen op het verwerkingsverbod voor bijzondere persoonsgegevens 10

2.3 Het beroepsgeheim 13

2.3.1 Algemeen: achtergrond en doelen 13

2.3.2 Reikwijdte 13

2.3.3 Doorbrekingsgronden voor het doorbreken van het beroepsgeheim 13

2.4 Wet aanvullende bepalingen verwerking persoonsgegevens in de zorg 15

2.4.1 Elektronische gegevensuitwisseling 15

2.5 Stappenplan voor een zorgvuldige uitwisseling van persoonsgegevens 15

2.5.1 Checklist anonimiseren 16

2.5.2 Schriftelijke afspraken 16

Deel III: Gegevensuitwisseling met samenwerkingspartners 17

3.1 Inleiding 17

3.2 Aandachtspunten bij specifieke samenwerkingsverbanden en -partners 17

3.2.1 Samenwerkingsverbanden in het sociaal, zorg- en veiligheidsdomein 17

3.2.2 Samenwerking in het kader van bemoeizorg 17

3.2.3 Samenwerking met de gemeente 18

3.2.4 Het verstrekken van informatie aan woningcorporaties 19

Deel IV: Toestemmingsformulier 20

Afkortingenlijst 22

Handreiking gegevensuitwisseling met samenwerkingspartners buiten de zorg

Deel I: Inleiding

1.1 Waarom deze Handreiking?

Steeds vaker wordt er door ggz-aanbieders en partners buiten de zorg samengewerkt. Ggz-aanbieders werken bijvoorbeeld veel samen met partners in het veiligheidsdomein (politie, justitie), het sociaal domein (denk aan gemeenten[1], woningbouwcoöperaties) en andere maatschappelijke organisaties. Deze samenwerking is noodzakelijk om maatschappelijke problemen aan te pakken en gezamenlijk te komen tot oplossingen die in het belang zijn van de cliënt[2] en de omgeving. Vaak gaat het hierbij om complexe, meervoudige problematiek, die geregeld op meerdere leefgebieden speelt. Het uitwisselen van gegevens kan hierbij noodzakelijk zijn.

Misverstand 1: de privacyregels en het beroepsgeheim zijn een obstakel

De wetgeving biedt niet altijd een (duidelijk) antwoord op de vraag of gegevens uitgewisseld mogen worden. Hierdoor is het toepassen van de wettelijke regels in de praktijk soms lastig. In samenwerkingen worden de privacyregels (waaronder de regels omtrent het beroepsgeheim) soms als een 'probleem' gezien. "Het mag niet van de privacywet" of "wij zijn gebonden aan het beroepsgeheim", wordt er dan gezegd. Ggz-aanbieders krijgen daarbij regelmatig van andere samenwerkingspartners te horen "jullie willen geen informatie verstrekken". Soms heeft het niet delen van informatie helemaal niets te maken met het 'niet willen', maar met handelingsverlegenheid: partijen weten niet precies wat er op grond van de privacywetgeving wél mag. Ook kan er een andere reden zijn om juist geen informatie te verstrekken, zoals ter bescherming van de belangen van de cliënt of een derde.

Deze handreiking biedt ggz-aanbieders handvatten om te kunnen beoordelen in hoeverre zij gegevens over cliënten mogen delen met samenwerkingspartners. Hoewel alle samenwerkingspartners – en dus ook ggz-aanbieders – inzien dat het delen van gegevens noodzakelijk kan zijn om te komen tot oplossingen, moet daarbij wel worden voldaan aan (vaak complexe) wet- en regelgeving. Deze handreiking is daarom ook bedoeld voor andere samenwerkingspartners. De handreiking legt uit waarom ggz-aanbieders in sommige gevallen bepaalde informatie over een cliënt niet op de door de samenwerkingspartner gewenste manier kunnen delen. Het doel van deze handreiking is om te laten zien onder welke voorwaarden en op welke manier de gegevens wél kunnen worden gedeeld om zo de samenwerking te bevorderen. Privacyregelgeving vormt hierbij geen obstakel maar is een hulpmiddel om te komen tot een zorgvuldige gegevensuitwisseling mét oog voor de privacy van de cliënt.

1.2 Voor wie is deze Handreiking bedoeld?

Deze handreiking is in de eerste plaats geschreven voor uitvoerende professionals van ggz-aanbieders en hun leidinggevenden. Ook voor juristen en beleidsadviseurs van ggz-aanbieders kan deze handreiking helpen om te beoordelen of het uitwisselen van gegevens met samenwerkingspartners mogelijk is. De handreiking is verder behulpzaam voor de uitvoerende professionals van de samenwerkingspartners en hun leidinggevenden. De handreiking laat namelijk zien aan welke normen de ggz-aanbieder gebonden is en onder welke voorwaarden het uitwisselen van gegevens wél mogelijk is. De samenwerkingspartners kunnen zo onderling komen tot passende afspraken.

[1] Strikt genomen worden taken in de wet neergelegd bij het college van burgemeester en wethouders van de gemeente. Voor de leesbaarheid zeggen wij in deze Handreiking steeds 'de gemeente'.

[2] Onder cliënt wordt ook 'patiënt' verstaan.

1.3 Leeswijzer

Voor de betekenis van vetgedrukte afkortingen zie de afkortingenlijst op de laatste pagina. In deel II van de Handreiking wordt beschreven met welke algemene regels een ggz-aanbieder rekening moet houden bij het uitwisselen van (cliënt)gegevens. De toepasselijke wet- en regelgeving wordt besproken aan de hand van praktijkvoorbeelden en er volgen belangrijke voorwaarden om te komen tot een zorgvuldige gegevensuitwisseling met samenwerkingspartners in algemene zin. Deel III spitst verder toe op de aandachtspunten bij gegevensuitwisseling met specifieke samenwerkingspartners. Deel IV van deze Handreiking bevat een model voor een toestemmingsformulier om de uitwisseling van gegevens die niet op andere gronden mogelijk is tóch mogelijk te maken.

Deel II: Algemeen deel

2.1 Inleiding

Bij het uitwisselen van gegevens met samenwerkingspartners is de ggz-aanbieder gebonden aan veel regelgeving. Er is niet één wet die volledig beschrijft wat er op het gebied van gegevensuitwisseling wel en niet mag. Op het niveau van grondrechten regelen het Europees Verdrag tot bescherming van de Rechten van de Mens (**EVRM**, artikel 8), het Handvest van de grondrechten van de Europese Unie (**Handvest**, artikel 8) en de **Grondwet** (artikel 10) dat iedereen recht heeft op bescherming van zijn persoonlijke levenssfeer en specifieker nog van zijn persoonsgegevens.[3] Privacy is daarmee een grondrecht. Dit grondrecht is niet absoluut. Er mag bij uitzondering een inbreuk op de privacy worden gemaakt in situaties waarvoor de wet dit regelt.

2.1.1 AVG en UAVG

De Algemene verordening gegevensbescherming (**AVG**) geeft op Europees niveau het algemene kader hoe om moet worden gegaan met de bescherming van persoonsgegevens. De AVG stelt algemene kaders en zorgvuldigheidseisen die voor alle (in ieder geval geautomatiseerde) verwerkingen van persoonsgegevens gelden. In Nederland is de AVG in de Uitvoeringswet Algemene verordening gegevensbescherming (**UAVG**) verder uitgewerkt met een aantal algemene regels die alleen voor Nederland gelden.[4]

Op grond van de AVG mag en (soms) moet de wetgever de verwerking van persoonsgegevens verder regelen in nationale wetgeving. De wetgever heeft dit in de UAVG gedaan én in de zogenaamde sectorspecifieke wet- en regelgeving voor diverse sectoren zoals de zorg, het sociaal domein of de strafrechtketen. Voor ggz-aanbieders is dan allereerst zorgwet- en regelgeving relevant, zoals de Wet op de geneeskundige behandelingsovereenkomst (**Wgbo**), de Wet maatschappelijke ondersteuning (**Wmo 2015**), de Jeugdwet (**Jw**), de Wet langdurige zorg (**Wlz**) en de Wet verplichte ggz (**Wvggz**). Ook andere (niet-zorgspecifieke) wetten zijn bij samenwerking rondom psychiatrische cliënten relevant, zoals de Participatiewet, de Wet gemeentelijke schuldhulpverlening en de Politiewet.

2.1.2 Beroepsgeheim

Voor ggz-aanbieders is daarnaast het op hen rustende beroepsgeheim van groot belang. Het beroepsgeheim is geregeld in onder meer de Wgbo (gericht op hulpverleners) en de Wet op de beroepen in de individuele gezondheidszorg (**Wet BIG**, gericht op individuele beroepsbeoefenaars), de Jeugdwet, Wvggz en richtlijnen en beroepscodes. Het beroepsgeheim verplicht zorgaanbieders en zorgverleners om geen informatie over de cliënt met anderen te delen. Het beroepsgeheim (zorgspecifiek) staat náást de (algemene) privacywetgeving in onder meer de AVG en UAVG. Hierna zal nog blijken dat het mogelijk is dat een gegevensuitwisseling tussen samenwerkingspartners op grond van de AVG, UAVG en de sectorspecifieke wetgeving is toegestaan, maar dat een ggz-aanbieder vanwege zijn beroepsgeheim bepaalde informatie over een cliënt toch niet mag delen.

2.2 (U)AVG: algemeen kader voor de verwerking van persoonsgegevens

Deze paragraaf beschrijft de algemene regels die gelden voor de verwerking van persoonsgegevens die volgen uit de AVG en de UAVG zoals het uitwisselen van gegevens tussen partijen. Deze paragraaf is daarom voor ggz-aanbieders en samenwerkingspartners van belang. Daarnaast geldt sectorspecifieke privacyregelgeving voor zowel samenwerkingspartner als ggz-aanbieders. Voor ggz-aanbieders geldt ook het (afgeleide) beroepsgeheim (zie par. 2.3).

[3] Hierna hebben wij het steeds over ‘privacy’. In de Handreiking wordt daarmee bedoeld het recht op bescherming van persoonsgegevens.

[4] De AVG en de UAVG en de Richtlijn (EU) 2016/680 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens door bevoegde autoriteiten met het oog op de voorkoming, het onderzoek, de opsporing en de vervolging van strafbare feiten of de tenuitvoerlegging van straffen, geïmplementeerd in de Wet politiegegevens (Wpg) en de Wet justitiële en strafvorderlijke gegevens (Wjsg) vormen in Nederland samen het algemeen regelgevend kader.

2.2.1 Toepassingsbereik (U)AVG

De AVG is alleen van toepassing op het (gedeeltelijk)geautomatiseerd of in een bestand[5] **verwerken** van **persoonsgegevens**.

Mondeling delen van informatie en de AVG

Als een ggz-aanbieder mondeling informatie over een cliënt deelt binnen een Zorg- en Veiligheidshuis maar er geen sprake is van een geautomatiseerde verwerking, er geen verwerking in een bestand plaatsvindt én de informatie ook niet bestemd is om in een bestand te worden opgenomen, is de AVG niet van toepassing. Maar op de ggz-aanbieder rust nog altijd het beroepsgeheim dat alleen bij een specifieke grond voor doorbreking kan worden doorbroken (zie par. 2.3). Kortom: ook al is de AVG niet van toepassing, toch mogen de patiëntgegevens niet zomaar worden gedeeld binnen het Zorg- en Veiligheidshuis. Het beroepsgeheim en de eisen op grond van de AVG zijn namelijk cumulatief.

Persoonsgegevens zijn gegevens die direct of indirect herleidbaar zijn tot een persoon (bijvoorbeeld de cliënt of andere betrokkenen zoals familieleden).[6] Een persoon is direct herleidbaar als op basis van de gegevens die voorhanden zijn de identiteit van die persoon direct kan worden vastgesteld (bijvoorbeeld omdat de naam van de betrokkene op het document staat). Indirect herleidbaar wil zeggen dat door een combinatie van gegevens, bijvoorbeeld de geboortedatum, woonplaats en specifieke problematiek, kan worden achterhaald om welke persoon het gaat.

Anoniem vs. pseudoniem

Als niet kan worden achterhaald om welke persoon het gaat, zijn de gegevens anoniem. Op anonieme gegevens is de AVG niet van toepassing. Anonieme gegevens zijn iets anders dan gepseudonomiseerde gegevens. Gegevens zijn gepseudonimiseerd als direct identificerende gegevens zijn verwijderd maar met aanvullende informatie kan worden achterhaald om wie het gaat. Gedacht kan worden aan het koppelen van verschillende bestanden waardoor achterhaald kan worden op welk individu de gegevens betrekking hebben. Het kan ook gaan om een combinatie van gegevens die een verstrekker aanlevert en de ontvanger reeds in zijn bezit heeft, die maken dat gepseudonimiseerde gegevens indirecte herleidbaar zijn. Op pseudonieme gegevens is de AVG wél van toepassing. Zie voor meer informatie over het anonimiseren van gegevens par. 2.5.1

Met het verwerken van persoonsgegevens worden alle handelingen met betrekking tot persoonsgegevens bedoeld zoals het vastleggen, bewaren, gebruiken en het anonimiseren van de gegevens. Ook het verstrekken van persoonsgegevens aan een samenwerkingspartner is een verwerking.

2.2.2 De (gezamenlijke)verwerkingsverantwoordelijke en de verwerker

De meeste verplichtingen die volgen uit de AVG worden opgelegd aan de **verwerkingsverantwoordelijke** of – als meerdere partijen samen verantwoordelijk zijn – aan de **gezamenlijke verwerkingsverantwoordelijken**. Daarnaast geldt een aantal verplichtingen voor de **verwerker**. Het is daarom belangrijk om met de samenwerkingspartner te bepalen wie welke rol(len) vervult. In het kort is de verwerkingsverantwoordelijke degene die het doel (het 'waarom') en de middelen (het 'hoe') van de verwerking van persoonsgegevens vaststelt. De verwerkingsverantwoordelijke is daarmee de partij die vaststelt of, en zo ja, welke gegevens worden verwerkt en met welk doel deze verwerking dan geschiedt en hoelang en wie er toegang toe heeft. Daarnaast beslist de verwerkingsverantwoordelijke op welke wijze de gegevensverwerking zal plaatsvinden. Als de samenwerkingspartners samen het doel en de middelen bepalen, zijn zij gezamenlijk verwerkingsverantwoordelijken (zie voorbeeld 1).[7]

[5] De persoonsgegevens moeten in dat geval in een bestand zijn opgenomen of bestemd zijn om daarin te worden opgenomen. Een bestand is een gestructureerd geheel van persoonsgegevens die volgens bepaalde criteria toegankelijk zijn. Een set papieren die min of meer chronologisch zijn geordend vormt nog geen 'bestand'. Een voorbeeld van een bestand is een papieren cliëntendossier. Zie recente rechtspraak van het Hof van Justitie van de Europese Unie, waarin het Hof overweegt dat het mondeling verstrekken van informatie een verwerking van persoonsgegevens vormt voor zover deze informatie in een bestand is opgenomen of bestemd is daarin te worden opgenomen: HvJ EU 7 maart 2024, C-740/22, ECLI:EU:C:2024:216, r.o. 39.

[6] In recente rechtspraak van (het Gerecht van) het Hof van Justitie van de Europese Unie lijkt te worden gezegd dat persoonsgegevens die door de verstrekker gepseudonimiseerd worden verstrekt aan de ontvanger, waarbij de ontvanger geen toegang heeft tot de sleutel om de gegevens te herleiden naar een individu, voor die ontvanger kunnen kwalificeren als anonieme gegevens (en dus niet als persoonsgegevens). Zie: CJEU 26 april 2023, T-557/20, ECLI:EU:T:2023:219, r.o. 100 (tegen deze uitspraak is hoger beroep aanhangig gemaakt); HvJ EU 9 november 2023, C-319/22, ECLI:EU:C:2023:837, r.o. 48. Indien dit een meer bestendige lijn wordt in de rechtspraak, kan dit voor deze Handreiking tot gevolg hebben dat niet iedere gegevensuitwisseling met een samenwerkingspartner buiten de zorg kwalificeert als een verwerking van persoonsgegevens. Dat zou de uitwisseling vanuit het oogpunt van de (U)AVG vergemakkelijken, maar laat het beroepsgeheim onverlet. Verder is het natuurlijk wel zo dat gegevensuitwisseling met samenwerkingspartners buiten de zorg vaak alleen nuttig is als men weet om welke persoon het gaat, bijvoorbeeld binnen een Zorg- en Veiligheidshuis of een casusoverleg. Het is dan ook de vraag hoe zinvol het verstrekken van gepseudonimiseerde gegevens is. Daar komt bij dat de verstrekker wél een verwerkingsgrondslag nodig heeft om de herleidbare gegevens te pseudonimiseren.

[7] De gezamenlijke verwerkingsverantwoordelijken moeten een onderlinge regeling treffen in de zin van artikel 26 AVG. Zie uitgebreid: 'Richtsnoeren 07/2020 over de begrippen "verwerkingsverantwoordelijke" en "verwerker" in de AVG', EDPB, 7 juli 2021, par. 93 e.v.

Voorbeeld 1: gezamenlijke verwerkingsverantwoordelijkheid vs. zelfstandige verwerkingsverantwoordelijkheid

De verschillende partijen die deelnemen aan een Zorg- en Veiligheidshuis maken gebruik van een gezamenlijke technische voorziening (een platform) om gegevens uit te wisselen. Voor de verwerkingen in dit systeem zijn alle deelnemende partijen gezamenlijk verwerkingsverantwoordelijk. Partijen bepalen gezamenlijk het doel en de middelen voor de verwerking: partijen kiezen er samen voor om met het oog op gegevensuitwisseling binnen het Zorg- en Veiligheidshuis gebruik te maken van één systeem. In artikel 2.27 lid 3 van de Wet gegevensverwerking door samenwerkingsverbanden (**Wgs**) zijn private zorgpartijen, zoals ggz-aanbieders, uitgesloten van deze gezamenlijke verwerkingsverantwoordelijkheid.

Als partijen niet samenwerken in het gezamenlijke platform, maar zij ieder vanuit hun eigen systemen op verzoek van een van de samenwerkingspartners gegevens delen, zijn zij in de regel zelfstandig verwerkingsverantwoordelijken. Van gezamenlijke verwerkingsverantwoordelijkheid is dan meestal geen sprake.[1] Dat kan anders zijn als de samenwerkingspartners gedetailleerde afspraken maken over de gegevensuitwisseling.

[1] Onder de Wgs kwalificeren de deelnemers van het Zorg- en Veiligheidshuis op grond van de wet als gezamenlijk verwerkingsverantwoordelijken voor de verwerking van persoonsgegevens door het samenwerkingsverband maar met uitzondering van (onder andere) de deelnemende zorgaanbieders.

De verwerker verwerkt persoonsgegevens in opdracht en ten behoeve van de verwerkingsverantwoordelijke. Het moet gaan om dienstverlening die betrekking heeft op het verwerken van persoonsgegevens (denk aan een IT-leverancier van een EPD).
De verwerker mag alleen op basis van de instructies van de verwerkingsverantwoordelijke handelen.[8]

2.2.3 Gewone persoonsgegevens en bijzondere typen persoonsgegevens

De AVG onderscheidt 'gewone' persoonsgegevens en 'bijzondere persoonsgegevens'. Daarnaast kunnen nog 'gevoelige' persoonsgegevens worden onderscheiden.

Bijzondere persoonsgegevens zijn persoonsgegevens waarvan de verwerking een grotere inbreuk maakt op de persoonlijke levenssfeer van een betrokkene.[9] Dat zijn gegevens over de gezondheidstoestand van de cliënt en gegevens die iets zeggen over diens godsdienst of levensovertuiging, ras, politieke opvattingen, seksuele leven, lidmaatschap van een vakvereniging of de verwerking van genetische gegevens en biometrische gegevens met het oog op de unieke identificatie van een persoon. Aan het verwerken van bijzondere persoonsgegevens zijn extra vereisten verbonden. Bijzondere persoonsgegevens mogen níet worden verwerkt (**verwerkingsverbod**), tenzij er een specifieke wettelijke uitzondering is die de verwerking toestaat. In paragraaf 2.2.5 wordt nader ingegaan op deze uitzonderingen.

Voorbeeld 2: al snel sprake van een (bijzonder) persoonsgegeven

In de praktijk wordt in een samenwerkingsrelatie regelmatig gevraagd naar zogenaamde 'dat-gegevens'. Zo wordt in een casusoverleg bijvoorbeeld door een samenwerkingspartner aan de ggz-aanbieder gevraagd of een bepaald persoon in zorg is of is geweest bij deze aanbieder. Oók 'dat-gegevens' moeten als (bijzondere) persoonsgegevens worden aangemerkt waarop de (U)AVG van toepassing is. Het feit dat iemand in zorg is bij een ggz-aanbieder is al een gezondheidsgegeven. Een ggz-aanbieder moet zich ervan bewust zijn dat hij – ook bij het verstrekken van 'dat-gegevens' – in de regel moet voldoen aan de eisen die de (U)AVG stellen aan de verwerking van gezondheidsgegevens (zie hierover meer in paragraaf 2.2.5).

'**Gevoelige persoonsgegevens**' zijn gegevens die niet expliciet in de AVG zijn benoemd als gevoelig, maar die wel een grotere impact hebben op iemands privacy dan gewone persoonsgegevens. Ook dit soort gevoelige persoonsgegevens moeten volgens de Autoriteit Persoonsgegevens (**AP**) extra worden beveiligd vanwege de mogelijk grote impact op het leven van betrokkenen bij een inbreuk op de beveiliging van deze gegevens. Persoonsgegevens die vanwege hun aard over het algemeen als privacygevoelig worden beschouwd, zijn: gegevens over elektronische communicatie zoals IP-adres, locatiegegevens, financiële gegevens (zoals inkomen of koopgedrag en het burgerservicenummer (BSN). Maar denk ook aan creditcardgegevens, (kopieën van) identiteitsbewijzen of gegevens over identiteitsbewijzen.

[8] De verwerkingsverantwoordelijke(n) en de verwerker moeten een verwerkersovereenkomst sluiten in de zin van artikel 28 AVG. Zie uitgebreid: 'Richtsnoeren 07/2020 over de begrippen "verwerkingsverantwoordelijke" en "verwerker" in de AVG', EDPB, 7 juli 2021, par. 93 e.v.

[9] Meer specifiek vallen onder 'persoonsgegevens over gezondheid' de gegevens over de gezondheidstoestand van de cliënt die informatie geven over de lichamelijke en geestelijke gezondheidstoestand van de cliënt en alle (andere) gegevens die de zorgverlener in de zorgverleningsrelatie over de cliënt te weten komt.

Een andere speciale categorie persoonsgegevens zijn **strafrechtelijke gegevens**. Op de verwerking van strafrechtelijke gegevens is de AVG ook van toepassing met uitzondering van verwerkingen voor de opsporing en vervolging van strafbare feiten door politie en justitie. Daarvoor geldt de Wet politiegegevens en/of de Wet justitiële en strafvorderlijke gegevens. Ook hiervoor is de hoofdregel dat er een verwerkingsverbod geldt tenzij sprake is van een wettelijke uitzondering.[10]

2.2.4 Beginselen

Bij de verwerking van persoonsgegevens, waaronder dus het verstrekken van gegevens aan een samenwerkingspartner, moet altijd worden voldaan aan de algemene uitgangspunten ('beginselen') van de AVG.[11] Hierna gaan wij in op de voor deze Handreiking belangrijkste beginselen.

Een rechtmatige grondslag

Voor het raadplegen, gebruiken en verstrekken van gegevens van en over de cliënt is (i) een verwerkingsgrondslag nodig: een wettelijk belang dat het beperken van de privacy van de cliënt rechtvaardigt en (ii) moet in de wet een expliciete uitzondering staan op het verwerkingsverbod van bijzondere persoonsgegevens (waar gezondheidsgegevens onder vallen). Daarnaast heeft de ggz-aanbieder een grond nodig om zijn beroepsgeheim te mogen doorbreken (zie par. 2.3.3).

Transparantie richting betrokkenen

Persoonsgegevens moeten op een transparante wijze worden verwerkt. Dat betekent dat de betrokkenen (bijv. de cliënt of een vertegenwoordiger) actief worden geïnformeerd (bijv. over het doel van de verwerking of de rechten die zij aan de AVG kunnen ontlenen). Die informatie moet hen in de gelegenheid stellen hun rechten ook daadwerkelijk te kunnen uitoefenen. Daarvoor is onder meer nodig dat de betrokkene wordt geïnformeerd op een wijze die voor de betrokkene begrijpelijk is en de informatie eenvoudig toegankelijk is.

Doelbinding

Als gegevens voor een bepaald doel worden verzameld – bijvoorbeeld voor het verlenen van (jeugd-)ggz– dan mogen deze gegevens in principe niet voor een ander doel worden gebruikt. Dit geldt ook als gegevens aan een samenwerkingspartner worden verstrekt voor een specifiek omschreven doel. Als de samenwerkingspartner de gegevens wil gebruiken voor een ander doel, bijvoorbeeld een gemeente die beleidsmetingen wil uitvoeren ten aanzien van jeugd-ggz, dan moet opnieuw worden getoetst of de AVG dit mogelijk maakt.

Noodzakelijkheid en dataminimalisatie

Als er een specifieke grondslag bestaat om de (bijzondere) persoonsgegevens aan een samenwerkingspartner te verstrekken, betekent dat niet dat alle gegevens van en over de cliënt mogen worden gedeeld. Het gaat om de voor het doel noodzakelijke gegevens. Dit vraagt een kritische houding van de ggz-aanbieder. Dat kan in bepaalde gevallen betekenen dat alleen de gevraagde gegevens worden ingevuld op een formulier, een samenvatting van objectieve feiten en omstandigheden wordt gegeven of dat maar een deel van het medisch dossier wordt verstrekt. Het overdragen van het gehele (medische) dossier zal maar zelden noodzakelijk zijn.

[10] In deze Handreiking wordt verder niet ingegaan op de verwerking van strafrechtelijke gegevens. Als er ook strafrechtelijke gegevens bij de uitwisseling worden betrokken, moeten de kaders van de AVG en/of de Wet politiegegevens en/of de Wet justitiële en strafvorderlijke gegevens ook worden betrokken.

[11] Dit zijn het beginsel van rechtmatigheid, behoorlijkheid en transparantie, het doelbindingsbeginsel, het beginsel van dataminimalisatie, het juistheidsbeginsel, het beginsel van opslagbeperking (samen met dataminimalisatie ook wel het noodzakelijkheidsvereiste), en het beginsel van integriteit en vertrouwelijkheid (artikel 5 AVG).

Passende beveiliging

De persoonsgegevens die worden verwerkt moeten goed worden beveiligd. Daarvoor moeten passende technische én organisatorische maatregelen worden genomen. De beveiligingsmaatregelen moeten worden afgestemd op onder andere de risico's als de gegevens ongeoorloofd worden geraadpleegd of doorgezonden. Gedacht kan worden aan het hanteren van een toegangsbeleid voor de toegang tot medische dossiers op functieniveau en het uitvoeren van periodieke loggingscontrole (ingebed in een beleid omtrent logging). Voor ggz-aanbieders die een zorginformatiesysteem gebruiken (zoals een EPD) vormt de NEN 7510 (in combinatie met de NEN 7512 en NEN 7513) de belangrijkste beveiligingsnormen. Hieraan moet een zorginformatiesysteem voldoen.

2.2.5 (Verwerkings-)grondslagen (U)AVG en uitzonderingen op het verwerkingsverbod voor bijzondere persoonsgegevens

De verwerking van persoonsgegevens in het kader van een samenwerking is alleen rechtmatig (en dus mogelijk) als de verstrekkende partij én de ontvangende partij ieder daarvoor een (eigen) **verwerkingsgrondslag** hebben.[12] Het feit dat de samenwerkingspartner een verwerkingsgrondslag heeft om de te ontvangen gegevens te verwerken, staat dus los van de vraag of de ggz-aanbieder een grondslag heeft om de gegevens te mogen verstrekken (zie misverstand 2).

Misverstand 2: de ontvanger heeft een verwerkingsgrondslag dus de ggz-aanbieder mag informatie verstrekken

Samenwerkingspartners vragen vaak bij de ggz-aanbieder om persoonsgegevens van de cliënt die zij nodig hebben voor eigen doeleinden (bijvoorbeeld een wettelijke taak) en waarvoor de samenwerkingspartner een verwerkingsgrondslag heeft. Denk daarbij aan de reclassering die informatie opvraagt bij de ggz-aanbieder. Het is onjuist dat de ggz-aanbieder de gegevens mag verstrekken omdat de ontvanger (in dit geval de reclassering) een verwerkingsgrondslag heeft. De ggz-aanbieder heeft zelf óók een verwerkingsgrondslag nodig om de gegevens aan de samenwerkingspartner te mogen verstrekken. De ggz-aanbieder kan als uitgangspunt geen beroep doen op de verwerkingsgrondslag van de samenwerkingspartner/ontvanger. Ook moet de ggz-aanbieder rekening houden met het beroepsgeheim dat op de gegevens rust. In het geval van het verzoek van de reclassering kan de ggz-aanbieder – bij gebrek aan een andere grondslag – de gegevens alleen aan de reclassering verstrekken als de cliënt daarvoor expliciet toestemming geeft. Als de zorgaanbieder forensische zorg levert kan de ggz-aanbieder op grond van art 2.6 lid 6 Wet forensische zorg (Wfz), indien noodzakelijk ten behoeve van het toezicht op de naleving van de voorwaarden inzake de verlening van forensische zorg, wel zonder toestemming van betrokkene de in dit artikel genoemde gegevens betreffende de behandeltrouw aan de reclassering of OM verstrekken.

Misverstand 3: er is een convenant, 'dus' gegevensuitwisseling mag

Bij samenwerkingen zie je in de praktijk regelmatig de volgende foutieve aanname: tussen de samenwerkingspartners is een (samenwerkings)convenant gesloten, 'dus' partijen mogen persoonsgegevens met elkaar uitwisselen. Een convenant kan echter nooit de grondslag zijn voor gegevensuitwisseling. Een convenant kan de wettelijke regels namelijk niet doorbreken. Gegevensuitwisseling mag alleen plaatsvinden als daarvoor een wettelijke grondslag bestaat (zie ook Tabel 1). Ongeacht de inhoud van het convenant moeten partijen zich dus houden aan de voor hen geldende wettelijke regels voor het uitwisselen van persoonsgegevens. Een convenant helpt partijen alleen om belangrijke samenwerkingsafspraken, zoals het doel van de samenwerking en de daarbij behorende gegevensuitwisseling en verantwoordelijkheidsverdelingen tussen partijen, nader uit te werken.

[12] Op grond van de AVG is géén nieuwe grondslag vereist voor de verdere verwerking van persoonsgegevens voor een ander doel dan het oorspronkelijke doel als sprake is van zogeheten 'verenigbaar gebruik'. Of daarvan sprake is, hangt af van meerdere factoren, waaronder de verhouding tussen het oorspronkelijke doel en het voorgenomen doel van de verdere verwerking en het type persoonsgegevens dat wordt verwerkt (artikel 6 lid 4). Daarbij kan ook een rol spelen in hoeverre het voor de cliënt te verwachten is dat zijn gegevens voor de verdere verwerking worden gebruikt (overweging 50). In deze handreiking blijft dit verenigbaar gebruik verder buiten beschouwing gelet op de geringe relevantie hiervan: bij de uitwisseling van gezondheidsgegevens blijft een uitzondering op het verwerkingsverbod voor de verwerking van bijzondere persoonsgegevens vereist (artikel 9) én moet het beroepsgeheim rechtmatig worden doorbroken.

De AVG kent zes verschillende grondslagen (artikel 6 AVG) die nader zijn uitgewerkt in Tabel 1. Als er ook bijzondere persoonsgegevens worden uitgewisseld (wat in de situatie van een ggz-aanbieder altijd het geval is, zie voorbeeld 2), is ook een uitzondering op het verwerkingsverbod nodig. De AVG kent tien uitzonderingen op het verwerkingsverbod (artikel 9 AVG). De voor de samenwerking relevante **uitzonderingen** zijn uitgewerkt in Tabel 2.[13]

Tabel 1: verwerkingsgrondslagen (artikel 6 AVG)

Grondslag	Toelichting
a. Toestemming	Het verwerken van persoonsgegevens is mogelijk op basis van een vrije, specifieke, ondubbelzinnige en geïnformeerde toestemming van de betrokkene/cliënt.
b. Uitvoering overeenkomst	Het verwerken van persoonsgegevens is noodzakelijk voor de uitvoering van de (behandelings-/zorg)overeenkomst waarbij de betrokkene/cliënt partij is.
c. Wettelijke verplichting	Het verwerken van persoonsgegevens is noodzakelijk om te voldoen aan een duidelijk in de wet omschreven verplichting.[14]
d. Vitaal belang	Het verwerken van persoonsgegevens is noodzakelijk ter bescherming van iemands leven of gezondheid (= leven of doodsituaties/ acute gevaarsituaties).
e. Taak van algemeen belang of in het kader van de uitoefening van openbaar gezag	Het verwerken van persoonsgegevens door een overheidsinstantie is noodzakelijk voor de vervulling van een taak van algemeen belang of uitoefening van openbaar gezag.
f. Gerechtvaardigd belang	Het verwerken van persoonsgegevens is noodzakelijk ter behartiging van een gerechtvaardigd belang van de ggz-aanbieder zelf of van een ander. Let op! deze grondslag kan niet worden ingeroepen door een overheidsinstantie als zij een taak van algemeen belang uitoefent.

Misverstand 4: de wettelijke of maatschappelijke taak van een samenwerkingspartner vormt een grondslag om gegevens te verstrekken

In sectorspecifieke wetten kan zijn geregeld dat de partij waarmee de zorgaanbieder samenwerkt een wettelijke of maatschappelijke taak heeft. Een zorgaanbieder heeft - in tegenstelling tot overheidsinstanties of overheidsorganen - geen wettelijke of maatschappelijke taak. Een wettelijke of maatschappelijke taak van een overheidspartij kan dan ook geen verplichting inhouden voor ggz-aanbieders om gegevens te verstrekken. Daarvoor heeft de ggz-aanbieder een andere, eigen grondslag nodig. Een wettelijke of maatschappelijke taak is niet hetzelfde als een wettelijke verplichting.

Tabel 2: Uitzonderingen op het verwerkingsverbod (artikel 9 AVG)

Grondslag	Toelichting: een uitzondering op het verwerkingsverbod geldt als:
a. Uitdrukkelijke toestemming	de betrokkene/cliëntvrije, specifieke, ondubbelzinnige, uitdrukkelijke en geïnformeerde toestemming geeft.
b. Uitvoering rechten en plichten arbeidsrecht, socialezekerheids- en socialebeschermingsrecht	uit wet- en regelgeving* een uitzondering volgt voor de uitoefening van rechten van de verwerkingsverantwoordelijke of betrokkene o.g.v. het arbeids-, sociale zekerheids- en/of sociale beschermingsrecht.
c. Vitaal belang	de verwerking noodzakelijk is ter bescherming van iemands leven of gezondheid én de betrokkene fysiek of juridisch niet in staat is om toestemming te geven·
g. Zwaarwegend algemeen belang	uit wet- en regelgeving* een uitzondering volgt voor een zwaarwegend algemeen belang.
h. Preventieve arbeidsgeneeskunde, beheren gezondheidszorgstelsels en –diensten of sociale stelsels en diensten	uit wet- en regelgeving* een uitzondering volgt voor een belang genoemd onder h én de verwerking geschiedt door (of onder verantwoordelijkheid van) een beroepsbeoefenaar die een beroepsgeheim heeft (lid 3).
i. Algemeen belang volksgezondheid, o.m. waarborgen kwaliteit en veiligheid	uit wet- en regelgeving* een uitzondering volgt voor verwerkingen inzake o.m. (de effecten op) de gezondheidstoestand, de behoeften aan gezondheidszorg en de toegang tot en financiering van gezondheidszorg.
j. Archivering, wetenschappelijk of historisch onderzoek of statistische doeleinden	uit wet- en regelgeving* een uitzondering volgt voor verwerkingen inzake archivering, wetenschappelijk onderzoek of statistische doeleinden voor een algemeen belang.

[13] Voor een uitgebreide toelichting bij de verwerkingsgrondslagen en de uitzonderingen op het verwerkingsverbod wordt verwezen naar de Guidelines, Recommendatoins & Best Practices van de European Data Protection Board ('EDPB') en deze uitleg van de Autoriteit Persoonsgegevens.

[14] In overweging 41 bepaalt de AVG dat voor een beroep op een wettelijke verplichting de wettelijke bepaling duidelijk en nauwkeurig moet zijn, en de toepassing daarvan voorspelbaar moet zijn voor degenen op wie deze van toepassing is. De Hoge Raad heeft dit uitgelegd als: "een wettelijke bepaling moet aangeven welke persoonsgegevens geregistreerd mogen worden en onder welke voorwaarden " (ECLI:NL:HR:2021:1814).

Een aantal uitzonderingen op het verwerkingsverbod kan alleen worden ingeroepen als uit andere wet- en regelgeving een concrete uitwerking van die uitzondering volgt. Bij de uitzonderingen waarvoor dit zo is, is in de tabel steeds een (*) toegevoegd. Voor samenwerkingspartners in de zorg volgen uitzonderingen op het verwerkingsverbod vaak uit de UAVG of uit de sectorspecifieke wetten. In onderstaande voorbeelden wordt toegelicht hoe dit in zijn werk gaat. Ook moeten de verwerkingen steeds noodzakelijk zijn voor het in artikel 6 AVG omschreven doel (zie daarvoor par. 2.2.4). Alleen als er een grondslag is voor de rechtmatige verwerking van persoonsgegevens komt men toe aan de vraag of er ook een uitzonderingsgrond is voor de verwerking van bijzondere persoonsgegevens.

Voorbeeld 3: grondslagen Zorg- en Veiligheidshuizen

Een ggz-aanbieder neemt deel aan een casusoverleg binnen een Zorg- en Veiligheidshuis over een jeugdige die ggz ontvangt van de ggz-aanbieder. Aan tafel zitten ook verschillende partijen buiten de zorg, zoals de Dienst Justitiële Inrichtingen (DJI), de gemeente en de politie. Het Zorg- en Veiligheidshuis werkt met een samenwerkings- en privacyconvenant, waarin afspraken staan over de samenwerking en gegevensuitwisseling binnen het Zorg- en Veiligheidshuis.

De ggz-aanbieder mag – ongeacht wat er in het samenwerkings- en privacyconvenant staat – alleen gegevens over de cliënt delen als hij daarvoor een verwerkingsgrondslag, een uitzondering op het verwerkingsverbod én een doorbrekingsgrond voor het beroepsgeheim heeft. De ontvanger moet bovendien een eigen grondslag en uitzonderingsgrond hebben voor de verwerking van deze bijzondere persoonsgegevens. Voor doorbreking van het beroepsgeheim zal in de regel toestemming nodig zijn, behoudens een conflict-van-plichten-situatie.[1]

Zie uitgebreid over de uitwisseling van gegevens in het zorg- en veiligheidsdomein vanaf p. 29 van deze Handreiking en het Handvat Gegevensuitwisseling bij samenwerking rond casuïstiek in het zorg- en veiligheidsdomein van januari 2022.

[1] Zie uitgebreid over wanneer sprake is van een conflict van plichtensituatie de Handreiking Beroepsgeheim van de Nederlandse ggz van 2025.

Voorbeeld 4: grondslagen gegevensuitwisseling bemoeizorg

Het meldpunt bemoeizorg van de gemeente waar Piet woont, wil in kaart brengen of er een noodzaak is voor de inzet van bemoeizorg bij Piet. Er zijn namelijk signalen binnengekomen vanuit de buurt waarin Piet woont dat Piet overlast veroorzaakt en dat zijn huis er erg verwaarloosd en vervuild uit ziet. Het meldpunt neemt contact op met de ggz-aanbieder in de regio om te vragen of Piet daar bekend is en wellicht in behandeling is.

De ggz-aanbieder, waar Piet inderdaad in behandeling is wegens een schizofrene stoornis, zal in dit geval (expliciete) toestemming moeten vragen aan Piet om de vraag van het meldpunt te mogen beantwoorden.[1] De ggz-aanbieder mag het beroepsgeheim niet zomaar doorbreken, ook niet als de ggz-aanbieder alleen wordt gevraagd óf Piet in beeld en wellicht in behandeling is. Als Piet hiervoor geen toestemming geeft, mag de gegevensdeling niet plaatsvinden.

Ontbreekt toestemming, dan zal niet snel sprake zijn van een conflict-van-plichten-situatie waardoor de ggz-aanbieder alsnóg met het meldpunt mag delen dat Piet in behandeling is bij de ggz-aanbieder. Ook als Piet steeds verder gaat in zijn overlastgevende gedrag richting specifiek één buurman en hierbij ook dreigementen begint te uiten, mag de ggz-aanbieder het beroepsgeheim niet snel doorbreken. De ggz-aanbieder heeft, als het gedrag van Piet voortkomt uit zijn psychische stoornis, immers de mogelijkheden van de Wvggz om verplichte zorg aan Piet te verlenen en zo het ernstig nadeel voor de buurman te voorkomen.

2.3 Het beroepsgeheim

2.3.1 Algemeen: achtergrond en doelen

Ggz-aanbieders hebben een beroepsgeheim. Het doel van dit beroepsgeheim is tweeledig. Enerzijds beschermt het beroepsgeheim de privacy van de cliënt zelf. Daarnaast waarborgt het beroepsgeheim de vrije toegang tot de gezondheidszorg. Als de cliënt weet dat zijn persoonsgegevens vertrouwelijk worden behandeld, zal de cliënt zich eerder – en daarmee tijdig – wenden tot een zorgverlener. Voor de geestelijke gezondheidszorg, waar bijna altijd sprake is van zeer gevoelige gegevens en kwetsbare cliënten, geldt dit natuurlijk nog meer. Uitgangspunt van het beroepsgeheim is dat een zorgverlener géén informatie over de cliënt aan anderen dan de cliënt verstrekt, tenzij er een grond is voor doorbreking.[15] Doorbreekt een zorgverlener zijn beroepsgeheim ten onrechte, dan kan hij hierop tuchtrechtelijk[16] of strafrechtelijk worden aangesproken. Zorgverleners gaan in de praktijk over het algemeen (al dan niet terecht) voorzichtig om met het verstrekken van cliëntinformatie aan derden omdat zij het beroepsgeheim heel belangrijk vinden voor de toegankelijkheid van de zorg en omdat de vertrouwelijkheid van hun relatie met een cliënt de basis is voor een goede behandelmogelijkheid.

2.3.2 Reikwijdte

Het beroepsgeheim is veelomvattend en geldt niet alleen voor 'medische gegevens'. De geheimhoudingsplicht ziet zowel op bewust vertrouwelijk gedane mededelingen als op alle overige informatie die de zorgverlener te weten is gekomen door het feit dat de cliënt bij hem in zorg is. Denk hierbij bijvoorbeeld aan het verstrekken van specifieke informatie die de cliënt over diens familie en/of over zijn woonomgeving met de zorgverlener heeft gedeeld, maar ook declaratiegegevens of gegevens over diens zorgverzekeraar. Zelfs het enkele feit dat de cliënt zich heeft gewend tot de ggz-aanbieder valt onder het beroepsgeheim (zie voorbeeld 6).

Het beroepsgeheim is onder andere geregeld in de Wet op de individuele beroepen in de gezondheidszorg (Wet BIG), in de Wgbo, de Jeugdwet, de Wmo 2015 of beroepscodes.[17] Omdat een behandelingsovereenkomst of zorgovereenkomst in de regel gesloten wordt met de ggz-aanbieder, rust op de instelling als geheel een beroepsgeheim. Ook in het verplichte kader van de Wvggz rust op de instelling als geheel (naast enkele met name genoemde functionarissen binnen de instelling) een beroepsgeheim.[18] Voor beroepsbeoefenaren die geen door de wet erkend beroepsgeheim hebben, maar in de uitoefening van hun beroep wel toegang hebben tot informatie die onder de reikwijdte van het beroepsgeheim valt, geldt een 'afgeleid' beroepsgeheim. De zwijgplicht is in dit geval vaak opgenomen in beroepscodes, een arbeidsovereenkomst of in een geheimhoudingsverklaring. Voor beroepsbeoefenaren met een afgeleid beroepsgeheim geldt ook een afgeleid verschoningsrecht.

2.3.3 Doorbrekingsgronden voor het doorbreken van het beroepsgeheim

Er bestaan vijf gronden voor het doorbreken van het beroepsgeheim. Belangrijk is dat een van deze doorbrekingsgronden op zichzelf onvoldoende is om persoonsgegevens uit te kunnen wisselen met een samenwerkingspartner. Voor het rechtmatig verstrekken van bijzondere persoonsgegevens (over de gezondheid van cliënten) door de hulpverlener is naast een doorbrekingsgrond voor het beroepsgeheim een grondslag om de gegevens te verstrekken noodzakelijk en een eigen verwerkingsgrondslag voor de ontvanger nodig. Ook moet er een uitzondering zijn voor de ontvanger (art. 9 AVG) op het verwerkingsverbod om de bijzondere persoonsgegevens te mogen verwerken (zie daarvoor par. 2.2.5).

[15] Onder 'anderen dan de cliënt' vallen niet de rechtstreeks betrokkenen bij de uitvoering van de behandelingsovereenkomst. Rechtstreeks betrokken hulpverleners mogen zonder toestemming van de cliënt informatie uitwisselen die noodzakelijk is voor de uitvoering van die behandelingsovereenkomst.

[16] Zie bijvoorbeeld: RTG Den Haag, 9 januari 2018, ECLI:NL:TGZRSGR:2018:12; CTG Den Haag, 15 mei 2014, ECLI:NL:TGZCTG:2014:192; RTG Eindhoven, 20 december 2013, ECLI:NL:TGZREIN:2013:64.

[17] Artikel 88 Wet BIG; artikel 7:457 BW; Voor meer informatie over het beroepsgeheim verwijzen wij naar de Handreiking Beroepsgeheim van de Nederlandse ggz van 2025: Handreiking-beroepsgeheim.pdf, de KNMG-richtlijn, 'Omgaan met medische gegevens' 2024 en de NVvP-Handreiking 'Beroepsgeheim & het conflict van plichten' 2013.

[18] Artikel 8:34 Wvggz.

Toestemming
De cliënt geeft expliciete toestemming voor het uitwisselen van gegevens met partij X voor een zo specifiek mogelijk omschreven doel. De cliënt begrijpt de gevolgen van zijn gegeven toestemming.

Wettelijke plicht
Uit de wet volgt een duidelijk omschreven plicht om informatie te verstrekken aan partij X. De zorgverlener heeft geen keuzevrijheid.

Zwaarwegend belang
Er is een zwaarwegend belang van de zorgverlener zelf of een ander dat in een specifiek geval zwaarder weegt dan het belang van de client bij geheimhouding.

Conflict van plichten
De zorgverlener bevindt zich in een overmachtssituatie omdat ernstig nadeel voor de cliënt of een ander dreigt en dit nadeel alleen kan worden voorkomen door de gegevens met een derde te delen.

Wettelijke bevoegdheid
Uit de wet volgt een bevoegdheid om informatie te verstrekken aan partij X. De zorgverlener maakt een afweging of hij van deze bevoegdheid gebruik wil maken.

Alleen “toestemming”, “wettelijke plicht”, “wettelijke bevoegdheid” en “conflict van plichten” kunnen doorbrekingsgronden zijn voor gegevensverstrekking buiten de zorg. De andere doorbrekingsgronden zijn specifiek voor het doorbreken van het beroepsgeheim binnen de zorg en blijven daarom buiten beschouwing in deze Handreiking.

Voorbeeld 5: Wanneer kan het beroepsgeheim worden doorbroken voor gegevensuitwisseling bij een Zorg- en Veiligheidshuis (ZVH)-overleg?
Tijdens een ZVH-overleg zitten veel verschillende partijen aan tafel. Het is begrijpelijk dat iedere partij er een eigen belang bij heeft om de gegevens over de cliënt met elkaar te delen. Elke partij heeft een eigen grondslag nodig voor het rechtmatig verwerken van persoonsgegevens en een uitzondering op het verbod gezondheidsgegevens te verwerken. De zorgaanbieder kan alleen het beroepsgeheim doorbreken als daarvoor geïnformeerde expliciete toestemming is van de cliënt. Er mogen niet meer persoonsgegevens worden gedeeld dan strikt noodzakelijk is. Soms is het voldoende de partner(s) in het ZVH te laten weten dat cliënt in behandeling is en bij wie. Ook kan het voldoende zijn bepaalde gegevens alleen te delen met de casuscoördinator.
NB: de Wgs geeft aan zorgaanbieders géén (nieuwe) grondslag voor het doorbreken van het beroepsgeheim. Zie Factsheet Wgs van de Nederlandse ggz 2025.

Voorbeeld 6: Conflict van plichten bij een dreigend gevaar voor anderen
Als een cliënt aan een zorgverlener meedeelt ruzie te hebben met een vriend en hem fysiek iets ernstigs aan te willen doen, kan een zorgverlener in een conflict van plichten komen. Als de zorgverlener de situatie inschat als een concrete en ernstige dreiging waarbij risico op ernstige schade voor de vriend bestaat, dat risico niet op een andere manier kan worden weggenomen dan door het beroepsgeheim te doorbreken en daarmee het risico kan worden weggenomen, dan mag de zorgverlener de politie informeren. Ook als de cliënt daarvoor geen toestemming geeft. In dat geval is sprake van een geoorloofde doorbreking van het beroepsgeheim. Onder welke omstandigheden een beroep op een conflict van plichten kan slagen, is nader uitgewerkt in de Handreiking Beroepsgeheim van de Nederlandse ggz van 2025 en de NVvP-Handreiking ‘Beroepsgeheim & het conflict van plichten’ 2013.

2.4 Wet aanvullende bepalingen verwerking persoonsgegevens in de zorg

2.4.1 Elektronische gegevensuitwisseling

Persoonsgegevens kunnen elektronisch worden uitgewisseld. In de toekomst zal de wet dit zelfs in steeds meer gevallen ook voorschrijven.[19] Voor elektronische gegevensuitwisseling moeten de nodige beveiligingsmaatregelen worden getroffen (zie daarvoor par. 2.2.4). Als zorgaanbieders onderling gebruikmaken van een elektronisch uitwisselingssysteem, moet daarnaast rekening worden gehouden met de Wet aanvullende bepalingen verwerking persoonsgegevens in de zorg (**Wabvpz** art. 15a lid 1). Deze wet schrijft voor dat cliënten expliciet toestemming moeten geven voor het beschikbaar stellen van hun persoonsgegevens door een zorgaanbieder voor andere zorgaanbieders via een elektronisch uitwisselingssysteem.

Deze wet geldt niet voor elektronische gegevensuitwisseling met samenwerkingspartners buiten de zorg, zoals de gemeente of justitie. Gegevens kunnen worden uitgewisseld met deze samenwerkingspartners door (i) de gegevens aan de samenwerkingspartner te sturen (bijvoorbeeld via beveiligde e-mail) of (ii) door zelf gegevens in te voeren in een digitale omgeving van de samenwerkingspartner. Daarbij moet wel goed worden omgegaan met de eisen die de AVG stelt op onder andere het gebied van beveiliging en dataminimalisatie. Ook is het raadzaam (en in sommige gevallen verplicht) om afspraken te maken over de gegevensuitwisseling. Zie hierover uitgebreid par. 2.2.2.

Voorbeeld 7: Mag een samenwerkingspartner toegang hebben tot het EPD?

Met de samenwerkingspartner buiten de zorg mogen alleen die gegevens worden uitgewisseld die de ggz-aanbieder mag delen met de samenwerkingspartner én die de samenwerkingspartner rechtmatig mag inzien. Het geven van toegang tot het EPD van de ggz-aanbieder is niet voor de hand liggend en snel in strijd met de wet. De wetgever heeft het elektronisch uitwisselen van gezondheidsgegevens tussen zorgaanbieders via een elektronisch uitwisselingssysteem (EPD) specifiek in een wet geregeld en daaraan extra eisen gesteld. Die regeling is niet van toepassing op anderen dan zorgaanbieders en dus niet op uitwisseling van persoonsgegevens met bijvoorbeeld gemeenten.

2.5 Stappenplan voor een zorgvuldige uitwisseling van persoonsgegevens

Bij iedere persoonsgegevensuitwisseling kan het hierna beschreven stappenplan doorlopen worden. In paragraaf 2.5.1 is nog een checklist voor het anonimiseren van persoonsgegevens opgenomen en in paragraaf 2.5.2 een toelichting op wanneer afspraken met de ontvangende partij verplicht of raadzaam zijn.

Stappenplan uitwisseling van persoonsgegevens	
Stap 1	Bepaal voor jezelf met welke samenwerkingspartner buiten de zorg je te maken hebt en voor welk doel de samenwerkingspartner de gegevens nodig heeft.
Stap 2	Stel vast of het om anonieme gegevens, pseudonieme of gewone persoonsgegevens gaat. Zie par. 2.2.1
Stap 3	Ga na of er voor het delen van (gepseudonimiseerde) persoonsgegevens of het anonimiseren van die gegevens een grond voor doorbreking van het beroepsgeheim bestaat én een verwerkingsgrondslag (artikel 6) én een uitzonderingsgrond op het verwerkingsverbod (artikel 9) in de AVG bestaat. Zie par. 2.2.5 en 2.3.3.
Stap 4	Verzamel de gegevens en controleer of je daarbij uitsluitend de voor het doel van de verstrekking noodzakelijke gegevens hebt opgenomen. Zie par. 2.2.4.
Stap 5	Beoordeel of de noodzakelijke beveiligingsmaatregelen zijn getroffen voor de verstrekking aan de ontvanger en door de ontvanger om de gegevens te kunnen delen. Zie par. 2.2.4.
Stap 6	Bepaal of je afspraken moet of wil maken met de samenwerkingspartner buiten de zorg waarmee gegevens worden uitgewisseld. Zie par. 2.5.2. De AVG kan tot afspraken verplichten maar ook als dit niet verplicht is, is het zeker bij structurele uitwisseling raadzaam om afspraken te maken. Denk hierbij aan afspraken over de doelen waarvoor de samenwerkingspartner de ontvangen gegevens mag gebruiken zeker als de ontvanger meerdere taken heeft waarvoor deze de persoonsgegevens zou kunnen gebruiken (een gegevensuitwisselingsovereenkomst).

[19] Zie de Wet elektronische gegevensuitwisseling in de zorg (Wegiz).

2.5.1 Checklist anonimiseren

Als gegevens anoniem zijn, is de AVG niet van toepassing. Anonieme gegevens zijn namelijk geen persoonsgegevens omdat ze niet tot een natuurlijk persoon herleidbaar zijn (zie ook par. 2.2.1). Voor de ggz-aanbieder en de samenwerkingspartner is er dan geen verwerkingsgrondslag nodig en hoeft er geen uitzondering op het verwerkingsverbod te bestaan om de gegevens onderling te mogen uitwisselen. Wel is het anonimiseren zelf een verwerking. Daarvoor is wél een verwerkingsgrondslag en een uitzondering op het verwerkingsverbod en een doorbrekingsgrond voor het beroepsgeheim vereist. Het Uitvoeringsbesluit Wet kwaliteit, klachten en geschillen zorg (**Uitvoeringsbesluit Wkkgz**) kent bijvoorbeeld de wettelijke verplichting (art. 6.1 lid 2 onder d) om persoonsgegevens over incidenten zo spoedig mogelijk te anonimiseren om bovenmatige gegevensverwerking te voorkomen. Onderstaande checklist helpt om te bepalen óf persoonsgegevens geanonimiseerd kunnen worden en zo ja, hoe dit aan te pakken.

Voorbeeld 8: “Dan maak je de gegevens toch gewoon anoniem?”

Ggz-aanbieders leveren, met subsidie van het ministerie, IPS-trajecten (Individuele Plaatsing en Steun) aan cliënten voor het vinden en behouden van een betaalde baan of studie. Een werkgeversvereniging wil graag ook geanonimiseerde gegevens ontvangen om te kunnen beoordelen hoe het aanbieden van banen via IPS-trajecten in de verschillende sectoren verloopt en daar waar nodig extra maatregelen te kunnen nemen. Dit doel ligt heel dicht aan tegen het doel waarvoor het ministerie subsidie verleent. In de subsidieregeling van het ministerie van Volksgezondheid, Welzijn en Sport (VWS) staat als voorwaarde dat de zorgaanbieder bepaalde persoonsgegevens moet verstrekken aan een onderzoeksinstelling voor het verdere beleid van VWS. Deze subsidieregeling biedt geen grondslag voor de ggz-aanbieders om de gevraagde gegevens te leveren aan de werkgeversvereniging, of deze eerst te anonimiseren. Anonimisering is ook een verwerkingshandeling. Dat het doel van de werkgeversvereniging in het verlengde ligt van het doel van de IPS-regeling doet niet ter zake.

NB: als de hulpverlener de gegevens zelf anonimiseert voor verstrekking is dit geen doorbreking van het beroepsgeheim.
Als aan de anonimisering derden te pas komen, is dat wél een doorbreking van het beroepsgeheim, waarvoor een doorbrekingsgrond is vereist. Soms is het mogelijk om gegevens te anonimiseren of analyses op data te doen zonder dat (persoons)gegevens ooit in leesbare vorm worden geraadpleegd door personen of worden uitgewisseld. Dan is geen grondslag, uitzonderingsgrond of doorbrekingsgrond van het beroepsgeheim nodig.

Checklist voor het verstrekken van anonieme gegevens	
Voorvraag: onderzoek of de gegevens zonder extra verwerkingshandelingen anoniem kunnen worden verstrekt. Als dat niet het geval is, heeft de ggz-aanbieder in ieder geval een verwerkingsgrondslag, een uitzondering op het verwerkingsverbod en een doorbrekingsgrond van het beroepsgeheim nodig om de gegevens te anonimiseren en dan te verstrekken aan de samenwerkingspartner. Loop onderstaande checklist af om te bepalen of de gegevens op een juiste manier zijn geanonimiseerd.	
1.	Bepaal welke gegevens noodzakelijk zijn voor het doel van de gegevensverstrekking.
2.	Stel jezelf vervolgens de vraag of het met een redelijke inspanning mogelijk is om de identiteit van de cliënt te achterhalen door deze gegevens te combineren met gegevens die de ontvanger al in zijn bezit heeft of waar deze makkelijk toegang toe heeft.
3.	Als dat niet het geval is, is de kans groot dat de te verstrekken gegevens anoniem zijn voor de ontvangende samenwerkingspartner.

2.5.2 Schriftelijke afspraken

Bij gegevensuitwisseling tussen twee of meer zelfstandig verwerkingsverantwoordelijken zijn afspraken niet verplicht. Maar als die gegevensuitwisseling structureel is, is het raadzaam om schriftelijke spraken te maken. Dat kan in een gegevensuitwisselingsovereenkomst of een andere vorm van een gemeenschappelijke regeling. In schriftelijke afspraken kunnen de partners dan afspreken dat zij ieder de gegevens zullen verwerken volgens de verplichtingen uit de AVG, op basis van welke grondslagen gegevens mogen worden verwerkt en voor welke doeleinden en dat zij elkaar inlichten als de gegevens die zij uitwisselen bij een van hen onderdeel zijn van een datalek. Die afspraken kunnen ook onderdeel zijn van een meeromvattende samenwerkingsovereenkomst.

Deel III: Gegevensuitwisseling met samenwerkingspartners

3.1 Inleiding

De ggz-aanbieders werken met veel verschillende partijen samen. In algemene zin geldt voor de gegevensuitwisseling met samenwerkingspartners een aantal uitgangspunten. Het gaat vaak om gevoelige informatie over de cliënt waarmee zorgvuldig moet worden omgegaan. De belangrijkste voorwaarden voor een zorgvuldige gegevensuitwisseling zijn behandeld in paragraaf 2.5 Vervolgens worden in paragraaf 3.2 een aantal samenwerkingsverbanden uitgelicht. Voor iedere samenwerkingsvorm gelden andere aandachtspunten die veelal – maar niet uitputtend – worden geregeld in de sectorspecifieke wetten.

3.2 Aandachtspunten bij specifieke samenwerkingsverbanden en -partners

Iedere samenwerkingsvorm geeft eigen uitdagingen als het gaat om het uitwisselen van persoonsgegevens. Naast dat een gegevensuitwisseling altijd zorgvuldig moet zijn, bestaan er vaak vragen over het al dan niet bestaan van een grondslag voor de uitwisseling van gegevens. Hierna volgen de belangrijkste aandachtspunten bij een samenwerking in het kader van: het sociaal-, zorg- en veiligheidsdomein, bemoeizorg, verschillende taken van de gemeente en vraagstukken op het gebied van wonen.

3.2.1 Samenwerkingsverbanden in het sociaal, zorg- en veiligheidsdomein

Samenwerkingsverbanden in het sociaal, zorg- en veiligheidsdomein hebben op dit moment geen zelfstandige wettelijke taak en ook geen eigen wettelijke basis om persoonsgegevens in het kader van hun samenwerking te mogen verwerken. Kenmerkend voor samenwerkingsverbanden in het sociaal domein en het zorg- en veiligheidsdomein is dat de samenwerking in dienst staat van een specifieke maatschappelijke opgave: het oplossen van ernstige probleemsituaties op het gebied van overlast, criminaliteit of veiligheid van personen waarbij de oorzaak van die probleemsituaties mede is gelegen in sociale of zorgproblematiek. Om een oplossing voor dergelijke probleemsituaties te kunnen vinden, is de inzet van verschillende partijen vereist, zoals: de gemeente, het sociaal wijkteam, woningcorporaties, politie, jeugdzorg en/of ggz-aanbieders.

Samenwerkingspartners hebben ieder een eigen grondslag nodig voor gegevensverwerking

Samenwerkingsverbanden van partners in het sociaal- of veiligheidsdomein met zorgaanbieders hebben meestal geen eigen wettelijke basis om persoonsgegevens te mogen verwerken. Dit heeft tot gevolg dat er juridisch gezien géén gegevensuitwisseling plaatsvindt tussen een van de samenwerkingspartners (bijvoorbeeld de ggz-aanbieder) en het samenwerkingsverband, maar tussen de betrokken samenwerkingspartners onderling. Dit betekent dat iedere samenwerkingspartner een eigen grondslag nodig heeft om persoonsgegevens te mogen delen met elke andere samenwerkingspartner in het samenwerkingsverband. Vervolgens hebben al deze andere samenwerkingspartners óók ieder een eigen grondslag nodig om de persoonsgegevens (verder) te mogen verwerken.

Dit is anders voor de Zorg- en Veiligheidshuizen. De Wgs regelt de wettelijke basis voor het als gezamenlijke verwerkingsverantwoordelijken verwerken van persoonsgegevens voor de taken van het Zorg- en Veiligheidshuis. Zorgaanbieders zijn echter uitgesloten van de gezamenlijke verwerkingsverantwoordelijkheid (zie artikel 2.27 lid 3 Wgs). Wel zijn zorgaanbieders aangemerkt als zogeheten 'deelnemers' van het Zorg- en Veiligheidshuis (artikel 2.27 lid 2 onder d en e Wgs). De Wgs regelt niet alleen de basis voor de gegevensverwerking binnen het Zorg- en Veiligheidshuis, maar bevat ook de grondslag voor verstrekking van gegevens door de deelnemers aan het Zorg- en Veiligheidshuis (zie artikel 2.29 en artikel 1.5 Wgs). Hetzelfde geldt voor de vereiste uitzondering op het verbod op verwerking van bijzondere persoonsgegevens, specifiek gezondheidsgegevens. De Wgs bepaalt expliciet dat een zorgaanbieder nog altijd een van de eigen doorbrekingsgronden voor het doorbreken van het beroepsgeheim nodig heeft (zie artikel 2.29 lid 2 Wgs en paragraaf 2.3).

Zie uitgebreid over de uitwisseling van gegevens in het zorg- en veiligheidsdomein het Handvat Gegevensuitwisseling bij samenwerking rond casuïstiek in het zorg- en veiligheidsdomein van november 2021. NB: Dit document is nog niet geüpdatet aan de hand van de Wgs en het Besluit gegevensverwerking door samenwerkingsverbanden (Bgs) Zie ook de Factsheet Wgs van de Nederlandse ggz 2025 (alleen voor leden van de Nederlandse ggz).

3.2.2 Samenwerking in het kader van bemoeizorg

Openbare geestelijke gezondheidszorg, vaak ‘bemoeizorg’ genoemd, kent nog geen (duidelijk) wettelijk kader. In de praktijk wordt wel aangenomen dat het organiseren van bemoeizorg een wettelijke taak is van de gemeente op grond van de Wmo 2015, namelijk het aanbieden van een ‘algemene voorziening’ mogelijk in aanloop naar een maatwerkvoorziening of naar ggz-hulpverlening. Meestal heeft een gemeente een meldpunt bemoeizorg of niet-acute zorg dat meldingen van burgers en professionals afhandelt. In de praktijk zie je ook wel dat een meldpunt bemoeizorgmeldingen oppakt én meldingen op grond van de Wvggz die voor de gemeente aanleiding zijn voor een verkennend onderzoek. De taak van het ‘bemoeizorgteam’, dat wil zeggen het feitelijk verlenen van de bemoeizorg, is vaak belegd bij een Gemeentelijke Gezondheidsdienst (GGD) of bij een ggz-aanbieder.

De ‘Handreiking gegevensuitwisseling bemoeizorg 2014’ geeft de geldende afspraken rond de uitwisseling van persoonsgegevens bij bemoeizorg weer.[20] In de huidige wetgeving is niet zonder meer een grondslag te vinden waarop de bemoeizorgverlener persoonsgegevens, waaronder gezondheidsgegevens, van de betrokkene kan verwerken.

Een (zorgverlener werkzaam bij een) ggz-aanbieder kan door het bemoeizorgteam worden bevraagd over een cliënt. Zo kan het zijn dat de ggz-aanbieder eerder (on)vrijwillige zorg heeft verleend aan de betrokkene, maar de betrokkene uiteindelijk uit zorg is gegaan en sindsdien ook niet meer in beeld is geweest bij de ggz-aanbieder. Het bemoeizorgteam kan de ggz-aanbieder vragen of betrokkene eerder in zorg was en wat de eerdere zorgverlening inhield. Maar de ggz-aanbieder kan daarop niet antwoorden zonder expliciete toestemming van de betrokkene/cliënt.
Voor het delen van gegevens over de cliënt door de ggz-aanbieder met (het meldpunt van) de gemeente is een grondslag in de zin van de AVG, een uitzondering op het verwerkingsverbod voor de verwerking van gezondheidsgegevens én een grond voor doorbreking van het beroepsgeheim vereist. De ggz-aanbieder zal voor doorbreking van het beroepsgeheim expliciete toestemming moeten vragen aan de cliënt.

3.2.3 Samenwerking met de gemeente

De gemeente kan bij het uitvoeren van haar publieke taken in het sociaal domein informatie nodig hebben van en over de cliënt. Hoewel de gemeente daar vaak een wettelijke grondslag voor heeft, betekent dat nog niet dat de ggz-aanbieder op verzoek van de gemeente gegevens over de cliënt mag verstrekken. Hierna volgen een aantal situaties waarin de gemeente de samenwerking opzoekt met de ggz-aanbieder.

Domeinoverstijgende beoordeling van de hulpvraag van een burger door de gemeente
Bij de gemeente komen verschillende hulpvragen binnen, vaak in het kader van een zogeheten ‘keukentafelgesprek’. Deze hulpvragen zijn vaak niet (uitsluitend) te plaatsen binnen één wettelijk kader. De gemeente kan uitdrukkelijke toestemming van betrokkene als grondslag hebben om de al verzamelde gegevens bijvoorbeeld in het kader van de Wmo 2015[21] te gebruiken voor de uitvoering van haar taken op basis van sommige andere wetten in het sociaal domein (zoals de Jeugdwet). Voor een ggz-aanbieder geldt dat persoonsgegevens kunnen worden verstrekt aan de gemeente voor het doel dat met cliënt is besproken. De toestemming van cliënt aan de zorgaanbieder om persoonsgegevens te verstrekken en het beroepsgeheim te doorbreken is doelgebonden. De ontvanger, de gemeente, mag die gegevens dus in principe niet gebruiken voor andere taken. Mocht de gemeente die gegevens ook willen gebruiken voor andere taken dan zal de gemeente daarvoor expliciet toestemming moeten vragen aan betrokkene, mits de sectorwetgeving dat toestaat.

Delen van gegevens ten behoeve van beleidsdoeleinden en kwaliteitsdoeleinden
De gemeente wil de gegevens van de ggz-aanbieder soms ook inzetten om nieuw beleid te kunnen vaststellen in beleidsplannen. In sectorspecifieke wetgeving is bijvoorbeeld de plicht opgenomen om beleidsplannen op te stellen over: (i) het te voeren beleid met betrekking tot maatschappelijke ondersteuning, (ii) door de gemeente te nemen beslissingen betreffende preventie en jeugdhulp, (iii) de te verrichten tegenprestatie als bedoeld in de Participatiewet en (iv) de richting die de gemeente geeft aan de integrale schuldhulpverlening aan de inwoners van de gemeente.[22] Daarnaast wenst de gemeente gegevens van de ggz-aanbieder soms ook te gebruiken voor kwaliteitsdoeleinden, bijvoorbeeld om de effectiviteit van de in de gemeente geleverde jeugdhulp of maatschappelijke ondersteuning te kunnen meten. In sommige gevallen kan het daarvoor noodzakelijk zijn om persoonsgegevens van en over de cliënt te verwerken. De gemeente gaat zelf na of voor de verwerking van deze gegevens ten behoeve van beleidsdoeleinden of kwaliteitsmetingen een verwerkingsgrondslag bestaat.

Belangrijk in dit verband is dat in de sectorspecifieke wetgeving (o.a. Jeugdwet, Besluit Jeugdwet, Wmo 2015 en Participatiewet) bepalingen zijn opgenomen die ggz-aanbieders een wettelijke verplichting als grondslag biedt om de persoonsgegevens van cliënten rechtstreeks, of via bijvoorbeeld het Centraal Bureau voor de Statistiek (**CBS**)[23], aan de gemeente te verstrekken ten behoeve van beleidsdoeleinden. Ggz-aanbieders kunnen dus binnen de grenzen van deze wettelijke bepalingen zonder toestemming van cliënten de daargenoemde gegevens verstrekken voor dat doel. Een dergelijke specifieke regeling is dus nodig om persoonsgegevens zonder toestemming van client te kunnen verstrekken voor beleidsdoeleinden of kwaliteitsdoeleinden.

[20] Zie de Handreiking gegevensuitwisseling bemoeizorg 2014 die voor zowel de KNMG als de Nederlandse ggz leidend is.
[21] Zie artikel 5.1.1 lid 4 Wmo 2015. Vergelijkbaar: artikel 8d Wet gemeentelijke schuldhulpverlening; artikel 9.1.3 lid 4 Wlz.
[22] Artikel 2.1.2 lid 1 Wmo 2015; artikel 2.2 lid 1 Jeugdwet; artikel 7 lid 1 onder c Participatiewet, artikel 2 Wet gemeentelijke schuldhulpverlening.
[23] Zie Besluit Jeugdwet § 7.5 en Regeling Jeugdwet artikel 7

Op dit moment is het gebruik van bestaande gezondheidsgegevens voor secundair gebruik, namelijk om beleid te maken of kwaliteit te meten en te bevorderen of wetenschappelijk onderzoek, niet generiek geregeld, maar in specifieke wetten (bijvoorbeeld in de Zorgverzekeringswet). De European Health Data Space verordening (EHDS) is in maart 2025 van kracht geworden en regelt in de nabije toekomst het gebruik van gezondheidsgegevens voor primair (binnen de zorgverlening) en secundair gebruik. Beschikbaarheid van de gezondheidsgegevens voor primair en secundair gebruik is het uitgangspunt met een opt-out mogelijkheid voor cliënt. Cliënten kunnen dan zelf centraal vastleggen dat zij (bepaalde van) hun beschikbare gezondheidsgegevens niet willen delen voor bepaalde doeleinden.

3.2.4 Het verstrekken van informatie aan woningcorporaties

Zorgaanbieders willen graag voorkomen dat een cliënt vanwege een huurachterstand en/of aanhoudende overlast zijn huis uitgezet wordt. Daarvoor wil de zorgaanbieder aan de woningcoöperatie laten weten dat cliënt in zorg is en wat meer tijd en ruimte vragen om de situatie zo aan te passen dat uithuiszetting wordt voorkomen. Daarvoor heeft de zorgaanbieder als grondslag voor rechtmatige verstrekking en als grondslag voor doorbreking van het beroepsgeheim expliciete toestemming nodig van cliënt of diens vertegenwoordiger. De woningcorporatie heeft een eigen grondslag nodig om gezondheidsgegevens over cliënt rechtmatig te mogen verwerken en een grondslag voor het doorbreken van het verwerkingsverbod.

Deel IV: Toestemmingsformulier

Met dit toestemmingsformulier geeft u toestemming aan [naam ggz-aanbieder] om de hierna omschreven gegevens te verstrekken aan [naam samenwerkingspartner] met als doel [beschrijving doel + toelichting]. [naam ggz-aanbieder] zal niet meer gegevens verstrekken aan [naam samenwerkingspartner] dan voor het vooraf bepaalde doel noodzakelijk is.

Gegevens ggz-aanbieder

Naam:	
Adres:	
Postcode en plaats:	

Met dit toestemmingsformulier geef ik, de cliënt (en/of mijn wettelijke vertegenwoordiger)

Gegevens cliënt

Naam cliënt:	
Geboortedatum:	
Adres:	
Postcode woonplaats:	

Indien van toepassing:

Gegevens vertegenwoordiger

Naam:	
Adres:	
Postcode en woonplaats:	
Telefoon:	

Basis voor vertegenwoordiging (aankruisen wat van toepassing is)

- ○ wettelijke vertegenwoordiging door ouder(s)/voogd (bij minderjarige tot 16 jaar en minderjarige vanaf 16 die niet in staat is tot een redelijke waardering van zijn/haar belangen).
- ○ benoeming door de rechtbank tot curator / mentor
- ○ schriftelijk gemachtigd door de cliënt
- ○ wettelijke vertegenwoordiging in de hoedanigheid van echtgenoot of partner / ouder / kind / broer of zus (bij meerderjarige die niet in staat is tot een redelijke waardering van zijn/haar belangen).

toestemming voor de verstrekking van de volgende gegevens door [naam ggz-aanbieder]
aan [naam samenwerkingspartner]:

Aan:

Gegevens ggz-aanbieder en/of hulpverlener

Naam:

Adres:

Postcode en plaats:

Voor het doel:

Door ondertekening van dit formulier verklaart de cliënt dat hij/zij heeft begrepen dat de gegeven toestemming te allen tijde mag worden ingetrokken.

Handtekening cliënt

Datum:

Handtekening (wettelijke) vertegenwoordiger(s)

Datum:

Afkortingenlijst

AVG	Algemene Verordening Gegevensbescherming
Bgs	Besluit gegevensverwerking door samenwerkingsverbanden
CBS	Centraal Bureau voor de Statistiek
CTG	Centraal Tuchtcollege voor de Gezondheidszorg
DJI	Dienst Justitiële Inrichtingen
EHDS	European Health Data Space
EPD	Elektronisch Patiëntendossier
EVRM	Europees Verdrag voor de Rechten van de Mens
GGD	Gemeentelijke Gezondheidsdienst
Handvest	Handvest van de grondrechten van de Europese Unie
IGJ	Inspectie Gezondheidszorg en Jeugd
Jw	Jeugdwet
Oggz	Openbare geestelijke gezondheidszorg
RTG	Regionaal Tuchtcollege voor de Gezondheidszorg
UAVG	Uitvoeringswet Algemene Verordening Gegevensbescherming
Wabvpz	Wet aanvullende bepalingen verwerking persoonsgegevens in de zorg
Wegiz	Wet elektronische gegevensuitwisseling in de zorg
Wet BIG	Wet op de Beroepen in de Individuele Gezondheidszorg
Wfz	Wet forensische zorg
Wgbo	Wet op de geneeskundige behandelingsovereenkomst
Wgs	Wet gegevensverwerking door samenwerkingsverbanden
Wkkgz	Wet kwaliteit, klachten en geschillen zorg
Wlz	Wet langdurige zorg
Wmo 2015	Wet maatschappelijke ondersteuning 2015
Wvggz	Wet verplichte geestelijke gezondheidszorg
ZVH	Zorg- en Veiligheidshuis

de Nederlandse ggz
Piet Mondriaanplein 25
3812 GZ Amersfoort

T +31 (0)33 460 89 00
E info@denederlandseggz.nl
www.denederlandseggz.nl

© de Nederlandse ggz, augustus 2025
Overname van teksten is toegestaan met bronvermelding.

samen zijn we **de Nederlandse ggz**