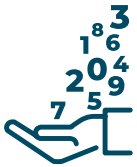
Leren Werken met Data
in de gehandicaptenzorg

AVG en privacy rondom data in de gehandicaptenzorg

Data steeds meer in gebruik, wie heeft welke verantwoordelijkheid en hoe zorg je voor vertrouwen?

ACADEMY HET DORP
Ministerie van Volksgezondheid, Welzijn en Sport
Academische Werkplaats ZoTeG
ZorgTechnologie in de Gehandicaptenzorg

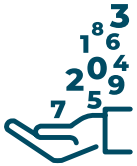


Voorwoord

Deze publicatie bestaat uit vier delen en is tot stand gekomen na een uitvraag over ‘AVG en privacy’ en het gebruik van data in gehandicaptenzorgorganisaties. De gestelde vragen zijn vervolgens door enkele juristen beantwoord. Zij hebben de vragen beantwoord vanuit het perspectief van gehandicaptenzorgorganisaties. De vragen variëren van het nu al benutten van data, het meer willen werken met data tot het gebruik van kunstmatige intelligentie (Artificial Intelligence, AI), nu en in de toekomst.

Elke publicatie staat op zichzelf, tezamen vormen ze een informatief naslagwerk over AVG en privacy rondom data in de gehandicaptenzorg. In de bijlage vind je daarnaast relevante begrippen, wetten, handige richtlijnen en hulpmiddelen rondom AVG.

Inhoud



Wat je eerst moet weten

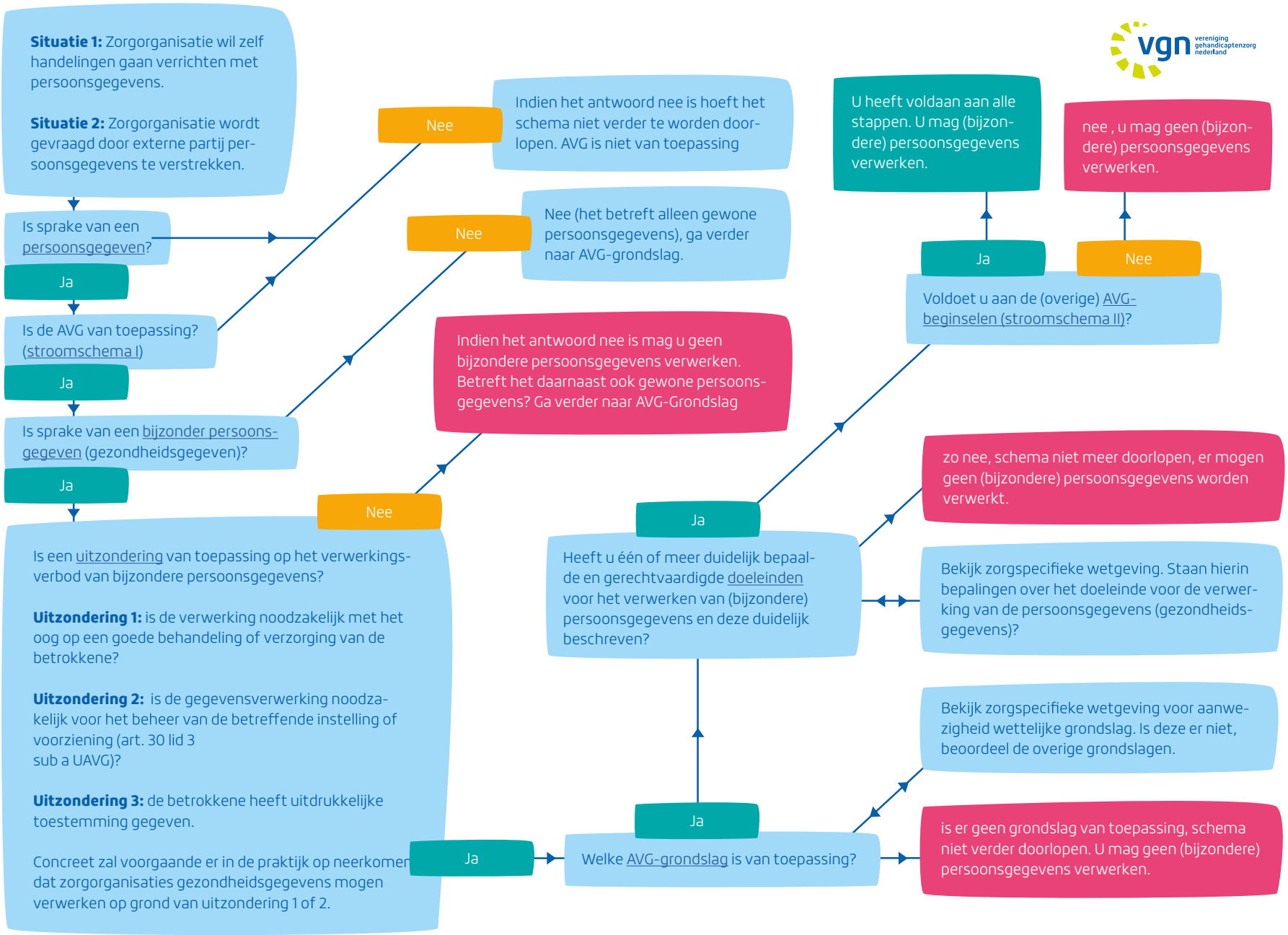
Wat is data?

Onder data in de gehandicaptenzorg verstaan wij digitale gegevens die doorlopend, al dan niet automatisch, worden verzameld via verschillende technologieën. Deze gegevens bevatten informatie over cliënten en over zorg- en ondersteuningsprocessen. Een ander woord voor data is het woord 'gegevens'.

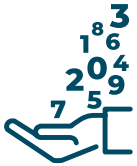
De eerste stap om te volgen

De eerste stap voor gehandicaptenzorgorganisaties die met data willen werken, is het volgen van dit stappenplan uit de VGN Handreiking Privacy (p.161). Dit helpt om te begrijpen of je gegevens mag verwerken. Vervolgens beantwoorden we enkele veelvoorkomende vragen uit de praktijk die je wellicht herkent.

Toelichting en aandachtspunt behorend bij het stappenplan (p.162):
Bij het verwerken van (bijzondere) persoonsgegevens is het beroepsgeheim (de geheimhoudingsplicht van de zorgprofessional) relevant. Naast het feit dat er voor het verwerken van bijzondere persoonsgegevens (gezondheidsgegevens) zowel een grondslag als een uitzondering op het verwerkingsverbod moet zijn (art. 9 AVG en art. 30 UAVG) dient de zorgprofessional zijn beroepsgeheim in acht te nemen, welke slechts onder bepaalde voorwaarden doorbroken kan worden, waarna verdere verwerking kan plaatsvinden.



VGN Handreiking Privacy (p.161), bescherming van persoonsgegevens van cliënten in de gehandicaptenzorg, VGN, juli 2019



In de zorgorganisatie wordt al met data gewerkt, wat als je data nog meer wilt gaan gebruiken?

Als zorgorganisatie gebruik je al data, maar er zijn nog meer mogelijkheden om met data de zorg te verbeteren. Door data slim in te zetten, kunnen processen worden geoptimaliseerd en cliënten nog beter worden ondersteund. Het is belangrijk om als zorgorganisatie vanaf het begin goed na te denken over privacy en de regels van de Algemene verordening gegevensbescherming (AVG). Dit betekent dat je vooraf onderzoek doet, je Privacy Officer en/of de Functionaris Gegevensbescherming erbij betrekt en zorgvuldig afweegt wat wettelijk en ethisch verantwoord is. Op deze manier bescherm je de privacy van zowel cliënten als medewerkers en til je de zorg naar een hoger niveau voor de toekomst.

Hoe houd je rekening met de privacy van cliënten in data-projecten?

Als zorgorganisatie is het belangrijk om verantwoord en zorgvuldig om te gaan met de persoonsgegevens van cliënten, zeker wanneer je met data-projecten werkt of dat in de toekomst wilt gaan doen, bijvoorbeeld met kunstmatige intelligentie (AI). Een goede eerste stap is het uitvoeren van een risicoanalyse, ook wel Data Protection Impact Assessment (DPIA) genoemd, nog voordat een data-project van start gaat. Hiermee krijg je een duidelijk overzicht van welke persoonsgegevens je wilt verwerken en voor welke doelen. In de zorg gaat dit vaak om gevoelige informatie, zoals gezondheidsgegevens. Dit zijn bijzondere persoonsgegevens en het is daarom belangrijk om deze extra zorgvuldig te behandelen.

Als gegevens eerder voor een ander doel zijn verzameld, kun je deze niet zomaar opnieuw gebruiken. Het is verstandig om altijd te controleren of het verwerken en gebruik van deze persoonsgegevens in het nieuwe project is toegestaan. Zelfs het anonimiseren van persoonsgegevens voor het verdere gebruik is een verwerkingshandeling. Je kunt intern laten beoordelen door de PO of FG of het is toegestaan door, te controleren of er een grondslag voor is, of dat laten doen door een andere expert, zodat je zeker weet dat je binnen de regels blijft.

Ook al kan een data-project, zeker met nieuwe technologieën zoals AI, veel opleveren voor de zorg in de toekomst, je moet altijd goed afwegen of dit voordeel opweegt tegen de mogelijke gevolgen voor de privacy van de cliënten en andere betrokkenen zoals medewerkers. De AVG stelt dat je hier zorgvuldig mee moet omgaan, maar naast de wet is het soms ook vanuit een ethisch oogpunt niet verantwoord om bepaalde gegevens te gebruiken.

Privacy-vriendelijke oplossingen integreren

Om ervoor te zorgen dat persoonsgegevens altijd voldoende beschermd blijven, is het goed om al vroeg in het proces te onderzoeken welke impact een data-project heeft op de betrokkenen en welke maatregelen je kunt nemen om deze bescherming te waarborgen. Door deze stappen vooraf te nemen, kun je makkelijker privacyvriendelijke oplossingen direct in het project integreren, zoals het principe van ‘privacy by design’. Dit betekent dat privacy een vast onderdeel is van je werkwijze. Dit betekent dat de organisatie systemen privacyvriendelijk moet ontwikkelen, inrichten en inzetten. Het helpt ook om het hele team vanaf het begin bewust te maken van het belang van privacy, zodat je tijdens het project samen kunt

inspelen op eventuele veranderingen die nieuwe privacyrisico's met zich meebrengen.

Waar moet je nog meer op letten bij gebruik van data in de zorg?

Bij het gebruik van data binnen een zorgorganisatie is het belangrijk om de belangen van cliënten altijd centraal te stellen. Naast de AVG, die vereist dat je betrokkenen goed informeert, spelen ook specifieke cliëntenrechten een rol. Denk aan het recht van cliënten om inzage te hebben in hun cliëntendossiers en dat zij goed geïnformeerd zijn wanneer je om toestemming vraagt voor het gebruik van hun data. Het is belangrijk dat cliënten expliciet geïnformeerde specifieke toestemming geven. Toestemming is alleen geldig als de client weet welke gegevens met welke doel door wie worden verwerkt, en daar expliciet toestemming voor geeft. De toestemming mag ook mondeling worden gegeven, maar moet worden vastgelegd zodat de organisatie later kan aantonen dat de toestemming is verkregen. Daarnaast is het raadzaam om bij complexe vraagstukken altijd ethische afwegingen te maken.

Wet- en regelgeving in de zorg

Naast de AVG zijn er verschillende andere wetten binnen de zorg waarmee je rekening moet houden, zoals:

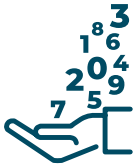
- Jeugdwet
- Wet aanvullende bepalingen verwerking persoonsgegevens in de zorg (Wabvpz)
- Wet op de geneeskundige behandelingsovereenkomst (WGBO)
- Wet kwaliteit, klachten en geschillen zorg (Wkkgz)
- Wet langdurige zorg (Wlz)
- Wet maatschappelijke ondersteuning (Wmo 2015)
- Wet marktordening gezondheidszorg (Wmg)
- Wet op de beroepen in de individuele gezondheidszorg (Wet BIG)
- Wet zorg en dwang (Wzd)
- Zorgverzekeringswet (Zvw)

Deze wetten bieden extra bescherming voor cliënten en stellen aanvullende eisen aan zorgorganisaties. Ook bepalen deze wetten en de regelgeving onder deze wetten nauwkeuriger welke gegevens onder welke voorwaarden met wie mogen of moeten worden gedeeld, juist voor beleidsbepaling.

Informatiebeveiliging: een must

Om de privacy van cliënten te waarborgen, is goede informatiebeveiliging onmisbaar. De AVG schrijft voor dat je niet alleen organisatorische, maar ook technische maatregelen treft om persoonsgegevens te beschermen en maatregelen neemt om het gedrag van mensen in overeenstemming met de regels te laten zijn. Daarnaast zijn zorgorganisaties verplicht om te voldoen aan de NEN 7510, NEN 7512 en NEN 7513. Dit betekent dat je samenwerking nodig hebt tussen verschillende afdelingen binnen de organisatie, zoals de Privacy Officer (PO), de Functionaris Gegevensbescherming (FG), de eventuele information security officer (ISO) en IT- en Security-teams. Door te zorgen voor veilige opslag en uitwisseling van gegevens, en regelmatig audits uit te voeren, kan de zorgorganisatie de veiligheid van systemen waarborgen en voldoen aan de eisen van de AVG.

Door deze stappen te volgen, zet je als zorgorganisatie belangrijke stappen richting verantwoord gebruik van data, waarbij de privacy van cliënten altijd voorop blijft staan.



Wie is binnen de zorgorganisatie verantwoordelijk voor beleid over privacy en AVG en het aantonen dat je voldoet aan de privacyregels volgens de AVG?

Als zorgorganisatie werk je dagelijks met gevoelige informatie van cliënten en medewerkers. Het is daarom belangrijk om te kunnen aantonen dat je zorgvuldig met deze gegevens omgaat en voldoet aan de privacyregels van de Algemene verordening gegevensbescherming (AVG). Dit heet de verantwoordingsplicht, ofwel accountability. Het bestuur draagt hiervoor de eindverantwoordelijkheid, maar de PO speelt een centrale rol bij het opstellen, bewaken en verbeteren van het privacy beleid. Een eventuele FG is een onafhankelijk adviseur en interne toezichthouder op het werken volgens de AVG en andere privacyregels.

Als er iets niet helemaal op orde is, is het belangrijk dit snel te signaleren en op te lossen. Door duidelijke verantwoordelijkheden vast te leggen en actief te blijven werken aan de privacy procedures, zorg je er als zorgorganisatie voor dat je niet alleen voldoet aan de wet, maar ook dat de privacy van cliënten en medewerkers goed beschermd blijft. Zo kun je met vertrouwen blijven groeien en innoveren, terwijl privacy en veiligheid altijd voorop staan.

Wie is verantwoordelijk voor de naleving van de AVG binnen de zorgorganisatie?

De AVG legt de verantwoordelijkheid bij zorgorganisaties om aan te tonen dat zij voldoen aan de privacyregels. Dit heet de verantwoordingsplicht, ofwel accountability. Maar hoe zorg je ervoor dat jouw organisatie hier goed mee omgaat, vooral als je steeds meer met data werkt en misschien zelfs naar de inzet van AI kijkt?

Het bestuur is eindverantwoordelijk voor het ontwikkelen en bewaken van het privacybeleid. In sommige gevallen is het ook nodig om een FG aan te stellen, die als onafhankelijke adviseur en interne toezichthouder fungeert. Dit helpt om ervoor te zorgen dat je als zorgorganisatie altijd goed op koers blijft, ook wanneer de organisatie zich verder ontwikkelt in het gebruik van data en nieuwe technologieën.

De AVG geeft ruimte om zelf te bepalen wie binnen de organisatie verantwoordelijk is voor de naleving van privacyregels. Wel zijn er enkele basisverplichtingen waar elke organisatie aan moet voldoen:

- Het bijhouden van een verwerkingsregister, waarin de organisatie gegevens over de verwerkingen van persoonsgegevens die zij uitvoeren overzichtelijk vastlegt.
- Het uitvoeren van een Data Protection Impact Assessment (DPIA) wanneer de zorgorganisatie nieuwe verwerkingen wil opstarten met waarschijnlijk hoge privacy risico's.
- Het onderhouden van een datalekregister, om zo transparant mogelijk te zijn over mogelijke incidenten, patronen daarin te kunnen herkennen en verbetermaatregelen in te zetten.
- Aantonen dat cliënten of andere betrokkenen daadwerkelijk toestemming hebben gegeven voor verwerkingen waarvoor dit nodig is.
- Kunnen onderbouwen of en waarom ervoor gekozen is om wel of geen FG aan te stellen, wanneer dit niet direct verplicht is.

- Een heldere privacyverklaring opstellen, die uitlegt hoe de zorgorganisatie met persoonsgegevens omgaat. Dit is niet hetzelfde als een privacy beleid; de verklaring is bedoeld voor cliënten en andere betrokkenen.

Naast deze verplichte stappen kun je ervoor kiezen om extra maatregelen te nemen, zoals het aansluiten bij een gedragscode of het opstellen van een uitgebreid privacybeleid. Dit toont aan dat je als zorgorganisatie proactief omgaat met gegevensbescherming, wat vertrouwen wekt bij cliënten en samenwerkingspartners.

Ook als een FG niet verplicht is, kan het waardevol zijn om er toch een aan te stellen. Deze persoon kan helpen om goed te adviseren over de steeds grotere rol van data binnen een zorgorganisatie, hoe die te managen en hoe toekomstige ontwikkelingen in goede banen te leiden. Veel zorgorganisaties geven een medewerker binnen de organisatie ook een rol als PO en/of geven de afdeling HR een actieve rol in het implementeren van privacybeleid. HR kan werkinstructies opstellen, trainingen organiseren en de naleving van privacyregels binnen de organisatie stimuleren. Zo zorg je ervoor dat iedereen binnen de zorgorganisatie goed weet hoe om te gaan met persoonsgegevens.

Hoe te controleren of je aan de AVG voldoet?

Het is belangrijk om te weten dat mogelijke hiaten in de naleving van de AVG risico's kunnen vormen voor cliënten, maar gelukkig kun je deze risico's goed beheersen door tijdig actie te ondernemen.

Een handige manier om te ontdekken waar verbeteringen nodig zijn, is door een privacy-audit of een privacy-nulmeting uit te voeren. Een zorgorganisatie kan dat zelf uitvoeren met interne medewerkers, of door een externe partij laten uitvoeren. Hierbij ga je stap voor stap na hoe jullie als zorgorganisatie omgaan met persoonsgegevens:

1. **Analyseren van alle persoonsgegevensverwerkingen** binnen de organisatie: het is goed om te kijken of je alle verwerkingen in beeld hebt.
2. **Controleren van de rechtmatigheid** van elke verwerking: is er een juiste grondslag voor deze verwerking?
3. **Toetsen aan de principes van dataminimalisatie en doelbinding**: wordt er alleen gewerkt met de strikt noodzakelijke gegevens en voor een duidelijk doel?
4. **Beveiligen van persoonsgegevens**: zijn er voldoende maatregelen getroffen om de gegevens te beschermen tegen verlies of ongeoorloofde toegang?

Tijdens een audit kijk je ook naar de inrichting van de organisatie. Als verantwoordelijkheden nog niet helemaal duidelijk zijn of als een FG verplicht is, maar nog niet is aangesteld, dan is dit een mooi moment om hiermee aan de slag te gaan.

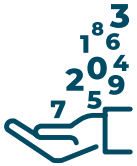
Het is ook verstandig om te checken of alle noodzakelijke documenten, zoals privacy verklaringen, het verwerkingsregister en de procedures voor datalekken en rechten van betrokkenen, up-to-date en compleet zijn.

Een andere stap is het in kaart brengen van samenwerkingen met externe partijen en de software die de zorgorganisatie gebruikt. Het is belangrijk om te weten of deze externe partijen goed omgaan met de gegevens die zij namens jullie verwerken.

Daarnaast is het waardevol om medewerkers te interviewen om te achterhalen of zij voldoende kennis hebben van de AVG om hun werk

AVG-conform te doen. Zo kun je gericht trainingen aanbieden als dat nodig blijkt.

Door deze stappen te doorlopen, krijg je een goed beeld van waar jullie als zorgorganisatie al sterk staan en waar nog verbeteringen mogelijk zijn. Dit helpt niet alleen om risico's te beperken, maar zorgt er ook voor dat je als zorgorganisatie klaar bent om verantwoord verder te groeien, bijvoorbeeld met nieuwe datatoepassingen of zelfs AI in de toekomst. Een systematische aanpak en een duidelijk verbeterplan zorgen ervoor dat je als zorgorganisatie de naleving van de AVG stap voor stap versterkt. Zo kan je als zorgorganisatie met een gerust hart data en innovatie inzetten om de zorg te verbeteren. Het kan een goede gelegenheid zijn om de privacy-audit uit te (laten) voeren tegelijkertijd met een audit voor de naleving van de NEN7510, omdat er enige overlap is tussen de normen die de NEN7510 stelt voor informatiebeveiliging en de privacy-verplichtingen uit de AVG.



Hoe vergroot je het vertrouwen in gebruik van data binnen je zorgorganisatie?

In zorgorganisaties, ook in de gehandicaptenzorg, is het belangrijk om open en eerlijk te zijn over het gebruik van persoonlijke gegevens. Door duidelijk te maken welke informatie je verzamelt, waarom je dit doet en hoe je de privacy beschermt, kun je het vertrouwen van cliënten en medewerkers vergroten. Het is ook belangrijk om hen te betrekken bij beslissingen over het gebruik van data en om de communicatie aan te passen aan hun wensen. Zo zorg je voor een veilige en betrouwbare omgeving voor iedereen die met persoonlijke gegevens werkt.

Hoe vergroot ik het vertrouwen in hoe data wordt gebruikt?

Als zorgorganisatie is het een mooie kans om door middel van data de zorg verder te verbeteren. Wanneer je zorgvuldig en transparant met persoonsgegevens omgaat, bouw je bovendien vertrouwen op bij cliënten en medewerkers. Door te laten zien hoe je data inzet om de gehandicaptenzorg te optimaliseren, versterk je dat vertrouwen.

Het is goed om open te zijn over welke gegevens je als zorgorganisatie verzamelt, en met welk doel. Dit helpt om cliënten en hun vertegenwoordigers gerust te stellen. Wanneer zij begrijpen waarom hun gegevens worden gebruikt en zien dat er netjes met hun data wordt omgegaan, zullen ze eerder bereid zijn om hieraan mee te werken. Transparantie en zorgvuldigheid staan hierbij centraal.

Cliënten in de gehandicaptenzorg hebben vaak te maken met beslissingen die voor hen worden genomen. Data-projecten zijn meestal bedoeld om de zorg als geheel te verbeteren, en minder direct voor de cliënt zelf. Daarom is het belangrijk om cliënten de ruimte te geven om te kiezen of ze willen deelnemen. Zorg ervoor dat je hen goed informeert, zodat ze een bewuste keuze kunnen maken. Wanneer een cliënt zelf niet in staat is tot het maken van de keuze is het belangrijk de wettelijk vertegenwoordiger te informeren en betrekken.

Veel organisaties verstrekken dit soort informatie via een privacyverklaring of privacyreglement (vaak op de website geplaatst), maar het kan waardevol zijn om ook andere manieren van communicatie in te zetten. Denk aan eenvoudige taal, video's, pictogrammen of gesproken teksten. Dit maakt de informatie toegankelijker, vooral voor cliënten met een beperking.

Een aandachtspunt bij het verstrekken van informatie is om goed te kijken naar wat een cliënt wél kan. Soms kan een cliënt zich moeilijk uiten, maar begrijpt hij of zij de informatie prima. De AVG vereist dat informatie voor cliënten afgestemd is op hun bevattingsniveau en makkelijk te begrijpen is.

Tot slot, als je als zorgorganisatie een nieuw data-project opstart, is het slim om cliënten en zorgprofessionals van het begin af aan te betrekken bij beslissingen over hoe persoonlijke data wordt verzameld, gebruikt en gedeeld. Dit versterkt niet alleen het vertrouwen, maar zorgt er ook voor dat je samen de beste keuzes maakt. Data is van grote waarde, en dat verdient zorgvuldige aandacht.

Bijlage

Begrippen, wetten, handige richtlijnen en hulpmiddelen over AVG voor de gehandicaptenzorg

Belangrijke begrippen

Cliënt
Een natuurlijke persoon die zorg- en/of ondersteuning of jeugdhulp ontvangt of zal gaan ontvangen.

Betrokkene
De betrokkene is degene van wie persoonsgegevens worden verwerkt. Vaak is dat de (toekomstige) cliënt. Maar soms is dit de (wettelijk) vertegenwoordiger, diegene die de cliënt vertegenwoordigt.

(Wettelijk) Vertegenwoordiger
De (wettelijk) vertegenwoordiger is de persoon die de cliënt vertegenwoordigt als de cliënt handelings- en/of wilsonbekwaam is. Er wordt onderscheid gemaakt tussen de situatie waarin de cliënt nog niet in zorg is en als de cliënt wel in zorg is. Meer lezen over dit onderscheid kan in het Model Privacy reglement van de VGN.

Data
Onder data in de gehandicaptenzorg verstaan wij digitale gegevens die doorlopend, al dan niet automatisch, worden verzameld via verschillende technologieën. Deze gegevens bevatten informatie over cliënten en over zorg- en ondersteuningsprocessen. Een ander woord voor data is het woord ‘gegevens’. Het woord ‘gegevens’ kan voor sommige cliënten makkelijker te begrijpen en herkennen zijn dan het woord ‘data’.

Persoonsgegevens
In de Algemene verordening gegevensbescherming (AVG) staat als definitie voor persoonsgegevens: ‘alle informatie over een geïdentificeerde of identificeerbare natuurlijke persoon’. Dit betekent dat informatie ofwel direct over iemand gaat, ofwel naar deze persoon te herleiden is.

Bijzondere persoonsgegevens
De AVG maakt onderscheid tussen ‘gewone’ en ‘bijzondere’ persoonsgegevens (de letterlijke term in de AVG is: ‘bijzondere categorieën van persoonsgegevens’). Bijzondere persoonsgegevens zijn gegevens die zó privacygevoelig zijn dat het grote(re) impact op iemand kan hebben als deze gegevens worden verwerkt. Daarom krijgen bijzondere persoonsgegevens extra bescherming in de AVG. Dit zijn o.a. gegevens over gezondheid, religie, ras, seksuele gerichtheid, biometrische en genetische gegevens.

Gezondheidsgegevens
Gegevens over iemands gezondheid zijn bijzondere persoonsgegevens. Deze gezondheidsgegevens staan bijvoorbeeld in een medisch dossier. Maar ook een dossier van een maatschappelijk werker of andere zorgprofessional kan zulke gegevens bevatten.

Gevoelige persoonsgegevens
De Autoriteit persoonsgegevens (AP) kent naast het onderscheid in de AVG tussen gewone en bijzondere persoonsgegevens ook nog een categorie “gevoelige” persoonsgegevens. Het gaat dan om gegevens waarmee gemakkelijk identiteitsfraude of financiële fraude kan worden gepleegd. Deze gevoelige gegevens vragen dus ook om extra bescherming. Bijvoorbeeld: gegevens over elektronische communicatie, locatiegegevens, financiële gegevens (bankrekeningnummer, creditcardgegevens maar ook gegevens over betaalgedrag) , het BSN en

gegevens over het identiteitsbewijs van een betrokkene of een kopie van het identiteitsbewijs.

Verwerkingen

Een verwerking van persoonsgegevens is alles wat een organisatie met persoonsgegevens kan doen, van verzamelen tot en met vernietigen.

Persoonsgegevens verwerken – wat is hiervoor nodig?

1. **Grondslag**: Je mag alleen persoonsgegevens verwerken als het echt niet anders kan. Dus: als zonder deze gegevens het doel niet bereikt kan worden. In de Algemene verordening gegevensbescherming (AVG) staan 6 redenen genoemd. De juridische naam voor die redenen is 'grondslagen'. Een grondslag is nodig om persoonsgegevens te mogen verwerken.

2. **Uitzonderingsgrond**: De verwerking van bijzondere persoonsgegevens, dus ook van gezondheidsgegevens, is in principe verboden tenzij er een uitzondering van toepassing is op het verwerkingsverbod. In de AVG staan een aantal uitzonderingen op dit verbod. Gezondheidsgegevens verwerken mag bijvoorbeeld als dat noodzakelijk is om iemand goede zorg of hulp te verlenen. In de Nederlandse Uitvoeringswet AVG staan nog een paar extra uitzonderingen (artikel 30 UAVG).

3. **Beroepsgeheim**: Bij het verwerken van gezondheidsgegevens is het beroepsgeheim (de geheimhoudingsplicht van de zorgprofessional) erg belangrijk. Naast het feit dat voor het verwerken van bijzondere persoonsgegevens (gezondheidsgegevens) zowel een grondslag als een uitzondering op het verwerkingsverbod van toepassing moet zijn dient de zorgprofessional zijn (afgeleide) beroepsgeheim in acht te nemen. Slechts onder bepaalde voorwaarden kan de zorgprofessional dat beroepsgeheim doorbreken en gezondheidsgegevens aan anderen verstrekken.

Persoonsgegevens verwerken – aan welke basisprincipes (beginselen) moet dat voldoen?

De AVG G kent 6 basisprincipes voor de verwerking van persoonsgegevens, in de AVG 'beginselen' genoemd. Iedereen die persoonsgegevens verwerkt, moet zich hieraan houden. En dit kunnen aantonen, dat heet de verantwoordingsplicht. De 6 AVG-beginselen zijn:

1. **Rechtmatigheid**: Behoorlijkheid en transparantie: om rechtmatig te zijn, moet een verwerking in elk geval zijn gebaseerd op een grondslag uit de AVG. Maar ook mag de verwerking niet in strijd zijn met andere wetgeving, zoals een wettelijke geheimhoudingsplicht. De verwerking moet ook 'behoorlijk' zijn. Dat betekent dat de verwerking niet (op een niet te rechtvaardigen manier) nadelig, discriminerend, onverwacht of misleidend mag zijn voor de betrokkenen. Verder moet het transparant zijn voor betrokkenen hoe en waarom een organisatie hun persoonsgegevens verwerkt. Dat betekent dat de organisatie hier open en duidelijk over moet communiceren. Verder moet het transparant zijn voor betrokkenen hoe en waarom een organisatie hun persoonsgegevens verwerkt. Dat betekent dat de organisatie hier open en duidelijk over moet communiceren.

2. **Doelbinding**: Organisaties mogen persoonsgegevens alleen verzamelen met een gerechtvaardigd doel. Dat doel moet specifiek zijn en vooraf uitdrukkelijk zijn omschreven. Organisaties mogen dus niet alvast persoonsgegevens gaan verzamelen omdat die misschien ooit van pas gaan komen. De organisatie mag de gegevens niet ineens voor een ander doel gaan verwerken.

3. **Dataminimalisatie**: Een organisatie mag niet meer persoonsgegevens verwerken dan strikt noodzakelijk is voor het doel waarvoor die gegevens worden verwerkt. Dit wordt 'dataminimalisatie' genoemd.

4. **Juistheid**: Organisaties moeten ervoor zorgen dat de gegevens juist zijn. En de gegevens actualiseren als dat nodig is. Mensen kunnen ook aan organisaties vragen hun persoonsgegevens aan te passen als die niet kloppen.

5. **Opslagbeperking**: Organisaties moeten persoonsgegevens verwijderen zodra die niet langer nodig zijn voor het oorspronkelijke doel waarvoor ze zijn verzameld. Organisaties mogen gegevens dus maar een bepaalde tijd bewaren.

6. **Vertrouwelijkheid en integriteit**: Organisaties moeten hun gegevensverwerkingen goed beveiligen. Er gelden extra strenge regels voor bijzondere persoonsgegevens.

Informed consent

Voor het ontstaan van een behandelingsovereenkomst inzake geneeskundige behandeling is het noodzakelijk dat de cliënt instemt met de voorgestelde geneeskundige behandeling. De informatieplicht van de behandelaar en het instemmingsvereiste vormen een twee-eenheid. Dit wordt ook wel 'informed consent' genoemd. Informed consent vloeit o.a. voort uit de Wet op de geneeskundige behandelings- overeenkomst (WGBO). De leden van de VGN passen de WGBO analoog toe.
Zie de richtlijn Wgbo.

Toestemming

Voor het doorbeken van het beroepsgeheim en het verstrekken van informatie (bijzondere persoonsgegevens) over een cliënt aan anderen, die niet rechtstreeks betrokken zijn bij de uitvoering van de geneeskundige behandelingsovereenkomst, is toestemming nodig van de cliënt. Die toestemming moet geïnformeerde, specifieke en in vrijheid gegeven toestemming zijn. Dat betekent dat cliënt moet weten welke persoonsgegevens (informatie) over hem/haar aan wie, voor welk doel worden verstrekt. Een model toestemmingsformulier is beschikbaar voor download.

Verwerker

De verwerker verwerkt persoonsgegevens in opdracht van en voor een andere organisatie, de opdrachtgever. De verwerker gebruikt de persoonsgegevens niet voor eigen doeleinden. De opdrachtgever neemt de belangrijke beslissingen en is de verwerkingsverantwoordelijke. De verwerkingsverantwoordelijke moet zorgen dat de verwerker ook aan de eisen van de AVG voldoet. Daarom sluit de verwerkingsverantwoordelijke met de verwerker een verwerkersovereenkomst waarin dat is vastgelegd. Hier vind je een link naar het model verwerkersovereenkomst van de BoZ, waarvan VGN onderdeel is.

Verwerkingsverantwoordelijke

Verwerkt de ene organisatie de persoonsgegevens voor eigen doeleinden, op basis van een eigen grondslag (geldige reden)? Dan neemt die organisatie wel belangrijke beslissingen en is die organisatie daarvoor dus ook de verwerkingsverantwoordelijke.

Overige begrippen

AI

Artificial intelligence. Kunstmatige intelligentie. AI is de mogelijkheid van een machine om mensachtige vaardigheden te vertonen - zoals redeneren, leren, plannen en creativiteit.

Anonimisering van gegevens

Bij anonimiseren worden de persoonsgegevens op zo'n manier aangepast dat ze niet meer herleidbaar zijn tot een individueel persoon, ook niet door ze te combineren met andere gegevens.

Compliance
Compliance binnen de zorg voor het werken met data is het voldoen aan de eisen die worden gesteld door wet- en regelgeving op gebied van o.a. het gezondheidsrecht, privacybescherming en informatiebeveiliging.

Data governance
Data governance betreft alle afspraken en spelregels waarmee je onder andere vastlegt hoe je van alle data gebruik wilt maken, wat de doelen ermee zijn, hoe je de kwaliteit waarborgt hoe lang deze wordt bewaard, wie toegang heeft en wanneer de data wordt verwijderd en hoe de veiligheid geregeld wordt.

Datalek (inbreuk)
Bij een datalek gaat het om toegang tot persoonsgegevens zonder dat dit mag of zonder dat dit de bedoeling is. Waarbij de oorzaak een inbreuk op de beveiliging van deze gegevens is. Ook het ongewenst vernietigen, verliezen, wijzigen of verstrekken van persoonsgegevens door zo'n inbreuk valt onder een datalek.

DPIA
Data Protection Impact Assessment (DPIA). Een DPIA is een instrument om vooraf de privacyrisico's van een gegevensverwerking in kaart te brengen, zodat de organisatie maatregelen kan nemen om deze risico's te verkleinen.

Functionaris Gegevensbescherming (FG)
Een Functionaris Gegevensbescherming (FG) houdt binnen een organisatie toezicht op en adviseert over de toepassing en naleving van de privacywetgeving.

NEN 7510 normen
NEN 7510-1 en NEN 7510-2 zijn normen die eisen stellen en handvatten geven aan organisaties op het aspect van informatiebeveiliging in de zorg.

PDCA-cyclus
De Plan-Do-Check-Act methode is een methode om stapsgewijs het werk en processen te verbeteren. Deze verbetermethode wordt de PDCA-cyclus genoemd.

Privacy Officer (PO)
De Privacy Officer (PO) helpt de organisatie bij het naleven van de AVG en andere regels op het gebied van privacy en informatiebeveiliging. Een PO geeft advies en biedt ondersteuning in de uitvoering, geeft interne trainingen en heeft een rol bij het onderzoeken en melden van datalekken.

Privacy by Design
Privacy by Design houdt in dat al bij het ontwerpen van producten en diensten privacybescherming en informatieveiligheid van persoonsgegevens het uitgangspunt is.

Privacy by Default
Privacy by Default houdt in dat de standaardinstellingen van een product of dienst (bijvoorbeeld een mobiele telefoon) privacy vriendelijk zijn.

Pseudonimisering
Pseudonimiseren is niet hetzelfde als anonimiseren. Bij gepseudonimiseerde gegevens is weliswaar niet direct duidelijk over welke personen de gegevens gaan, maar de gegevens kunnen alsnog herleidbaar zijn tot specifieke personen door aanvullende gegevens met elkaar te combineren.

Handige richtlijnen en hulpmiddelen over AVG voor de gehandicaptenzorg

Er zijn verschillende richtlijnen en hulpmiddelen beschikbaar die de naleving van de AVG binnen de gehandicaptenzorg makkelijker maken.

- Een van de meest praktische hulpmiddelen in Nederland is de Handreiking Privacy van de Vereniging Gehandicaptenzorg Nederland (VGN). Deze handreiking biedt een duidelijke vertaalslag van de wettekst naar de dagelijkse praktijk.
- Aanvullend hierop zijn enkele handige hulpmiddelen beschikbaar: het herziene model privacyreglement van de VGN, het herziene model toestemmingsformulier van VGN en tot slotte de BoZ model verwerkersovereenkomst.
- De Autoriteit Persoonsgegevens biedt niet alleen algemene informatie over de AVG, maar heeft ook secties die specifiek gericht zijn op de zorgsector.
- Op de website van de Rijksoverheid kunnen organisaties snel informatie vinden over de rechten van cliënten en privacy kwesties die relevant zijn voor hun dagelijkse werkzaamheden.
- Een nuttig hulpmiddel is de AVG-Helpdesk voor Zorg, Welzijn en Sport, waar organisaties praktische informatie en antwoorden op veel gestelde vragen kunnen vinden.
- De herziene KNMG-richtlijn Omgaan met medische gegevens biedt artsen duidelijke handvatten voor het zorgvuldig en verantwoord verwerken van medische gegevens, in lijn met de vereisten van de Wgbo (wet geneeskundige behandelingsovereenkomst). Deze richtlijn is ook relevant voor de gehandicaptenzorg.
- Op het Kennisplein Gehandicaptensector zijn antwoorden op veel gestelde vragen te vinden over het thema medisch beroepsgeheim en privacy.

Relevante wetgeving voor privacybescherming en informatiebeveiliging in de zorgsector

AI Verordening

Artificial Intelligence Verordening. Op 21 mei 2024 heeft de Europese Raad goedkeuring gegeven aan de AI Act. Doel van de wet is het bevorderen van de ontwikkeling en invoering van veilige en betrouwbare AI-systemen op de interne markt van de Europese Unie (EU). Door zowel private als publieke partijen. Daarnaast is het doel de grondrechten van EU-burgers te beschermen en innovatie op het gebied van AI in Europa te stimuleren. Zo moeten bijvoorbeeld eerst de gevolgen voor grondrechten van mensen worden beoordeeld, voordat een AI-systeem met een hoog risico wordt ingevoerd.

AVG

Algemene verordening gegevensbescherming. De AVG is sinds 25 mei 2018 van toepassing in de hele Europese Unie (EU) en geldt voor iedereen die persoonsgegevens verwerkt

Jeugdwet

De Jeugdwet is bedoeld voor kinderen, jongeren en ouders die hulp nodig hebben bij het opgroeien of opvoeden.

MDR

Medical Device Regulation. Europese regelgeving voor medische hulpmiddelen. Het doel is om veilig gebruik van medische hulpmiddelen te garanderen.

Wabvpz

Wet aanvullende bepalingen verwerking persoonsgegevens in de zorg.

Wet BIG
Wet op de beroepen in de individuele gezondheidszorg. De Wet BIG is er om te zorgen dat de kwaliteit van onze gezondheidszorg hoog is en blijft. Ook beschermt de Wet BIG patiënten tegen ondeskundig en onzorgvuldig handelen van zorgprofessionals.

WGBO
Wet op de geneeskundige behandelingsovereenkomst regelt de rechten en plichten van zowel cliënten als zorgprofessionals.

Wkkgz
Wet kwaliteit, klachten en geschillen zorg. Dit gaat o.a. over het verwerken van gezondheidsgegevens voor kwaliteit van zorg en de afhandeling van klachten.

Wlz
Wet langdurige zorg. Deze wet regelt zware, intensieve zorg voor kwetsbare ouderen, mensen met een handicap en mensen met een psychische aandoening die 24 uur per dag zorg in de nabijheid nodig hebben of permanent toezicht.

WMG
Wet Marktordening Gezondheidszorg. Het doel van de Wet Marktordening Gezondheidszorg (WMG) is meer concurrentie te krijgen in de zorg. Het belang van de cliënt staat hierbij voorop.

Wmo 2015
Wet maatschappelijke ondersteuning 2015. Gemeenten moeten zorgen voor het ondersteunen van de zelfredzaamheid en participatie van mensen met een beperking, chronische psychische of psychosociale problemen. De ondersteuning moet erop gericht zijn dat mensen zo lang mogelijk thuis kunnen blijven wonen. De gemeente geeft ondersteuning thuis maar levert ook beschermd wonen en opvang.

Wzd
Wet zorg en dwang. De Wet zorg en dwang regelt de rechten en verplichtingen van cliënten, zorgaanbieders en zorgprofessionals bij onvrijwillige zorg of onvrijwillige opname van mensen met een verstandelijke beperking en mensen met een psychogeriatrische aandoening (zoals dementie).

UAVG
Uitvoeringswet Algemene Verordening Gegevensbescherming. De UAVG is de Nederlandse wet die de Algemene Verordening Gegevensbescherming (AVG) uitvoert.

Zvw
Zorgverzekeringswet. Het zorgstelsel in Nederland wordt geregeld met vier stelselwetten: de Zorgverzekeringswet (Zvw), de Wet langdurige zorg (Wlz), de Wet maatschappelijke ondersteuning (Wmo) en de Jeugdwet.

Toezicht autoriteiten op gebied van AVG

AP
Autoriteit Persoonsgegevens. Nederlandse toezichtorganisatie op gebruik van data.

EDPB
European Data Protection Board. Een onafhankelijk Europees orgaan dat erop toeziet dat de Algemene verordening gegevensbescherming consequent wordt toegepast en dat de samenwerking tussen de gegevensbeschermingsautoriteiten van de EU bevordert.

Colofon

Redactie
Ellen van den Broek en Suzan Vlaming

Met dank aan
Juristen Maria Pereira en Alexandra Reijerse voor het opstellen van de teksten
Juristen van de Vereniging Gehandicaptenzorg Nederland (VGN) voor het meelezen

Disclaimer
De reikwijdte van de AVG en de specifieke wet- en regelgeving op het gebied van privacy voor de zorgsector is complex en veelomvattend. Deze publicatie geeft de antwoorden van onafhankelijke juristen op vragen over AVG en privacy in relatie tot het gebruik van data in de gehandicaptenzorg. Deze publicatie weerspiegelt de stand van wetgeving en jurisprudentie ten tijde van het moment van publicatie (december 2024).

Over het programma
Deze publicatie is gemaakt in het programma 'Leren Werken met Data in de gehandicaptenzorg', dat wordt uitgevoerd door Academy Het Dorp en Academische Werkplaats ZorgTechnologie in de Gehandicaptenzorg (ZoTeG), met financiering van het ministerie van VWS. Het is onderdeel van de Toekomstagenda 'Zorg en ondersteuning van mensen met een beperking' (2023-2026). Over 'data' in de Toekomstagenda:

"We willen dat de gehandicaptensector meer inzicht krijgt in de effecten van het gebruik van data op de kwaliteit van zorg en ondersteuning, zodat zorgaanbieders bewuster kunnen kiezen voor de wijze waarop zij data gebruiken om de zorg te optimaliseren."

Voor meer informatie, bezoek de website www.lerenwerkenmetdata.nl.

Bronvermelding
Alle informatie uit deze publicatie mag overgenomen worden, mits met juiste bronvermelding:
Van den Broek, E., & Vlaming, S. (Reds.). (2024). AVG en privacy rondom data in de gehandicaptenzorg: Wie heeft welke verantwoordelijkheid en hoe zorg je voor vertrouwen? Arnhem: Leren Werken met Data in de gehandicaptenzorg/Academische Werkplaats ZoTeG.

Kemperbergerweg 139e
6816 RP Arnhem
www.academyhetdorp.nl
Contact: data@academyhetdorp.nl

ACADEMY HET DORP

Ministerie van Volksgezondheid, Welzijn en Sport

Academische Werkplaats ZoTeG
ZorgTechnologie in de Gehandicaptenzorg