



Leren Werken
met Data
in de gehandicaptenzorg

AVG en privacy rondom data
in de gehandicaptenzorg

Vorbereiden op een toekomst met data en AI

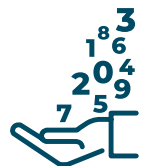


Deze publicatie bestaat uit vier delen en is tot stand gekomen na een uitvraag over 'AVG en privacy' en het gebruik van data in gehandicaptenzorgorganisaties. De gestelde vragen zijn vervolgens door enkele juristen beantwoord. Zij hebben de vragen beantwoord vanuit het perspectief van gehandicaptenzorgorganisaties. 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.



Voorwoord	2
Wat je eerst moet weten	4
Wat is data?	4
De eerste stap om te volgen	4
Wat als je als gehandicaptenzorgorganisatie ook iets met AI wilt gaan doen?	6
Mag AI gebruikt worden om de zorg te optimaliseren?	6
Wat zegt de AVG over gebruik van AI?	8
Wat zijn de specifieke AVG-uitdagingen bij het gebruik van AI in de zorg?	9
Wie is verantwoordelijk als een AI-systeem een verkeerde beslissing neemt die invloed heeft op de zorg of privacy van een cliënt?	9
Hoe kunnen zorgorganisaties zich voorbereiden op de toekomst in het werken met data?	10
Hoe kan je als zorgorganisatie proactief inspelen op veranderingen in de privacywetgeving?	10
Hoe kan je als zorgorganisatie periodiek controleren of de dataverwerking nog steeds voldoet aan de AVG?	11
Wat zijn de ontwikkelingen op het gebied van privacy en datagebruik in de zorgsector?	11
Bijlage	13
Belangrijke begrippen	13
Overige begrippen	15
Handige richtlijnen en hulpmiddelen over AVG voor de gehandicaptenzorg	17
Relevante wetgeving voor privacybescherming en informatiebeveiliging in de zorgsector	17
Toezicht autoriteiten op gebied van AVG	18
Colofon	19



Wat je eerst moet weten

Wat is data?

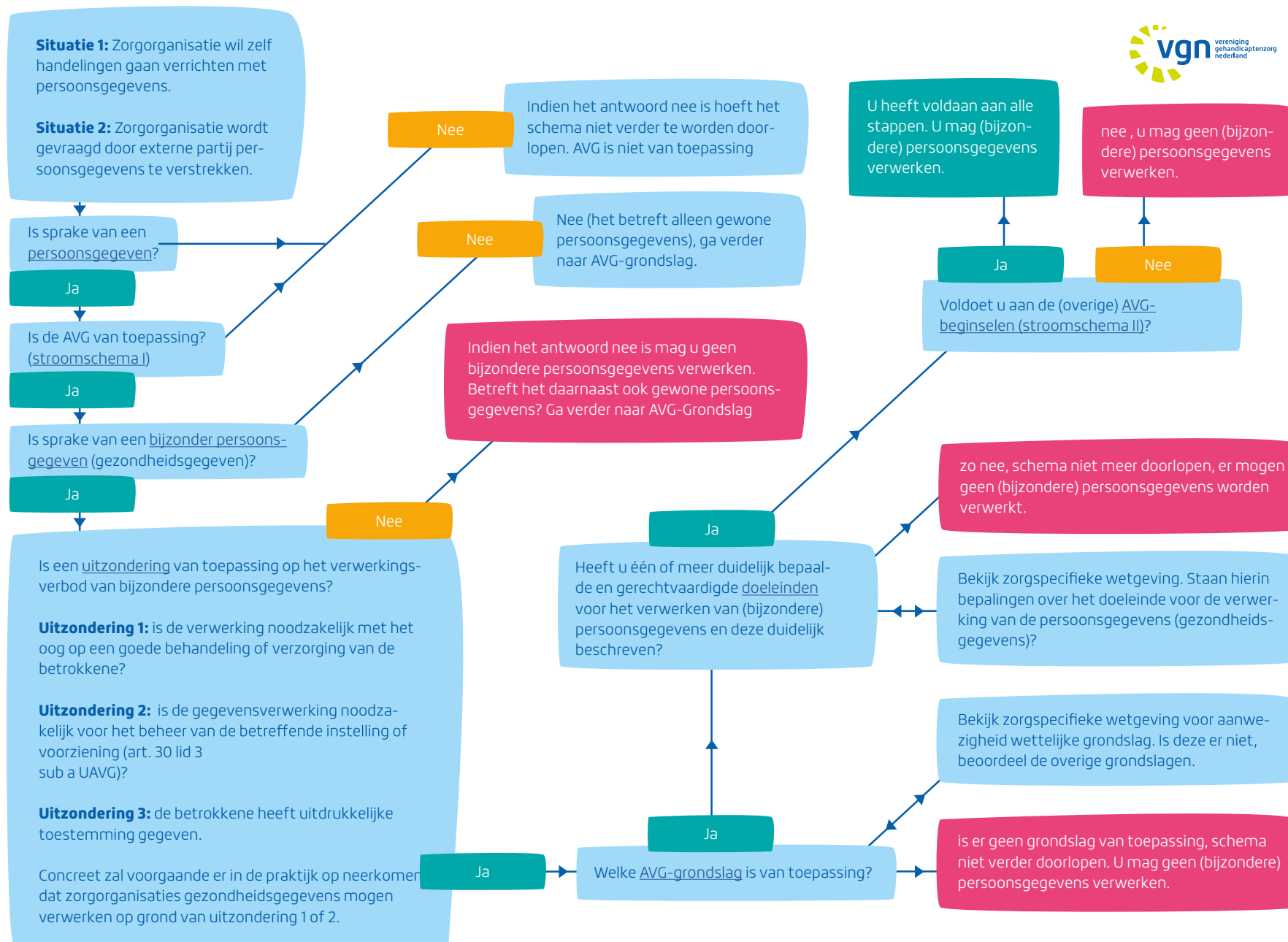
Onder [data in de gehandicaptenzorg](#) verstaan wij digitale gegevens die doorlopend, al dan niet automatisch, worden verzameld via verschillende technologieën. Deze gegevens bevatten informatie over cliënten en over zorg- en ondersteuningsprocessen. Een ander woord voor data is het woord 'gegevens'.

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



Wat als je als gehandicapten-zorgorganisatie ook iets met AI wilt gaan doen?

AI (kunstmatige intelligentie) biedt mooie kansen om de zorg in de gehandicaptensector te verbeteren. Hoe zorgorganisaties AI op een verantwoorde en effectieve manier kunnen inzetten is nog volop in onderzoek en ontwikkeling. Het is belangrijk om vanaf de start van het AI-gebruik goed om te gaan met wet- en regelgeving over AI en over privacy. Denk aan de AI Verordening, de Algemene verordening gegevensbescherming (AVG), specifieke privacyregels voor de zorgsector en het beroepsgeheim. Door duidelijke doelen te stellen en cliënten, medewerkers en andere betrokkenen vanaf het begin mee te nemen, kun je een goede start maken.

Om AI veilig te gebruiken, is het goed om te letten op mogelijke risico's. Voordat een zorgorganisatie een product of dienst kan inzetten waar AI een onderdeel van is, moet de organisatie bepalen of het volgens de AI Verordening gaat om een systeem met een hoog risico. Als dat zo is, dan moet het product waarin AI wordt toegepast zelf aan allerlei eisen voldoen maar ook de manier waarop het product of de dienst door de zorgorganisatie wordt ingezet. Zorg dat de data die je gebruikt voldoet aan de AVG- en andere privacyregels, gebruik bijvoorbeeld geanonimiseerde gezondheidsgegevens en verzamel alleen wat echt nodig is. Het anonimiseren van gezondheidsgegevens is ook een verwerking waarvoor een grondslag en een uitzonderingsgrond noodzakelijk zijn. Tenslotte moet ook aan de regels over het beroepsgeheim worden voldaan.

Mag AI gebruikt worden om de zorg te optimaliseren?

Het gebruik van AI in de zorg biedt veel mogelijkheden en roept ook vragen op. Of een specifiek project haalbaar is en hoe de AI Verordening, de AVG en ander privacyregels voor de zorg (inclusief het beroepsgeheim) hierop van toepassing zijn, hangt af van de aard van het project. Dit verschilt per situatie en vereist een zorgvuldige afweging en soms extra maatregelen. Als zorgorganisatie is het belangrijk om vooraf helder te hebben wat je met AI wilt bereiken. Stel in de organisatie een team samen dat zich gaat bezighouden met de inzet en toepassingen van AI. Maak ook heldere afspraken over wie waarvoor verantwoordelijk is. Zorg ervoor dat er in dat groepje zowel zorginhoudelijke medewerkers en andere medewerkers die met het product of systeem moeten werken, als IT-medewerkers en privacy-deskundigen deelnemen. Raadpleeg eventueel een jurist. Dit helpt bij het vaststellen van het (juridisch) kader en geeft inzicht in de mogelijkheden.

De AI Verordening is altijd van toepassing. Het doel van de verordening is dat AI-systemen die organisaties (binnen de EU) gebruiken, veilig zijn en fundamentele rechten van betrokkenen respecteren. Het maakt niet uit of die AI-systemen binnen of buiten de EU zijn ontwikkeld. AI-systemen worden onderverdeeld in verschillende risicocategorieën. Afhankelijk van de categorie waarin een AI-systeem valt, gelden zwaardere, minder zware of geen regels. De AI Verordening is al van kracht maar sommige regels gaan pas over enige tijd in werking om de leveranciers de tijd te geven hun producten en diensten aan te passen aan die regels. Het kan een (groot) risico voor zorgorganisaties opleveren als ze nu producten en diensten inzetten waarin al wel AI-systemen zijn toegepast, maar die nog niet voldoen aan de eisen uit de AI Verordening. Vooraf een goede risico-inventarisatie uitvoeren is dus noodzakelijk. AI-toepassingen in medische hulpmiddelen (bijvoorbeeld in alarmsystemen of in

medische software) zijn in elk geval systemen met een hoog risico. Voor medische hulpmiddelen geldt daarnaast nog de Verordening Medische Hulpmiddelen (Medical Device Regulation of MDR).

Voorbeelden van AI-toepassingen in de zorg:

- AI kan ingezet worden om grote hoeveelheden data te analyseren, wat kan bijdragen aan betere kwaliteitsanalyses;
- AI kan helpen bij het ontwikkelen van modellen voor deze analyses;
- Het is ook mogelijk om de ontwikkelde AI-modellen daadwerkelijk in te zetten in de praktijk;
- AI kan daarnaast (medische of handelings)adviezen geven aan zorgprofessionals of cliënten.

En er zijn nog veel meer toepassingen te bedenken.

Afhankelijk van het type AI-project kan de AVG een grotere of kleinere rol spelen. Ook de zorgspecifieke wetgeving (zoals de Wet op de Geneeskundige Behandelingsovereenkomst (WGBO), de Wet kwaliteit, klachten en geschillen zorg (Wkkgz) en aansprakelijkheids- en ethische vraagstukken, zijn belangrijke aspecten om mee te nemen.

Realiseer je dat het gebruik van een openbaar beschikbare AI-chatbots voor het maken van verwijsbrieven of het samenvatten van grotere hoeveelheden tekst over cliënten, meestal een schending van het beroepsgeheim oplevert als die gegevens direct of indirect te koppelen zijn aan een individueel persoon. De zorgorganisatie verstrekt immers individuele gezondheidsgegevens aan de leveranciers die de AI-chatbots ter beschikking stellen. Deze leveranciers slaan de ingevoerde gegevens meestal op om die te gebruiken ter verbetering en verdere ontwikkeling van de AI-chatbot. Vaak zonder dat duidelijk is wat die bedrijven precies met deze gegevens gaan doen. Ook heeft de zorgorganisatie dan geen verwerkersovereenkomst met die tech-bedrijven om te zorgen dat zij zich aan de verplichtingen uit de AVG houden.



Tip:

Laat je als zorgorganisatie niet weerhouden om met AI te starten. Wel is het verstandig om een goed doordacht plan te maken, zodat het project soepel verloopt en niet in een later stadium vastloopt op juridische aspecten. Dit voorkomt onnodige investeringen en zorgt voor een betere basis.

Wat zegt de AVG over gebruik van AI?

De AVG geldt voor persoonsgegevens. Wanneer AI geen persoonsgegevens verwerkt, is de AVG strikt genomen niet van toepassing.



Tip:

Beschouw de AVG bij AI-projecten als een nuttige leidraad voor het veilig en verantwoord opzetten van een project. Zeker in de zorg, waar vaak gewerkt wordt met gevoelige persoonsgegevens, is dit een waardevolle aanpak.

Hier zijn enkele belangrijke punten uit de AVG die relevant kunnen zijn:

- De AVG bevat beginselen die voorwaarden stellen aan de manier van omgaan met persoonsgegevens en een grondslag voor de verwerking is noodzakelijk. Daarnaast moet voor de ontvanger van gezondheidsgegevens een uitzonderingsgrond op het verwerkingsverbod van toepassing zijn om gezondheidsgegevens te mogen verwerken. Houd deze voorwaarden bij elk AI-project in gedachten.
 - Alle persoonsgegevens die verkregen zijn van en over cliënten, zijn bijzondere persoonsgegevens. Daarvoor gelden dus naast de AVG-verplichtingen ook andere verplichtingen uit de privacyregels voor de zorgsector, zoals regels over het elektronisch delen van gezondheidsgegevens (Wabvpz) en over het beroepsgeheim (WGBO);
 - Zorgdata die geen persoonsgegevens zijn kunnen gebruikt worden in AI-systemen voor andere zorgdoelen dan zorg leveren zoals wetenschappelijk onderzoek, innovatie, beleidsvorming. Dat heet secundair gebruik. NB: Ook hier geldt dat het anonimiseren van persoonsgegevens een aparte verwerkingshandeling is waarvoor de zorgorganisatie een grondslag én uitzonderingsgrond moet hebben. Daarnaast moet voldaan zijn aan de regels over het beroepsgeheim.
- Secundair gebruik van bijzondere persoonsgegevens over de behandeling van een specifieke cliënt om AI-modellen te trainen ter verbetering van de zorg, is in zijn algemeenheid niet toegestaan zonder voorafgaande geïnformeerde toestemming van de cliënt. Voor aanbieders van AI-systemen kent de AI Verordening enkele bij uitzonderingen voor specifieke doelen onder strikte voorwaarden (art. 10 lid 5 AI Verordening).
 - Het uitvoeren van een Data Protection Impact Assessment (DPIA) is aan te raden bij AI-projecten, zelfs als het niet verplicht is. De vragen die bij een DPIA gesteld worden, helpen om risico's in kaart te brengen en kunnen bijdragen aan een veiliger en beter project. Dit vergroot de acceptatie van AI binnen de zorgorganisatie en bij cliënten.
 - Wees transparant over wat je wilt doen en waarom;
 - Een punt van aandacht is ook het voldoen aan de AVG-beginselen van opslagbeperking en het niet langer bewaren van persoonsgegevens dan voor het doel noodzakelijk. Het is vaak mogelijk om zonder kopieën te werken en de opslagduur van tot de persoon herleidbare gegevens kan vaak ook worden beperkt door te anonimiseren zodra het kan. Zoek waar mogelijk naar alternatieve oplossingen en stel jezelf de vraag: Kan het ook anders?

Wat zijn de specifieke AVG-uitdagingen bij het gebruik van AI in de zorg?

Er zijn verschillende uitdagingen bij het gebruik van AI in de zorg, waaronder:

- Het duidelijk afbakenen van de doelen van het AI-project;
- Het op tijd betrekken van alle relevante stakeholders, waaronder de Privacy Officer (PO), Functionaris Gegevensbescherming (FG) of juridisch adviseur, zodat zij gezamenlijk een goed begrip ontwikkelen van het project;
- Het feit dat data vaak economische waarde heeft, wat verborgen agenda's kan veroorzaken;
- Het risico van bias in de data, die onvolledig of incorrect kan zijn. Dit kan leiden tot foute uitkomsten in de AI-modellen;
- Het kan voorkomen dat een succesvol AI-project niet in gebruik wordt genomen vanwege ethische bezwaren of verschillen in de manier waarop mensen omgaan met risico's die AI-beslissingen met zich meebrengen;
- Soms komen AI-projecten niet van de grond omdat de zorgorganisatie terugdeinst voor eventuele risico's, of omdat vooraf te veel juridische obstakels worden gezien.

Deze uitdagingen hoeven geen obstakel te vormen, maar maken duidelijk dat creativiteit, transparantie en een goed plan essentieel zijn om AI-projecten succesvol te implementeren.

Wie is verantwoordelijk als een AI-systeem een verkeerde beslissing neemt die invloed heeft op de zorg of privacy van een cliënt?

De zorgorganisatie blijft altijd verantwoordelijk voor het leveren van goede zorg. Als een derde partij is ingeschakeld om een AI-project uit te voeren of AI-gestuurde software te leveren, is het belangrijk om duidelijke contractuele afspraken te maken over de verantwoordelijkheden. Denk hierbij aan de overeenkomst van opdracht of dienstverleningsovereenkomst, de algemene voorwaarden, de verwerkersovereenkomst en de Service Level Agreement. Daarnaast is de AI Verordening en vaak ook de MDR van toepassing. Daarin zijn ook verplichtingen en aansprakelijkheden voor de producent en leverancier geregeld. Een goede risicobeoordeling vooraf helpt om mogelijke schade te beperken en zorgt voor een solide basis om eventuele juridische risico's te beheersen.



Hoe kunnen zorgorganisaties zich voorbereiden op de toekomst in het werken met data?

In de gehandicaptenzorg maken zorgorganisaties steeds meer gebruik van data om de zorg te verbeteren. Dit biedt mooie kansen om cliënten beter te ondersteunen. Het is echter ook belangrijk dat zorgorganisaties goed omgaan met privacy, de regels van de Algemene verordening gegevensbescherming (AVG). Daarom is het cruciaal dat zorgorganisaties zich niet alleen aan de huidige wetgeving houden, maar ook vooruitkijken naar nieuwe ontwikkelingen, zoals nieuwe technologieën en kunstmatige intelligentie (AI).

Door regelmatig processen te evalueren en op de hoogte te blijven van de nieuwste trends in de zorg, kunnen zorgorganisaties flexibel en innovatief blijven. Zo zorgen ze ervoor dat ze altijd voldoen aan de wet, de privacy van cliënten en medewerkers beschermen, en klaar zijn om nieuwe kansen te benutten. Op deze manier blijven ze toekomstbestendig in de snel veranderende zorgwereld.

Hoe kan je als zorgorganisatie proactief inspelen op veranderingen in de privacywetgeving?

Voor de Nederlandse zorgsector zijn vooral de Europese AVG, de AI Verordening en de uitwerking in de UAVG als algemene privacyregelgeving van belang. Er zijn steeds meer richtlijnen en uitleg over de toepassing van de begrippen en bepalingen uit de AVG beschikbaar, opgesteld door de Nederlandse Autoriteit Persoonsgegevens (AP) en de Europese samenwerkende privacy toezichthouders in de European Data Protection Board (EDPB). Nederland kent daarnaast specifieke privacywetgeving voor de zorg over de omgang met gezondheidsgegevens, waaronder het beroepsgeheim.

Omdat de totstandkoming van Europese en Nederlandse wetgeving tijd kost, biedt dit vaak ruimte om je als zorgorganisatie voor te bereiden op eventuele wijzigingen en nieuwe regels. Brancheorganisaties weten vaak welke ontwikkelingen er spelen en de overheid geeft online beleidsmatige maar ook praktische informatie over al deze ontwikkelingen voor zorgorganisaties en wat zij ter voorbereiding kunnen doen.

Daarnaast ontwikkelen technologische mogelijkheden zich vaak heel snel. Innovaties zoals AI en nieuwe datatoepassingen zijn voor steeds meer organisaties te gebruiken. De vraag is echter of het verstandig is om direct in te springen op elke nieuwe technologie. Het is aan te raden om de tijd te nemen om met een duidelijk doel in te spelen op de technologische vooruitgang.

Bovenstaande betekent echter niet dat je niet iets kan doen. Door goed voorbereid te zijn als zorgorganisatie, kun je op het juiste moment de juiste stappen zetten.

1. Bepaal je prioriteiten als organisatie: wat heb je nodig en wat zijn je doelen? Heb je oplossingen nodig voor personeelstekorten of wil je

meer regie geven aan cliënten? Of wil je misschien aan de slag met AI om preventieve zorg te verbeteren of om onderzoek te doen? Neem deze prioriteiten jaarlijks op in je jaarplan.

2. Werk samen met een sterk team: stel een team samen van interne medewerkers en externe specialisten die de organisatie, de geschiedenis en de toekomstplannen goed kennen. Dit zorgt ervoor dat je snel kunt reageren op nieuwe ontwikkelingen of projecten. Externe adviseurs kunnen je dan ook tijdig op de hoogte brengen van relevante veranderingen en risico's.
3. Zorg voor een heldere opdracht: geef het team een duidelijke taak en zorg dat het management het proces ondersteunt. Bepaal van tevoren welke risico's je als zorgorganisatie per project bereid bent te accepteren en wat het doel van het project is. Goede samenwerking tussen afdelingen is essentieel om onnodige misverstanden, angst of tegenwerking te voorkomen. Met een duidelijke opdracht en goede communicatie kun je dataprojecten tot een succes maken.

Hoe kan je als zorgorganisatie periodiek controleren of de dataverwerking nog steeds voldoet aan de AVG?

Het naleven van de AVG is een doorlopend proces. Om ervoor te zorgen dat je dataverwerkingen blijven voldoen aan de AVG, is regelmatige monitoring en evaluatie van groot belang. Voor structurele dataverwerkingen is het verstandig om privacy een vaste plaats te geven binnen de PDCA-cyclus van je organisatie. Dit helpt je om continu zicht te houden op alle processen. Bepaal daarnaast welke aspecten je wilt monitoren en hoe je deze gaat evalueren. Gelukkig hoeft je dit niet helemaal zelf uit te vinden. Veel organisaties hebben dit proces al goed ingericht en kunnen als voorbeeld dienen. Het belangrijkste is dat signalen binnen de organisatie goed worden opgevangen en bij de juiste personen terechtkomen.

Voor projecten die minder structureel zijn, zoals tijdelijke dataprojecten, is het goed om vooraf na te denken over de data governance. Dit betekent dat je afspraken maakt over welke data wordt gebruikt, hoe lang deze wordt bewaard, wie toegang heeft en wanneer de data wordt verwijderd. Het is ook belangrijk om vast te leggen wie veranderingen in het proces mag doorvoeren en wanneer een nieuwe DPIA nodig is. Door deze afspraken helder vast te leggen in de data governance, zorg je dat projecten soepel verlopen binnen de vooraf bedachte AVG kaders.

Wat zijn de ontwikkelingen op het gebied van privacy en datagebruik in de zorgsector?

De Europese Unie heeft een Europese Data Strategie vastgesteld. De strategie voor data richt zich op het centraal stellen van mensen bij de ontwikkeling van technologie en op het verdedigen en bevorderen van Europese waarden en rechten in de digitale wereld. Zo zijn er al diverse Verordeningen op dit gebied die al in werking zijn getreden en dus ook in Nederland gelden, zoals de Algemene Verordening Gegevensbescherming (AVG), de Data Governance Verordening (Data Governance Act) en in aanvulling daarop de Data verordening (Data Act) en de AI Verordening (AI Act). Deze algemene Verordeningen op het gebied van data en persoonsgegevens zijn rechtstreeks geldig in Nederland en bevatten bepalingen die van belang zijn voor de zorgsector.

Ook de EU stelt voor verschillende sectoren aparte verordeningen vast. De zorgsector is de eerste sector waarvoor dat gebeurt. Het gaat dan vooral om de geneeskundige zorg. De Europese Unie wil, net als Nederland, bevorderen dat burgers meer grip op en zeggenschap over hun gezondheidsdata krijgen. Zo moeten gezondheidsgegevens in de EU makkelijker kunnen worden uitgewisseld binnen de zorg, om de cliënt in alle EU-landen overal goede zorg te kunnen verlenen (bijvoorbeeld als je op vakantie bent). Ook wordt het hergebruik van geanonimiseerde

of gepseudonimiseerde zorgdata voor wetenschappelijk onderzoek, innovatie en beleidsvorming geregeld. Daarvoor is de [European Health Data Space \(EHDS\)](#) vastgesteld, waarvan de inwerkingtreding in 2025 wordt verwacht. Al deze verordeningen vormen een samenhangend geheel.

Ook Nederland heeft een [Nationale Visie en Strategie op het gezondheidsinformatiestelsel](#) vastgesteld waarin de visie op de digitalisering van de zorg beschreven is. Zorg voor de burger of de cliënt vindt immers steeds meer plaats door verschillende zorgprofessionals en naasten tegelijk, of in ketenopvolging. Deze ontwikkeling stelt nieuwe eisen aan de beschikbaarheid van medische gegevens. In het document staat beschreven hoe de zorgpartijen en de overheid deze aanpassingen voor zich zien tot 2035 en welke stappen daarin worden genomen.

De ontwikkelingen op het gebied van privacy en datagebruik gaan snel, het is daardoor lastig om een compleet en actueel overzicht te geven van deze ontwikkelingen. Wat vandaag belangrijk lijkt, kan morgen alweer verouderd zijn. De vraag is dan ook of je als zorgorganisatie ernaar moet streven om zelf alles actief in de gaten te houden.

Het is daarom verstandig om als zorgorganisatie bepaalde functionarissen aan te wijzen die de ontwikkelingen op het gebied van zorginnovatie, informatiebeveiliging en privacy volgen en weten waar ze algemene en gespecialiseerde informatie kunnen halen. Zij kunnen adviseren over de onderwerpen die specifiek voor jullie zorgorganisatie relevant zijn, op basis van jullie jaarplan en doelen. Zorg dat je periodiek wordt bijgepraat over wat relevant is voor jullie organisatie nu, zodat je als organisatie altijd goed voorbereid bent op wat komen gaat. Zo blijf je niet alleen up-to-date, maar kun je ook snel inspelen op veranderingen en kansen in een dynamische omgeving.

Ook kan je externe partijen actief volgen via nieuwsbrieven of LinkedIn-updates en op die manier op de hoogte blijven van de ontwikkelingen die op dat moment belangrijk zijn voor jouw organisatie.



Bijlage

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

Belangrijke begrippen

Clïënt

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 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.

Redactie

Ellen van den Broek en Suzan Vlaming

Met dank aan

Juristen Josine van der Brug en Alexandra Reijerse voor het opstellen van de teksten

Juristen van de Vereniging Gehandicaptenzorg Nederland (VGN) voor het meelesen

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: Voorbereiden op een toekomst met data en AI. Arnhem: Leren Werken met Data in de gehandicaptenzorg/ Academische Werkplaats ZoTeG.

© Academy Het Dorp, 2024

Kemperbergerweg 139e

6816 RP Arnhem

www.academyhetdorp.nl

Contact: data@academyhetdorp.nl

