



Leren Werken  
met Data  
in de gehandicaptenzorg

AVG en privacy rondom data  
in de gehandicaptenzorg

# Huidig beleid op gebied van AVG & proactief privacy van cliënten beschermen



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.



|                                                                                                                                    |           |
|------------------------------------------------------------------------------------------------------------------------------------|-----------|
| <b>Voorwoord</b>                                                                                                                   | <b>2</b>  |
| <b>Wat je eerst moet weten</b>                                                                                                     | <b>4</b>  |
| Wat is data?                                                                                                                       | 4         |
| De eerste stap om te volgen                                                                                                        | 4         |
| <b>Huidig beleid op gebied van AVG: wat wordt er nu al verwacht van zorgorganisaties?</b>                                          | <b>6</b>  |
| Wat doet de zorgorganisatie nu al op gebied van AVG en andere privacyregels in de zorg?                                            | 6         |
| Hoe informeer je medewerkers het beste over wat de organisatie doet op gebied van AVG en andere privacyregels in de zorg?          | 8         |
| Hoe informeer je cliënten het beste over wat de organisatie doet op gebied van AVG?                                                | 8         |
| <b>Hoe kunnen zorgorganisaties in de gehandicaptenzorg proactief AVG-risico's beheersen en de privacy van cliënten beschermen?</b> | <b>9</b>  |
| Hoe kunnen zorgorganisaties risico's bij het werken met data beperken?                                                             | 9         |
| Wat zijn de mogelijke juridische consequenties als zorgorganisaties data verkeerd gebruiken of onvoldoende beveiligen?             | 10        |
| <b>Bijlage</b>                                                                                                                     | <b>12</b> |
| Belangrijke begrippen                                                                                                              | 12        |
| Overige begrippen                                                                                                                  | 14        |
| Handige richtlijnen en hulpmiddelen over AVG voor de gehandicaptenzorg                                                             | 16        |
| Relevante wetgeving voor privacybescherming en informatiebeveiliging in de zorgsector                                              | 16        |
| Toezicht autoriteiten op gebied van AVG                                                                                            | 17        |
| <b>Colofon</b>                                                                                                                     | <b>18</b> |



# Wat je eerst moet weten

## Wat is data?

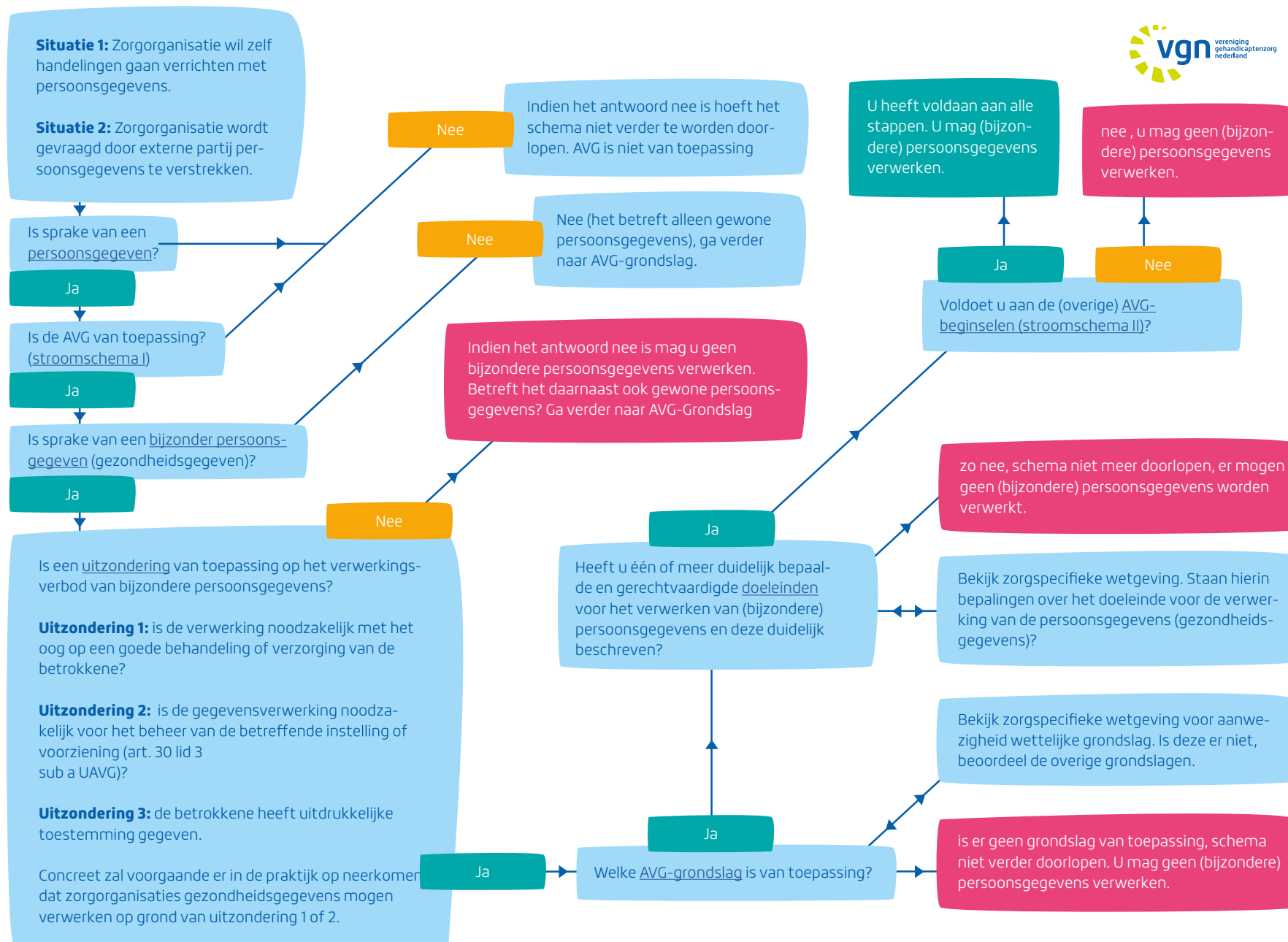
Onder [data in de gehandicaptenzorg](#) verstaan wij digitale gegevens die doorlopend, al dan niet automatisch, worden verzameld via verschillende technologieën. Deze gegevens bevatten informatie over cliënten en over zorg- en ondersteuningsprocessen. Een ander woord voor data is het woord 'gegevens'.

## 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



## Huidig beleid op gebied van AVG: wat wordt er nu al verwacht van zorgorganisaties?

Werken met persoonsgegevens in de zorg vraagt om zorgvuldigheid en de Algemene verordening gegevensbescherming (AVG) helpt ons hierbij. Voor zorgorganisaties in de gehandicaptenzorg is het niet alleen belangrijk om aan de AVG te voldoen, maar ook aan de privacyregels die specifiek voor de zorgsector gelden en rekening te houden met het beroepsgeheim. De zorgorganisatie moet medewerkers en cliënten duidelijk informeren over welke persoonsgegevens van hen worden verwerkt en hoe hun privacy wordt beschermd.

Door open en duidelijk te communiceren en goed bij te houden welke gegevens de zorgorganisatie verwerkt, versterk je het vertrouwen. Dit zorgt ervoor dat cliënten en medewerkers zich veilig voelen binnen de organisatie. Het uitvoeren van Data Protection Impact Assessments (DPIA) en het maken van heldere richtlijnen helpt niet alleen om de wet te volgen, maar ook om een privacy bewuste cultuur te creëren waarin iedereen zich gehoord en beschermd voelt.

Privacybescherming is dus niet alleen een verplichting, maar ook een kans om de organisatie sterker en klaar voor de toekomst te maken!

### Wat doet de zorgorganisatie nu al op gebied van AVG en andere privacyregels in de zorg?

Waarschijnlijk heeft de zorgorganisatie al stappen gezet om te voldoen aan de AVG en zorgspecifieke privacyregels, maar er is vaak nog ruimte voor verbetering. Het is verstandig om eerst een goed overzicht te krijgen van de huidige situatie. Welke privacy maatregelen zijn al getroffen? Wie is verantwoordelijk voor privacy binnen de organisatie? En welke persoonsgegevens worden precies verwerkt? Door deze vragen te beantwoorden, krijg je een duidelijker beeld van de stand van zaken en kun je gericht werken aan het verbeteren van de compliance.



#### Tip:

Het is soms lastig om alles goed te overzien als je er middenin zit. Een frisse blik van een buitenstaander kan helpen om blinde vlekken op te sporen en verbeterpunten te ontdekken.

Er is geen eenduidige aanpak voor het voldoen aan de AVG en andere privacyregels, omdat de wetgeving per organisatie anders kan uitpakken. Wat voor de ene zorgorganisatie geldt, hoeft niet voor de andere te gelden. De AVG biedt richtlijnen, maar de toepassing hangt af van de specifieke context. Privacyvraagstukken zijn ook vaak niet eenvoudig met 'ja of nee' te beantwoorden. Zo maakt de rol van de zorgorganisatie een groot verschil: ben je verwerkingsverantwoordelijke of verwerker bij een specifieke verwerking van persoonsgegevens? Om aan alle privacyregels te voldoen, moet dus elke verwerking getoetst worden aan de wetgeving.

Compliance met de AVG begint met het respecteren van de zes basisprincipes voor het verwerken van persoonsgegevens en het kunnen aantonen dat deze binnen de zorgorganisatie worden toegepast. Dit betekent dat je persoonsgegevens op een rechtmatige, behoorlijke en transparante manier moet verwerken. Zorg ervoor dat de gegevens juist en actueel zijn. Voor je persoonsgegevens verwerkt, moet je nagaan of je het doel ook op een minder ingrijpende manier kunt bereiken. Verwerk alleen de strikt noodzakelijke gegevens om het doel te bereiken, bewaar ze niet langer dan nodig is en pseudonimiseer of anonimiseer de gegevens zodra dat kan.

Als zorgorganisatie heb je ook een documentatieplicht. Dit houdt in dat je een intern register moet bijhouden van alle gegevensverwerkingen (het verwerkingsregister). Ook moet een datalekkenregister worden bijgehouden, waarin incidenten worden vastgelegd. Daarnaast heb je een informatieplicht. Je moet cliënten, bezoekers en medewerkers informeren over de gegevensverwerkingen en hun rechten. Vertel wie je bent, waarom je persoonsgegevens verzamelt en gebruikt, en hoe ze hun rechten kunnen uitoefenen. Dat kan de organisatie doen in een algemene privacyverklaring die ook op de website wordt geplaatst en in specifieke brochures over specifieke verwerkingen voor bepaalde doelen.

Wanneer je andere organisaties inschakelt die als verwerker optreden, moet je een verwerkersovereenkomst sluiten. Denk bijvoorbeeld aan een dienstverlener die de salarisadministratie voor de organisatie uitvoert, of IT-dienstverleners. Dit is nodig om de onderlinge verantwoordelijkheden duidelijk vast te leggen. Mocht de andere organisatie zelf met een verwerkersovereenkomst komen, neem dan de tijd om deze grondig te controleren. Let daarbij ook op of de derde partij passende beveiligingsmaatregelen heeft getroffen. Zorg ervoor dat de in de verwerkersovereenkomst vermelde beveiligingsmaatregelen aansluiten bij de aard van de diensten die worden geleverd. VGN

adviseert de standaard verwerkersovereenkomst te gebruiken die de Brancheorganisaties Zorg partijen samen hebben vastgesteld. Hier vind je een link naar die standaard verwerkersovereenkomst:

[Model verwerkersovereenkomst](#).

Ook is het nodig om te beoordelen of je als zorgorganisatie verplicht bent om een Functionaris Gegevensbescherming (FG) aan te stellen. Zelfs als dit niet verplicht is, kan het verstandig zijn een FG of anders een Privacy Officer (PO) te benoemen. In de gehandicaptenzorg, waar veel gevoelige gegevens worden verwerkt, is het risico op privacy schending groter. Een FG of een PO heeft kennis van privacywetgeving en de praktijk, wat helpt bij naleving.

Ten slotte moet je nagaan of je verplicht bent een DPIA uit te voeren. Een DPIA is nodig als een verwerking een hoog privacy risico oplevert. Het helpt om de privacy-impact van het project in kaart te brengen.

Door deze stappen te volgen, is de zorgorganisatie goed op weg om AVG-compliant te worden en de privacy van betrokkenen optimaal te beschermen.

## Hoe informeer je medewerkers het beste over wat de organisatie doet op gebied van AVG en andere privacyregels in de zorg?

Het zijn de medewerkers op de werkvloer die goed zicht hebben op wat er speelt. Tegelijkertijd ervaren zij de privacyregels mogelijk als een belemmering in hun werk. Door hen bewust te maken van het belang van privacy, kun je dit beeld veranderen en voorkomen dat de privacyregels in de praktijk niet worden opgevolgd.

Als organisatie heb je bovendien een verantwoordingsplicht. Een onderdeel van die verantwoordingsplicht is het creëren van bewustzijn bij medewerkers. Privacy bewustzijn is iets waar je continu aandacht aan moet besteden. Het is belangrijk dat het 'privacy awareness-programma' up-to-date is en goed aansluit op de behoeften van de medewerkers.

Om kennis effectief over te brengen, kun je een e-learning inzetten of een training in spelvorm organiseren. Vermijd langdradige webinars die niet tot de verbeelding spreken en focus juist op praktische, alledaagse voorbeelden. Wees creatief: je kunt bijvoorbeeld elke maand een nieuw privacy thema introduceren. Houd tot slot rekening met de doelgroep en blijf verre van juridisch jargon.



### Tip:

Laat alle nieuwe medewerkers verplicht een e-learning voltooien met basisinformatie over privacy.

Creëer binnen de organisatie een cultuur van openheid en transparantie. Stimuleer medewerkers om over privacy te praten en zorg dat ze gemakkelijk vragen kunnen stellen over privacy kwesties. Domme vragen bestaan niet.



### Tip:

Zorg voor een gestructureerde aanpak om 'privacy awareness' in de organisatie te bevorderen. Dit kun je doen door een eigen programma op te zetten of aan te sluiten bij een bestaand bewustwordingsprogramma van een andere organisatie.

## Hoe informeer je cliënten het beste over wat de organisatie doet op gebied van AVG?

Om cliënten en hun (wettelijk) vertegenwoordigers goed te informeren over wat een organisatie doet met de AVG, is transparantie heel belangrijk. Volgens het transparantiebeginsel moet informatie over de verwerking van persoonsgegevens eenvoudig, toegankelijk en begrijpelijk zijn. Dit betekent dat organisaties duidelijke en simpele taal moeten gebruiken.

- **Houd rekening met het begripsniveau van de doelgroep:** zorg ervoor dat de informatie makkelijk te vinden is. Maak, waar dit logisch en gepast is, gebruik van visuele hulpmiddelen zoals pictogrammen, animatiefilmpjes en tekeningen.
- **Gebruik eenvoudige en duidelijke taal:** zorg ervoor dat de informatie over de gegevensverwerking in begrijpelijke en eenvoudige taal wordt gecommuniceerd. Vermijd jargon en complexe zinnen.



# Hoe kunnen zorgorganisaties in de gehandicaptenzorg proactief AVG-risico's beheersen en de privacy van cliënten beschermen?

In de gehandicaptenzorg is het werken met bijzondere, gevoelige en andere persoonsgegevens heel normaal. Het is belangrijk dat zorgorganisaties hier zorgvuldig mee omgaan. Door goed na te denken over mogelijke risico's en deze actief aan te pakken, kun je niet alleen datalekken voorkomen, maar ook de privacy van cliënten beschermen. Dit begint met goede beveiligingsmaatregelen en het trainen van medewerkers, zodat zij weten hoe ze op de juiste manier met gegevens moeten omgaan.

Met deze stappen zorgt de organisatie voor een veilige omgeving waarin cliënten en medewerkers vertrouwen hebben in de bescherming van hun informatie. Een sterke aanpak van risico's versterkt de reputatie van de organisatie en helpt problemen in de toekomst te voorkomen.

## Hoe kunnen zorgorganisaties risico's bij het werken met data beperken?

Binnen de gehandicaptenzorg is het werken met gevoelige data onvermijdelijk. Cliënten en anderen moeten erop kunnen vertrouwen dat hun gegevens veilig zijn en dat er zorgvuldig mee wordt omgegaan. Dit betekent dat gezondheidsgegevens en gevoelige gegevens, niet via kanalen zoals WhatsApp of onbeveiligde e-mail mogen worden gedeeld.

Het (per ongeluk) verwijderen, kwijtraken, delen of wijzigen van gegevens, of het geven van ongewenste toegang tot persoonlijke informatie, kan grote gevolgen hebben. Dit kan niet alleen de privacy van cliënten schaden, maar ook de zorgorganisatie zelf problemen geven. Denk aan reputatieschade, juridische kosten en boetes. Daarom is het heel belangrijk om de risico's bij het omgaan met deze gegevens goed onder controle te houden.

Volgens de AVG moeten organisaties zorgen voor passende maatregelen om de beveiliging van gegevens te waarborgen. Wat 'passend' is, hangt af van de situatie, zoals de beschikbare technologie en het soort gegevens dat wordt verwerkt. Voor gezondheidsgegevens is altijd een extra hoog beveiligingsniveau nodig. Zorgorganisaties zijn verplicht op het gebied van informatiebeveiliging aan de NEN 7510, NEN 7512 en NEN 7513 te voldoen. Deze norm kent verplichtingen op het gebied van technische en organisatorische maatregelen maar kijkt ook naar menselijk gedrag.



### Tip:

Begin met een inventarisatie van alle mogelijke risico's. Door de verschillende risico's in kaart te brengen, kan de organisatie gerichte maatregelen kiezen om deze risico's effectief te beperken. Betrek verschillende personen uit de organisatie in dit proces om vanuit verschillende perspectieven een completer beeld van de risico's te krijgen (bijvoorbeeld in een brainstormsessie). Als blijkt dat een bepaalde verwerking waarschijnlijk een hoog risico met zich meebrengt, moet vooraf een DPIA worden uitgevoerd.

Zodra de risico's in beeld zijn, kunnen maatregelen worden genomen om deze te beperken. Technische maatregelen kunnen bijvoorbeeld het regelmatig maken van back-ups en het gebruik van virusscanners zijn. Organisatorische maatregelen kunnen bestaan uit het opstellen van gedragscodes, geheimhoudingsovereenkomsten en verwerkersovereenkomsten. Voor het bepalen van passende maatregelen kan gebruik worden gemaakt van de maatregelen die in bijvoorbeeld de NEN 7510-2 staan.

In een gegevensbeschermingsbeleid documenteert de zorgorganisatie hoe zij omgaat met gegevensbescherming, zowel technisch als organisatorisch. Het is belangrijk om zo concreet mogelijk vast te leggen welke maatregelen er zijn getroffen om persoonsgegevens te beschermen. Blijf dan ook niet hangen in het herhalen van algemene principes, maar geef duidelijke en specifieke voorbeelden van hoe de organisatie de privacy van betrokkenen waarborgt.

In de gehandicaptenzorg moet in het bijzonder aandacht worden besteed aan het risico op onbedoelde datalekken wanneer medewerkers gegevens over cliënten delen. Training en bewustwording zijn hierbij essentieel. Medewerkers moeten bijvoorbeeld bewust worden gemaakt van de risico's van het delen van persoonsgegevens via mobiele apparaten of onveilige kanalen zoals WhatsApp.



**Tip:**

WhatsApp is geen veilig kanaal om bijzondere persoonsgegevens mee uit te wisselen (bijvoorbeeld met collega's). Een foto of filmpje waarop een cliënt te zien is, is al snel een bijzonder persoonsgegeven omdat daaruit vaak informatie over de gezondheid van de cliënt kan worden afgeleid (zoals een lichamelijke of verstandelijke beperking).

Daarnaast is het belangrijk om gebruik te maken van technologie die helpt om menselijke fouten te voorkomen. Denk bijvoorbeeld aan beveiligde communicatieplatforms zoals Zorgmail, Ziwer of Siilo.



**Tip:**

Risico's kunnen ontstaan door samenwerkingen met externe partijen of door het gebruik van software van anderen. Daarom is het belangrijk om goed in kaart te brengen met wie je samenwerkt en welke software er gebruikt wordt.

## **Wat zijn de mogelijke juridische consequenties als zorgorganisaties data verkeerd gebruiken of onvoldoende beveiligen?**

Helaas komen cybercriminaliteit, datalekken en andere incidenten steeds vaker voor. Het is daarom niet de vraag of een incident zal plaatsvinden in de zorgorganisatie, maar wanneer het gebeurt.

Het is belangrijk dat medewerkers datalekken zo snel mogelijk melden bij een vast contactpersoon binnen de zorgorganisatie zodat die de gevolgen van een datalek kan beperken door zo nodig maatregelen te nemen. Bij een datalek is de zorgorganisatie verplicht dit zonder onredelijke vertraging aan de Autoriteit Persoonsgegevens (AP) te melden, en, indien mogelijk, uiterlijk binnen 72 uur nadat de organisatie kennis heeft genomen van het datalek. Als het niet waarschijnlijk is dat het datalek een risico inhoudt voor de rechten en vrijheden van de betrokkenen, is melding niet vereist, maar dit vraagt om een zorgvuldige risico-inschatting door de organisatie. De melding bij de AP moet via het officiële [Meldformulier datalekken](#) worden ingediend, beschikbaar op de website

van de AP. In sommige gevallen is melding aan de AP niet voldoende: als het datalek waarschijnlijk een hoog risico vormt voor de rechten en vrijheden van de betrokkenen, moet de organisatie hen rechtstreeks informeren over wat er is gebeurd en welke gegevens mogelijk zijn gelekt.



**Tip:**

Het is belangrijk om binnen de organisatie bewustzijn te creëren rondom datalekken. Zorg ervoor dat medewerkers een datalek kunnen herkennen, begrijpen waarom het belangrijk is om een datalek te melden en weten hoe ze dit op de juiste manier moeten rapporteren.

Als de zorgorganisatie een datalek niet (of niet correct) meldt, of op andere wijze haar verplichtingen onder de AVG niet nakomt, kunnen de consequenties ernstig zijn. Allereerst kan het zijn dat de persoonsgegevens niet veilig zijn en door schade aan de gegevens geen goede zorg kan worden verleend. Daarnaast bestaat er het risico op imagoschade voor de organisatie en heeft de AP de bevoegdheid om sancties op te leggen aan organisaties die de privacywetgeving overtreden. Als blijkt dat een organisatie de regels van de AVG niet naleeft, kan zij in het uiterste geval een boete krijgen van maximaal 20 miljoen euro of 4% van de wereldwijde jaaromzet, afhankelijk van welk bedrag hoger is.

Naast boetes kan de AP ook een last onder dwangsom opleggen. Dit betekent dat de organisatie een overtreding van de AVG binnen een bepaalde termijn moet herstellen. Wordt de overtreding niet tijdig opgelost, dan moet de organisatie een boete betalen per tijdseenheid (bijvoorbeeld per week) totdat de overtreding is gecorrigeerd. Dit systeem stimuleert organisaties om snel actie te ondernemen.

De AP kan ook een berisping geven bij een inbreuk op de AVG. Hiermee stelt de AP officieel de overtreding vast en laat zij weten deze af te keuren. Een berisping wordt vaak opgelegd wanneer dit meer gepast is dan een bestuurlijke boete, bijvoorbeeld bij kleinere inbreuken. De AP beoordeelt dit op basis van de omstandigheden, zoals de ernst van de overtreding en de impact op de betrokkenen.

De organisatie moet zich ervan bewust zijn dat betrokkenen (zoals cliënten of medewerkers) zelf ook stappen kunnen ondernemen bij een schending van hun rechten onder de AVG. Zij kunnen niet alleen een klacht indienen bij de AP, maar ook een civiele procedure starten bij de rechter. Dit kan leiden tot schadeclaims.

Naast de juridische consequenties bestaat er ook een groot risico op reputatieschade. Als de organisatie in een rapport van de AP wordt genoemd of als het incident op een andere manier publiciteit krijgt, kan dit erg vervelend zijn. Hoewel incidenten nooit volledig uit te sluiten zijn, kan een goed geïmplementeerd privacy- en informatiebeveiligingsbeleid de schade zeker helpen beperken. Dit maakt het beantwoorden van vragen door toezichthouders naar aanleiding van een incident in ieder geval veel eenvoudiger. Bovendien zorgt een goede voorbereiding ervoor dat de organisatie, zelfs in stressvolle situaties zoals bij een datalek, snel en adequaat kan handelen.



## 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.
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 Lucia Spaans 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](http://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: Huidig beleid op gebied van AVG & proactief privacy van cliënten beschermen. Arnhem: Leren Werken met Data in de gehandicaptenzorg/Academische Werkplaats ZoTeG.

© Academy Het Dorp, 2024

Kemperbergerweg 139e

6816 RP Arnhem

[www.academyhetdorp.nl](http://www.academyhetdorp.nl)

Contact: [data@academyhetdorp.nl](mailto:data@academyhetdorp.nl)

