vereniging gehandicaptenzorg nederland

Handreiking privacy

Bescherming van persoonsgegevens van cliënten in de gehandicaptenzorg

Voorwoord

< Terug naar de inhoudsopgave

Voor u ligt de handreiking privacy, een uitgave van de Vereniging Gehandicaptenzorg Nederland (VGN). Zorgorganisaties in de gehandicaptenzorg hebben veel aandacht voor de bescherming van privacy van cliënten. Sinds de Algemene Verordening Gegevensbescherming (AVG) van kracht is, 25 mei 2018, heeft dit onderwerp nog meer aandacht gekregen. Daarnaast heeft de AVG ook veel vragen opgeroepen zoals: Mogen er persoonsgegevens van de cliënt uitgewisseld worden met het zorgkantoor of de gemeente? Mag het BSN nummer van de cliënt worden opgenomen in de administratie van de zorgorganisatie?

Privacyvraagstukken in de (gehandicapten)zorg kunnen complex zijn. Naast de AVG kent de gehandicaptenzorg namelijk specifieke regels over de bescherming van persoonsgegevens, bijvoorbeeld in de Wlz en de Jeugdwet. De handreiking bevat informatie over hoe de regels in elkaar zitten. De reikwijdte van de handreiking is beperkt tot privacy in relatie tot de Wlz, de Zvw, de Jeugdwet en de Wmo 2015. Privacy in relatie tot forensische zorg valt buiten de reikwijdte van deze handreiking.

De VGN heeft veel gestelde vragen opgehaald bij een groot aantal leden van de VGN. Daaruit is deze handreiking ontstaan. Naast antwoorden omvat de handreiking bruikbare stroomschema's en stappenplannen. Hiermee hebben zorgorganisaties een tool in handen om te kunnen beoordelen of persoonsgegevens uitgewisseld mogen worden. Het doel van de handreiking is om leden van de VGN wegwijs te maken in de privacywetgeving in relatie tot specifieke zorgwetgeving die op hen van toepassing is. Dit maakt de handreiking uniek, omdat privacyvraagstukken integraal worden benaderd.

De handreiking is bedoeld voor medewerkers van zorgorganisaties in de gehandicaptenzorg die zich bezighouden met het onderwerp privacy, zoals stafmedewerkers, beleidsmedewerkers, kwaliteitsmedewerkers en Functionarissen Gegevensbescherming. De handreiking is in eerste instantie niet geschreven voor begeleiders. Daarvoor verwijzen wij naar 'Juridische kennis: zo zit het!' op het Kennisplein Gehandicaptensector.

Wij hopen dat deze handreiking behulpzaam is bij de beantwoording van privacyvraagstukken in uw organisatie.
De handreiking is tot stand gekomen in samenwerking met mr. Danielle Kikken en mr. Lorette Fruijtier.

Tevens dank aan:
Carante Groep (mr. Ronald Kitsz en drs. Natascha de Rijke (FG))
Amarant (mr. ir. ing. Stephan van der Pol (FG))
De Parabool (Kaspar Visman (SO) René Blokhuis (FG))
De Twentse Zorgcentra (Christina Khouri (FG))

Vanuit de VGN betrokken:
mr. Lilly Wijnbergen
mr. Marijke Delwig
ing. Stefan Clement
drs. Han Huizinga

Frank Bluiminck
Directeur VGN

Inleiding

< Terug naar de inhoudsopgave

In deze handreiking vindt u handige stroomschema's en stappenplannen waardoor zorgorganisaties zelf kunnen beoordelen of het uitwisselen van persoonsgegevens toegestaan is en zo ja of de uitwisseling aan de huidige wet- en regelgeving voldoet. Daarnaast geeft deze handreiking antwoord op veel gestelde vragen omtrent privacy in de gehandicaptenzorg (FAQ's).

De handreiking bestaat uit vier modules. Een aantal onderwerpen komen in meerdere modules terug. De modules kunnen los van elkaar maar ook in gezamenlijkheid gebruikt worden. Via clickables worden directe verwijzingen binnen de module of naar elders (bijv. de website Autoriteit Persoonsgegevens) aangeboden. Bij het gebruiken van FAQ's is het advies om altijd naar de context te blijven kijken waarbinnen het vraagstuk speelt. Daarvoor kunnen de stroomschema's worden gebruikt in Module 4.

De handreiking heeft een gelaagde opbouw, van praktisch naar theoretisch.

Module 1 gaat in op actuele privacyvraagstukken die zich voordoen bij het gebruiken van digitale techniek (pc's, laptops, tablets, smartphones etc.) waaronder ook het inzetten van camera's in de zorg. Module 2 beschrijft het verstrekken van cliëntgegevens binnen de zorgorganisatie (zorgverleners, cliënten, (wettelijk) vertegenwoordigers) en daarbuiten (externe personen en organisaties). Vervolgens schetst Module 3 de privacy aandachtspunten specifiek belicht vanuit het organisatieperspectief. En tot slot kan in Module 4 de inhoudelijke verdieping worden gevonden. Deze laatste module biedt op gestructureerde wijze inzicht in de algemene beginselen en uitgangspunten op het gebied van privacy zoals deze verankerd zijn in de AVG en de UAVG en hoe deze bepalingen zich verhouden tot zorgspecifieke wetgeving.

Doel

Deze handreiking is bedoeld voor medewerkers van zorgorganisaties in de gehandicaptenzorg die zich bezighouden met het onderwerp privacy, zoals stafmedewerkers, beleidsmedewerkers, kwaliteitsmedewerkers en Functionarissen Gegevensbescherming. Het doel van de handreiking is hen wegwijs te maken in de privacywetgeving in relatie tot specifieke zorgwetgeving en daarnaast stapsgewijs eigen maken met de wijze waarop een privacyvraagstuk dient te worden beoordeeld. Privacyvraagstukken laten zich meestal niet beantwoorden met een eenvoudig 'ja of nee'. Het antwoord is afhankelijk van de context waarbinnen de persoonsgegevens worden gebruikt. De handreiking biedt het kader hiertoe.

Wanneer een interface-element de zichtbaarheid van de tekst belemmert, dan kunt u deze meestal uitschakelen in de instellingen van het programma waardoor dit element verdwijnt en de tekst volledig zichtbaar wordt.

Inhoudsopgave

< Terug naar de inhoudsopgave

Inhoudsopgave

< Terug naar de inhoudsopgave

Inhoudsopgave

< Terug naar de inhoudsopgave

Inhoudsopgave

< Terug naar de inhoudsopgave

Inhoudsopgave

< Terug naar de inhoudsopgave

Inhoudsopgave

< Terug naar de inhoudsopgave

Inhoudsopgave

< Terug naar de inhoudsopgave

Inhoudsopgave

< Terug naar de inhoudsopgave

Inhoudsopgave

< Terug naar de inhoudsopgave

Inhoudsopgave

< Terug naar de inhoudsopgave

Inhoudsopgave

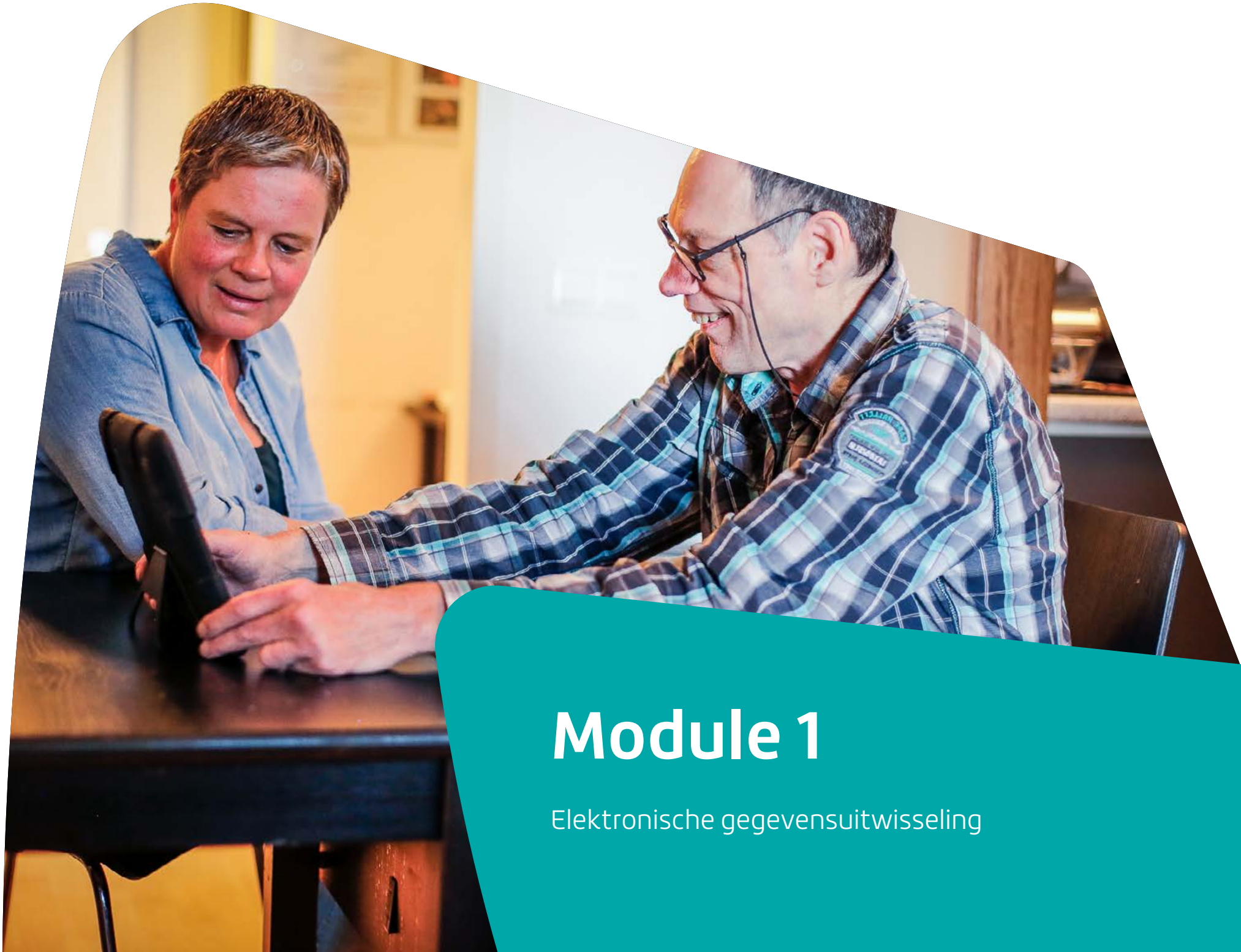
< Terug naar de inhoudsopgave

Inhoudsopgave

< Terug naar de inhoudsopgave

Inhoudsopgave

< Terug naar de inhoudsopgave



Module 1

Elektronische gegevensuitwisseling

Module 1 - elektronische gegevensuitwisseling

- Gebruik van e-mail
- Mobiele apparaten (inclusief Whatsapp)

Inleiding

In deze module wordt ingegaan op privacyvraagstukken die voortvloeien uit het gebruik van onder meer computers, laptops, tablets, mobiele telefoons en camera's in de zorg. Hierover bestaan in de praktijk vragen hoe bij het gebruik van deze apparatuur op de juiste manier kan worden gehandeld met inachtneming van de bescherming van persoonsgegevens van de cliënt.

Bij zorgorganisaties bestaat behoefte aan meer informatie over: het per e-mail verzenden van cliëntgegevens (Deel B); het gebruiken van mobiele apparaten, onder andere tablets, smartphones, voor zorg- en sociale doeleinden (Deel C) en het inzetten van het camera's in het kader van de zorg- en dienstverlening en/of algehele veiligheid (Deel D). Aan deze elementen wordt specifiek aandacht geschonken. In deze module worden zoveel mogelijk praktische handvatten aangeboden met waar nodig een verwijzing naar andere modules. Gestart wordt met een korte beschrijving van de wettelijke voorschriften voor een zorgorganisatie op het gebied van beveiligingsmaatregelen voor IT-systemen (Deel A)

Deel A Informatiebeveiliging algemeen

1 Met welke IT-middelen voldoen zorgorganisaties aan de AVG?

Een onderdeel van de verantwoordingsplicht voor de verwerkingsverantwoordelijke (artikel 5 lid 2 AVG) is dat deze moet kunnen aantonen dat bij de gegevensverwerking passende technische en organisatorische beveiligingsmaatregelen zijn genomen (artikel 32 AVG). Deze beveiligingsmaatregelen moeten laten zien op welke wijze de zorgorganisatie voldoet aan het naleven van de AVG-beginselen, meer concreet of de getroffen maatregelen in verhouding staan tot de aard en doeleinden van de gegevensverwerking. Daarbij staat het de verwerkingsverantwoordelijke vrij zijn eigen ICT-systeem (besturingsprogramma's, software, apparatuur) te kiezen.

Klik hier voor het overkoepelende stappenplan om te beoordelen of de zorgorganisatie handelt volgens de AVG.

< Terug naar de inhoudsopgave

2 Wat betekent passende technische en organisatorische beveiligingsmaatregelen?

Dit houdt in dat de verwerkingsverantwoordelijke (de zorgorganisatie) zodanige maatregelen moet treffen om te waarborgen dat **een veiligheidsniveau** wordt gerealiseerd **dat past bij de veiligheidsrisico's.** Daarvoor moeten dus eerst de risico's worden geïnventariseerd om vervolgens die maatregelen te kiezen die deze risico's kunnen beperken.

2.1 Waar bestaat de risico-inventarisatie uit?

De risico-inventarisatie moet zich richten op het mogelijke risico van vernietiging, verlies, wijziging, ongeoorloofde verstrekking van of ongeoorloofde toegang tot doorgezonden, opgeslagen of anderszins verwerkte gegevens → hetzij per ongeluk hetzij onrechtmatig en waarbij dit tot lichamelijke materiële of immateriële schade kan leiden.

Voorbeelden van risico's zijn het per ongeluk wissen van foto's of opnames van een cliënt die zijn gemaakt in het kader van de zorg- en dienstverlening en een hack in het IT-systeem. Dit zijn situaties waar een betrokkene schade door kan lijden en geïnventariseerd moeten worden voorafgaand aan het nemen van passende beveiligingsmaatregelen.

2.2 Hoe kan een zorgorganisatie een keuze maken uit beveiligingsmaatregelen?

Bij het maken van een keuze voor een bepaalde beveiligingsmaatregel moet de zorgorganisatie altijd uitgaan van:

- de stand van de techniek en de uitvoeringskosten afgezet tegen de risico's die uit de risico-inventarisatie voortkomen; en
- de aard of gevoeligheid van de te beschermen persoonsgegevens (artikel 32 lid 1 AVG).

De wetgever heeft in artikel 32 AVG een aantal beveiligingsmaatregelen genoemd die zo nodig moeten worden genomen om een beveiligingsniveau te waarborgen dat is afgestemd op de risico's. Let wel: de genoemde beveiligingsmaatregelen zijn niet uitputtend, er kunnen andere beveiligingsmaatregelen geschikt(er) zijn afhankelijk van de concrete situatie.
Let op: ook een IT-organisatie waaraan een zorgorganisatie haar IT-activiteiten (deels) uitbesteedt, dient zich bij het verwerken van persoonsgegevens aan de AVG te houden. Er zal dan sprake zijn van een verwerker in de zin van artikel 28 AVG waarmee de zorgorganisatie een verwerkersovereenkomst moet afsluiten.

2.3 Welke mogelijke beveiligingsmaatregelen zijn er?

In artikel 32 AVG worden diverse beveiligingsmaatregelen genoemd die zo nodig genomen kunnen worden om een op de risico's afgestemd beveiligingsniveau te waarborgen.

< Terug naar de inhoudsopgave

De genoemde maatregelen zijn niet uitputtend, andere maatregelen kunnen geschikt(er) zijn afhankelijk van de concrete situatie:

a. Pseudonimisering en versleuteling van de persoonsgegevens.
   Pseudonimiseren: is het verhullen van iemands identiteit voor derden. Een voorbeeld is het vervangen van de naam door een cliëntnummer. Een pseudoniem is een persoonsgegeven waarop de AVG van toepassing is.
   Versleutelen (encryptie): is het langs wiskundige weg omzetten van gegevens tot een onbruikbare reeks tekens zodanig dat zonder de sleutel de gegevens niet toegankelijk zijn. (Zie ook onderdeel 7.2 voor een uitleg over deze methoden.)
b. Maatregelen die ervoor zorgen dat het verwerkingssysteem of dienst de vertrouwelijkheid, integriteit, beschikbaarheid en veerkracht kan garanderen.
   Dit betekent in feite de betrouwbaarheid van de informatiebeveiliging. De vraag moet worden gesteld in hoeverre de zorgorganisatie kan rekenen op haar eigen informatiesysteem op het gebied van beschikbaarheid, integriteit en vertrouwelijkheid. Veerkracht houdt in of het informatiesysteem bestand is tegen bedreigingen en flexibel is (kan er voldaan worden aan (veranderende) eisen met betrekking tot de continuïteit van het systeem)?
c. De herstelmogelijkheden bij een fysiek of technisch incident.
   In welke mate en op welke manier is een zorgorganisatie in staat om na een incident of inbreuk, adequaat de juiste herstelmaatregelen te nemen?
d. Het regelmatig testen, beoordelen en evalueren van de doeltreffendheid van de beveiligingsmaatregelen. Voor een blijvend passend beveiligingsniveau is inbedding van de zogeheten plan-do-check-act-cyclus in de dagelijkse praktijk van de zorgorganisatie noodzakelijk.

Klik ook hier voor meer algemene informatie over de passende technische en organisatorische maatregelen die de verwerkingsverantwoordelijke in het kader van het naleven van de AVG-verplichtingen moet nemen.

3 NEN-normen in de zorg

In het Besluit elektronische gegevensverwerking door zorgaanbieders (hangend onder de Wet aanvullende bepalingen verwerking van persoonsgegevens in de zorg (Wabvpz)) is neergelegd dat een zorgorganisatie dient te voldoen aan de volgende NEN-normen:

- 7510 (informatiebeveiliging in de zorg);
- 7512 (vertrouwensbasis voor gegevensuitwisseling);
- 7513 (logging van toegang tot het patiëntdossier);

< Terug naar de inhoudsopgave

- aankomende norm NEN-7521. Deze laatste norm wordt in 2019 verwacht en gaat expliciet in op gegevensuitwisseling tussen zorgprofessionals en zorgorganisaties rond de behandeling van een cliënt.

Aandachtspunt:
In aanvulling op NEN 7510 is in mei 2019 de veldnorm NTA 7516 Eisen voor veilige e-mail en chatapplicaties gepubliceerd. Zie onderdeel 6 van deze module waar deze norm verder wordt beschreven. De NTA 7516 is niet opgenomen in het Besluit elektronische gegevensverwerking door zorgaanbieders. Op grond van de AVG bestaat echter een brede(re) verplichting voor de verwerkingsverantwoordelijke tot het treffen van passende technische en organisatorische (beveiligings)maatregelen bij de verwerking van persoonsgegevens. Deze verplichting brengt met zich mee dat zorgorganisaties handelen in lijn met de relevante NEN-normen en de veldnorm NTA 7516.[1]

Werkingssfeer Wabvpz en Besluit

De Wabvpz is van toepassing op de zorgaanbieder genoemd in artikel 1 Wkkgz. Dit betekent dat bovengenoemd Besluit, met daarin de NEN-normen, van toepassing is op zorgorganisaties die onder de Wlz en Zvw vallen, maar niet op zorgorganisaties die enkel ondersteuning (Wmo 2015) en/of jeugdhulpverlening (Jeugdwet) bieden. In de lagere regelgeving van deze wetten zijn wel diverse bepalingen over informatiebeveiliging opgenomen:

- Wmo 2015: in artikel 3 Uitvoeringsregeling Wmo 2015 is opgenomen dat de gegevensverwerking, bedoeld in artikel 5.2.9 lid 6 Wmo voldoet aan NEN-ISO-IEC 27001 en NEN-ISO-IEC 27002.
  Dit betreft de situatie waarin het BSN wordt uitgewisseld of persoonsgegevens indien de persoon geen BSN heeft.
- Jeugdwet: Een soortgelijke bepaling geldt voor de jeugdhulpverlening. In artikel 6 van de Regeling Jeugdwet is bepaald dat de beveiliging van gegevensverwerking voldoet aan NEN-ISO-IEC 27001 en NEN-ISO-IEC 27002 of daaraan gelijkwaardige normen. Ook hier betreft het, het gebruik van het BSN en de situatie waarbij persoonsgegevens worden verwerkt als aan de jeugdige geen BSN is toegekend (artikel 7.2.1 en 7.2.4 Jeugdwet).

Aandachtspunt:
In het geval in de zorgorganisatie alleen sprake is van ondersteuning en/of jeugdhulpverlening de verwerking van persoonsgegevens dan dient de zorgorganisatie zich niet te beperken tot de hierboven genoemde wettelijke bepalingen in de Wmo 2015 en/of Jeugdwet omtrent informatiebeveiliging. Zoals eerder benoemd bestaat op grond van de AVG een brede(re) verplichting voor de verwerkingsverantwoordelijke tot het treffen van passende technische en organisatorische (beveili-

1 NEN 7510-1, pagina 11 en 12 jo. NTA 7516 pagina 4.

< Terug naar de inhoudsopgave

gings)maatregelen bij de verwerking van persoonsgegevens. Deze verplichting brengt met zich mee dat zorgorganisaties handelen in lijn met de relevante NEN-normen en de veldnorm NTA 7516.[2]

4 Van welke op de markt beschikbare digitale diensten kunnen zorgaanbieders gebruik maken om persoonsgegevens (bestanden) te verzenden?

Het antwoord op deze vraag zal allereerst afhankelijk zijn van het IT-(veiligheids)beleid dat door de zorgorganisatie wordt gehanteerd. Met dit beleid moet invulling worden gegeven aan de AVG-verplichting van de verwerkingsverantwoordelijke tot het nemen van passende technische en organisatorische beveiligingsmaatregelen.

Er bestaan vele diensten die het mogelijk maken digitale bestanden te versturen. Om zorgorganisaties op weg te helpen bij het maken van een keuze dient een afweging te worden gemaakt tussen de aard van de persoonsgegevens (gewone of bijzondere persoonsgegevens), de grootte van de bestanden en voor welk doel de persoonsgegevens verzonden dienen te worden. Op grond van deze afweging kan blijken dat bepaalde diensten zich niet laten lenen voor digitale verzending van (bijzondere) persoonsgegevens. Zo is het meestal niet mogelijk om met gratis diensten afspraken te maken over hoe zij met de persoonsgegevens moeten omgaan (denk aan opslag, beveiliging, het gebruik van de persoonsgegevens). Deze mogelijkheid bestaat daarentegen wel bij de diensten die hun producten tegen betaling aanbieden.
Geadviseerd wordt te kiezen voor een dienst waarmee de zorgorganisatie nadere afspraken kan maken over de wijze van omgaan met persoonsgegevens, waaronder beveiligingsmaatregelen.

Hierna volgen enkele suggesties om een denkkader te bieden:

- Beveiligde e-mailprogramma's zijn geschikt voor het uitwisselen van dagelijkse berichten met kleine bijlagen: Zorgmail/ Zivver, KPNMessenger. (Zie verder over het gebruik van e-mail deel B.)
- Liquid files is geschikt voor de transfer van bestanden als deze te groot zijn voor e-mail: pas daarbij altijd versleuteling toe.
- Siilo messenger of Kanta messenger (varianten op Whatsapp) kunnen geschikt zijn voor het uitwisselen van korte berichten tussen zorgprofessionals en/of cliënten.

(Zie verder over gebruik van WhatsApp onderdeel C(ii).

2 NEN 7510-1, pagina 11 en 12 jo. NTA 7516 pagina 4.

< Terug naar de inhoudsopgave

Beoordeel of deze varianten geschikt zijn en kijk of met deze partijen afspraken gemaakt kunnen worden over de omgang, het gebruik en de beveiliging van persoonsgegevens.

Aandachtspunt:
De AVG is risico gestuurde wetgeving. Dit houdt in dat de zorgorganisatie bij elke gegevensverwerking, dus ook bij het digitaal verzenden van (bijzondere) persoonsgegevens, moet nagaan welke risico's dit met zich mee kan brengen voor de betrokkenen. Op grond daarvan moet de zorgorganisatie beoordelen welke verzendingsmethode het meest passend is. Bij beoordeling en besluitvorming moet de zorgorganisatie rekening houden met:

- de stand van de techniek;
- de uitvoeringskosten;
- de aard, omvang, context en het doel van de verwerking;
- de risico's voor de betrokkenen.

Deze elementen bepalen in hoeverre de maatregelen haalbaar zijn. Technische mogelijkheden zijn steeds in ontwikkeling, dit brengt met zich mee dat de gekozen technische maatregelen periodiek moeten worden herzien.

Zie voor meer informatie over de AVG-verplichtingen voor de zorgorganisatie op het gebied van beveiligingsmaatregelen module 3.

Deel B E-MAIL

5 Kent de AVG expliciete bepalingen over het gebruiken van e-mail?

Nee, de AVG kent geen expliciete voorschriften omtrent e-mailgebruik, maar ook hier geldt dat de verwerkingsverantwoordelijke een brede verplichting heeft tot het treffen van passende technische en organisatorische (beveiligings)maatregelen. Dit brengt met zich mee dat zorgorganisaties werken conform de relevante NEN-normen en veldnormen omtrent informatiebeveiliging.[3] In mei 2019 is een veldnorm gepubliceerd die nadere eisen bevat voor veilig gebruik van e-mail en chatapplicaties in de zorg: NTA 7516. Daarnaast moet bij het e-mailen rekening worden gehouden met zorgspecifieke wetgeving in het kader van de geheimhoudingsplicht van de zorgorganisatie/zorgprofessional. Vanzelfsprekend dient ook rekening te worden gehouden met de eisen van de (U)AVG omtrent het verwerken van persoonsgegevens, klik hier voor het overkoepelende stappenplan om te beoordelen of de zorgorganisatie handelt volgens de AVG.

3 NEN 7510-1, pagina 11 en 12 jo. NTA 7516 pagina 4.

< Terug naar de inhoudsopgave

6 NTA 7516: Eisen voor veilige e-mail en chatapplicaties in de zorg

In het najaar van 2018 is op initiatief van het Informatieberaad Zorg het project Veilige Mail gestart waarin IT-leveranciers en zorgorganisaties hebben gewerkt aan het ontwikkelen van een norm en het vaststellen van standaarden voor veilige e-mail en het stimuleren van interoperabiliteit tussen oplossingen, die veilig e-mailen ondersteunen. Hierbij werd ook het nomeringsinstituut NEN betrokken. Dit traject heeft geleid tot NTA[4] 7516 *Medische informatica – Eisen voor veilige e-mail en chatapplicaties (uitwisseling van ad-hoc berichten met persoonlijke gezondheidsinformatie)*.

Zie vraag 6.2 voor de werkingssfeer van de NTA 7516.

6.1 Wat regelt de norm Eisen voor veilige e-mail en chatapplicaties?

De norm bevat uitgangspunten voor het gebruik van ad hoc[5] e-mail en chatapplicaties (al dan niet aangeboden via een berichtenportaal) en beoogt te realiseren dat de elektronische uitwisselingssystemen van de verschillende leveranciers[6] op elkaar gaan aansluiten. Dit laatste brengt met zich mee dat de norm ook van toepassing is op uitwisseling van gegevens met externe zorgprofessionals. Het uiteindelijke doel is dat e-mail en chatapplicaties als een veilige vorm van uitwisseling van persoonlijke gezondheidsinformatie worden gebruikt. De norm bevat diverse eisen, die voor een deel uit de wet (met name de AVG) en voor een deel uit gebruikerswensen zijn voortgevloeid.

4 Nederlandse technische afspraak.

5 Met ad-hoc wordt bedoeld gegevensuitwisseling voor een bepaald geval of situatie (e-mail en chatapplicaties) waarbij de verzender en ontvanger allebei een mens zijn en waar tevoren geen specifieke afspraken konden worden gemaakt over eisen ten aanzien van beschikbaarheid, integriteit en vertrouwelijkheid.
Automatisch berichtenverkeer valt niet onder ad-hoc berichtenverkeer. Niet tot het ad-hoc berichtenverkeer hoort in ieder geval EDI-FACT-, HL7-, StUF- en conform IHE-standaarden gestructureerde berichten (definitie 3.2 NTA 7516).

6 De veldnorm is dus ook relevant voor leveranciers die oplossingen bieden voor ‘ongestructureerde, a-synchrone en ad-hoc uitwisseling van persoonlijke gezondheidsinformatie’, zoals e-mail, messenger- en chatfunctionaliteiten.

< Terug naar de inhoudsopgave

Persoonlijke gezondheidsinformatie (definitie 3.29)
Informatie over een identificeerbare persoon die verband houdt met de lichamelijke of geestelijke gesteldheid van, of de verlening van zorgdiensten aan, de persoon in kwestie, waaronder ook kan worden begrepen:

a. informatie over de registratie van de persoon voor de verlening van zorgdiensten vanuit het zorgdomein, desg wenst het maatschappelijke domein en in voorkomende gevallen het domein van politie en justitie;
b. informatie over betalingen of het in aanmerking komen voor zorg met betrekking tot de persoon;
c. een aan een persoon toegewezen nummer, symbool of bijzonderheid als unieke identificatie van die persoon voor medische doeleinden;
d. alle informatie over de persoon die wordt vergaard tijdens het verlenen van zorgdiensten aan de persoon;
e. informatie die is ontleend aan een beproeving of onderzoek van een lichaamsdeel of lichaamseigen stof;
f. identificatie van een persoon (bijvoorbeeld een zorgprofessional) als verlener van zorg aan de persoon.

6.2 Op welke zorgsectoren is de norm van toepassing (werkingssfeer)?

De norm is op alle zorgsectoren van toepassing. Dat wil zeggen voor de Wlz, Zvw, Wmo 2015 en de Jeugdwet. Op grond van de AVG bestaat een brede verplichting voor de verwerkingsverantwoordelijke tot het treffen van passende technische en organisatorische (beveiligings)maatregelen bij de verwerking van persoonsgegevens. Deze verplichting brengt met zich mee dat zorgorganisaties handelen in lijn met de relevante NEN-normen en de veldnorm NTA 7516. [7]

6.3 Op wie is de norm van toepassing?

De norm is van toepassing op het uitwisselen van e-mail en chatberichten tussen professionals onderling en tussen professionals en personen (cliënten, mantelzorgers en (wettelijk) vertegenwoordigers). Onder professionals wordt verstaan de personen die beroepsmatig met gezondheidsinformatie werken: zorgprofessionals, IT-medewerkers en andere medewerkers in de zorgorganisatie.

7 NEN 7510-1, pagina 11 en jo. NTA 7516 pagina 4.

< Terug naar de inhoudsopgave

6.4 Wat regelt de norm?

NTA 7516 bevat uitgangspunten die in acht moeten worden genomen voor het realiseren van het veilig uitwisselen van persoonlijke gezondheidsinformatie via e-mail of via chatapplicaties (al dan niet aangeboden via een berichtenportaalfunctionaliteit).

De norm benoemt:

- Algemene uitgangspunten rondom het ad-hoc verkeer (e-mail en chatapplicaties) (hoofdstuk 5 van NTA 7516);
- Eisen (technisch en organisatorisch) rondom het gebruik van e-mail en chatapplicaties voor de professionals (hoofdstuk 6 van NTA 7516);
- Eisen voor de leveranciers waaraan hun product minstens moet voldoen inclusief de mogelijkheid dat ad-hoc verkeer tussen diensten van verschillende leveranciers mogelijk is (hoofdstuk 7 van NTA 7516);
  Daarnaast bevat de norm:
- Uitgangspunten voor de zorgprofessional bij het uitwisselen van persoonlijke gezondheidsinformatie via e-mail en chatapplicaties met cliënten, mantelzorgers en (wettelijk) vertegenwoordigers: wat mogen zij (minimaal) verwachten? (bijlage A van NTA 7516).
- Aanbevelingen die door de zorgprofessional kunnen worden gegeven aan cliënten (etc.) over wat zij zelf in de thuissituatie zouden kunnen doen om het communicatieverkeer zo veilig mogelijk te houden (bijlage B van NTA 7516).

6.5 Op welke digitale functionaliteiten is de norm *niet* van toepassing?

De norm is niet van toepassing op:

- Realtimecommunicatiediensten zoals (beeld)bellen;
- Het versturen van berichten via een fax;
- Het e-mailen tussen personen (cliënten, (wettelijk) vertegenwoordigers en verwanten) onderling (privéredenen);
- Filetransfer toepassingen als WeTransfer en Dropbox;
- Niet-elektronische communicatie, waaronder het uitwisselen van papieren dossier;
- Uitwisseling van gestructureerde informatie (bijvoorbeeld met behulp van IHE-standaarden).

Voor deze digitale mogelijkheden zijn (vooralsnog) geen nadere randvoorwaarden bepaald.
Op grond van de AVG bestaat echter een brede verplichting voor de zorgorganisatie (verwerkingsverantwoordelijke) tot het

< Terug naar de inhoudsopgave

treffen van passende technische en organisatorische (beveiligings)maatregelen bij de verwerking van persoonsgegevens. Deze verplichting brengt met zich mee dat zorgorganisaties dienen te handelen in lijn met de relevante NEN-normen en de veldnorm NTA 7516.

7. Juridische en technische uitgangspunten

7.1 Wat zijn belangrijke juridische (privacy) uitgangspunten voor veilig e-mailverkeer in de zorg?

Neem bij e-mailverkeer ten minste de hierna genoemde juridische uitgangspunten in acht:

- Persoonsgegevens mogen alleen worden verwerkt wanneer daarvoor vooraf welbepaalde en uitdrukkelijk omschreven doelen zijn vastgesteld en daarvoor een grondslag aanwezig is.
  Wanneer het gaat om bijzondere persoonsgegevens, zoals gegevens over de gezondheid, moet er behalve een rechtmatige verwerkingsgrondslag ook sprake zijn van een uitzonderingsgrond (een ontheffing op het verbod tot het verwerken van bijzondere persoonsgegevens). Zie module 4 voor het wettelijk kader.
- Wanneer het bijzondere persoonsgegevens (gezondheidsgegevens) betreft moet de zorgorganisatie/zorgprofessional zich daarnaast houden aan zijn geheimhoudingsplicht/het medisch beroepsgeheim. Nagegaan moet worden of de zorgorganisatie/zorgprofessional op grond van de Wgbo, Wlz, Wmo 2015 en/of Jeugdwet[8] tot verzending mag overgaan. Dat betekent dat de zorgprofessional of de zorgorganisatie moet beoordelen of het beroepsgeheim mag worden doorbroken. Zie module 2 vraag 16.
- Er moet voldaan zijn alle beginselen van de AVG. Zie voor een uitgebreide omschrijving module 4, het overkoepelende stappenplan in deze module kan hiervoor worden gebruikt. Na het doorlopen daarvan kan worden beoordeeld of e-mailverzending kan plaatsvinden.
- Tot slot: Verstuur alleen die persoonsgegevens die voor het doel (van verzending, de ontvanger) noodzakelijk zijn en beperk in dat kader zoveel mogelijk het verzenden van bijzondere persoonsgegevens.

7.2 Wat zijn de technische uitgangspunten voor veilig e-mailverkeer in de zorg?

In het algemeen wordt opgemerkt dat de apparatuur waarmee e-mail kan worden verzonden zoals computer (desktop), laptops, tablets, smartphones voldoende beveiligd moeten zijn. Dat geldt vervolgens ook voor de communicatieprogramma's (het e-mailprogramma). In dit kader wordt gewezen op de uitgangspunten genoemd in de norm Eisen voor veilige e-mail en chatapplicaties (NTA 7516) welke van toepassing is op het berichtenverkeer tussen zorgprofessionals onderling en tussen zorgprofessional en cliënt, mantelzorger en (wettelijk) vertegenwoordiger.

8 Geheimhoudingsplicht: artikel 7:457 BW, artikel 9.1.2 lid 5 Wlz, artikel 5.3.3 Wmo 2015 en artikel 7.3.11 Jeugdwet.

< Terug naar de inhoudsopgave

Hierna enkele technische uitgangspunten in het kader van veilig e-mailen in de zorg. Het betreft geen uitputtende opsomming:

- Er is sprake van een beveiligd serverpark en beveiligde infrastructuur. De switches en routers werken aan de hand van veiligheidsprotocollen en zijn voor veilig gebruik ingesteld door gebruikers en cliënten.
- Er is sprake van computers met een up-to-date virusscanner, firewall en recente patches voor software waarmee gewerkt wordt.
- Bij e-mail uitwisseling van cliëntgegevens dienen maatregelen getroffen te worden die de privacy van de cliënt waarborgen. Hierbij dienen gegevens minimaal versleuteld verstuurd te worden. Maak gebruik van beschikbare 'secure e-mail' (veilige mail) programma's en/of communiceer via een 'secure' (veilige) verbinding, dit is een versleutelde/encrypted server.

Versleuteling (encryptie) van gegevens:
Dit is een manier om berichten met behulp van algoritmen onleesbaar te maken. Alleen de persoon die over de juiste wiskundige formule (algoritme) beschikt kan het oorspronkelijke bericht weer leesbaar maken. Deze formule heet de sleutel.

Variant 1 symmetrische encryptie: de verzender en ontvangen hebben dezelfde sleutel. Dit vereist dat de verzender vooraf een sleutel met de ontvanger uitwisselt. De sleutel zet de onleesbare data weer terug in leesbare data. (Een wachtwoord op een computer kan overigens ook als een sleutel worden gezien).

Variant 2 a-symmetrische encryptie: de verzender en ontvanger hebben verschillende sleutels. Het bericht (de data) wordt onleesbaar gemaakt met een publieke (openbare) sleutel door de verzender en de ontvanger gebruikt zijn privésleutel om het bericht weer leesbaar te maken.

- Bij voorkeur worden e-mails over cliënten niet in het e-mailprogramma zelf bewaard, om te voorkomen dat computervirussen vat krijgen op de vertrouwelijke gegevens. Van deze e-mails kunnen, mits noodzakelijk voor de te verrichte werkzaamheden, geprinte, papieren versies in het dossier worden opgenomen of digitaal in het ECD worden opgeslagen (scan). In het geval de zorgorganisatie e-mails print, is het advies om deze niet langer te bewaren dan voor het doel noodzakelijk is

< Terug naar de inhoudsopgave

c.q. met inachtneming van een specifiek wettelijke bewaartermijn en worden bewaard in een afgesloten kast of ruimte. Een andere optie is om essentiële informatie in het kader van de zorg- en dienstverlening welke in de geprinte mails staat daaruit over te nemen en registeren in het ECD. Voor de volledigheid wordt opgemerkt dat ook in het geval van digitale gegevens (net zoals bij 'papieren' persoonsgegevens) de persoonsgegevens niet langer bewaard mogen worden voor het doel noodzakelijk dan wel in achtneming van een wettelijke bewaartermijn.

- Lokaal gebruik (op de werkplek): de toegang tot de computer moet beveiligd zijn, bijvoorbeeld door middel van wachtwoorden. Daarnaast kan de computer zijn voorzien van een screensaver die beveiligd is met een wachtwoord (zodat de toegang tot de gegevens op de computer ook beperkt is op het moment dat de zorgprofessional is ingelogd maar niet op zijn (werk)plek aanwezig is).
- Extern gebruik van het bedrijfsnetwerk van de zorgorganisatie: hanteer two factor authentication (twee stappen authenticatie).[9]

FAQ's E-MAIL

8 Mogen cliëntgegevens, waaronder gezondheidsgegevens, per mail worden gestuurd naar collega's of naar externe zorgorganisaties of behandelaars?

Er bestaan geen expliciete wettelijke vereisten voor het uitwisselen van persoonsgegevens (gezondheidsgegevens) van een cliënt via e-mail. Wel dient de verwerkingsverantwoordelijke (zorgorganisatie) op grond van de AVG passende technische en organisatorische (beveiligings)maatregelen te treffen. Deze verplichting brengt met zich mee dat zorgorganisaties handelen in lijn met de relevante NEN-normen en de veldnorm NTA 7516. De norm NTA 7516 bevat diverse eisen inzake uitwisseling van berichten via e-mail en chatapplicaties, deze norm is van toepassing op het berichtenverkeer tussen zorgprofessionals onderling (intern en extern) en tussen zorgprofessionals met cliënten, patiënten, mantelzorgers en (wettelijk) vertegenwoordigers.

Behalve deze technische aspecten dient ook beoordeeld te worden of de ontvanger de persoonsgegevens wel mag ontvangen op grond van de (U)AVG en het medisch beroepsgeheim/geheimhoudingsplicht. Wanneer het gaat om bijzondere persoonsgegevens, zoals gegevens over de gezondheid, moet er sprake zijn van een uitzonderingsgrond (een ontheffing op het verbod tot het verwerken van bijzondere persoonsgegevens) én een grondslag op grond waarvan de verwerking rechtmatig

9 Dit is een authenticatie methode waarbij eerst twee stappen succesvol moeten zijn doorlopen om ergens toegang tot te krijgen. Stap 1 is meestal het invoeren van een gebruikersnaam en wachtwoord op de computer. Stap 2 is het invoeren van een code op de computer die wordt verkregen via sms of een code die is gegenereerd via een speciale authenticatie app op een smartphone. Alleen bij het doorlopen van deze 2 stappen verkrijgt men toegang.

< Terug naar de inhoudsopgave

kan plaatsvinden. Daarbij moet tegelijkertijd ook rekening worden gehouden met medisch beroepsgeheim van de zorgprofessional wat met zich meebrengt dat deze in beginsel geen gegevens aan derden mag verstrekken, behalve onder bepaalde voorwaarden. Klik hier voor de voorwaarden die kunnen leiden tot het doorbreken van het medisch beroepsgeheim.

Verstrek zo min mogelijk bijzondere persoonsgegevens, alleen die informatie die de ontvanger voor het doel nodig heeft. Wanneer er geen beveiligde mailverbinding (zowel intern of extern) is, dan is het advies verzending per e-mail achterwege te laten en een alternatief te kiezen.

9 Mag de (wettelijk) vertegenwoordiger (bijzondere) persoonsgegevens van de zorgorganisatie per e-mail ontvangen of zelf mailen?

Het antwoord is ja, mits voldaan wordt aan bepaalde uitgangspunten. Bezien vanuit de zorgorganisatie is het advies gezondheidsgegevens nooit via onbeveiligde mail berichten te versturen en de verzending dus versleuteld of op een andere veilige manier te laten plaatsvinden zodat de zorgorganisatie zeker weet dat ook de (wettelijk) vertegenwoordiger wordt bereikt. De e-mail verzending dient beveiligd plaats te vinden om te voorkomen dat het e-mailbericht tijdens verzending wordt onderschept (hackers).

De veldnorm *Eisen voor veilige e-mail en chatapplicaties* (NTA 7516) bevat technische en organisatorische uitgangspunten voor de zorgorganisatie om berichtenverkeer - e-mail en chatten - veilig te laten plaatsvinden.

Perspectief van cliënt

Daarnaast beschrijft de norm wat de ontvanger (cliënt, patiënt, mantelzorger en (wettelijk) vertegenwoordiger) mag verwachten van het berichtenverkeer afkomstig van de zorgorganisatie. Zoals:

- dat het bericht veilig is en dat er door de cliënt veilig op kan worden geantwoord;
- dat het bericht te lezen is zonder dat de ontvanger een account heeft van een leverancier waarvan de zorgorganisatie gebruik maakt;
- dat de afzender duidelijk herkenbaar is voor de ontvanger.

Zie voor de overige punten bijlage A van NTA 7516.

< Terug naar de inhoudsopgave

Verder is in de norm opgenomen wat ondernomen kan worden om de digitale informatie uitwisseling in de thuissituatie (van en naar de zorgorganisatie/zorgprofessional) veilig te laten plaatvinden. Hiertoe worden in bijlage B van NTA 7516 enkele aanbevelingen gedaan die de zorgorganisatie kan oppakken richting de cliënt (etc.). Zoals:

- zijn de draadloze verbindingen veilig geconfigureerd;
- is de afzender ook daadwerkelijk de cliënt (etc.);
- klopt het e-mailadres van de zorgprofessional met het adres dat de ontvanger heeft.

Zie voor de overige punten bijlage B van NTA 7516.

Hoe?

Middels mondelinge en/of schriftelijke voorlichting kan de zorgorganisatie daar kenbaarheid aan geven. Informeer de cliënt en/of (wettelijk) vertegenwoordiger tijdens een intake gesprek (bij in zorg nemen) op welke wijze de zorgorganisatie omgaat met de bescherming van persoonsgegevens. (Dit vloeit voort uit de informatieplicht van de verwerkingsverantwoordelijke aan de betrokkene).

Tot slot

Neem bovenstaande voorwaarden en het bepaalde over beveiligingsmaatregelen in artikel 32 AVG in acht om een veilige e-mailomgeving te creëren. Verstrek bij de verzending zo min mogelijk gezondheidsgegevens, alleen die informatie die de (wettelijk) vertegenwoordiger voor het doel (de aanleiding van de mail) nodig heeft.

10 De zorgorganisatie heeft (nog) geen beveiligde mail, mogen dan geen cliëntgegevens naar anderen buiten de organisatie verzonden worden?

Geadviseerd wordt om cliëntgegevens (waaronder gezondheidsgegevens) niet via onbeveiligde mail te versturen omdat het risico op inbreuk van persoonsgegevens (datalek) groot is.

Een cliënt of (wettelijk) vertegenwoordiger zal veelal geen beveiligd e-mail systeem hebben, daartoe is deze ook niet verplicht. Het systeem van de verzender (zorgorganisatie) moet daarom in staat zijn om het hele traject veilig te doorlopen (NTA 7516).

Mocht het toch een enkele keer echt noodzakelijk zijn, dat cliëntgegevens, waaronder ook gezondheidsgegevens, via een onbeveiligde verbinding gemaild moeten worden neem dan de volgende punten in aanmerking:

< Terug naar de inhoudsopgave

- Vermeld zo min mogelijk bijzondere persoonsgegevens (in de mailtekst zelf en indien mogelijk in de bijlagen die worden meegestuurd);
- Voeg pas nadat de mail is opgesteld de personen toe voor wie het bericht bestemd is, en controleer nog een keer extra deze geadresseerde(n) en e-mailadres(sen) voordat op 'verzenden' wordt geklikt;
- Bescherm de bijlagen met een wachtwoord;
- Stel de "bevestiging van bezorgen" in het mailprogramma in. Mocht het onverhoopt misgaan dan wordt dit hierdoor eerder duidelijk.

11. Mogen zorgorganisaties gezondheidsgegevens per e-mail naar toeleveranciers (zijnde geen zorgorganisaties) sturen? Bijvoorbeeld een orthopedisch schoenmaker?

De zorgorganisatie dient voorafgaand aan deze verzending eerst stil te staan bij het feit dat het verboden is bijzondere persoonsgegevens, waaronder gezondheidsgegevens, te verwerken (artikel 9 AVG).

In artikel 30 lid 3 sub a AVG is daarop een uitzondering gemaakt voor hulpverleners (zorgprofessionals) en instellingen of voorzieningen voor gezondheidszorg en maatschappelijke dienstverlening mits de gegevensverwerking noodzakelijk is:

- voor een goede behandeling van de betrokkene;
- of voor het beheer van de instelling of voorziening (artikel 30 lid 3 sub a UAVG).

Daarnaast geldt het verwerkingsverbod niet als de cliënt of (wettelijk) vertegenwoordiger zijn uitdrukkelijke toestemming (artikel 9 lid 2 sub a AVG) heeft gegeven voor de uitwisseling.

Concreet betekent dit, dat in een situatie als deze - waarin bijzondere persoonsgegevens uitgewisseld gaan worden met een toeleveranciers - de uitdrukkelijke toestemming van de cliënt of (wettelijk) vertegenwoordiger vereist is (artikel 9 lid 2 sub a AVG). Deze beoordeling van de gegevensuitwisseling op grond van de AVG moet worden bezien in combinatie met het medisch beroepsgeheim van de zorgprofessional. Dit beroepsgeheim kan slechts onder bepaalde voorwaarden worden doorbroken.

Tot slot dient de zorgorganisatie (ook hier) na te gaan of er sprake is van passende technische en organisatorische maatregelen ter beveiliging van de persoonsgegevens (artikel 32 AVG). Kan de e-mailuitwisseling veilig en verantwoord plaatsvinden? Neem daarbij de technische uitgangspunten, genoemd in 7.2, in acht.

< Terug naar de inhoudsopgave

Deel C Mobiele apparaten

Inleiding

Een **mobiel apparaat** (mobile device) is in feite een computer die in één hand is te houden. Deze apparaten geven in veel gevallen altijd en overal toegang tot informatie en/of communicatie (telefoonverkeer, mailen, verschillende mogelijkheden om berichten uit te wisselen, fotograferen en filmen). Voorbeelden van mobiele apparaten zijn mobiele telefoons, smartphones, laptops, notebooks, tablets en smartwatches. Deze apparaten kennen vele toepassingsmogelijkheden om informatie te delen: naast e-mailen bestaan diverse berichtenprogramma's zoals WhatsApp. Een groter publiek wordt bereikt als men gebruik maakt van social media (Facebook, Instagram, Snapchat etc.).

Deel C bestaat uit drie aparte onderdelen. Eerst wordt ingegaan op de algemene toepassingsmogelijkheden van mobiele apparaten in het kader van de zorg- en/of dienstverlening (klik hier voor i). Vervolgens wordt aandacht geschonken aan het communicatiemiddel WhatsApp en de daarbij behorende juridische vraagstukken (klik hier ii). Tot slot wordt de inzet van mobiele apparaten voor sociale doeleinden behandeld en de privacy issues die daarbij kunnen spelen (klik hier iii).

Subonderdeel C (i) Zorg- en/of dienstverlening

Mobiele apparaten worden steeds meer ingezet in de zorg. Een mobiel apparaat biedt bijvoorbeeld de mogelijkheid om gezondheidsgegevens over een cliënt snel uit te wisselen met collega's.

12 Doorloop privacy stappenplan

Voorafgaand aan de inzet van mobiele apparaten waarbij persoonsgegevens, waaronder gezondheidsgegevens, verwerkt gaan worden, moet worden beoordeeld of deze gegevensverwerking op grond van de AVG en UAVG mag plaatsvinden. Dit betekent dat allereerst moet worden nagegaan of sprake is van een uitzonderingsgrond op het verbod tot gegevensverwerking én of er een grondslag aanwezig is voor een rechtmatige verwerking (uitwisseling). Gebruik hiervoor het overkoepelende stappenplan. Tegelijkertijd moet worden beoordeeld in hoeverre de gegevensverwerking mogelijk is met inachtneming van het medisch beroepsgeheim/geheimhoudingsplicht van de zorgprofessional. Een doorbreking daarvan mag slechts onder bepaalde voorwaarden plaatsvinden.

Na het doorlopen van bovengenoemde aspecten kan tot besluitvorming worden gekomen om al dan niet mobiele apparaten in de zorg- en/of dienstverlening in te zetten.

< Terug naar de inhoudsopgave

Aandachtspunt:
Met betrekking tot de inzet van mobiele apparaten in de zorg- en/of dienstverlening is het van fundamenteel belang antwoord te krijgen op de vraag of sprake is van één of meer duidelijk bepaalde en gerechtvaardigde doeleinden voor het verwerken van gezondheidsgegevens (artikel 5 lid 1 sub b AVG). De zorgorganisatie moet daarbij grondig afwegen of de verwerking van de gezondheidsgegevens op deze wijze echt noodzakelijk is in het belang van de zorg- en/of dienstverlening. Verstrek enkel die gegevens die de ontvanger voor zijn doel (werkzaamheden) nodig heeft.

13 Hoe kan een zorgorganisatie het gebruik van mobiele apparaten in het kader van de zorg- en/of dienstverlening het beste inbedden?

Formuleer intern beleid: voorafgaand aan de inzet van mobiele apparaten (waarbij persoonsgegevens uitgewisseld gaan worden) dient hierover intern beleid te worden opgesteld. Uit dit beleid moet in ieder geval blijken wanneer, waarvoor, hoe, door wie deze apparaten worden ingezet en op welke wijze het gebruik veilig en verantwoord kan plaatsvinden en onderbouw op welke wijze wordt gehandeld met inachtneming van de AVG.

Maak afspraken: maak duidelijke praktische gebruikersafspraken met zorgprofessionals en/of cliënten en (wettelijk) vertegenwoordigers en leg dit schriftelijk vast.

Voorgaande punten vloeien voort uit de verantwoordingsplicht in artikel 5 lid 2 AVG. De verwerkingsverantwoordelijke (de zorgorganisatie) moet kunnen aantonen dat de deze de verplichtingen die in artikel 5 lid 1 AVG zijn opgenomen, naleeft. Daarnaast zijn het opstellen van procedures vereisten in het kader van het naleven de wettelijke principes “goede zorg” en “goed hulpverlenerschap” zoals neergelegd in de Wkkgz, Wmo 2015, de Jeugdwet en de Wgbo.

14 Mobiele apparaat: privé apparaat (BYOD[10]) of apparaat verstrekt door de zorgorganisatie?

Het heeft de voorkeur dat de zorgorganisatie aan haar medewerkers mobiele apparaten ter beschikking stelt die in het kader van de zorg- en/of dienstverlening worden gebruikt. De zorgorganisatie (als verwerkingsverantwoordelijke) moet veiligheidsmaatregelen treffen conform artikel 32 AVG. Derhalve wordt de inzet van een privé apparaat afgeraden, omdat de kans op een datalek groter is omdat de telefoon ook voor privé doeleinden wordt gebruikt.

10 BYOD staat voor Bring your own device. Dit moet worden onderscheiden van CYOD: choose your own device. Dit betekent dat de zorgorganisatie mobiele apparaten ter beschikking stelt waaruit gekozen kan worden. Het voordeel hiervan is dat de zorgorganisatie de beheersbaarheid op grond van een beperkte selectie aan producten optimaal kan organiseren.

< Terug naar de inhoudsopgave

Subonderdeel C (ii) WhatsApp en andere chatapplicaties in de zorg- en/of dienstverlening

Doordat mobiele apparaten film-, foto- en geluidsopnamefuncties kennen, net zoals 'gewone' camera's en geluidsapparatuur, zijn in onderdeel D (inzet camera's) veel gestelde vragen opgenomen over het gebruiken van deze functies in het kader van de zorg- en/of dienstverlening.

Inleiding

WhatsApp is een gratis middel dat snel, toegankelijk en laagdrempelig is en zich daardoor leent voor efficiënte gegevensuitwisseling binnen de zorg. Met WhatsApp kunnen berichten, bestanden, foto's en video's worden verstuurd. Het kan handig zijn om foto's te maken van pagina's uit een werkplan en deze te sturen aan collega's of een foto maken van een cliënt en deze ter beoordeling sturen naar een AVG-arts of een begeleider of dat er via de chatberichten informatie over een cliënt met een collega wordt gedeeld.

15 Bestaan er regels over het gebruik van chatapplicaties in de zorg?

Ja, in mei 2019 is de norm Eisen voor veilige e-mail en chatapplicaties (NTA 7516) gepubliceerd. Deze norm bevat randvoorwaarden voor het gebruik van ad hoc[11] e-berichtenverkeer via e-mail en chatapplicaties (al dan niet aangeboden via een berichtenportaal) en beoogt te realiseren dat de elektronische uitwisselingssystemen van de verschillende leveranciers op elkaar gaan aansluiten. (WhatsApp is eveneens een chatapplicatie.)
Het uiteindelijk doel is dat e-mail en chatapplicaties als een veilige vorm van uitwisseling van persoonlijke gezondheidsinformatie worden gebruikt.
De uitgangspunten welke voor chatapplicaties op grond van deze norm in acht moeten worden genomen zijn dezelfde als voor veilig e-mailgebruik.[12]

11 Met ad-hoc berichtenverkeer wordt bedoeld gegevensuitwisseling voor een bepaald geval of situatie waarbij de verzender en ontvanger allebei een mens zijn en waar tevoren geen specifieke afspraken konden worden gemaakt over eisen ten aanzien van beschikbaarheid, integriteit en vertrouwelijkheid. Automatisch berichtenverkeer valt niet onder ad-hoc berichtenverkeer. Niet tot het ad-hoc berichtenverkeer hoort in ieder geval EDIFACT-, HL7-, StUF- en conform IHE-standaarden gestructureerde berichten (definitie 3.2 NTA 7516).

12 In onderdeel 6.2.3 NTA 7516 is opgenomen dat in een volgende versie van de norm specifieke implementatie-eisen voor chatapplicaties kunnen worden opgenomen.

< Terug naar de inhoudsopgave

Chatapplicaties: een verzameling van ICT-diensten/producten voor ad-hoc berichtenverkeer1 anders dan e-mail (definitie 3.12).
Onder chatapplicaties worden ook messenger en instantmessaging-toepassingen verstaan.

16 Mogen zorgprofessionals een foto van een wond bij een cliënt of andere gezondheidsgegevens over de cliënt delen via WhatsApp met een collega?

Wat betreft het delen van foto's en andere persoonsgegevens, waaronder gezondheidsgegevens, via WhatsApp moet worden beoordeeld of de collega deze gegevens mag ontvangen, ervan uitgaande dat de gegevens herleidbaar zijn tot een persoon. Als een foto of andere informatie niet herleidbaar is tot een individueel persoon dan is er geen sprake van een persoonsgegeven. De AVG is dan niet van toepassing. Het versturen van persoonsgegevens via WhatsApp is dan mogelijk.

Kijk, indien nodig, in het overkoepelend stappenplan of het toegestaan is de persoonsgegevens te verwerken; de AVG kent een verbod op het verwerken van bijzondere persoonsgegevens (waaronder gezondheidsgegevens). Voor de zorg zijn daarop uitzonderingen gemaakt. Daarnaast heeft de zorgprofessional jegens de cliënt (en/of (wettelijk) vertegenwoordiger) een medisch beroepsgeheim/geheimhoudingsplicht in acht te nemen. Klik hier wanneer doorbreking mag plaatsvinden. Kort samengevat, in het kader van deze vraag, zal de gegevensuitwisseling via WhatsApp tussen collega's mogen plaatsvinden, omdat dit noodzakelijk zal zijn ten behoeve van de zorg- en dienstverlening van de cliënt. Daarnaast geldt het medisch beroepsgeheim niet voor zorgprofessionals en hun vervangers die rechtstreeks bij de zorgverlening van de cliënt zijn betrokken.[13]

ECHTER, WhatsApp is een publiek netwerk en er kan niet gegarandeerd worden dat anoniem ook echt anoniem is. Een foto bijvoorbeeld bevat metadata die herleidbaar kan zijn tot de locatie waar en het tijdstip waarop de foto gemaakt is waardoor een persoon toch direct of indirect geïdentificeerd kan worden. Daarnaast kan niet met zekerheid worden gesteld dat de beveiligingssystemen van WhatsApp voldoende zijn. Ook al is bij WhatsApp sprake van end-to-end-encryptie (versleuteling). Andere risico's zijn dat foto's vaak automatisch worden opgeslagen op het apparaat zelf en/of in de cloud; dat andere apps op de smartphone automatisch toegang kunnen hebben tot foto's in het apparaat; of dat de foto of andere informatie per ongeluk naar een andere persoon in de contactlijst wordt gestuurd. Het risico op een datalek is daarom hoog.

13 Betreft het daarentegen een externe behandelaar dan is hiervoor eerst de uitdrukkelijke toestemming van de cliënt en/of (wettelijk) vertegenwoordiger vereist. Een externe behandelaar is een behandelaar die geen directe dienstverlening is aangegaan met de zorgorganisatie en waarmee de betrokkene een aparte behandelingsovereenkomst of zorg- en/of dienstverleningsovereenkomst heeft afgesloten.

< Terug naar de inhoudsopgave

Daarnaast bevinden de servers van WhatsApp zich in een derde land.[14] Het is toegestaan persoonsgegevens vanuit de EU (Nederland) aan een derde land te verstrekken, mits dat land voldoende bescherming, waarborgen biedt voor de betrokkene. Maar met betrekking tot WhatsApp, als zijnde een gratis dienst, zijn daarover geen nadere afspraken te maken, zie onderdeel 4 in deze module.

ADVIES: vanwege de aanwezige risico's wordt het niet aangeraden om bijzondere persoonsgegevens (waaronder gezondheidsgegevens) via WhatsApp met elkaar uit te wisselen. Ook in geval van zakelijke mobiele apparaten verstrekt door de zorgorganisatie zelf verdient WhatsApp niet de voorkeur, vanwege het ontbreken van voldoende vertrouwelijkheid.

Let op: het voorgaande is ook van toepassing op Facebook Messenger of andere apps waarvan de veiligheid en betrouwbaarheid onvoldoende vaststaat.

17 Bestaan er veiligere alternatieven dan WhatsApp?

WhatsApp is onvoldoende transparant in de beveiliging die wordt gehanteerd, hoe profielen van gebruikers worden opgebouwd, waar gegevens worden opgeslagen, door wie en hoe deze gegevens worden gebruikt. Met Facebook als eigenaar van WhatsApp kunnen geen afspraken worden gemaakt over de omgang en beveiliging van persoonsgegevens. Het wordt daarom sterk afgeraden WhatsApp toe te passen in het kader van de zorg- en/of dienstverlening.

14 Derde landen zijn alle landen buiten de EU, met uitzondering van de landen in de Europese Economische Ruimte (EER). Dit zijn Noorwegen, Liechtenstein en IJsland. Deze drie landen kennen een gelijkwaardig niveau van bescherming van persoonsgegevens.

< Terug naar de inhoudsopgave

Er zijn inmiddels diverse varianten op WhatsApp beschikbaar die veiliger zijn. Zoals Siilo messenger (communicatie tussen zorgprofessionals) en Kanta messenger (een berichtenprogramma dat door zorgprofessionals en cliënten). Beoordeel of deze varianten geschikt zijn en kijk of met deze partijen afspraken gemaakt kunnen worden over de omgang, het gebruik en de beveiliging van persoonsgegevens. Daarnaast dient de zorgorganisatie te handelen met inachtneming van de norm Eisen voor veilige e-mail en chatapplicaties (NTA 7516). Hou verder rekening met het feit dat de AVG risico gestuurde wetgeving is. Dit houdt in dat de zorgorganisatie bij elke gegevensverwerking, dus ook bij het gebruik van chatapplicaties, moet nagaan welke risico's dit met zich mee kan brengen voor de betrokkenen. Op grond daarvan moet de zorgorganisatie beoordelen welke applicatie het meest passend is. Bij deze beoordeling en besluitvorming moet altijd rekening worden gehouden met:

- de stand van de techniek;
- de uitvoeringskosten;
- de aard, omvang, context en het doel van de verwerking;
- de risico's voor de betrokkenen.

Deze elementen bepalen in hoeverre de maatregelen haalbaar zijn. Technische mogelijkheden zijn steeds in ontwikkeling, dit brengt ook met zich mee dat de gekozen technische maatregelen periodiek moeten worden herzien. Zie voor meer informatie over de AVG-verplichtingen voor de zorgorganisatie module 3.

18 (Wettelijk) vertegenwoordiger en/of cliënt staat erop om via WhatsApp of andere onveilige app te communiceren. Wat moet de zorgorganisatie doen?

WhatsApp is niet gegarandeerd veilig, het gebruik van WhatsApp in de zorg wordt om die reden afgeraden. Er zijn andere apps die veiliger zijn om snel met een cliënt of (wettelijk) vertegenwoordiger te communiceren.

Als verwerkingsverantwoordelijke (zorgorganisatie) dient de zorgorganisatie te handelen conform de AVG. Bespreek daarom met de cliënt en/of (wettelijk) vertegenwoordiger dat in het kader van de bescherming van zijn of haar persoonsgegevens gekozen wordt voor communicatie via een andere app (dan WhatsApp). Daarnaast staan in de norm Eisen voor veilige e-mail en chatapplicaties uitgangspunten voor de zorgorganisatie om met de cliënt en/of (wettelijk) vertegenwoordiger om een situatie van veilig e-mailen en chatten in de thuissituatie te creëren.

< Terug naar de inhoudsopgave

Subonderdeel C (iii) Sociale doeleinden

Inleiding

Tegenwoordig kunnen cliënten, (wettelijk) vertegenwoordigers en/of verwanten door het gebruik van smartphones en social media snel op de hoogte worden gebracht van laatste nieuwtjes over de zorgorganisatie, aankomende sociale activiteiten of dat er een impressie wordt gegeven via beeld en/of geluid na een sociale activiteit. De zorgorganisatie heeft bijvoorbeeld een Facebook-pagina of een Instagram-account. Maar ook op de website (internet, intranet) van de zorgorganisatie of via WhatsApp kunnen dit soort berichten gedeeld worden. Van belang is om hier te handelen met in achtneming van de privacywetgeving. In dit onderdeel ligt vooral accent op het maken van foto's en filmpjes in het kader van sociale doeleinden en het delen hiervan via social media

19 Privacywetgeving en social media

Ook ten aanzien van het delen van persoonsgegevens (foto's, filmpjes etc.) via social media dient te worden voldaan aan de privacywetgeving. Zie het overkoepelende stappenplan in module 4 om te beoordelen of de zorgorganisatie de persoonsgegevens mag verwerken (lees: persoonsgegevens delen via social media).

20 Hoe voldoet een zorgorganisatie aan de wet- en regelgeving met betrekking tot het verwerken van persoonsgegevens via social media?

Het is niet zomaar toegestaan om een foto, film van een cliënt te delen op social media als aan de hand van deze beelden (of geluid) de cliënt (of een andere persoon) kan worden geïdentificeerd of identificeerbaar is. Er is dan sprake van een persoonsgegeven in de zin van artikel 4 onderdeel 1 AVG. Dit is ook al het geval bij het plaatsen van een tekstberichtje op social media waarin verwezen wordt naar een direct of indirect herleidbare persoon. Voorgaande betekent dat voor het mogen plaatsen van beeld- of geluidsmateriaal of andere informatie op social media gehandeld moet worden in lijn met de uitgangspunten van de AVG en om uitdrukkelijke toestemming moet worden gevraagd aan de cliënt of (wettelijk) vertegenwoordiger.

Er is specifiek sprake van uitdrukkelijke toestemming omdat:

1. via de beelden, geluiden, teksten duidelijk kan worden dat sprake is van een lichamelijke, verstandelijke of zintuiglijke beperking bij een cliënt waardoor deze informatie moet worden beschouwd als een bijzonder persoonsgegeven; en
2. ook al zou een beperking niet blijken uit de geplaatste informatie zelf dan nog ontstaat er een bijzonder persoonsgegeven, omdat het plaatsen op social media een activiteit is van de zorgorganisatie waardoor een relatie kan worden gelegd tussen een individu en een eventuele zorgbehoefte.

< Terug naar de inhoudsopgave

Er kan geen beroep worden gedaan op de AVG-uitzondering dat de beelden 'binnen huiselijke kring' worden gebruikt. Het plaatsen van het materiaal op social media houdt namelijk verband met zakelijke activiteiten; de activiteiten van de zorgorganisatie.

Advies voor de praktijk

Bespreek tijdig de social media activiteiten van de zorgorganisatie met de cliënt of (wettelijk) vertegenwoordiger. Een goed moment hiervoor is bij in zorg name van de cliënt. De zorgorganisatie kan de cliënt en/of (wettelijke) vertegenwoordiger op dat moment om toestemming vragen. Een model toestemmingsformulier is aan deze handreiking toegevoegd. Hierin staan verschillende opties beschreven waarvoor toestemming kan worden gegeven. Het is van belang dit goed met de cliënt en/of (wettelijk) vertegenwoordiger door te spreken. Geef de cliënt of de (wettelijk) vertegenwoordiger de gelegenheid hierover na te denken.

Het toestemmingsformulier kan al eerder worden toegestuurd of worden meegegeven bij het eerste gesprek met de cliënt of (wettelijk) vertegenwoordiger. Voeg het ondertekende toestemmingsformulier vervolgens toe aan het cliëntdossier en bespreek het periodiek met de cliënt of (wettelijk) vertegenwoordiger.

De cliënt of (wettelijk) vertegenwoordiger mag zijn toestemming altijd intrekken waarna de verwerking direct moet worden gestaakt. Op deze mogelijkheid tot intrekking moet de cliënt of (wettelijk) vertegenwoordiger voorafgaand aan de ondertekening van het toestemmingsformulier zijn geattendeerd.

Zie vraag 5 van module 2 voor het antwoord op de vraag wie toestemming geeft.

21 Zijn foto's en filmpjes bijzondere persoonsgegevens?

Ja, foto's en filmpjes, waarop personen geïdentificeerd of identificeerbaar zijn, worden beschouwd als een bijzonder persoonsgegeven. Uit de beelden kan namelijk iemands geloofsovertuiging, ras/etnische herkomst of gegevens over de gezondheid worden afgeleid (lichamelijke of verstandelijke beperking).

< Terug naar de inhoudsopgave

Bijzondere persoonsgegevens (artikel 9 lid 1 AVG):
"Persoonsgegevens waaruit ras of etnische afkomst, politieke opvattingen, religieuze of levensbeschouwelijke overtuigingen of het lidmaatschap van een vakbond blijken, genetische gegevens, biometrische gegevens, gegevens over de gezondheid en ook gegevens met betrekking tot iemands seksueel gedrag of seksuele gerichtheid."

Het is in beginsel verboden deze persoonsgegevens te verwerken behalve als sprake is van een uitzonderingsgrond en de betrokkene voor verwerking uitdrukkelijke toestemming heeft gegeven. Voor de gehandicaptenzorg is in dit geval artikel 30 UAVG van belang.

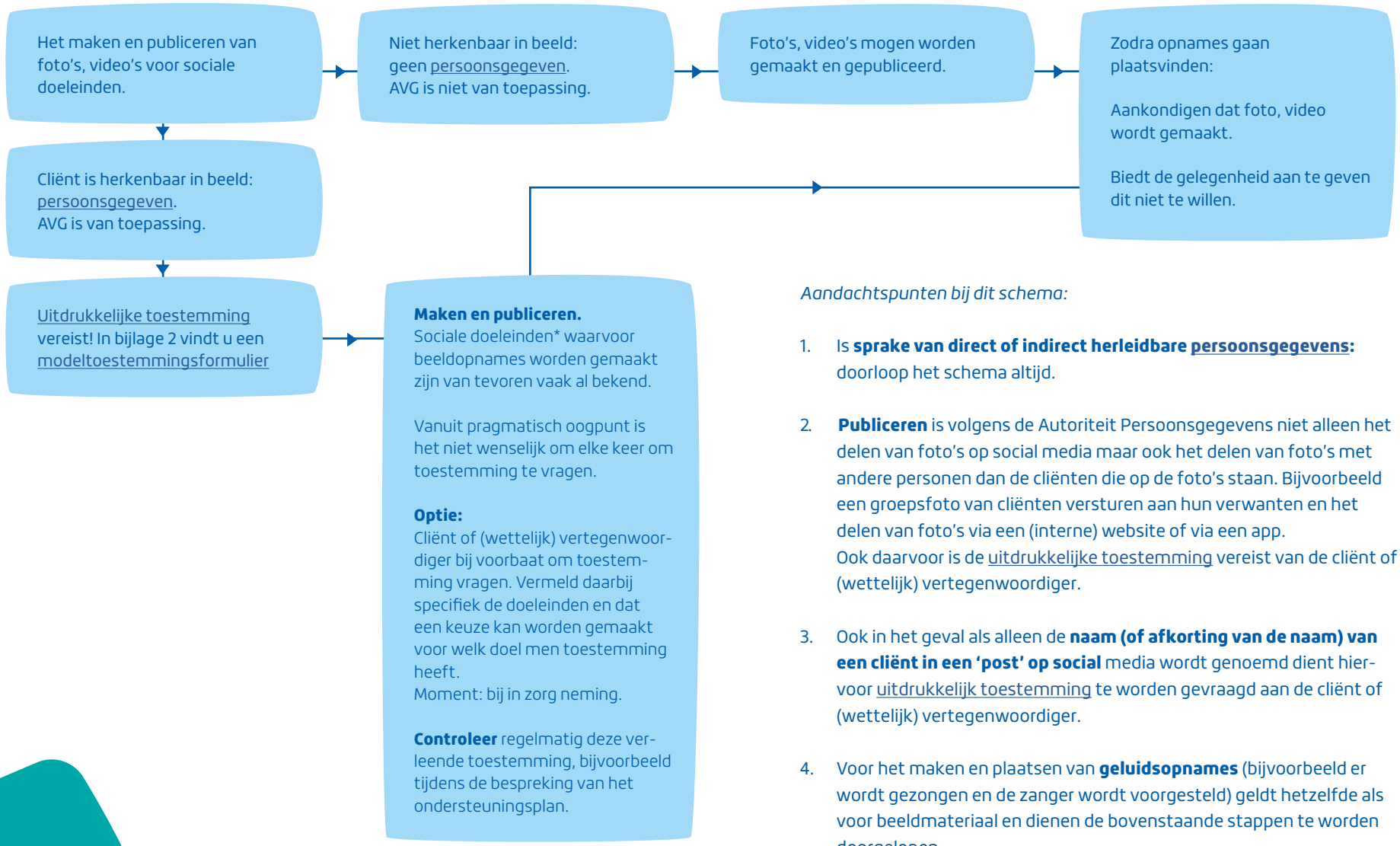
Doelgerichte benadering AP (2016): beveiligingsbeelden
Met betrekking tot het maken van camerabeelden in het kader van het beschermen van de veiligheid van personen en hun eigendommen heeft de Autoriteit Persoonsgegevens in 2016 een doelgerichte benadering geïntroduceerd. Als het doel van de camerabeelden is personen of goederen te beveiligen dan worden deze gegevens niet beschouwd als bijzondere persoonsgegevens (en geldt er geen verwerkingsverbod in de zin artikel 9 AVG).
Het is niet duidelijk of de AP deze benadering nog steeds zo hanteert. Zie meer informatie over beveiligingsbeelden vraag 35 en verder.

22 Er wordt geen toestemming door cliënt of (wettelijk) vertegenwoordiger verleend, wat moet een zorgorganisatie doen?

Wil een cliënt of de (wettelijke) vertegenwoordiger niet dat er foto's of filmpjes worden gemaakt ten behoeve van social media dan moet de zorgorganisatie daar in de praktijk rekening mee houden en voorkomen dat de cliënt (direct of indirect herleidbaar) in beeld komt.

23 Cliënt wil het wel, maar (wettelijke) vertegenwoordiger niet. Wat kan een zorgorganisatie doen?

In het geval een (wettelijk) vertegenwoordiger niet wil dat er beeld- en geluidsopnames worden gemaakt, maar de cliënt vindt het wel goed dan dient te worden beoordeeld of de cliënt over deze keuze wilsbekwaam ter zake is. Als dat het geval is mogen foto's, films worden gemaakt. Leg deze afweging en het uiteindelijke besluit vast in het cliëntdossier. Zie voor de duidelijkheid het schema hierna met betrekking tot foto's en filmpjes.



*Facebook, Instagram, Twitter, LinkedIn, nieuwsbrief, folders, intranet, website.

Aandachtspunten bij dit schema:

1. Is **sprake van direct of indirect herleidbare persoonsgegevens:** doorloop het schema altijd.

2. **Publiceren** is volgens de Autoriteit Persoonsgegevens niet alleen het delen van foto's op social media maar ook het delen van foto's met andere personen dan de cliënten die op de foto's staan. Bijvoorbeeld een groepsfoto van cliënten versturen aan hun verwanten en het delen van foto's via een (interne) website of via een app.
   Ook daarvoor is de uitdrukkelijke toestemming vereist van de cliënt of (wettelijk) vertegenwoordiger.

3. Ook in het geval als alleen de **naam (of afkorting van de naam) van een cliënt in een 'post' op social** media wordt genoemd dient hiervoor uitdrukkelijk toestemming te worden gevraagd aan de cliënt of (wettelijk) vertegenwoordiger.

4. Voor het maken en plaatsen van **geluidsopnames** (bijvoorbeeld er wordt gezongen en de zanger wordt voorgesteld) geldt hetzelfde als voor beeldmateriaal en dienen de bovenstaande stappen te worden doorgelopen.

< Terug naar de inhoudsopgave

24 Moet een zorgorganisatie een foto of film verwijderen als de toestemming ontbreekt?

Ervan uitgaande dat sprake is van een geïdentificeerde of identificeerbare persoon en:

- door hem of namens hem geen uitdrukkelijke toestemming is verleend of
- de verleende toestemming wordt ingetrokken of
- er wordt expliciet om verwijdering gevraagd.

In die gevallen moet het beeldmateriaal verwijderd worden van social media waarop deze geplaatst is. Ook als het een groepsfoto betreft.
Een alternatief om het beeldmateriaal te behouden is de persoon die (achteraf heeft aangegeven) niet in beeld te willen komen totaal onherkenbaar te maken (anonimiseren). Het is zorgvuldig dit dan nog even met de persoon in kwestie te bespreken.

25 Opnames of fotograferen voor t.v., krant of radio

Voor professionele opnames, fotoreportage, t.v., krant of radio moet de uitdrukkelijke toestemming te hebben worden verkregen van cliënten of (wettelijke) vertegenwoordigers en de medewerkers die daarbij aanwezig zullen zijn én daarnaast van de zorgorganisatie (persoon die rechtsgeldig bevoegd is daarvoor toestemming te geven, zoals voorzitter Raad van Bestuur).

26 Professionele fotograaf (filmcrew) komt langs en overlegt een quitclaim overeenkomst. Wat is dat?

Dit is een overeenkomst, vaak een formulier, tussen een fotograaf/filmer en de geportretteerde waarin aan de geportretteerde wordt gevraagd toestemming te verlenen voor het mogen (publiceren) van de foto's of filmmateriaal en daarmee afstand doet van zijn portretrecht.

Een verleende toestemming in het kader van een quitclaim overeenkomst kan in beginsel niet meer worden ingetrokken. Dat betekent dat de betrokkene zijn toestemming niet meer kan intrekken als persoonsgegevens (waaronder dus ook foto's en films) gebruikt worden voor journalistieke doeleinden en voor academische, artistieke of literaire uitdrukkingsvormen (artikel 43 lid 2 UAVG). Een quitclaim kan alleen aangetast worden wanneer er sprake is van onredelijke voorwaarden of als andere verplichtingen in deze quitclaim-overeenkomst niet zijn nagekomen. Men doet dan een beroep op bepalingen in het verbintenissenrecht.

< Terug naar de inhoudsopgave

Aandachtspunt:
Mocht de zorgorganisatie een fotograaf inhuren of worden benaderd door een tv-bedrijf voor een reportage waarbij een quitclaim overeenkomst wordt overlegd, kijk dan eerst goed naar de voorwaarden die in deze overeenkomst staan. Wanneer de cliënt of zijn (wettelijk) vertegenwoordiger de quitclaim overeenkomst tekent wordt daarmee toestemming verleend tot het mogen gebruiken van het beeldmateriaal. De zorgorganisatie kan hierin een faciliterende rol vervullen.

27 Hoe lang mogen foto's, films, geluidsopnames van cliënten die voor social media zijn gebruikt bewaard worden?

In het geval het beeld- en/of geluidsmateriaal direct of indirect herleidbaar is naar een persoon geldt de hoofdregel uit artikel 5 lid 1 sub e AVG: het beeld- en/of geluidsmateriaal mag *niet langer worden bewaard dan voor het doel noodzakelijk is.*

De verwerkingsverantwoordelijke (de zorgorganisatie) moet in dat geval termijnen bepalen wanneer de gegevens worden gewist dan wel momenten bepalen waarop periodiek wordt getoetst of de gegevens gewist moet worden (overweging 39 AVG). Maak bij het bepalen van deze termijnen een belangenafweging tussen het verwerkingsdoel en de mogelijke gevolgen voor de betrokkene (maakt het bewaren al niet inbreuk op zijn privacy).

In het geval een cliënt of andere persoon niet via beeld- en/of geluid kan worden geïdentificeerd of identificeerbaar is, is geen sprake van een persoonsgegeven in de zin van de AVG: dan gelden er geen bewaartermijnen.

Aandachtspunt:
In onderhavige vraag betreft het persoonsgegevens welke voor sociale doeleinden worden gebruikt. De bewaartermijn (van 15 jaar) op grond van artikel 7:454 lid 3 Wgbo is hier niet aan de orde. Klik hier voor een totaaloverzicht van de wettelijke bewaartermijnen in de zorg (zoals schriftelijke gegevens, financiële gegevens etc.).

Deel D Inzet van camera's in de zorgorganisatie

Inleiding

Het expliciet inzetten van camera's (vast of via mobiele apparaten) in een zorgorganisatie kan een rol vervullen in het kader van de zorg- en/of dienstverlening van een cliënt zoals bijvoorbeeld het opnemen van een gesprek tussen een persoonlijk begeleider en een cliënt of ten behoeve van een onderwijsactiviteit (subonderdeel i). Een ander doel betreft het structureel en/of incidenteel inzetten van camera's in het kader van algemeen veiligheidsbeleid ten behoeve van het beschermen

< Terug naar de inhoudsopgave

van de eigendommen, cliënten, medewerkers en bezoekers van een zorgorganisatie (zie subonderdeel ii). Daarnaast kan cameragebruik ingezet worden als een vorm van toezichthoudende domotica. Dit onderdeel ontbreekt in deze versie van de handreiking en zal worden aangevuld wanneer de handreiking wordt herzien in het kader van de inwerkingtreding van de Wet zorg en dwang.

Subonderdeel D (i) Beeld- en geluidsopnames

28. Mag een begeleidingsgesprek tussen een cliënt en een persoonlijk begeleider worden gefilmd via vaste camera of camerafunctie via mobiel apparaat?

Dit is mogelijk, mits de volgende voorwaarden en aandachtspunten in acht worden genomen:

1. Voorafgaand aan de opname moet het doel waarvoor de opname nodig is specifiek zijn bepaald en zijn vastgelegd in het cliëntdossier. De opname dient te worden vernietigd als deze niet meer voor het doel noodzakelijk is. Is een opname vanuit zorginhoudelijk oogpunt maar één keer nodig om terug te zien, dan moet deze daarna worden vernietigd. (Zie punt 4 als de gegevens langer nodig zijn).
2. Voordat de opname wordt gemaakt moet de cliënt of de (wettelijk) vertegenwoordiger hierover worden geïnformeerd én zijn uitdrukkelijke toestemming geven.
3. De opnames die worden gemaakt in het kader van de zorg- en dienstverlening vallen onder het medisch beroepsgeheim en zullen onderdeel uit moeten maken van het cliëntdossier als deze opnames in het belang zijn van de verdere zorg- en dienstverlening aan de cliënt.
4. Dit betekent dat ook voor deze beeldopnames de bewaartermijn van 15 jaar (na einde zorg) geldt en de betrokkene - cliënt en/of (wettelijk) vertegenwoordiger - een beroep op zijn privacyrechten kan doen (recht op inzage, afschrift en vernietiging etc.).
5. De opnames mogen niet voor een ander doel worden gebruikt, behalve als de cliënt of (wettelijk) vertegenwoordiger hiervoor uitdrukkelijk toestemming verleend. Verstrekking van de beelden aan anderen dan de cliënt mag alleen met toestemming van de cliënt of (wettelijk) vertegenwoordiger. Onder anderen wordt niet verstaan: andere zorgprofessionals of diens plaatsvervangers die betrokken zijn bij de zorg- en dienstverlening van de cliënt.

Het bovenstaande geldt ook voor geluidsopnames.

< Terug naar de inhoudsopgave

29. Is het mogelijk opnames te maken in het kader van onderwijs/intervisie activiteiten ten behoeve van zorgprofessionals van de zorgorganisatie?

Ja, dit kan. Dergelijke opnames kunnen nodig zijn om te beoordelen hoe een persoonlijk begeleider een gesprek voert met een cliënt. Het doel van deze opname is dan niet de zorg- en dienstverlening aan de cliënt maar de onderwijsactiviteit. Er zijn enkele voorwaarden en aandachtspunten:

1. De cliënt of zijn (wettelijk) vertegenwoordiger moet worden geïnformeerd over het doel van de opname, hoe lang deze bewaard wordt en wie de opname mag zien.
2. De cliënt of zijn (wettelijk) vertegenwoordiger moet voor deze opname zijn uitdrukkelijke toestemming geven. Immers, de opnames (de gegevensverwerking) vindt plaats voor een ander doel dan diens zorg- en dienstverlening.
3. Deze opnames maken geen onderdeel uit het dossier van de cliënt.
4. Als de opname is gebruikt in het kader van de onderwijsactiviteit dan moet deze daarna worden vernietigd.

30 Mag een kopie/scan van het legitimatiebewijs van een cliënt in het ECD worden opgenomen?

Nee, dat is niet toegestaan. Er bestaat geen wettelijke verplichting tot het opnemen van een kopie/scan van het legitimatiebewijs van een cliënt in de administratie van zorgorganisatie. Slechts bepaalde organisaties zijn op grond van de wet geoorloofd een kopie/scan van het identiteitsbewijs op te nemen: zoals overheidsinstanties, banken, notarissen en levensverzekeraars.

Een cliënt is wel verplicht zich op het moment dat hij in zorg komt te identificeren aan de hand van een geldig identiteitsbewijs,[15] bijvoorbeeld een paspoort of identiteitskaart. De gegevens op het identiteitsbewijs, zoals het nummer van het identiteitsbewijs, het type identiteitsbewijs en het Burgerservicenummer moeten vervolgens worden overgenomen (genoteerd) in de administratie van de zorgorganisatie. De identificatieplicht in de zorg en het opnemen van het Burgerservicenummer is geregeld in:

- de Wabvpz (artikel 4 t/m 6);
- de Wmo 2015 (artikel 2.3.4 en 5.2.9);
- de Jeugdwet (artikel 10.4 lid 3 sub a, 7.2.1 t/m artikel 7.2.4)

15 Paspoort; Nederlandse identiteitskaart; ID-kaart of paspoort EER-land; Nederlands vreemdelingendocument; rijbewijs. (Een rijbewijs kan niet als identiteitsbewijs worden gebruiken bij de Belastingdienst (tenzij de Belastingdienst anders aangeeft); een uitkeringsaanvraag; binnenlands vreemdelingentoezicht; inschrijving voor een opleiding bij een onderwijsinstelling; indiensttreding bij een nieuwe werkgever.

< Terug naar de inhoudsopgave

31 Mogen foto's van cliënten (met hun naam daaronder) op aanwezigheidsborden/presentielijsten staan op woon- of dagbestedingslocaties, ook zichtbaar voor buitenstaanders?

Het komt in de gehandicaptenzorg voor dat er in woningen of dagbestedingslocatie foto's van cliënten (al dan niet voorzien van hun namen) op aanwezigheidsborden hangen of op presentielijsten staan. In het kader van de zorg- en dienstverlening is het voor zorgprofessionals en andere zorgmedewerkers (waaronder ook flexwerkers en stagiaires) noodzakelijk om de cliënten te herkennen, zodat zij weten welke cliënten op een dagbestedingslocatie zorg ontvangen of welke cliënt in welk appartement woont. Het voorkomt daarnaast persoonsverwisselingen, bijvoorbeeld bij het toedienen van medicatie.

Aangenomen mag worden dat het gebruiken van foto's van cliënten in deze specifieke situaties noodzakelijk is voor een goede behandeling of verzorging; er is sprake van een uitzondering op het verwerkingsverbod (artikel 30 lid 3 sub a UAVG). Daarnaast dient voor het gebruiken van deze foto's een grondslag voor een rechtmatige verwerking (een rechtmatig gebruik) aanwezig te zijn. De grondslag hiervoor kan gevonden worden in artikel 6 lid 1 sub b AVG, de verwerking van de persoonsgegevens is noodzakelijk voor de uitvoering van een overeenkomt, in dit geval de zorg- en dienstverleningsovereenkomst. (artikel 6 lid 1 sub b AVG).

32 Mag een (pas)foto van de cliënt worden opgenomen in het (elektronisch) cliëntdossier?

Nee, behalve als het opnemen van de (pas)foto noodzakelijk is voor de behandeling of zorg van de cliënt (artikel 30 lid 3 sub a UAVG) en noodzakelijk is voor de uitvoering van de zorg- en dienstverleningsovereenkomst (artikel 6 lid 1 sub b AVG). In dat geval is het toegestaan een (pas)foto op te nemen zonder daarvoor uitdrukkelijke toestemming te vragen aan de cliënt of (wettelijk) vertegenwoordiger. Het kan per zorgorganisatie verschillen hoe en wanneer het (elektronisch) cliëntdossier wordt ingezet en of het dan noodzakelijk is om over de (pas)foto te kunnen beschikken. Let op: het moet door de zorgorganisatie duidelijk en aantoonbaar zijn vastgelegd dat opname van de pasfoto in het (elektronisch) cliëntdossier noodzakelijk is. Weeg dit zorgvuldig af, gebruik hiervoor het overkoepelend stappenplan.

Ontbreekt de noodzakelijkheid dan mag een foto niet worden opgenomen behalve als de cliënt of zijn (wettelijk) vertegenwoordiger hiervoor zijn uitdrukkelijke toestemming heeft gegeven.

< Terug naar de inhoudsopgave

33 Hoe lang moeten foto's, films, geluidsopnames van cliënten in het kader van de zorg- en dienstverlening bewaard worden?

Betreft het beeld- en/of geluidmateriaal dat in het kader van de zorg- en/of dienstverlening van een cliënt is gemaakt en dit materiaal dient om die reden onderdeel uit te maken van het cliëntdossier dan geldt een bewaartermijn van 15 jaar[16] na einde van deze zorg- en dienstverlening. Let op: gedurende deze periode dient het ook technisch mogelijk te blijven om het beeld en/of geluidsmateriaal te kunnen gebruiken (is de bijbehorende software nog beschikbaar of dient andere software te worden aangeschaft?)
Is de cliënt of een andere persoon niet direct of indirect herleidbaar is dan geldt er geen bewaartermijn. Er is immers geen sprake van een persoonsgegeven.
Klik hier voor een totaaloverzicht van de wettelijke bewaartermijnen in de zorg (zoals schriftelijke gegevens, financiële gegevens etc.).

34 Mogen foto's, films (sociale doeleinden) van cliënten langer bewaard worden, bijvoorbeeld vanuit historisch oogpunt?

Hoofdregel: foto's en/of films, waarop personen indirect of direct herleidbaar zijn, mogen niet langer worden bewaard dan het doel waarvoor ze oorspronkelijk zijn verzameld, behalve als de cliënt en/of (wettelijk) vertegenwoordiger hiervoor uitdrukkelijke toestemming heeft verleend.
Ter illustratie: stel een cliënt staat op een foto gemaakt tijdens een sociale activiteit van de zorgorganisatie. Zolang de client in zorg is, kan deze foto worden gebruikt voor sociale doeleinden, mits dat echt noodzakelijk is. Mocht de cliënt uit zorg gaan, dan verdwijnt het doeleinde waarvoor de foto bewaard moet blijven. De zorgorganisatie kan de foto aan de client meegeven (ook digitaal) en eventuele kopieën zal de zorgorganisatie moeten vernietigen.
Vaak zullen er meerdere cliënten op een foto staan, het is dan aan de zorgorganisatie om goed te beoordelen tot hoe lang het noodzakelijk is deze foto's, films te bewaren in relatie tot de sociale doeleinden waarvoor ze ooit zijn verzamelend.

16 In 2018 heeft de Minister voor Medische Zorg een wetsvoorstel ingediend om de Wgbo aan te passen. Een van die wijzigingen betreft het verlengen van de bewaartermijn tot 20 jaar met als start van deze termijn het moment waarop de laatste wijziging is aangebracht. Ten tijde van het schrijven van deze handreiking is het wetsvoorstel door de Eerste Kamer aangenomen met als verwachting dat de wet per 1 januari 2020 in werking treedt. De handreiking wordt dan op dit punt aangepast.

< Terug naar de inhoudsopgave

Uitzonderingen:

De AVG kent in artikel 5 lid 1 sub e de mogelijkheid om persoonsgegevens langer te bewaren in het kader van - wetenschappelijk of - historisch onderzoek of - statistische doeleinden.
Omdat bij beeldmateriaal sprake is van bijzondere persoonsgegevens moet voor het langer mogen bewaren van deze gegevens voldaan zijn aan **alle** hierna genoemde voorwaarden:

1. er is sprake van wetenschappelijk of historisch onderzoek of statistische doeleinden;
2. het onderzoek dient een algemeen belang;
3. het vragen van uitdrukkelijke toestemming van de cliënt of (wettelijk) vertegenwoordiger is onmogelijk gebleken of kost een onevenredige inspanning;
4. en er is voorzien in bepaalde waarborgen dat de persoonlijke levenssfeer niet onevenredig wordt geschaad;
   Welke waarborgen dat zijn, is afhankelijk van het concrete geval. Er zal dus goed gekeken moeten worden naar de aard en strekking van het onderzoek en de persoonsgegevens die het betreft. Zodra het onderzoek kan worden bereikt zonder persoonsgegevens dan moet met het gebruik daarvan worden gestopt.

   In het geval sprake is van wetenschappelijk onderzoek of statistiek geldt als **extra voorwaarde:**
5. dat de cliënt of (wettelijk) vertegenwoordiger geen uitdrukkelijk bezwaar heeft gemaakt tegen het verstrekken van gegevens ten behoeve van wetenschappelijk onderzoek of statistiek (artikel 7:458 lid 2 sub c BW).

Overleden personen: AVG niet van toepassing – wel medisch beroepsgeheim

Zijn er op de foto's of filmpjes personen te zien die inmiddels zijn overleden, dan is de AVG niet langer van toepassing. Gegevens van overledenen zijn geen persoonsgegevens volgens de AVG, omdat deze personen volgens de wet geen natuurlijke personen meer zijn. Niettemin blijft het medisch beroepsgeheim gelden na het overlijden van de cliënt. Het beroepsgeheim heeft betrekking op alle gegevens die de hulpverlener in de uitoefening van zijn beroep over de cliënt te weten is gekomen. Dit geheim geldt dus ook voor alle gegevens die onderdeel uitmaken van het cliëntendossier.

< Terug naar de inhoudsopgave

Wetenschappelijk onderzoek: dit kan fundamenteel onderzoek, toegepast onderzoek en technologische ontwikkeling en demonstratie zijn. Wetenschappelijk onderzoek wordt ruim opgevat onder de AVG. Het is niet beperkt tot onderzoek dat met publieke middelen wordt betaald.

Historisch onderzoek: historisch onderzoek en onderzoek voor genealogische doeleinden (onderzoek naar geschiedenis, herkomst, ontwikkeling van een onderwerp, voorwerp etc.). De AVG is zoals eerder gezegd niet van toepassing op overleden personen. Er bestaat ruimte voor de lidstaten om hier eigen regels over te stellen. De Nederlandse wetgever heeft dit nog niet gedaan, ondanks advies van de Autoriteit Persoonsgegevens dit wel te doen.

Statistische doelen: dit betekent dat het resultaat van de verwerking niet uit persoonsgegevens bestaat, maar uit geaggregeerde gegevens. (Dit resultaat en de persoonsgegevens mogen niet worden gebruikt als ondersteunend materiaal voor maatregelen of beslissingen die een bepaalde natuurlijke persoon betreffen.)

Subonderdeel D (ii) Bewakingscamera's in zorgorganisatie in het kader van algemene veiligheid

Inleiding

Ten behoeve van het beschermen van eigendommen en de bescherming van cliënten, familieleden, bezoekers, zorgprofessionals en andere medewerkers in de zorgorganisatie kunnen camera's worden ingezet. Deze inzet is meestal langdurend en structureel van aard.

Soms kan er sprake zijn van een tijdelijke inzet van een camera bijvoorbeeld bij of in het appartement van een cliënt omdat er bijvoorbeeld diefstallen hebben plaatsgevonden. Dit incidentele gebruik kan in de zorgorganisatie algemeen bekend zijn, maar ook verborgen (heimelijk) cameragebruik komt voor.

Via FAQ's wordt in dit subonderdeel beschreven hoe de inzet van camera's zich verhoudt tot de AVG. Deze FAQ's gaan alleen in op situaties waarin personen of persoonsgegevens in beeld komen.

< Terug naar de inhoudsopgave

35 Is de AVG van toepassing op bewakingstoezicht via camera's in een zorgorganisatie?

Ja. In geval van cameratoezicht zal in de meeste gevallen sprake zijn van persoonsgegevens in de zin van artikel 4 onderdeel 1 AVG, omdat personen direct herkenbaar (geïdentificeerd) in beeld worden gebracht. Ook als een persoon niet direct herkenbaar in beeld komt, kan daarvan sprake zijn omdat de persoon op grond van andere factoren zoals zijn kleding, haardracht of tatoeage identificeerbaar is.

Daarnaast dient het inzetten en gebruiken van camera's als een verwerking van persoonsgegevens in de zin van artikel 4 onderdeel 2 AVG worden beschouwd. Het betreffen verrichtingen, handelingen met persoonsgegevens waarbij het niet uitmaakt of de beelden al dan niet worden opgeslagen. Ook het live uitkijken van beelden is dus een verwerking van persoonsgegevens waarop de AVG van toepassing is.

Staan er **geen personen** op de beelden of zijn de personen **niet identificeerbaar** dan is de **AVG niet van toepassing.** Klik hier voor stroomschema I 'Is de AVG van toepassing?'.

Degene die beslist over de inzet van camera's is de verwerkingsverantwoordelijke. In het kader van deze handreiking is dat de zorgorganisatie, de Raad van Bestuur.

36 Kunnen beveiligingsbeelden worden gekwalificeerd als bijzondere persoonsgegevens (zoals gezondheidsgegevens)?

Allereerst wordt opgemerkt dat over dit punt geen juridische eenduidigheid bestaat, ook niet in verschenen jurisprudentie hierover. Strikt genomen is sprake van een bijzonder persoonsgegevens in de zin van artikel 9 lid 1 AVG, omdat uit de beelden kan worden afgeleid dat bij een persoon sprake is van een lichamelijke of verstandelijke beperking of wat diens religie of afkomst is. Dit brengt met mee dat het verboden is deze bijzondere persoonsgegevens te verwerken behalve als een beroep kan worden gedaan op een van de uitzonderingen genoemd in lid 2 van dit artikel (noodzakelijk met het oog op een goede behandeling of verzorging en noodzakelijk voor het beheer van de instelling of voorziening). Deze uitzonderingen zijn echter zodanig van aard dat deze zich niet goed zullen lenen voor het specifiek inzetten van camerabeveiliging, behalve als de betrokkene zijn uitdrukkelijke toestemming daarvoor verleend. Maar dit laatste is niet (altijd) praktisch omdat dan elke (nieuwe) bezoeker eerst om toestemming moet worden gevraagd voordat deze het terrein en/of de zorgorganisatie betreedt.

< Terug naar de inhoudsopgave

Pragmatische benadering

Tegenover deze strikte leer staat een pragmatische benadering. Deze benadering werd ten tijde van de Wbp gehanteerd door de Autoriteit Persoonsgegevens en houdt in als het cameragebruik als **doel heeft personen of goederen te beveiligen** dit meestal niet wordt aangemerkt als een verwerking van bijzondere persoonsgegevens. Deze lijn kan ook worden doorgetrokken naar de inzet van beveiligingscamera's in een zorgorganisatie. Als dit plaatsvindt ter beveiliging van cliënten, bezoekers en zorgprofessionals of andere medewerkers wordt het registreren van deze beelden niet beschouwd als verwerken van bijzondere persoonsgegevens. Onduidelijk is of deze benadering nog steeds mag worden gehanteerd met de komst van de AVG. De Autoriteit Persoonsgegevens heeft zich hier nog niet over uitgesproken. De Nederlandse wetgever heeft beoogd, daar waar de AVG ruimte biedt, het regime van de Wbp te handhaven. Het is verdedigbaar dat de pragmatische benadering nog steeds passend is onder de AVG.

Conclusie:

Uitgaande van de doelgerichte (pragmatische) benadering worden deze beveiligingsbeelden niet beschouwd als bijzondere persoonsgegevens (gezondheidsgegevens) en geldt er geen verwerkingsverbod (artikel 9 lid 1 AVG).

Voorgaande betekent niet dat de AVG niet van toepassing is, dat is wel het geval. Er blijft immers sprake van een verwerking van persoonsgegevens. Dit brengt met zich dat beveiligingscamera's pas kunnen worden ingezet nadat is voldaan aan een aantal voorwaarden. Vraag 37 t/m 40 behandelen enkele situaties uit de praktijk, in vraag 41 wordt een overzicht gegeven van de elementen waaraan ten minste moet zijn voldaan voordat tot camera inzet kan worden overgegaan.

(Zie onderdeel D(i) voor beelden die specifiek in het kader van de zorg- en dienstverlening worden gemaakt en vanaf 19 voor beelden in het kader van social media.)

37 Mag een zorgorganisatie beveiligingscamera's ophangen?

Ja, ter bescherming van eigendommen en voor de bescherming van cliënten, bezoekers, zorgprofessionals en andere medewerkers mogen camera's worden opgehangen, mits aan de volgende voorwaarden wordt voldaan:

- de zorgorganisatie moet een **gerechtvaardigd belang** hebben op grond van artikel 6 lid 1 sub f AVG: in deze situatie het beschermen van eigendommen en/of personen;
- het cameragebruik moet voldoen aan het **noodzakelijkheidsvereiste**: het is alleen toelaatbaar als het doel (het beschermen van de eigendommen en/of personen) niet op een andere manier kan worden bereikt;

< Terug naar de inhoudsopgave

- de **inbreuk** op de privacy moet **zo beperkt** mogelijk zijn: geen camera's in toilet-en/of doucheruimtes;
- iedereen moet gewezen worden op het cameragebruik (**informatieplicht**). Het moet voor iedereen duidelijk zichtbaar zijn dat er camerabeveiliging is.

Dit kan door de camera's duidelijk zichtbaar te plaatsen bij bijvoorbeeld de ingang van de zorgorganisatie, in gemeenschappelijke ruimtes of op het parkeerterrein.

Ook dient er een bordje "camerabewaking" bij de ingang van de zorgorganisatie en/of bij de ingang van het terrein te worden opgehangen.

Zie vraag 41 voor een beoordelingskader met daarin de elementen waaraan ten minste moeten zijn voldaan voordat tot de inzet van camera's kan worden overgegaan.

38 Vallen beveiligingsbeelden onder het medisch beroepsgeheim?

Camerabeelden, waarop een patiënt/cliënt herleidbaar is, vallen in het algemeen onder het medisch beroepsgeheim. Ook als een cliënt zich voor het eerst tot een zorgverlener wendt door een zorgorganisatie te betreden. Het is mogelijk dit beroepsgeheim jegens de cliënt te doorbreken in het geval van een conflict van plichten.[17] Denk bijvoorbeeld aan de situatie waarin de politie om beveiligingsbeelden zou kunnen verzoeken.

Een uitspraak van de Hoge Raad uit 2018 zegt verder het volgende: "Camerabeelden waaruit de identiteit van een patiënt of een (toekomstige) hulpverleningsrelatie valt af te leiden, kunnen onder beroepsgeheim en aldus onder het verschoningsrecht van een arts vallen. Dat op de camerabeelden ook bezoekers en begeleiders te zien zijn en dat de betreffende locaties voor iedereen toegankelijk zijn, maakt dat niet anders."[18]

17 KNMG-richtlijn Omgaan met medische gegevens, KNMG, mei 2018, pagina 88.
18 HR 10 april 2018, ECLI:NL:HR:2018:553.

< Terug naar de inhoudsopgave

39 Mag een zorgorganisatie een verborgen camera (heimelijk) ophangen?

Nee, dat mag in beginsel niet.
Maar zijn er duidelijke vermoedens (gegronde redenen) aanwezig voor ernstig onrechtmatig handelen door cliënten en/of dan mag onder bepaalde voorwaarden gebruik worden gemaakt van heimelijk cameratoezicht. Denk bijvoorbeeld aan diefstal of fraude.

Voorwaarden:

- Het lukt de zorgorganisatie niet, ondanks diverse inspanningen, een eind te maken aan de diefstal, fraude of ander onrechtmatig gedrag.
- De controle met de verborgen camera is tijdelijk. Permanent heimelijk cameratoezicht is niet toegestaan!
- Het doel waarvoor het heimelijk toezicht plaatsvindt betreft een specifiek doel dat strikt is omschreven.
- De privacyinbreuk op cliënten, bezoekers en zorgprofessionals (en andere medewerkers) is zo klein mogelijk. Dus geen camera's in bijvoorbeeld toiletruimtes of behandelruimtes.
- De zorgorganisatie heeft haar medewerkers er vooraf op gewezen dat verborgen camera's in bepaalde situaties (diefstal of fraude) mogelijk zijn. Dit dient dan te zijn opgenomen in het personeelsreglement of in een reglement cameratoezicht. Wat betreft cliënten en/of bezoekers kan dit worden opgenomen in het huishoudelijk reglement van de zorgorganisatie dat aan cliënten kan worden uitgereikt en op een centrale plek in de zorgorganisatie kan worden opgehangen, bijvoorbeeld bij de receptie, ontvangstbalie.
- De zorgorganisatie informeert zo spoedig mogelijk de betrokken zorgprofessionals en andere medewerkers en cliënten achteraf over het gebruik van de verborgen camera. En legt uit en licht toe – voor zover als mogelijk is op grond van de AVG – waarom sprake moest zijn van verborgen cameragebruik. (Het is vanzelfsprekend dat hierbij niet de bedoeling is dat persoonsgegevens worden verstrekt).
- Er is een DPIA uitgevoerd. (Behalve als het gaat om bestaand beleid voor de inzet van heimelijk cameratoezicht en de Autoriteit Persoonsgegevens dit in het verleden al heeft goedgekeurd en de verwerking in de tussentijd niet is veranderd.)[19]
- Is uit de DPIA naar voren gekomen dat de beoogde inzet van (verborgen) camera's een hoog privacyrisico oplevert? En lukt het de zorgorganisatie niet om maatregelen te vinden om dit risico te beperken? Dan moet de zorgorganisatie met de AP overleggen voordat cameratoezicht wordt gestart.

19 Onder de Wbp moest een werkgever heimelijk cameratoezicht vooraf bij de Autoriteit Persoonsgegevens melden en een voorafgaand onderzoek door de AP aanvragen. De AP toetste of het gebruik van de verborgen camera voldeed aan de wettelijke eisen. Met de inwerkingtreding van de AVG dient in plaats daarvan door de organisatie een DPIA te worden uitgevoerd.

< Terug naar de inhoudsopgave

Mocht later blijken dat heimelijk filmen in openbare ruimtes niet gerechtvaardigd was dan kan de gefilmde hiervan aangifte doen op grond van artikel 441b Wetboek van Strafrecht.

Of iets wel of niet gerechtvaardigd zal dienen te blijken uit de onderbouwing die de zorgorganisatie verstrekt en of de gefilmde personen in kwesties hiermee akkoord gaan.

Strafrechtelijk onderzoek
Indien na het doen van aangifte een strafrechtelijk onderzoek volgt dan is het mogelijk dat de politie de zorgorganisatie om de camerabeelden verzoekt. Hierbij wordt opgemerkt dat een zorgorganisatie niet vanzelfsprekend tot het verstrekken van deze beelden dient over te gaan, vanwege het beroepsgeheim en het verschoningsrecht dat aan de orde kan zijn. Het verstrekken van deze en andere persoonsgegevens aan politie of justitie valt verder buiten het bestek van de handreiking. Daarvoor wordt verwezen naar de VGN Publicatie Medisch beroepsgeheim en verschoningsrecht.

40 Mogen familieleden, (wettelijk) vertegenwoordiger of de cliënt zelf een verborgen camera in de woning/appartement/kamer ophangen omdat zij diefstal door een zorgprofessional of een andere medewerker vermoeden?

Dit mag in beginsel niet. Bezien vanuit het strafrecht is dit strafbaar op grond van artikel 139f lid 1 Wetboek van Strafrecht. Er mag niet heimelijk gefilmd worden in een woning of op een andere niet voor het publieke toegankelijke plaats. Bezien vanuit de privacywetgeving is het eveneens niet toelaatbaar vanwege de grote inbreuk op de persoonlijke levenssfeer op andere cliënten, zorgprofessionals of andere medewerkers.

Mocht als gevolg van het heimelijk filmen blijken dat het vermoeden van de cliënt/(wettelijk) vertegenwoordiger/familie bevestigd wordt dan geeft dat hen de mogelijkheid om op grond van het proportionaliteits- en subsidiariteitsbeginsel in de AVG te onderbouwen dat sprake was van zodanige omstandigheden dat het heimelijk filmen toelaatbaar was. Zij zullen dan moeten aantonen dat het belang van de gefilmde (bijvoorbeeld een zorgprofessional of andere cliënt) minder zwaar weegt dan het belang waarvoor gefilmd werd.

Ook de rechter kan in dit geval oordelen dat het filmen gerechtvaardigd was en kan de beelden meenemen in de bewijsvoering. Is dat niet zo dan kan sprake zijn van onrechtmatig verkregen bewijs.

< Terug naar de inhoudsopgave

Mocht achteraf echter blijken dat er geen sprake was van bijzondere omstandigheden dan kan degene die gefilmd is aangifte doen bij de politie op grond van artikel 139f lid 1 Wetboek van Strafrecht. Hiervan heeft men natuurlijk alleen weet als het heimelijk filmen bekend wordt gemaakt door bijvoorbeeld de familie of als de zorgorganisatie er zelf (per toeval) weet van krijgt. Zodra de zorgorganisatie hiervan op de hoogte is, is het advies om het beoordelingskader te doorlopen.

Strafrechtelijk onderzoek
Indien na het doen van aangifte een strafrechtelijk onderzoek volgt dan is het mogelijk dat de politie de zorgorganisatie om de camerabeelden verzoekt. Hierbij wordt opgemerkt dat een zorgorganisatie niet vanzelfsprekend tot het verstrekken van deze beelden dient over te gaan, vanwege het beroepsgeheim en het verschoningsrecht dat aan de orde kan zijn. Het verstrekken van deze en andere persoonsgegevens aan politie of justitie valt verder buiten het bestek van de handreiking. Daarvoor wordt verwezen naar de VGN Publicatie Medisch beroepsgeheim en verschoningsrecht.

41 Beoordelingskader inzetten camera vanuit algemene veiligheid

Voorafgaand aan het inzetten van camera's voor structureel en/of incidenteel gebruik dient een afweging plaats te vinden over onder meer doel en noodzaak. Om zorgorganisaties daarmee verder op weg te helpen is een kader opgesteld ter ondersteuning bij de besluitvorming hierover. **Alle** hierna genoemde elementen dienen in acht te worden genomen bij het nemen van een beslissing over het inzetten van camera's ten behoeve van algemene veiligheid.

I Bescherming van persoonsgegevens

De zorgorganisatie moet beoordelen of deze inzet plaatsvindt met in achtneming van de AVG-beginselen in artikel 5 AVG en de voorwaarden voor een rechtmatige gegevensverwerking in artikel 6 AVG. Zoals bij vraag 36 aangegeven geldt met betrekking tot het inzetten van beveiligingscamera's geen verwerkingsverbod omdat geen sprake is van het registeren van bijzondere persoonsgegevens.

Onderstaand de belangrijkste punten op een rij, welke ook door de Autoriteit Persoonsgegevens als essentieel worden geacht.

1. **Doelbinding:** waarom zijn de beelden nodig? Wat is het doel van deze gegevensverwerking? Heeft het te maken met de veiligheid van personen en/of zaken, toezicht op de werkplek? Dit doel dient helder en concreet te worden omschreven
2. **Informatieplicht:** de cliënt/(wettelijk) vertegenwoordiger, medewerker dienen over voldoende informatie te beschikken over het cameratoezicht. De zorgorganisatie moet ervoor zorgen dat cliënten, bezoekers en zorgmedewerkers weten dat er een camera hangt en voor welk doel deze er hangt. Bijvoorbeeld door bordjes op te hangen.

< Terug naar de inhoudsopgave

3. **Gerechtvaardigd belang:** De zorgorganisatie moet een gerechtvaardigd belang hebben voor het cameratoezicht. Bijvoorbeeld diefstal tegengaan of cliënten, bezoekers en medewerkers beschermen.
   Dit betekent dat er geen toestemming van de betrokkene nodig is indien sprake is van de AVG grondslag gerechtvaardigd belang.
4. **Noodzaak:** cameratoezicht in een zorgorganisatie is alleen mogelijk als dit echt noodzakelijk is.
   Subsidiariteit: De zorgorganisatie moet nagaan of er misschien minder ingrijpende maatregelen mogelijk zijn. Dat is in de praktijk wellicht moeilijk te bepalen. Uitgangspunt kan zijn 'des te verder van het lichaam, des te minder ingrijpend'. Maar ook welk middel zal de cliënt zelf als minst ingrijpend ervaren. Bij het inzetten van camera's moet kunnen worden aangetoond dat alle mogelijke alternatieven zijn verkend en dat de betreffende maatregel echt nodig is.
   Proportionaliteit: dit brengt met zich mee dat de zorgorganisatie na moet denken over de plaats, bereik en (duur van het) gebruik van de camera's.
5. **DPIA:**[20] Als de zorgorganisatie een grootschalig en/of systematisch cameratoezicht inzet om diefstal tegen te gaan of cliënten, bezoekers en personeel te beschermen, moet een DPIA (gegevensbeschermingseffectbeoordeling) worden uitgevoerd. Dit is bijvoorbeeld het geval als de zorgorganisatie structureel of gedurende een langere periode cameratoezicht inzet voor dit doel.
   Incidenteel heimelijk cameratoezicht: wil de zorgorganisatie dit in of bij een bepaalde ruimte inzetten (waaronder ook bij of in kamer/appartement cliënt), dan moet hiervoor altijd eerst een DPIA worden uitgevoerd.
6. **Passende technische en organisatorische maatregelen:** beveiligen en bewaren (wie mag iets doen met de beelden en als ze opgenomen worden, hoe lang worden ze bewaard en hoe worden ze vernietigd?)
   - Zorg dat onderhoud geborgd is, bijvoorbeeld door onderhoudscontracten en merk storingen tijdig op.
   - Test technologie bij ingebruikname en na onderhoud.
   - Analyseer meldingen over techniek (wat is de basale oorzaak van een melding: technisch of personele oorzaak).
   - Voer afgekeurde techniek af, om te voorkomen dat deze te goeder trouw toch gebruikt wordt omdat deze nog ergens staat. (Zoals het wissen van schijven die niet meer worden gebruikt, dit door het volledig formateren van de schijf).
   - Beveilig de camera's fysiek goed (dat ze niet weggenomen kunnen worden door onbevoegden).
   - Bewaartermijn: De zorgorganisatie mag de beelden niet langer bewaren dan noodzakelijk.

20 Behalve als het gaat om bestaand beleid voor de inzet van heimelijk cameratoezicht en de Autoriteit Persoonsgegevens dit in het verleden al heeft goedgekeurd en de verwerking in de tussentijd niet is veranderd. Onder de Wbp moest een werkgever heimelijk cameratoezicht vooraf bij de Autoriteit Persoonsgegevens melden en een voorafgaand onderzoek door de AP aanvragen. De AP toetste of het gebruik van de verborgen camera voldeed aan de wettelijke eisen. Met de inwerkingtreding van de AVG dient in plaats daarvan door de organisatie een DPIA te worden uitgevoerd.

< Terug naar de inhoudsopgave

Bewaartermijn structureel cameragebruik (veiligheid): de beelden mogen niet langer worden bewaard dan noodzakelijk. De huidige richtlijn daarvoor is **4 weken.**
Maar als er een incident is vastgelegd, bijvoorbeeld een diefstal, dan mag de zorgorganisatie de desbetreffende beelden bewaren totdat dit is afgehandeld.
Bewaar termijn heimelijk cameratoezicht: direct vernietigen na gebruik, tenzij de opnames nog nodig zijn als bijvoorbeeld bewijsmateriaal in het kader van strafrechtelijk onderzoek.

7. **Rechten van betrokkenen:** Daarnaast kunnen de betrokkenen een beroep doen op hun rechten.
   En gelden vanzelfsprekend de overige verplichtingen voor een verwerkingsverantwoordelijke voortkomende uit de AVG.
8. **Extra aandachtspunt:** Bezien in relatie tot een cliënt die (in)direct herleidbaar op de beveiligingsbeelden te zien is, vallen deze camerabeelden in het algemeen onder het medisch beroepsgeheim en mogen deze niet zomaar verstrekt worden aan derden.

II Betrek cliëntenraad en OR van de zorgorganisatie

Een onderbouwd besluitvoornemen om cameratoezicht in te zetten en het beleid hierin moeten tijdig voor advies aan de OR én de cliëntenraad worden voorgelegd. Dit vloeit voort uit de Wet medezeggenschap cliënte zorginstellingen (Wmcz) en de Wet op de ondernemingsraden (WOR).

Cliëntenraad

Aan de cliëntenraad komt een verzwaard adviesrecht toe, omdat het systematisch bewaken van de kwaliteit van zorg aan cliënten een voor cliënten geldende regeling betreft dan wel een algemeen beleid op het gebied van veiligheid (artikel 4 jo. artikel 3 lid 1 en j Wmcz).

Geadviseerd wordt om voorafgaand daaraan eerst oriënterend in gesprek te gaan met de cliëntenraad.

Verzwaard advies recht houdt in dat de zorgorganisatie alleen van het advies van de cliëntenraad kan afwijken als de zorgorganisatie bij de commissie van vertrouwenslieden (die op grond van artikel 10 Wmcz moet zijn ingesteld) voldoende aannemelijk kan maken dat hij hiervoor gegronde redenen heeft. De commissie van vertrouwenslieden moet dan vaststellen dat de zorgorganisatie bij afweging van de betrokken belangen in redelijkheid tot zijn voornemen heeft kunnen komen (art. 4 lid 2 Wmcz).

< Terug naar de inhoudsopgave

Ondernemingsraad

De OR heeft instemmingsrecht op het besluit tot het inzetten van cameratoezicht (artikel 27 lid 1 sub k en l WOR).
Het instemmingsrecht brengt met zich mee dat de OR een bindend oordeel kan uitspreken over een aantal onderwerpen van sociaal beleid, het gaat dan om belangrijke veranderingen van de arbeidsvoorwaarden en belangrijke veranderingen van de arbeidsomstandigheden.

Als de zorgorganisatie van het voorgenomen besluit geen instemming van de OR heeft verkregen, dan kan de zorgorganisatie de kantonrechter toestemming vragen om het besluit te nemen. Deze geeft slechts toestemming, als de beslissing van de OR om geen instemming te geven onredelijk is, of het voorgenomen besluit van de zorgorganisatie nodig is vanwege zwaarwegende bedrijfsorganisatorische, bedrijfseconomische of bedrijfssociale redenen (artikel 27 lid 4 WOR).

Module 2

Privacy in de relatie cliënt - zorgprofessional

Module 2 - Privacy in de relatie cliënt - zorgprofessional

- Verstrekking van de cliënt gegevens
- Recht op inzage en afschrift + bewaartermijn en vernietiging

Inleiding

Deze module bestaat uit twee delen die ingaan op de 'privacyrelatie' cliënt - zorgprofessional. Deel A beschrijft het verstrekken (uitwisselen) van cliëntgegevens binnen de zorgorganisatie met collega's en het verstrekken door de zorgprofessional/zorgorganisatie aan externe (zorg)organisaties. Hiermee wordt ingezoomd op een specifiek element in de definitie verwerking van persoonsgegevens artikel 4 sub 2 AVG (zie de vetgedrukte woorden).

> *Verwerking:*
> Elke bewerking of elk geheel van bewerkingen van persoonsgegevens, al dan niet geautomatiseerd, **zoals het** verzamelen, vastleggen, ordenen, structureren, opslaan, bijwerken of wijzigen, **opvragen**, raadplegen, gebruiken, **verstrekken door middel van doorzending, verspreiden of op andere wijze ter beschikking stellen,** samenbrengen of combineren, en ook het afschermen, wissen of vernietigen van gegevens.

Met de term "verwerken" wordt daaronder dus ook het verstrekken c.q. uitwisselen van persoonsgegevens bedoeld.

In deel B wordt ingegaan op het recht van inzage en afschrift van de betrokkene ('privacyrecht') in combinatie het medisch beroepsgeheim, de geheimhoudingsplicht. Naast het feit dat voor het verwerken van bijzondere persoonsgegevens (gezondheidsgegevens) sprake moet zijn van een uitzondering op het verwerkingsverbod (artikel 30 UAVG) dient de zorgprofessional zijn medisch beroepsgeheim (geheimhoudingsplicht) in acht te nemen waarvan een doorbreking slechts onder bepaalde voorwaarden kan plaatsvinden. In het kader van deze module brengt dat met zich mee dat de zorgprofessional niet zomaar cliëntgegevens mag verstrekken.

Verder wordt in dit deel ook aandacht geschonken aan de wettelijke bewaartermijnen en (privacyrecht) vernietiging van cliëntdossier. Deze module is vooral praktisch van aard met verwijzingen naar de andere modules in de handreiking.

< Terug naar de inhoudsopgave

Deel A Gegevensuitwisseling binnen en buiten de zorgorganisatie

1 Gegevensverstrekking de basis: wie, wanneer, waarom?

Op hoofdlijnen kan een onderscheid worden gemaakt tussen het verstrekken van cliëntgegevens binnen de zorgorganisatie waar de cliënt zorg- en/of dienstverlening ontvangt en het verstrekken van cliëntgegevens naar anderen die niet werkzaam of verbonden zijn aan de zorgorganisatie. Denk bij dit laatste aan het verstrekken van cliëntgegevens aan ziekenhuizen of individuele zorgaanbieders zoals een huisarts of een tandarts in het kader van een behandeling. Daarnaast werken zorgorganisaties geregeld met elkaar samen in de zin van onderaannemerschap waarbij ook uitwisseling van cliëntgegevens plaatsvindt. En verder het verstrekken van cliëntgegevens aan instanties zoals het zorgkantoor, gemeentes of het CAK. De doeleinden voor het verstrekken van cliëntgegevens kunnen derhalve zorginhoudelijk, financieel en/of administratief van aard zijn.

2 Verwerking van (bijzondere) persoonsgegevens mag niet zomaar plaatsvinden.

Artikel 9 lid 1 AVG kent een **verbod** op het verwerken van bijzondere[1] persoonsgegevens, waaronder gezondheidsgegevens. Dit verbod is ingegeven vanuit het feit dat deze persoonsgegevens naar hun aard bijzonder gevoelig zijn vanwege hun relatie met de grondrechten en fundamentele vrijheden van personen. Deze persoonsgegevens genieten extra bescherming doordat is geregeld dat het in beginsel verboden is deze bijzondere persoonsgegevens te verwerken. Op dit verbod bestaan echter uitzonderingen. Er geldt een ontheffing van het verwerkingsverbod voor hulpverleners (zorgprofessionals) en instellingen of voorzieningen voor onder meer gezondheidszorg en maatschappelijke dienstverlening mits de gegevensverwerking (van gezondheidsgegevens) noodzakelijk is:

- voor een goede behandeling van de betrokkene;
- of voor het beheer van de instelling of voorziening. Onder beheer valt het waarborgen van de kwaliteit van de verleende zorg, intercollegiale toetsing door hulpverleners (zorgprofessional) onderling (kwaliteitsbeheer).

Deze uitzondering is opgenomen in artikel 30 lid 3 sub a UAVG.
Voorgaande betekent dat zorgorganisaties voor de gehandicaptenzorg gezondheidsgegevens mogen verwerken.

Het verwerkingsverbod geldt daarnaast ook niet als de betrokkene uitdrukkelijke toestemming heeft verleend voor deze gegevensverwerking (artikel 9 lid 2 sub a en artikel 6 lid 1 sub a AVG.)

1 In de gehandicaptensector maken cliënten vaak nog gebruik van hun eigen huisarts.

< Terug naar de inhoudsopgave

Dit neemt niet weg dat vóórdat de verwerking feitelijk plaatsvindt ook een van de grondslagen genoemd in artikel 6 lid 1 AVG aanwezig moet zijn. Alleen dan is sprake van een rechtmatige gegevensverwerking. Heeft een gegevensverwerking plaatsgevonden zonder dat daarvoor een grondslag aanwezig was dan is deze verwerking onrechtmatig. Verder moet voldaan zijn aan de algemene AVG-beginselen met betrekking tot het zorgvuldig omgaan met persoonsgegevens (artikel 5 AVG).

Aandachtspunt:
Bij het verwerken van (bijzondere) persoonsgegevens is het medisch beroepsgeheim (de geheimhoudingsplicht) van de zorgprofessional relevant. Naast het feit dat voor het verwerken van bijzondere persoonsgegevens (gezondheidsgegevens) eerst sprake moet zijn van een uitzondering op het verwerkingsverbod (artikel 30 UAVG) dient de zorgprofessional zijn medisch beroepsgeheim, in acht te nemen welke slechts onder bepaalde voorwaarden doorbroken kan worden, waarna een verdere verwerking mag plaatsvinden. Zie vraag 16 en 17 van deze module.

Klik hier voor het overkoepelend stappenplan hoe om te gaan met een privacyvraagstuk.

3 Hoe kan een zorgprofessional beoordelen of hij/zij persoonsgegevens mag verwerken?

Een leidraad om te beoordelen welke AVG-grondslag van toepassing is, is de volgende.

Vertrekpunt 1:

- De feiten. Welke persoonsgegevens betreft het; zijn het gewone persoonsgegevens of bijzondere; wie heeft deze gegevens nodig en waarvoor?

Vertrekpunt 2:

- Is de verwerking van bijzondere persoonsgegevens noodzakelijk voor een goede behandeling van de betrokkene of voor het beheer van de organisatie of
- heeft betrokkene uitdrukkelijke toestemming gegeven voor het verwerken van de bijzondere persoonsgegevens?

< Terug naar de inhoudsopgave

Vertrekpunt 3:

- Loop de grondslagen langs in artikel 6 AVG → begin met grondslag 2 t/m 6.
- Zijn 2 t/m 6 niet van toepassing dan kan gekeken worden naar grondslag 1: toestemming vragen aan de betrokkene.

Kan geen beroep worden gedaan op grondslag 2 t/m 6 en betrokkene wil geen toestemming verlenen dan mag de gegevensverwerking niet plaatsvinden.

Kies de meest geschikte grondslag

Het is van belang de grondslag te kiezen die het meest geschikt is met in achtneming van de algemene beginselen voor gegevensverwerking genoemd in artikel 5 AVG.

Ter verduidelijking:

In het geval wordt besloten tot het vragen om toestemming van de betrokkene en de verleende toestemming wordt later ingetrokken, dan is het niet mogelijk om terug te vallen op de grondslag gerechtvaardigd belang (artikel 6 lid 1 sub f AVG). Hierdoor kunnen mogelijke bedrijfsactiviteiten in het geding komen.

Klik hier voor het overkoepelend stappenplan ter beoordeling van een privacyvraagstuk.

4 Kunnen meerdere grondslagen uit artikel 6 AVG tegelijkertijd van toepassing zijn?

Ja, deze situatie kan zich ook voordoen. Kies de grondslag die het meest in lijn is met de AVG-beginselen in artikel 5 AVG. Wees bewust bij het vragen om toestemming dat deze altijd kan worden ingetrokken. Zie vraag 3. Derhalve is het vertrekpunt: begin met het beoordelen of grondslag 2 t/m 6 van toepassing kunnen zijn en eindig dan vervolgens met grondslag 1 (toestemming vragen).

< Terug naar de inhoudsopgave

5 Toestemming: wie verleent deze?

De AVG spreekt over de betrokkene die toestemming verleent voor het verstrekken van zijn/haar persoonsgegevens. In de gehandicaptenzorg kan sprake zijn van een (wettelijk) vertegenwoordiger die namens de cliënt diens belangen behartigd in het geval de cliënt dat niet zelf kan (wilsonbekwaam ter zake). De VGN heeft de betrokkenen als volgt geduid:

- zorgvrager (toekomstig cliënt);
- cliënt;
- wettelijk vertegenwoordiger (mentor, curator, ouders, voogd);
- schriftelijk gemachtigde;
- belangenbehartiger[2] (de echtgenoot, de geregistreerd partner, de levensgezel, een ouder, een kind, een broer of zuster).

Daarnaast heeft de VGN een onderscheid gemaakt in twee feitelijke situaties omtrent het verlenen van toestemming: vóór aanvang van zorg en tijdens de zorg- en/of dienstverlening. Zie de tabellen hierna.

2 In 2018 heeft de Minister voor Medische Zorg bij de Tweede Kamer een wetsvoorstel ingediend om de Wgbo aan te passen. Een van die wijzigingen betreft het toevoegen van grootouder en kleinkind van de patiënt als belangenbehartiger (artikel 7:465 lid 3 BW). Ten tijde van het schrijven van deze handreiking is het wetsvoorstel door de Eerste Kamer aangenomen met als verwachting dat de wet per 1 januari 2020 in werking treedt. De handreiking zal dan worden aangepast.

< Terug naar de inhoudsopgave

Vóór aanvang zorg- en/of dienstverlening	
In het geval	**Toestemming door**
Cliënt minderjarig tot en met 15 jaar	Ouder(s) en/of voogd(en)[3]
Cliënt 16 jaar of ouder en wilsbekwaam	Cliënt zelf[4]
Cliënt minderjarig en wilsonbekwaam ter zake	Ouder(s) en/of voogd(en)[5]
Cliënt meerderjarig en wilsonbekwaam ter zake	Curator[6] of mentor[7] Schriftelijke gemachtigde[8] (Schriftelijk gemachtigde: de door cliënt aangewezen persoon die op basis van een schriftelijke opdracht van cliënt zelf deze vertegenwoordigt in geval van wilsonbekwaamheid en de cliënt bijstaat in de behartiging van zijn belangen. Let op: het betreft de situatie waarin cliënt schriftelijke machtiging heeft gegeven toen deze wilsbekwaam was om daarover te beslissen.)

3 art. 5 UAVG jo. art. 1:233 jo. art 1:245 BW.
4 art. 5 UAVG.
5 art. 1:233 jo. 1:245 BW.
6 art. 1:378 BW.
7 art. 1:450 BW.
8 art. 3:60 BW e.v.

< Terug naar de inhoudsopgave

Tijdens de zorg- en/of dienstverlening	
In het geval	**Toestemming door**
Cliënt niet ouder dan 11 jaar	Ouder(s) en/of voogd(en)[9]
Cliënt 12 tot en met 15 jaar	Ouder(s) en/of voogd(en) én cliënt mits deze wilsbekwaam is.[10]
Cliënt 16 jaar of ouder en wilsbekwaam	Cliënt zelf[11]
Cliënt minderjarig en wilsonbekwaam ter zake	Ouder(s) en/of voogd(en)[12]
Cliënt meerderjarig en wilsonbekwaam ter zake	Curator of mentor[13] Schriftelijke gemachtigde[14] (Schriftelijk gemachtigde: de door cliënt aangewezen persoon die op basis van een schriftelijke opdracht van cliënt zelf deze vertegenwoordigt in geval van wilsonbekwaamheid en de cliënt bijstaat in de behartiging van zijn belangen. Let op: het betreft de situatie waarin cliënt schriftelijke machtiging heeft gegeven toen deze wilsbekwaam was om daarover te beslissen.)
Cliënt meerderjarig en wilsonbekwaam ter zake en een wettelijk vertegenwoordiger (ouder(s), voogd(en), curator, mentor) of schriftelijk gemachtigde ontbreekt dan wel dat deze personen niet in de hoedanigheid wensen op te treden.	Belangenbehartiger[15] (De belangenbehartiger kan in het geval van een meerderjarige cliënt zijn: de echtgenoot, de geregistreerd partner, de levensgezel, een ouder, een kind, een broer of zuster.)

9 art. 7:465 lid 1 BW.
10 art. 7:450 lid 2 BW.
11 art. 7:447 BW.
12 art. 7:465 lid 2 BW.
13 art. 7:465 lid 2 BW.
14 art. 7:465 lid 3 BW.
15 art. 7:465 lid 3 BW.

< Terug naar de inhoudsopgave

6 Hoe (op welke wijze) moet toestemming worden gegeven (artikel 7 AVG)?

De AVG schrijft niet voor op welke wijze toestemming gevraagd en verkregen moet worden. Dit betekent dat er dus verschillende vormen voor het verlenen van toestemming kunnen worden gehanteerd. Bijvoorbeeld via een schriftelijke verklaring, met elektronische middelen (zoals het online plaatsen van vinkje in een vakje) of een mondelinge verklaring.

Als maar duidelijk blijkt, **aantoonbaar is**, dat de betrokkene:

- vrijelijk (vrije wil);
- specifiek (geen blanco volmacht);
- geïnformeerd (over aard en doel van de verwerking);
- ondubbelzinnig (geen twijfel aanwezig)

met de verwerking van zijn persoonsgegevens heeft ingestemd.

7 Wat betekent een uitdrukkelijk gegeven toestemming?

Ten aanzien van bijzondere persoonsgegevens, waaronder dus ook gezondheidsgegevens, geldt een strenger toestemmingsregime! De AVG spreekt in dat verband over toestemming die uitdrukkelijk moet zijn verkregen (artikel 9 AVG en art. 22 UAVG).[16]

Uitdrukkelijk heeft betrekking op de manier waarop de toestemming tot uitdrukking wordt gebracht. Er moet sprake zijn van een expliciete bevestiging van de toestemming door middel van een verklaring. Een schriftelijke verklaring ligt dan voor de hand, maar dat hoeft niet.

De Groep Gegevensbescherming artikel 29 heeft aangegeven dat in de digitale of online context het voorstelbaar is dat een betrokkene de vereiste verklaring kan verstrekken door het invullen van een elektronisch formulier, door het versturen van een e-mail, door het uploaden van een gescand document waarop de handtekening van de betrokkene staat, of door middel van een elektronische handtekening. In theorie kan het gebruik van mondelinge verklaring ook voldoende zijn om geldige uitdrukkelijke toestemming te verkrijgen, maar dit kan voor de verwerkingsverantwoordelijke moeilijk te bewijzen zijn dat bij het opnemen van de verklaring voldaan is aan alle voorwaarden voor geldige uitdrukkelijke toestemming.

16 Dit onderdeel wordt ook besproken in module 4 in het belang van het beschrijven van het gehele wettelijk kader. Voor de volledigheid treft u dit aspect ook hier aan.

< Terug naar de inhoudsopgave

Advies

Geadviseerd wordt dat de zorgorganisatie waar dat mogelijk is een directe verklaring door de cliënt en/of (wettelijk) vertegenwoordiger laat ondertekenen om zo eventuele twijfels en gebrek aan bewijs over de aantoonbaarheid van de gegeven toestemming te voorkomen. In bijlage 2 is een modeltoestemmingsformulier opgenomen. Zie vraag 5 voor wie toestemming geeft.[17]

8 Geheimhoudingsplicht - Wgbo, Wlz, Wmo 2015, Jeugdwet

Leden van de VGN passen de Wgbo naar analogie toe bij hun zorg- en dienstverlening.[18] De Wgbo regelt de relatie tussen de zorgprofessional en cliënt en kent diverse privacy bepalingen zoals het recht op inzage in het cliëntdossier en het recht op vernietiging.

Daarnaast hebben leden van de VGN ook te maken met de Wlz, Wmo 2015 en de Jeugdwet. Ook deze wetten kennen privacy bepalingen (resp. artikel 9.1.2 lid 5 Wlz, artikel 5.3.3 Wmo 2015 en artikel 7.3.11 Jeugdwet). Het kenmerk van de zorgwetten is dat zij zijn opgesteld vanuit het gedachtegoed: de rechten van de cliënt.

De privacybepalingen in de zorgwetten bestaan naast de AVG-bepalingen en worden gezamenlijk toegepast. Omdat er in de praktijk veel vragen leven over de verhouding van deze wetten ten opzichte van de AVG wordt dit hierna verder uitgewerkt aan de hand van FAQ's toegespitst op het recht op inzage en afschrift van persoonsgegevens.

9 Op welke personen is het medisch beroepsgeheim van toepassing?

Deze geheimhouding geldt voor zorgprofessionals en hun waarnemers.
Deze personen krijgen in hun werk regelmatig te maken met persoonlijke informatie over hun cliënten. Op papier, digitaal of mondeling. Zij moeten daar vertrouwelijk mee omgaan, zij hebben derhalve een geheimhoudingsplicht. Dit is onder meer neergelegd in artikel 7:457 lid 1 BW (Wgbo). De zorgprofessional (zorgorganisatie) draagt er zorg voor: dat zonder toestemming van de cliënt geen inlichtingen over de cliënt, inzage in of afschrift van de bescheiden van de cliënt aan anderen worden verstrekt tenzij er sprake is van overmacht of van vereisten uit andere wet- en regelgeving. Zie ook vraag 16 van deze module.
Voor andere medewerkers in de zorg kan sprake zijn van een afgeleid medisch beroepsgeheim.

17 Groep gegevensbescherming artikel 29, Richtsnoeren inzake toestemming overeenkomstig Verordening 2016/679, pagina 21).

18 De VGN heeft in 2008 voor haar leden een richtlijn gemaakt over de toepassing van de WGBO in de gehandicaptensector. De richtlijn is op 3 april 2008 aangenomen door de Algemene Ledenvergadering en is op 1 januari 2009 ingegaan. Meer informatie vindt u hier: http://www.vgn.nl/artikel/2171.

< Terug naar de inhoudsopgave

10 Wat is een afgeleid medisch beroepsgeheim en voor wie geldt dat?

Mensen die in de zorg werken, maar niet direct betrokken zijn bij de zorg- en/of dienstverlening hebben een van deze zorgprofessional afgeleid medisch beroepsgeheim. Dit houdt in dat zij uit hoofde van hun beroep op de hoogte kunnen raken van cliëntgegevens. Dat kunnen bijvoorbeeld zijn: de bestuurders van de zorgorganisaties, secretaresses, stagiaires, schoonmakers en IT-medewerkers.[19] Ook voor hen geldt derhalve een geheimhoudingsplicht.

11 Hoe om te gaan met geheimhouding bij vrijwilligers en mantelzorgers?

Vrijwilligers of mantelzorgers die af en toe een handje komen helpen in de zorgorganisatie vallen niet onder het afgeleid beroepsgeheim zoals dat wel geldt voor secretaresses of stagiaires.

Vrijwilligers

In het geval van vrijwilligers dient de geheimhouding te worden geregeld in de vrijwilligersovereenkomst. Tevens moet bij elke cliënt worden bepaald wat de vrijwilliger aan informatie (gegevens) nodig heeft om zijn werk goed te kunnen doen.

Mantelzorger (geen (wettelijk) vertegenwoordiger)

De zorgprofessional mag zonder toestemming van de cliënt of (wettelijk) vertegenwoordiger geen informatie over de cliënt aan een mantelzorger verstrekken. Deze geheimhouding geldt niet als de cliënt of zijn (wettelijk) vertegenwoordiger daarvoor toestemming heeft gegeven.

Als een cliënt een mantelzorger heeft, is het dus raadzaam met de cliënt of (wettelijk) vertegenwoordiger af te spreken met welke cliëntgegevens de mantelzorger bekend mag raken; met andere woorden dat voor het verstrekken van deze gegevens uitdrukkelijke toestemming is verleend. Leg dit vast in het cliëntdossier.

12 Mogen cliëntgegevens binnen de zorgorganisatie onderling worden uitgewisseld met collega's?

Binnen één zorgorganisatie, tussen collega's onderling, kan een onderscheid worden gemaakt tussen de verwerking van cliëntgegevens ten behoeve van een zorginhoudelijk doel en een financieel-administratief doel. Waarbij wordt opgemerkt dat onder de zorgorganisatie de stichting wordt verstaan. Heeft de stichting meerdere locaties dan vallen deze nog steeds onder dezelfde zorgorganisatie.

19 Artikel 7:464 BW in samenhang met artikel 7:457 BW.

< Terug naar de inhoudsopgave

a. Verwerken van cliëntgegevens ten behoeve van de zorg- en of dienstverlening

De gegevens welke noodzakelijk zijn bij de uitvoering van de zorg- en/of dienstverlening en/of jeugdhulp zijn zonder toestemming beschikbaar voor de zorgprofessionals die rechtstreeks bij de uitvoering van de zorg- en dienstverlening en/of jeugdhulp zijn betrokken. Dit geldt ook voor de waarnemers van de zorgprofessionals. Ook andere collega's (geen zorgprofessionals) die uit hoofde van hun beroep met cliëntgegevens in aanraking komen (zoals secretaresses, stagiaires) mogen deze persoonsgegevens verwerken. Het betreffen in het bijzonder medische gegevens én andere gegevens die verband houden met de gezondheid. Denk in de gehandicaptensector aan behandelgegevens/rapportages van onder andere paramedici, psychologen, orthopedagogen en persoonlijk begeleiders die van belang zijn voor goede zorg en ondersteuning.

"Slechts die gegevens die men nodig heeft."
In alle gevallen geldt dat zorgprofessionals of andere collega's slechts de beschikking krijgen over die (bijzondere) persoonsgegevens welke noodzakelijk zijn voor het verrichten van hun werkzaamheden.
In de praktijk kan dit betekenen dat een AVG-arts volledig toegang heeft tot de gegevens van een cliënt, omdat dit noodzakelijk is voor zijn werkzaamheden. En een persoonlijk begeleider 'slechts' voor een klein gedeelte van het dossier, aangezien alleen dat deel voor zijn werkzaamheden relevant is.

AVG-grondslag

Het verwerken van cliëntgegevens in het kader van de zorg- en/of dienstverlening (zorginhoudelijk doel) vindt zijn verwerkingsgrondslag in artikel 6 lid 1 sub b AVG. De gegevens zijn noodzakelijk ter uitvoering van de zorg- en/of dienstverleningsovereenkomst[20] die tussen de cliënt en de zorgorganisatie tot stand is gekomen. Maar ook mogelijk in een wettelijke verplichting (artikel 6 lid 1 sub c AVG) tot het verwerken van deze gegevens, zoals artikel 5.1.2 lid 1 Wmo 2015 waarin is beschreven dat een aanbieder die een maatwerkvoorziening levert bevoegd is tot het verwerken van persoonsgegevens, waaronder gezondheidsgegevens.

20 Een zorg- en/of ondersteuningsrelatie wordt in de gehandicaptenzorg veelal via schriftelijke overeenkomst geregeld. Bij de jeugdhulpverlening is dat (nog) niet het geval, maar ook hier kan een beroep op artikel 6 lid 1 sub b AVG worden gedaan. De AVG kent namelijk geen vormvereiste met betrekking tot dit onderdeel. Ook de artikelen 6:217 BW (het tot stand van een overeenkomst) en 7:446 BW (Wgbo, behandelingsovereenkomst) kennen geen vormvereiste. Dit brengt met zich mee dat een overeenkomst zowel schriftelijk als mondeling kan zijn.

< Terug naar de inhoudsopgave

Dit toont (dus) aan dat voor eenzelfde gegevensverwerking meerdere grondslagen van toepassing kunnen zijn. Breng dit goed voor de zorgorganisatie in beeld.

b. Verwerken van cliëntgegevens ten behoeve van een financieel-administratief doel

De cliëntgegevens die noodzakelijk zijn ten behoeve van de (financiële) administratie van de zorgorganisatie dienen binnen de zorgorganisatie inzichtelijk te zijn voor de personen die deze nodig hebben in het kader van hun financieel-administratieve werkzaamheden.

De verwerking heeft betrekking op administratieve gegevens die de zorgorganisatie zelf genereerd zoals het opstellen van declaraties voor geleverde zorg. Deze declaraties zijn uiteindelijk bestemd voor het zorgkantoor, de zorgverzekeraar of de gemeente. Het heeft ook betrekking op het verwerken van (persoons)gegevens die door de cliënt zelf verstrekt zoals uitkeringsgegevens, salaris of bankafschriften welke met het oog op de zorg- en/of dienstverlening voor de zorgorganisatie noodzakelijk zijn om te verkrijgen.

AVG-grondslag

De interne verwerking van financieel-administratieve persoonsgegevens kan zijn rechtmatigheid vinden in meerdere grondslagen: de verwerking is noodzakelijk voor de uitvoering van de zorg- en/of dienstverleningsovereenkomst (artikel 6 lid 1 sub b AVG) of op grond van een wettelijke verplichting (artikel 6 lid 1 sub c AVG) bijvoorbeeld neergelegd in zorgspecifieke wetgeving.

13 Cliëntgegevens komen per ongeluk terecht bij collega die geen betrokkenheid heeft met deze cliënt. Wat moet de collega doen?

Deze collega, ongeacht zijn functie, heeft een geheimhoudingsplicht. Zorgprofessionals hebben een geheimhoudingsplicht op grond van de Wgbo en de Wet Big. Niet-zorgprofessionals die vanwege hun beroep wel met cliëntgegevens maken kunnen krijgen, hebben een afgeleid medisch beroepsgeheim. Daarnaast regelt de CAO Gehandicaptenzorg een geheimhoudingsplicht. Deze geheimhoudingsplicht geldt voor iedereen waarop de CAO Gehandicaptenzorg van toepassing is.

Zodra men (ontvanger en/of verzender) zich realiseert dat deze abusievelijke informatieverstrekking heeft plaatsgevonden, dient men hiervan een interne melding te doen op grond van het protocol datalekken van de zorgorganisatie. Dit laatste geldt ook als men de gegevens per ongeluk naar een persoon of organisatie buiten de zorgorganisatie heeft gestuurd.

< Terug naar de inhoudsopgave

14 Mogen cliëntgegevens per post worden verstuurd aan een (wettelijk) vertegenwoordiger of externe zorgprofessional?

Ja, mits het gebeurt met zo min mogelijk risico's. Verstuur in ieder geval de persoonsgegevens van een cliënt in een gesloten envelop. Uiteraard is het ook van belang om de gegevens van de geadresseerde goed te controleren, zodat men zeker weet dat de post aan de juiste persoon wordt gestuurd. Als het om gevoelige informatie gaat, zoals bijzondere persoonsgegevens, is het sterk aan te raden om een veiliger bezorgmethode te kiezen dan de gewone post. Bijvoorbeeld de post per koerier(sbedrijf) of aangetekend te versturen. Dit om het risico dat post in verkeerde handen valt, zo klein mogelijk te maken.

Beoordeel vóór verzending of de (wettelijk) vertegenwoordiger en/of de externe zorgprofessional de bijzondere persoonsgegevens mag ontvangen, gezien de geheimhoudingsplicht en verstrek vervolgens alleen die gegevens die voor de ontvanger noodzakelijk zijn.

15 Mogen stagiaires, studenten, onderzoeksorganisaties ten behoeve van wetenschappelijk of historisch onderzoek bijzondere persoonsgegevens verwerken?

Ja, het verrichten van wetenschappelijk onderzoek of historisch onderzoek of het verwerken van bijzondere persoonsgegevens ten behoeve van statistische doelen is mogelijk via twee routes

a. Na uitdrukkelijk verkregen toestemming van de cliënt of (wettelijk) vertegenwoordiger (artikel 9 lid 2 sub a AVG en artikel 22 lid 2 sub a AVG). De uitdrukkelijke toestemming van de cliënt en/of de (wettelijk) vertegenwoordiger is vereist, omdat de persoonsgegevens voor een ander doel worden gebruikt dan waarvoor ze oorspronkelijk - de zorg/ondersteuningsrelatie - zijn verzameld.
b. Door een beroep te doen op artikel 24 UAVG. Dit artikel kent een ontheffingsverbod op het verwerken van bijzondere persoonsgegevens als:
    i. dat noodzakelijk is voor wetenschappelijk of historisch onderzoek of statistische doeleinden én;
    ii. het onderzoek een algemeen belang dient (bijvoorbeeld in het belang van de volksgezondheid) én;
    iii. het vragen van uitdrukkelijke toestemming onmogelijk blijkt of een onevenredige inspanning kost.

Het heeft de voorkeur eerst voor optie a te kiezen.

Bij de uitvoering van de bovengenoemde doeleinden geldt als **wettelijke verplichting** dat zodanige **waarborgen** zijn getroffen dat de persoonlijke levenssfeer van de betrokkene niet onevenredig wordt geschaad (artikel 24 sub d UAVG). Welke waarborgen dat zijn is afhankelijk van het concrete geval. Er kunnen bijvoorbeeld voorschriften worden opgesteld over wie

< Terug naar de inhoudsopgave

toegang tot de gegevens heeft, over de geheimhouding omtrent het onderzoek en over de presentatie van de resultaten van het onderzoek. Denk verder aan het aggregeren van gegevens en (de wijze van) pseudonimiseren.

Zie vraag 38 in verband met het langer mogen bewaren van bijzondere persoonsgegevens in het kader van deze doeleinden.

Doorbreking medisch beroepsgeheim

16 Wanneer mag het medisch beroepsgeheim worden doorbroken?

Op de hoofdregel dat de zorgprofessional vanwege zijn medisch beroepsgeheim geen informatie over de cliënt aan anderen mag verstrekken, bestaan een aantal uitzonderingen. Zo geldt het medisch beroepsgeheim niet ten opzichte van:

1. de rechtstreeks bij de zorgverlening van de cliënt betrokken zorgprofessionals en hun vervangers (artikel 7:457 lid 2 Wgbo);
2. de (wettelijk) vertegenwoordiger(s) van de cliënt (artikel 7:457 lid 3 Wgbo) .

Daarnaast geldt het medisch beroepsgeheim niet:

3. als de cliënt of (wettelijk) vertegenwoordiger zijn uitdrukkelijke toestemming heeft gegeven voor het verstrekken van de gegevens;
4. in geval van veronderstelde toestemming van de cliënt;

Verder bestaat een mogelijkheid tot het doorbreken van het medisch beroepsgeheim op grond van:

5. een wettelijke bepaling welke met zich mee brengt dat de zorgprofessional cliëntinformatie moet verstrekken;
6. conflict van plichten;

Aandachtspunt 1:
Naast de uitzonderingen op het medisch beroepsgeheim zal aan de eisen van de (U)AVG voldaan moeten worden voordat bijzondere persoonsgegevens van de cliënt mogen worden uitgewisseld. Dit betekent dat er sprake moet zijn van een uitzonderingsgrond én een (verwerkings)grondslag op het verbod om bijzondere persoonsgegevens te mogen uitwisselen. Klik hier voor het overkoepelende stappenplan om te beoordelen of de zorgorganisatie handelt volgens de AVG.

Aandachtspunt 2:
Verstrek alleen die cliëntgegevens die voor de ontvanger noodzakelijk zijn.

< Terug naar de inhoudsopgave

17. Wanneer is sprake van een conflict van plichten op grond waarvan het medisch beroepsgeheim mag worden doorbroken?

Conflict van plichten betekent dat de zorgprofessional in een zodanige situatie is komen te verkeren waarin een ander belang zwaarder weegt dan zijn medisch beroepsgeheim.
Door dan inlichtingen te verstrekken (met andere woorden het schenden van de geheimhoudingsplicht) kan ernstig nadeel bij een ander, de cliënt of zichzelf worden voorkomen. Deze uitzondering op het beroepsgeheim is in de rechtspraak ontwikkeld. Voordat doorbreking van het medisch beroepsgeheim op grond van conflict van plichten kan plaatsvinden moet zijn voldaan aan alle hierna genoemde criteria:

1. Is alles geprobeerd om toestemming te krijgen?
2. Als het beroepsgeheim niet worden doorbroken, ontstaat er dan ernstige schade voor een ander of de cliënt zelf?
3. Is er gewetensnood ontstaan door het handhaven van het beroepsgeheim?
4. Is er geen andere manier om ernstige schade te voorkomen?
5. Zal het doorbreken van het beroepsgeheim vrijwel zeker leiden tot het voorkomen of beperken van ernstige schade?

Aandachtspunt
Alleen direct relevante gegevens mogen worden verstrekt en zo min mogelijk persoonsgegevens. In geval van twijfel en ook als daar behoefte aan bestaat wordt aangeraden de situatie met een collega en/of leidinggevende te bespreken.

< Terug naar de inhoudsopgave

18. Geldt het medisch beroepsgeheim na overlijden?

Ja, na het overlijden van de cliënt geldt nog steeds de geheimhoudingsplicht, het medisch beroepsgeheim. Hier bestaan een aantal uitzonderingen op die op basis van jurisprudentie zijn ontwikkeld:[21]

1. De overledene heeft iemand tijdens zijn leven gemachtigd om na zijn overlijden zijn dossier in te zien. Met andere woorden de cliënt heeft bij leven toestemming gegeven voor deze specifieke inzage.
2. Een persoon die uit hoofde van zijn of haar verantwoordelijkheid voor de overledene ook na overlijden aanspraak kan maken op het dossier: de (wettelijk) vertegenwoordiger. Als deze persoon al inzage in het dossier had tijdens het leven van de cliënt, dan mogen zij dat ook daarna hebben.[22]

Bij overlijden van de cliënt eindigt het mentorschap en de onder curatele stelling van rechtswege. Het recht op inzage voor mentoren en curatoren werkt na overlijden door.

21 De Minister voor Medische Zorg heeft in 2018 een wetsvoorstel ingediend ter aanpassing van Wgbo onder andere op het inzagerecht voor nabestaanden in het medisch dossier van een overleden patiënt. Het wetsvoorstel bevat de volgende drie gronden voor inzage:
1. De overleden patiënt heeft bij leven toestemming gegeven voor inzage na overlijden en deze toestemming is schriftelijk of elektronisch vastgelegd.
2. Een nabestaande of een persoon als bedoeld in 7:465 lid 3 BW die op grond van de Wet kwaliteit, klachten en geschillen zorg (Wkkgz) een mededeling van een zorgaanbieder heeft ontvangen dat een incident (art. 10 lid 3 Wkkgz) heeft plaatsgevonden.
3. De nabestaande heeft een zwaarwegend belang bij inzage en kan aannemelijk maken dat dit belang wordt geschaad, de inzage moet noodzakelijk zijn voor de behartiging van dit belang.
Daarnaast is in het wetsvoorstel het inzagerecht voor ouders en/of voogd van een overleden kind tot 16 jaar verruimd. Bij leven hebben de ouders of voogd van een kind in het kader van de Wgbo diverse verantwoordelijkheden en rechten (afhankelijk van de leeftijd van het kind). De wetgever vindt het in de rede liggen om de ouders en/of voogd bij een kind dat de leeftijd van zestien jaar nog niet had bereikt recht op inzage te geven na overlijden van het kind. Dit inzagerecht wordt niet verleend als dat in strijd is met het goed hulpverlenerschap. Ten tijde van het schrijven van deze handreiking (juni 2019) is het wetsvoorstel in de Eerste Kamer aangenomen, met als verwachte datum van inwerkingtreding 1 januari 2020. De handreiking zal dan worden aangepast.

22 De wetswijziging van de Wgbo brengt met zich mee dat de ex-mentor van een overleden patiënt geen inzagerecht meer heeft, behalve als sprake is van een zwaarwegend belang. De praktijk zal moeten uitwijzen of dit stand houdt. Tweede Kamerlid Renkema heeft in dit kader een motie ingediend (TK 2018-2019, 34994, nr. 16), welke ook is aangenomen, waarin wordt verzocht om in de nog op te stellen handreiking expliciet aandacht te geven aan de positie van een ex-mentor of vertegenwoordiger ten opzichte van een wilsonbekwame patiënt omtrent het inzagerecht in het medisch dossier, ook na diens overlijden. De handreiking zal dan worden aangepast.

< Terug naar de inhoudsopgave

3. Als de toestemming van de cliënt kan worden verondersteld. Bijvoorbeeld bij een naaste die tijdens het leven van de cliënt betrokken was bij de zorg- en/of dienstverlening.
4. Als een wet daartoe verplicht. Zo kent artikel 10 lid 3 Wkkgz de verplichting dat als een incident in de zorgverlening heeft plaatsgevonden waarbij de cliënt is overleden de zorgorganisatie ook aan de nabestaande doorgeeft wat de aard en toedracht van het incident is geweest.
5. Als een zwaarwegend belang speelt en verondersteld kan worden dat de cliënt wel toestemming zou hebben gegeven. Over deze uitzondering moet niet te snel besloten worden. Een zwaarwegend belang is bijvoorbeeld dat het dossier nodig is in verband met een onderzoek naar een medische fout. Een zwaarwegend belang kan ook aan de orde zijn bij het aanvechten van een testament door nabestaanden. Als er een andere manier is om de informatie te verkrijgen dan verdient dat altijd de voorkeur.
6. Een laatste uitzondering betreft in het geval van conflict van plichten. Als er een situatie is dat er gevreesd moet worden voor ernstig (levens)gevaar voor anderen.

Verstrekken van gegevens aan externe zorgorganisaties en/of zorgprofessionals niet werkzaam bij de zorgorganisatie.

19. Mag een zorgprofessional gegevens uitwisselen met bijvoorbeeld de huisarts, het ziekenhuis of een psycholoog van een cliënt?

Nee, voor het verstrekken van gegevens aan deze externe behandelaren is de toestemming van de cliënt of zijn (wettelijk) vertegenwoordiger vereist. Toestemming is vereist omdat de cliënt met deze externe behandelaar een eigen behandelrelatie heeft waar de zorgorganisatie buiten staat. Wanneer een zorgorganisatie op structurele basis een externe behandelaar of zorgorganisatie wil ‘inhuren’ dan is sprake van onderaanneming.

Zou de zorgorganisatie (zorgprofessional) deze gegevens wel verstrekken, zonder toestemming van de cliënt of (wettelijk) vertegenwoordiger, dan wordt daarmee de geheimhoudingsplicht op grond van artikel 7:457 BW, artikel 7.3.11 Jeugdwet, artikel 5.3.3 Wmo 2015 of artikel 9.1.2 lid 5 Wlz geschonden.

Voor de goede orde: het betreft bij deze vraag de situatie waarin de **externe** zorgorganisatie of **externe** individuele zorgaanbieder zijn **eigen behandelrelatie/zorg- en dienstverleningsovereenkomst** met de cliënt heeft. Dit moet worden onderscheiden van onderaannemerschap zoals bedoeld in vraag 21.

< Terug naar de inhoudsopgave

Aandachtspunt
Om uitdrukkelijke toestemming kan worden gevraagd op het moment dat een persoon in zorg komt, dit kan via een toestemmingsformulier. Leg goed en duidelijk uit waarvoor deze toestemming nodig is. Een voorbeeld voor een modeltoestemmingsformulier is opgenomen in de handreiking.

20. Kan er ook sprake zijn van veronderstelde toestemming van een cliënt zodat er toch gegevens aan externe zorgorganisaties of individuele zorgaanbieders kunnen worden verstrekt?

Op grond van de Wgbo kan sprake zijn van veronderstelde toestemming wat mogelijk maakt dat gegevens zonder toestemming mogen worden verstrekt. Dat doet zich voor bij:

- een doorverwijzing naar een andere zorgorganisatie (zoals een doorverwijzing van een arts-AVG naar een medisch specialist);
- ketenzorg waar de zorg- en of dienstverlening is gekoppeld aan een bepaalde aandoening en het tot op bepaalde hoogte te voorzien is welke hulpverleners daarbij betrokken zullen zijn.

Aandachtspunt
Het is van belang om betrokkene tijdig in duidelijke en heldere bewoordingen te informeren over deze (en ook andere) gegevensuitwisselingen. Dit vloeit voort uit de informatieplicht van de verwerkingsverantwoordelijke (zorgorganisatie) in artikel 13 AVG. Dit biedt de cliënt de mogelijkheid zijn (veronderstelde) toestemming in te trekken (artikel 7 lid 3 AVG).

21 De zorgorganisatie maakt gebruik van een onderaannemer. Mag deze onderaannemer cliëntgegevens ontvangen?

Als de zorgorganisatie cliënten in zorg heeft die bijvoorbeeld dagbesteding willen ontvangen in een zorgboerderij en de zorgorganisatie heeft deze voorziening niet in huis, dan kan hiervoor een onderaannemingsovereenkomst worden gesloten met deze zorgboerderij.

Aan een onderaannemer mogen cliëntgegevens worden verstrekt, mits de cliënt en/of (wettelijk) vertegenwoordiger daarvoor uitdrukkelijke toestemming heeft gegeven.

Een andere zienswijze is dat aan een onderaannemer cliëntgegevens mogen worden verstrekt op basis van de grondslag dat de gegevens noodzakelijk zijn voor de uitvoering van een overeenkomst (artikel 6 lid 1 sub b AVG); in dit geval de zorg- en dienstverleningsovereenkomst. In de praktijk is echter nog onvoldoende uitgekristalliseerd of deze lijn gevolgd kan worden.

< Terug naar de inhoudsopgave

Dit komt omdat uit de AVG voortvloeit dat bij de grondslag “uitvoering van een overeenkomst” de betrokkene (cliënt of (wettelijk) vertegenwoordiger) zelf partij moet zijn bij de overeenkomst. In het geval van onderaanneming komt geen overeenkomst tot stand tussen de onderaannemer en betrokkene, maar tussen de zorgorganisatie (hoofdaannemer) en onderaannemer. Derhalve wordt in het kader van de zorgvuldigheid **geadviseerd** om vooralsnog uitdrukkelijke toestemming voor deze gegevensuitwisseling te vragen.

Verstrek enkel die cliëntgegevens die de onderaannemer voor zijn werkzaamheden nodig heeft.

Aandachtspunt:
Bij aanvang van de zorg- en/of dienstverlening kan bij voorbaat om toestemming van de cliënt of (wettelijk) vertegenwoordiger worden gevraagd om in geval van onderaannemerschap cliëntgegevens te mogen uitwisselen. Zie hiervoor het model toestemmingsformulier.

Het is verder van belang om betrokkene tijdig in duidelijke en heldere bewoordingen te informeren over deze (en ook andere) gegevensuitwisselingen. Dit vloeit voort uit de informatieplicht van de verwerkingsverantwoordelijke (zorgorganisatie) in artikel 13 AVG.

In onderhavige situatie dient om de toestemming van de betrokkene te worden gevraagd vóórdat de uitwisseling mag plaatsvinden. Als een betrokkene toestemming heeft verleend voor een gegevensverwerking is het niet mogelijk dat hij (alsnog) bezwaar kan maken tegen de verwerking. Wel kan de betrokkene zijn toestemming intrekken, waarna de verwerking zal moeten worden gestaakt.

22 Mag een zorgorganisatie cliëntgegevens verstrekken aan externe organisaties zoals het zorgkantoor, een gemeente, CIZ, UWV of het CAK?

In de regel is dit mogelijk omdat vaak sprake zal zijn van gegevensverstrekking op basis van een wettelijke verplichting voor de vrager (zorgkantoor, gemeente of het CIZ) of voor de zorgorganisatie om de gegevens te moeten verstrekken. Dit antwoord is schematisch uitgewerkt in bijlage 1.

< Terug naar de inhoudsopgave

23. Wanneer mag de zorgorganisatie een BSN verwerken?

BSN

Een nationaal identificatienummer is een bij wet vastgesteld uniek nummer. In Nederland is het bekendste nationale identificatienummer het Burgerservicenummer (BSN).

Het BSN mag bij de verwerking van persoonsgegevens alleen worden gebruikt ter uitvoering van een wet dan wel voor de doeleinden bij de wet bepaald (artikel 46 UAVG). Voor andere dan in de wet genoemde doelen is het verwerken van het BSN niet toegestaan, dit is dus verboden.

Zorgorganisaties in de gehandicaptenzorg mogen een BSN alleen gebruiken als dit in een specifieke wet is bepaald én alleen voor het specifieke doel dat in die wet staat omschreven.

De volgende wetten geven regels voor het verwerken van een BSN in de gehandicaptenzorg:

- Wet aanvullende bepalingen verwerking persoonsgegevens in de zorg (Wabvpz) (artikel 4 en verder)
  De Wabvpz geldt voor zorgaanbieders als bedoeld in de Wet kwaliteit, klachten en geschillen zorg (Wkkgz): het betreft hier onder andere zorgaanbieders voor Wlz-zorg.
- Wlz (artikel 9.1.1)
- Wmo 2015 (artikel 5.2.9)
- Jeugdwet (artikel 7.2.1 - artikel 7.2.4)

Let op:

Ontbreekt een wettelijke grondslag en doel voor het gebruiken van het BSN, dan kan het verbod om het BSN te gebruiken niet worden doorbroken door toestemming aan betrokkenen te vragen voor het gebruik van hun BSN.

Een BSN is volgens de AVG (artikel 9 lid 1 AVG) en de UAVG (artikel 1 UAVG) geen bijzonder persoonsgegeven. Het BSN is echter wel van gevoelige aard en bij onrechtmatige verwerking bestaat een risico op misbruik van persoonsgegevens en identiteitsfraude.

< Terug naar de inhoudsopgave

Wlz en BSN

De Wlz biedt een grondslag voor het verwerken van het BSN van cliënten. Op grond van artikel 9.1.1. lid 2 Wlz en artikel 5 Wabvpz stelt de zorgorganisatie de identiteit en het BSN van de cliënt vast wanneer deze zich voor de eerste keer tot de zorgorganisatie wendt ter verkrijging van zorg.

Een zorgorganisatie gebruikt het BSN van een cliënt met het doel te waarborgen dat de, in het kader van de zorgverlening, te verwerken persoonsgegevens op die cliënt betrekking hebben (artikel 4 Wabvpz).

De zorgorganisatie is verplicht het BSN van de cliënt op te nemen in zijn administratie bij het vastleggen van persoonsgegevens met betrekking tot de zorgverlening (artikel 8 Wabvpz).

Op grond van artikel 9 Wabvpz vermeldt de zorgorganisatie bij het verstrekken van persoonsgegevens aan andere zorgaanbieders[23] met betrekking tot het verlenen van zorg, het CIZ met betrekking tot de indicatiestelling en het zorgkantoor met betrekking tot de Wlz verstrekking, steeds het BSN van de cliënt.

Wmo 2015 en BSN

De Wmo 2015 (artikel 5.2.9) biedt een grondslag voor het verwerken van het BSN door een zorgorganisatie en het uitwisselen daarvan met andere instellingen zoals het CAK, de SVB, het college van burgemeester en wethouders, de toezichthoudende ambtenaren, het AMHK en de zorgverzekeraar met het doel te waarborgen dat de, in het kader van de uitvoering van deze wet te verwerken, persoonsgegevens ook op die persoon betrekking hebben. Dit staat uitgewerkt in artikel 5.2.2 Wmo 2015. Zorgorganisaties zijn verplicht de identiteit van een cliënt vast te stellen (artikel 5.2.8. Wmo 2015) en het BSN in de administratie opnemen.

Aandachtspunt

Wanneer een zorgorganisatie in de hoedanigheid van hoofdaannemer een overeenkomst met een onderaannemer heeft voor het leveren van een algemene voorziening of een maatwerkvoorziening ingevolge de Wmo 2015, geldt artikel 5.2.9 Wmo 2015 niet als wettelijke grondslag voor het verstrekken van het BSN. Dit komt omdat de onderaannemer niet kan worden beschouwd als een aanbieder ingevolge artikel 1.1.1. lid 1 Wmo 2015: “natuurlijke persoon of rechtspersoon die jegens het college gehouden is een algemene voorziening of een maatwerkvoorziening te leveren”. De onderaannemer valt niet onder deze definitie, omdat deze geen relatie heeft met het college van burgemeester en wethouders maar met de hoofd-

23 Zorgaanbieder in de zin van de Wkkgz (waaronder Wlz- en Zvw-zorgaanbieders).

< Terug naar de inhoudsopgave

aannemer (de zorgorganisatie). Dit betekent dat de hoofdaannemer op een andere wijze met de onderaannemer over de cliënt dient te communiceren. Daarvoor kunnen de 'gewone' persoonsgegevens worden gebruikt zoals voornaam, achternaam in combinatie met de geboortedatum. Let op: voordat deze persoonsgegevens met elkaar worden uitgewisseld, dient hiervoor de uitdrukkelijke toestemming van de cliënt of zijn (wettelijk) vertegenwoordiger te zijn verkregen (zie vraag 21 over onderaanneming).

Jeugdwet en BSN

De Jeugdwet biedt een grondslag voor het verwerken van het BSN door de zorgorganisatie die deze zorg verleent. In artikel 7.2.1 Jw is bepaald dat de zorgorganisatie het BSN van een jeugdige mag gebruiken met als doel (van dit BSN-gebruik) te waarborgen dat de persoonsgegevens die in het kader van de Jeugdwet worden verwerkt ook op deze jeugdige betrekking hebben.

De zorgorganisatie stelt het BSN van een jeugdige vast wanneer zij voor de eerste keer contact met hem heeft (artikel 7.2.2 Jw). De zorgorganisatie neemt het BSN van de jeugdige op in de administratie (artikel 7.2.4 Jw).

24 Mag een vervoersbedrijf/taxibedrijf kennis krijgen over gezondheidsgegevens van cliënten die het bedrijf naar de dagbesteding brengt?

Nee, behalve als de cliënt of zijn (wettelijk) vertegenwoordiger daarvoor uitdrukkelijk toestemming heeft gegeven. Een andere AVG-grondslag zal in dit soort situaties niet van toepassing zijn.

Aandachtspunt

Om deze uitdrukkelijke toestemming kan worden gevraagd op het moment dat een persoon in zorg komt. Leg goed en duidelijk uit waarvoor deze toestemming nodig is. In geval van vervoer kan het van belang zijn dat de vervoerder kennis krijgt van gezondheidsgegevens van de cliënt om cliënt veilig te vervoeren. Bijvoorbeeld als cliënt lijdt aan epilepsie.

Een voorbeeld voor een modeltoestemmingsformulier is opgenomen in de handreiking.

< Terug naar de inhoudsopgave

Deel B Cliëntdossier: recht op inzage en afschrift, bewaartermijn, vernietiging

25 Cliëntdossier aanleggen

Het vormen van een dossier, het vastleggen van afspraken voor en met een cliënt in de gehandicaptenzorg vloeit als verplichting voort uit meerdere wetten, te weten:

- Wgbo (artikel 7:454, lid 1): de dossierplicht voor de hulpverlener.
- Wlz (artikel 8.1.3): de verplichtingen tot het opstellen van een ondersteuningsplan.
- Jeugdwet (artikel 7.3.8): de verplichting tot het inrichten van een dossier.

Deze verplichtingen houden in dat de zorgaanbieder een dossier inricht met betrekking tot de zorg- en dienstverlening voor een cliënt. Hij houdt hierin aantekening van de relevante gegevens over de gezondheid van de cliënt en gegevens die direct verband houden met de zorg- en dienstverlening. In de Wmo 2015 is geen expliciete verplichting opgenomen tot het inrichten van een dossier, maar dit kan worden afgeleid uit de aard en strekking van de wet met daarin diverse bepalingen over gegevens en het verwerken daarvan (onder meer inzake de besluitvorming voor maatwerkvoorziening en PGB in hoofdstuk 2 Wmo 2015 en hoofdstuk 5 “Gegevensverwerking”).

Inhoud cliëntdossier (niet uitputtend en voor zover van toepassing op de zorgorganisatie):

- NAW-gegevens
- levenshistorie
- ondersteuningsplan
- testscores
- perspectief/beleving van cliënt of (wettelijk vertegenwoordiger)
- methodische vragenlijsten
- juridische status
- de ondersteuning
- risico-inventarisaties
- BSN
- zorg- en dienstverleningsovereenkomst
- diagnostische informatie
- medische informatie
- (wettelijke) vertegenwoordiger
- correspondentie • financiële gegevens
- verklaring wilsbekwaamheid
- behandeladviezen
- de begeleiding
- MIC-meldingen etc.

< Terug naar de inhoudsopgave

Digitale en/of papieren cliëntdossiers
De gegevens van een cliënt in de gehandicaptenzorg worden veelal digitaal vastgelegd in een Elektronisch Cliëntendossier (ECD). Er zijn verschillende ICT-leveranciers die een ECD aanbieden. Alhoewel zorgorganisaties veelal digitaal gegevens verwerken, zullen daarnaast ook nog papieren dossiers bestaan, zoals werkmappen in groepswoningen en overdrachtsmappen. Ongeacht of het digitale of papieren cliëntdossiers betreffen gelden dezelfde beginselen en uitgangspunten. Dus ook als het gaat om bewaartermijnen en het treffen van passende technische en organisatorische beveiligingsmaatregelen door de verwerkingsverantwoordelijke (zorgorganisatie). Papieren dossiers dienen op een beveiligde plek bewaard te worden, zoals een afgesloten kast en/of ruimte. Zie voor meer informatie over beveiligingsmaatregelen module 1 en module 3.

AVG: Recht van de betrokkene op inzage en afschrift cliëntdossier

26 Wie is de betrokkene in de gehandicaptenzorg?
De VGN heeft de betrokkene als volgt gespecificeerd. Dit kan zijn de:

- zorgvrager (toekomstig cliënt);
- cliënt;
- wettelijk vertegenwoordiger (mentor, curator, ouders, voogd);
- schriftelijk gemachtigde;
- belangenbehartiger (de echtgenoot, de geregistreerd partner, de levensgezel, een ouder, een kind, een broer of zuster).

Zie ook vraag 5 van deze module.

27 Welke privacyrechten kent de AVG naast het recht op inzage?
De 'privacyrechten' van de betrokkenen worden uitgebreid behandeld in module 3 en worden hierna voor de volledigheid allemaal kort aangestipt. Deze module gaat daarna verder in op praktijksituaties omtrent het recht van inzage en afschrift in relatie tot zorgspecifieke wetgeving.

Rechten (artikel 12 t/m 22 AVG):

1. **Recht op transparante informatie over de verwerkingen** (artikelen 13, 14 AVG)
   De betrokkene heeft het recht om te weten of, en zo ja welke persoonsgegevens de zorgorganisatie verwerkt en waarom zij dat doen.

< Terug naar de inhoudsopgave

2. **Recht op inzage (en afschrift) van de persoonsgegevens** (artikel 15 AVG)
De betrokkene heeft het recht om de persoonsgegevens, die de zorgorganisatie van de betrokkene verwerkt, in te zien. De betrokkene heeft ook het recht op een afschrift (kopie) van die gegevens.

3. **Recht op rectificatie van de gegevens als deze niet kloppen** (artikel 16 AVG)
De betrokkene heeft het recht om de zorgorganisatie te vragen zijn persoonsgegevens te verbeteren als ze niet meer kloppen of aan te vullen als ze niet volledig zijn. Ook mag de betrokkene de zorgorganisatie vragen om een verklaring aan zijn cliëntdossier toe te voegen. Het recht op rectificatie betreft feitelijke gegevens en gaat niet over verklaringen van bevindingen die medewerkers in een cliëntdossier hebben opgenomen.

4. **Recht op gegevenswissing (recht op vergetelheid)** (artikel 17 AVG)
De betrokkene heeft het recht om vergeten te worden. Dit betekent dat de betrokkene de zorgaanbieder mag vragen zijn persoonsgegevens te wissen, verwijderen of vernietigen als:
   - de zorgorganisatie de persoonsgegevens van de betrokkene niet langer nodig heeft voor het doel waarvoor deze zijn verwerkt;
   - de betrokkene zijn toestemming voor verwerking intrekt en er geen andere juridische grond voor verwerking aanwezig is;
   - de zorgorganisatie de persoonsgegevens van de betrokkene onterecht heeft verwerkt;
   - er sprake is van een wettelijke bepaling die de zorgorganisatie verplicht tot het wissen of verwijderen van de persoonsgegevens van de betrokkene;
   - de betrokkene gegrond bezwaar heeft gemaakt tegen de gegevensverwerking.

   Wanneer het **gezondheidsgegevens** van de betrokkene betreft, hoeft de zorgorganisatie de persoonsgegevens in een aantal situaties niet te verwijderen, te wissen of te vernietigen. Zie hiervoor module 3.

5. **Recht op beperking van de verwerking** (artikel 18 AVG)
De betrokkene mag de zorgorganisatie vragen tijdelijk zijn persoonsgegevens niet te gebruiken zolang een bepaald probleem of bezwaar dat gaat over de verwerking van deze persoonsgegevens nog niet is opgelost.

6. **Recht op overdraagbaarheid van gegevens (dataportabiliteit)** (artikel 20 AVG)
De betrokkene mag de zorgorganisatie verzoeken zijn persoonsgegevens aan hem te verstrekken op een manier die het

< Terug naar de inhoudsopgave

voor de betrokkene makkelijk maakt om zijn gegevens te hergebruiken en door te geven aan een andere (zorg)organisatie.

Echter, dit recht geldt enkel:

- voor persoonsgegevens die door de betrokkene zelf zijn verstrekt;
- én de betrokkene voor de verwerking toestemming heeft verleend of verwerking kon plaatsvinden ter uitvoering van een overeenkomst;
- én de verwerking geautomatiseerd plaatsvindt.

Het recht op dataportabiliteit geldt niet voor niet-geautomatiseerde (papieren) bestanden.

7. **Recht van bezwaar** (artikel 21 AVG)
   De betrokkene mag bezwaar maken tegen de gegevensverwerking door de zorgorganisatie als de zorgzorgorganisatie deze verwerking heeft gebaseerd op de AVG-grondslag 'taak van publiek algemeen belang of uitoefening van openbaar gezag' (artikel 6 lid 1 sub e AVG) of 'gerechtvaardigd belang' (artikel 6 lid 1 sub f AVG). Dit omdat deze twee grondslagen het meest onbepaald en algemeen zijn met veel beoordelingsruimte voor de verwerkingsverantwoordelijke. Geen bezwaar is dus **niet** mogelijk als de betrokkene toestemming heeft gegeven voor de verwerking, betrokkene kan wel zijn toestemming intrekken waarna de verwerking zal moeten worden gestaakt.

28 Kennen de 'zorgwetten (Wgbo, Jeugdwet, Wmo 2015, Wlz)' een recht op inzage en afschrift voor de cliënt of (wettelijk) vertegenwoordiger?

Ja, in de Wgbo (artikel 7:456), de Jeugdwet (artikelen 7.3.10, 7.3.11) en de Wmo 2015 (artikelen 5.3.2, 5.3.3) wordt een recht op inzage in en afschrift van het cliëntdossier aan de betrokkene toegekend.

In artikel 8.1.3 lid 7 Wlz is bepaald dat de verzekerde of vertegenwoordiger desgevraagd een afschrift van het ondersteuningsplan ontvangt.

29 Bestaat er een verschil tussen inzage op grond van de zorgwetten in het cliëntdossier en inzage op grond van de AVG in de persoonsgegevens?

Ja, er moet een onderscheid worden gemaakt in een inzageverzoek van de cliënt of (wettelijk) vertegenwoordiger in het cliëntdossier en een inzageverzoek op grond van de AVG. Wordt namelijk een beroep op dit laatste gedaan dan betekent dit dat deze inzage **ook** betrekking heeft op persoonsgegevens die niet in het cliëntdossier zijn opgenomen, maar wel worden

< Terug naar de inhoudsopgave

verwerkt door de zorgorganisatie.

30 Inzien of afschrift (kopie)?

In de Wgbo, Jeugdwet en Wmo 2015 staat expliciet vermeld dat betrokkene recht heeft op inzage en afschrift. De Wlz spreekt enkel over het verstrekken van een afschrift.

In artikel 15 AVG staat dat de betrokkene recht heeft op inzage. Hieronder moet worden verstaan het inzien van de persoonsgegevens (bij de zorgorganisatie) maar ook het verstrekken van kopieën, afschriften aan de betrokkene.

Dit betekent dat niet altijd duidelijk is wat het verzoek van de cliënt en/of (wettelijk) vertegenwoordiger is. Beoordeel daarom altijd grondig het verzoek van de betrokkene: wat wenst de cliënt en/of (wettelijk) vertegenwoordiger, inzage en/of afschrift op grond van de AVG of op grond van een specifieke zorgwet? Vraag dit bij twijfel na.

31 Mag de zorgprofessional een inzageverzoek van een (wettelijk) vertegenwoordiger (gedeeltelijk) weigeren?

Dat is mogelijk als de zorgprofessional heeft beoordeeld dat door deze inzage de bescherming van de persoonlijke levenssfeer (rechten of vrijheden) van een ander wordt geschaad. Om een voorbeeld te noemen. Stel, dat zorgprofessionals vermoeden dat een cliënt een andere cliënt stelselmatig pest. In dat geval mag de zorgprofessional het inzageverzoek van een (wettelijk) vertegenwoordiger weigeren als in het cliëntdossier de naam van de andere cliënt (vermoedelijke pester) vermeld staat. Een andere optie is dat de zorgprofessional het inzageverzoek gedeeltelijk weigert, bijvoorbeeld door informatie over de andere cliënt af te schermen.

Een andere reden om inzage (gedeeltelijk) te weigeren is als de zorgprofessional van mening is dat hij door de inzage niet handelt als een ‘goed hulpverlener’; als door deze inzage het belang van de cliënt zelf zou kunnen worden geschaad. Bijvoorbeeld als een wilsonbekwame cliënt aan de persoonlijk begeleider vraagt hem te helpen met het vinden van een betaalde professional voor seksueel contact waarbij de cliënt heeft aangegeven dat zijn (wettelijk) vertegenwoordiger dit niet mag weten. (Onder de voorwaarde dat wordt vastgesteld dat de cliënt met betrekking tot dit verzoek wilsbekwaam ter zake is.)

Of ingeval van een vermoeden kindermishandeling bij een minderjarige cliënt.

< Terug naar de inhoudsopgave

32 Mag de zorgprofessional een inzageverzoek van een cliënt (gedeeltelijk) weigeren?

Als door de zorgprofessional wordt beoordeeld dat door de inzage de persoonlijke levenssfeer van een ander (dan de cliënt) wordt geschaad mag een inzageverzoek (gedeeltelijk) worden geweigerd. Gedacht kan worden aan de situatie dat een verwant of ander de (wettelijk) vertegenwoordiger van de cliënt vertrouwelijke informatie over zichzelf aan de zorgprofessional heeft verstrekt. Voor het (geheel of gedeeltelijk) weigeren van een inzageverzoek maakt het niet uit of de cliënt wilsbekwaam of wilsonbekwaam is.

33 Heeft een minderjarige wilsbekwame cliënt inzagerecht?

a. Het inzagerecht bij cliënten jonger dan 12 jaar wordt door de ouders en/of voogd(en) uitgeoefend;[24]
b. Een **12- tot en met 15-jarige cliënt, wilsbekwaam ter zake,** heeft recht op inzage, maar ook zijn ouders/voogd(en) hebben een inzagerecht. Zij kunnen gezamenlijk een verzoek tot inzage doen, maar ook apart;[25]

Wanneer alleen de ouders/voogd(en) om inzage verzoeken, beoordeelt de zorgprofessional of het verzoek van de ouders/voogd(en) in strijd is met het beginsel van goed hulpverlenerschap. Indien er sprake is van strijdigheid met het goed hulpverlenerschap dan kan de zorgprofessional besluiten de inzage door de ouders/voogd(en) geheel of gedeeltelijk te weigeren.

c. **Een wilsbekwame cliënt vanaf 16 jaar** heeft een zelfstandig inzagerecht.[26]

34 Mag de cliënt of (wettelijk) vertegenwoordiger de werkaantekeningen van de zorgprofessional inzien?

Nee, persoonlijke werkaantekeningen van een arts (huisarts of arts verstandelijk gehandicapten), persoonlijk begeleider of orthopedagoog[27] zijn een geheugensteuntje voor de eigen gedachtenvorming. Deze maken geen onderdeel uit van het cliëntdossier en zijn daarom niet toegankelijk voor de cliënt of (wettelijk) vertegenwoordiger. Het is van belang hierop goed te letten tijdens het registreren van gegevens door de zorgprofessional.

24 Op grond van art. 7:457 lid 3 BW jo art. 7:465 lid 1 BW.
25 Op grond van art. 7:457 lid 3 BW jo. art. 7:450 lid 2 jo. 7:456 BW.
26 Op grond van art. 7:447 lid 1 BW jo. art. 7:456 BW.
27 Uit de Wgbo vloeit voort dat werkaantekeningen van een arts geen onderdeel uitmaken van het medisch dossier. Vanwege analoge toepassing van de Wgbo door de leden van de VGN brengt dit met zich mee dat werkaantekeningen van de persoonlijk begeleider of de orthopedagoog eveneens geen onderdeel uitmaken van het cliëntdossier. De richtlijn Wgbo vindt u hier: http://www.vgn.nl/artikel/2171.

< Terug naar de inhoudsopgave

Mocht de zorgprofessional langer dan 2 weken gebruik maken van zijn persoonlijke werkaantekeningen (“ze achter de hand houdt”) dan is het advies dan op te nemen in het cliëntdossier, omdat zij dan niet langer als werkaantekeningen kunnen worden beschouwd. Zodra deze gegevens onderdeel uitmaken van het cliëntdossier heeft de cliënt of (wettelijk) vertegenwoordiger daarop een inzagerecht.

Wettelijke bewaartermijnen

35 Hoe lang moet een cliëntdossier bewaard worden?

De bewaartermijn is afhankelijk van het type gegevens die het betreft. De AVG kent geen expliciete bewaartermijnen en spreekt over bewaren zolang voor het doel noodzakelijk is. In het schema op de volgende pagina zijn bewaartermijnen voor de gehandicaptenzorg opgenomen. De zorgorganisatie dient deze termijn te hebben opgenomen in intern databeleid.

Betrokkene	Persoonsgegevens	Bewaartermijn	Wet	Aandachtspunt
Cliënt	Medische gegevens en andere gegevens die verband houden met de gezondheid: o.a. behandelgegevens AVG-arts, psychologen, orthopedagogen en begeleiders van belang voor goede zorg en ondersteuning.	**15 jaar** of zoveel langer als redelijkerwijs uit de zorg van een goed hulpverlener voortvloeit.	Wgbo	Start looptijd van deze termijn vanaf moment dat de gegevens zijn vervaardigd.[28] De VGN adviseert om deze termijn te starten vanaf het einde van de behandeling.[29]
	Bopz-dossier	**5 jaar**	Wet Bopz	Na afloop beschikking. Eerder vernietigen op verzoek van cliënt is niet toegestaan.
	Documenten m.b.t. beschermingsmaatregelen	**2 jaar**	Wet Bopz	Na beëindigen maatregel.
Cliënt	Financiële en administratieve gegevens: 1. Door de instelling zelf gegeneerde administratieve gegevens voor de betaling van geleverde zorg.	**7 jaar**	Algemene wet inzake rijksbelastingen. Besluit fiscaal bestuursrecht.	Start looptijd: vanaf einde zorgverlening.
	2. Door cliënt zelf verstrekt. Zoals uitkering of salaris, bankafschriften.	Zolang de zorg duurt, tenzij dit op grond van andere wet- en regelgeving niet toegestaan is, zoals de AVG.	AVG	
(Wettelijk) vertegenwoordigers	Zoals naam, adres, e-mail, telefoonnummer.	Zo lang voor het doel noodzakelijk.	AVG	

Aandachtspunt

Wat betreft de financiële administratie van een zorgorganisatie wordt opgemerkt dat met de Belastingdienst afspraken gemaakt kunnen worden over de vorm (elektronisch of op papier) waarin gegevens bewaard kunnen worden.

28 In 2018 heeft de Minister voor Medische Zorg een wetsvoorstel ingediend om de Wgbo aan te passen. Een van die wijzigingen betreft het verlengen van de bewaartermijn tot 20 jaar met als start van deze termijn het moment waarop de laatste wijziging is aangebracht. Ten tijde van het schrijven van deze handreiking (juni 2019) is het wetsvoorstel door de Eerste Kamer aangenomen met als verwachting dat de wet per 1 januari 2020 in werking treedt. De handreiking wordt dan op dit punt aangepast.

29 Richtlijn WGBO, VGN 2008. De richtlijn Wgbo vindt u hier: http://www.vgn.nl/artikel/2171.

< Terug naar de inhoudsopgave

36 De bewaartermijn is verstreken, wat moet een zorgorganisatie doen?

Na afloop van de bewaartermijn vernietigt de zorgorganisatie de gegevens. Indien het gegevens betreft die hij van de cliënt heeft ontvangen, geeft hij deze aan de cliënt terug, zoals bijvoorbeeld bankafschriften, uitkeringsgegevens of privéfoto's.

37 Op welke wijze moeten digitale/papieren gegevens (na de bewaartermijn) worden vernietigd?

De zorgorganisatie moet goed stilstaan bij de manier waarop gegevens worden bewaard en vernietigd. Zeker als het bijzondere persoonsgegevens betreft zoals gezondheidsgegevens. Een datalek moet worden voorkomen. Om te voldoen aan de wettelijke verplichtingen voortkomend uit de AVG heeft de zorgorganisatie hierop een intern databeleid nodig. Hierin dient te staan welke gegevens hoe lang bewaard zullen blijven en de wijze waarop deze gegevens vernietigd gaan worden. Dit vloeit voort uit het AVG-beginsel van "dataminimalisatie/opslagbeperking" genoemd in artikel 5 lid 1 sub e AVG.

Als gegevens digitaal zijn opgeslagen, is het mogelijk om via speciaal daartoe ontwikkelde systemen gegevens automatisch te laten vernietigen op een van tevoren aangegeven tijdstip.

Als sprake is van papieren cliëntgegevens (dossiers) is een geschikte vernietigingsmethode bijvoorbeeld een papierversnipperaar.

Onderdeel van dit databeleid is ook het geven van voorlichting (training, posters op de werkplek) aan zorgprofessionals en andere medewerkers. Dat zij weten in het geval zij te maken hebben/krijgen met het vernietigen van gegevens op welke wijze dit dan moet gebeuren.

Wanneer een organisatie overstapt van papieren dossiers naar digitale dossiers, dan mogen de originele papieren dossiers pas worden vernietigd als de zorgorganisatie voor een goede beveiliging van het digitale dossier heeft gezorgd.

< Terug naar de inhoudsopgave

38 Mogen (bijzondere) persoonsgegevens langer bewaard worden?

Gewone persoonsgegevens
Langer bewaren mag alleen als deze langere archivering van de persoonsgegevens nodig is in het kader van het algemeen belang; voor wetenschappelijk of historisch onderzoek; of voor statistische doeleinden (artikel 5 lid 1 sub e AVG). De zorgorganisatie (verwerkingsverantwoordelijke) moet vervolgens waarborgen - door het nemen van passende technische en organisatorische maatregelen - dat niet meer gegevens worden gebruikt dan voor het onderzoeksdoel, de statische doeleinden noodzakelijk is (artikel 89 lid 1 AVG). Het pseudonimiseren van de persoonsgegevens kan als een dergelijke (waarborgings)maatregel worden beschouwd.

Bijzondere persoonsgegevens
Gaat het om het langer bewaren van bijzondere persoonsgegevens, waaronder gezondheidsgegevens, dan gelden de aanvullende regels uit artikel 9 AVG en in het bijzonder artikel 24 UAVG.

Langer bewaren voor historisch of wetenschappelijk onderzoek en statistische doeleinden is mogelijk, mits aan **alle** hierna genoemde voorwaarden is voldaan:

1. er is sprake van wetenschappelijk of historisch onderzoek of statistische doeleinden;
2. het onderzoek dient een algemeen belang;
3. het vragen van uitdrukkelijke toestemming van de cliënt of (wettelijk) vertegenwoordiger is onmogelijk gebleken of kost een onevenredige inspanning;
4. en er is voorzien in bepaalde waarborgen dat de persoonlijke levenssfeer niet onevenredig wordt geschaad;
   Welke waarborgen dat zijn, is afhankelijk van het concrete geval. Er zal dus goed gekeken moeten worden naar de aard en strekking van het onderzoek en de persoonsgegevens die het betreft. Zodra het onderzoek kan worden bereikt zonder persoonsgegevens dan moet met het gebruik daarvan worden gestopt.

In het geval sprake is van wetenschappelijk onderzoek of statistiek geldt als **extra voorwaarde:**
5. dat de cliënt of (wettelijk) vertegenwoordiger geen uitdrukkelijk bezwaar heeft gemaakt tegen het verstrekken van gegevens ten behoeve van wetenschappelijk onderzoek of statistiek (artikel 7:458 lid 2 sub c BW).[30]

30 Dit betreft een aanvullende versterkende bepaling, vanuit een specifieke zorgwet, op de AVG.

< Terug naar de inhoudsopgave

Aandachtspunt 1:
Gegevens van overleden personen zijn geen persoonsgegevens (meer) volgens de AVG, omdat overledenen volgens AVG wet geen natuurlijke personen meer zijn. Dit betekent echter niet dat het medisch beroepsgeheim van een zorgprofessionaal eindigt met het overlijden van persoon. Dit blijft in stand, zie vraag 18.

Aandachtspunt 2:
Foto's, beeld- en/of geluidmateriaal van cliënt(en) tijdens sociale activiteiten mogen niet langer bewaard worden dan voor het doel noodzakelijk is, behalve als er (dus) sprake is van een van de hierboven genoemde doeleinden. Kijk voor meer informatie over dit onderwerp module 1.

Overige FAQ's

39 Hoe kan een zorgorganisatie handelen als een (wettelijk) vertegenwoordiger zijn persoonsgegevens niet wil verstrekken?

Als een (wettelijk) vertegenwoordiger zijn persoonsgegevens, zoals bijvoorbeeld zijn telefoonnummer, adresgegevens of e-mailadres, niet wil verstrekken is het voor de zorgprofessional niet mogelijk om contact met hem op te nemen.

De zorgprofessional moet echter met een (wettelijk) vertegenwoordiger kunnen overleggen als een cliënt zelf niet in staat is tot een redelijke waardering van zijn belangen ter zake (wilsonbekwaam is ter zake). In deze situatie geval gedraagt de (wettelijk) vertegenwoordiger zich in zo'n geval niet zoals "een goed vertegenwoordiger betaamt". In eerste instantie moet de zorgprofessional hierover in gesprek gaan met de (wettelijk) vertegenwoordiger om duidelijk te maken waarom contact tussen de zorgorganisatie en de (wettelijk) vertegenwoordiger noodzakelijk is. Bij blijvende weigering van de (wettelijk) vertegenwoordiger om zijn persoonsgegevens te verstrekken, kan de zorgorganisatie in het uiterste geval een benoeming van een (andere) wettelijk vertegenwoordiger (mentor, curator) verzoeken bij de rechter.

< Terug naar de inhoudsopgave

Wetenschappelijk onderzoek – historisch onderzoek – statistische doelen volgens de AVG

Wetenschappelijk onderzoek: dit kan fundamenteel onderzoek, toegepast onderzoek en technologische ontwikkeling en demonstratie zijn. Wetenschappelijk onderzoek wordt ruim opgevat onder de AVG. Het is niet beperkt tot onderzoek dat met publieke middelen wordt betaald.

Historisch onderzoek: historisch onderzoek en onderzoek voor genealogische doeleinden (onderzoek naar geschiedenis, herkomst, ontwikkeling van een onderwerp, voorwerp etc.). De AVG is zoals eerder gezegd niet van toepassing op overleden personen. Er bestaat ruimte voor de lidstaten om hier eigen regels over te stellen. De Nederlandse wetgever heeft dit nog niet gedaan, ondanks advies van de Autoriteit Persoonsgegevens dit wel te doen.

Statistische doelen: dit betekent dat het resultaat van de verwerking niet uit persoonsgegevens bestaat, maar uit geaggregeerde gegevens. Dit resultaat en persoonsgegevens mogen niet worden gebruikt als ondersteunend materiaal voor maatregelen of beslissingen die een bepaalde natuurlijke persoon betreffen.

De zorgorganisatie kan over een wettelijk vertegenwoordiger (zijnde de curator, mentor of bewindvoerder) ook een klacht indienen bij de kantonrechter van de rechtbank in het rechtsgebied (arrondissement) waar de cliënt woont. De kritiek op de taakuitoefening moet dan duidelijk beschreven en onderbouwd worden met beschrijving van situaties waarin de huidige wettelijk vertegenwoordiger niet (voldoende) of niet op correcte wijze de belangen van de cliënt behartigt. De zorgorganisatie moet vragen of de rechter wil nagaan of er een gewichtige reden aanwezig is om de wettelijk vertegenwoordiger te berispen of te vervangen.

40 Zijn digitale en gescande documenten rechtsgeldig?

Door het digitaliseren van papieren dossiers kan wellicht de zorg ontstaan of digitale documenten rechtsgeldig zijn. De vraag of iets rechtsgeldig is zal zich voordoen als deze stukken onderdeel uitmaken van een gerechtelijke procedure. Digitaal (en gescand) bewijs is in de eerste plaats toelaatbaar in een rechtszaak. Behalve als een wet expliciet schriftelijk (papier) bewijs eist. Vervolgens zal de vraag zijn of het digitale (en gescande) document voldoende bewijskracht heeft. De rechter zal meer bewijskracht toekennen aan een document wanneer hij overtuigt is van de betrouwbaarheid van het document. De betrouwbaarheid van een document wordt vergroot door een elektronische handtekening.

< Terug naar de inhoudsopgave

41 Hoe moeten zorgprofessionals omgaan met persoonsgegevens van cliënten op gebruikte verpakkingen (medicatie of anderszins)?

Gegevens van cliënten op verpakkingen, zoals naam, adres of geboortedatum, zijn persoonsgegevens. Bij verpakkingen kan bijvoorbeeld gedacht worden etiketten op medicijndoosjes of -flesjes, Baxterverpakkingen of verpakkingen van incontinentiemateriaal. Deze persoonsgegevens moeten vernietigd worden als ze niet meer nodig zijn. In principe moet de zorgprofessional deze dus direct verwijderen zodra hij ermee klaar is. In de praktijk is het geen probleem om deze persoonsgegevens eerst te verzamelen en periodiek te vernietigen, maar dan moet er ook wel voor gezorgd worden dat een tijdelijke verzamelbak niet toegankelijk is. Dit betekent dat verpakkingen met persoonsgegevens niet in de 'gewone' prullenmand mogen worden gedeponeerd. Een praktische oplossing is dat de zorgorganisatie zorgt voor een afgesloten container.

Module 3

Privacy vanuit organisatieperspectief

Module 3 - Privacy vanuit organisatieperspectief

Inleiding

Deze module beschrijft op hoofdlijnen de belangrijkste gevolgen van de AVG voor zorgorganisaties in de gehandicaptenzorg. De module volgt zoveel mogelijk de opbouw (systematiek) van de AVG om zo overzichtelijk in beeld te brengen welke verplichtingen uit de AVG voortvloeien.

Het doel is concreet inzicht te bieden in thema's en vragen specifiek bezien vanuit het organisatieperspectief. Onderwerpen kunnen in meerdere modules aan de orde komen of men wordt via clickables rechtstreeks geleid naar beschrijvingen in de andere modules.

Zorgorganisaties in de gehandicaptenzorg verwerken persoonsgegevens van onder meer cliënten, (wettelijk) vertegenwoordigers en medewerkers.[1] Zorgorganisaties hebben te maken met privacybepalingen op grond van de AVG, UAVG en zorgspecifieke wetgeving. Persoonsgegevens mogen alleen worden verwerkt wanneer daarvoor vooraf welbepaalde en uitdrukkelijk omschreven doelen zijn vastgesteld én daarvoor een grondslag aanwezig is, bijvoorbeeld de toestemming van de betrokkene of een wettelijke plicht. Wanneer het gaat om bijzondere persoonsgegevens, zoals gegevens over de gezondheid, moet er naast een grondslag ook sprake zijn van een uitzonderingsgrond. Ook moeten zij - uitzonderingsgevallen daargelaten - de betrokkene laten weten wat zij met de persoonsgegevens (gaan) doen. Naast het feit dat voor het verwerken van bijzondere persoonsgegevens (gezondheidsgegevens) sprake moet zijn van een uitzondering op het verwerkingsverbod (artikel 30 UAVG) dient de zorgprofessional zijn medisch beroepsgeheim (geheimhoudingsplicht) in acht te nemen welke slechts doorbroken kan worden onder bepaalde voorwaarden, waarna verdere verwerking mag plaatsvinden. De doorbreking van het medisch beroepsgeheim komt specifiek in module 2 aan de orde.

Centraal in deze module staan de verplichtingen voor de verwerkingsverantwoordelijke en de verwerker. Deze kan verwerkers inschakelen om een verwerking te laten uitvoeren. Veelal is de rol van de zorgorganisatie die van verwerkingsverantwoordelijke.

1 De bescherming van persoonsgegevens in relatie tot medewerkers valt buiten het bestek van deze handreiking. Meer informatie hierover kunt u vinden in de notitie van de Brancheorganisaties Zorg (BoZ) Veel gestelde vragen en antwoorden Privacy en arbeidsrelatie (versie juli 2018). Deze notitie is via secretariaat@vgn.nl op te vragen.

< Terug naar de inhoudsopgave

Leeswijzer:
De module laat zich als volgt lezen: eerst wordt de AVG-systematiek verduidelijkt, vervolgens worden de rechten van betrokkenen beschreven, daarna is er expliciet aandacht voor de plichten van de zorgorganisatie in hoedanigheid van verwerkingsverantwoordelijke.

AVG-systematiek

1 Beginselen inzake de verwerking van persoonsgegevens (artikel 5 AVG)

Verwerking van persoonsgegevens valt onder het grondrecht ter eerbiediging van de persoonlijke levenssfeer (artikel 10 Grondwet).[2] Iedere verwerking moet dit grondrecht respecteren. De AVG gaat uit van zes basisbeginselen waaraan elke verwerking van persoonsgegevens moet voldoen. Dus ook de gegevensverwerking waarvan sprake is in de zorgwetten zoals de Wlz en de Jeugdwet.

Bedoeling van de AVG-beginselen

Deze beginselen zijn bedoeld als algemene borging en werken door in de interpretatie van de rechten en plichten elders uit de AVG. De basisbeginselen hebben een zelfstandige betekenis als norm. Een betrokkene kan zich er rechtstreeks op beroepen bij de Autoriteit Persoonsgegevens of de rechter om bijvoorbeeld een belangenafweging anders te laten uitvallen of een bepaalde verwerking te doen staken. Er staan administratieve geldboeten op het niet naleven van deze basisbeginselen (artikel 83 lid 5 sub a AVG).
Elke verwerking van persoonsgegevens door een (zorg)organisatie moet dus in lijn zijn met deze beginselen.

Klik hier voor het overkoepelend stappenplan hoe om te gaan met een privacyvraagstuk.

2 Welke beginselen zijn er?

Het beginsel van rechtmatigheid, behoorlijkheid en transparantie (artikel 5 lid 1 sub a AVG)
De betrokkene dient te weten dat zijn persoonsgegevens worden verwerkt en waarom dit gebeurt. De gegevensverwerking moet rechtmatig zijn. Daarvan is sprake als is voldaan aan minimaal één van de genoemde grondslagen in artikel 6 AVG.

2 Op Europees niveau is het recht op eerbiediging van de persoonlijke levenssfeer vastgelegd in artikel 8 van het Europees Verdrag voor de Rechten van de Mens en de Fundamentele Vrijheden (EVRM) en artikel 17 van het Internationaal Verdrag inzake Burgerrechten en Politieke Rechten (IVBPR).

< Terug naar de inhoudsopgave

Behoorlijkheid betekent dat er 'netjes' moet worden omgegaan met de persoonsgegevens binnen de zorgorganisatie. Dit heeft enerzijds betrekking op het nemen van beveiligingsmaatregelen en anderzijds op organisatorische en cultuurkenmerken van het omgaan met gegevens.

> Een beveiligingsmaatregel is bijvoorbeeld dat het wachtwoord van een computer in een zorgwoning niet bij de computer ligt en daardoor voor iedereen zichtbaar is.
> Een voorbeeld van een cultuurkenmerk is dat medewerkers niet in bijzijn van familie van cliënten over de gezondheid van andere cliënten in gesprek gaan.

Transparantie vereist dat zorgorganisaties informatie verstrekken aan personen van wie zij persoonsgegevens verwerken. Zij moeten de betrokkenen informeren welke persoonsgegevens worden verwerkt en waarom. Volgens het transparantiebeginsel moeten informatie en communicatie in verband met de verwerking van die persoonsgegevens beknopt, eenvoudig toegankelijk en begrijpelijk zijn.

> Vertaald naar de doelgroepen in de gehandicaptenzorg betekent dit dat de informatie zo concreet en toegespitst mogelijk is, gemakkelijk te vinden en te raadplegen is en begrijpelijk is (geen juridische taal of technisch vakjargon). Het gebruik van visuele hulpmiddelen, zoals pictogrammen of korte animatiefilmpjes, is voor cliënten zeker aan te raden.

Het transparantiebeginsel wordt in de AVG uitgewerkt in twee informatieplichten:

- te verstrekken informatie wanneer persoonsgegevens bij de betrokkene worden verzameld (artikel 13 AVG); en
- te verstrekken informatie wanneer de persoonsgegevens niet van de betrokkene zijn verkregen (artikel 14 AVG).

Deze informatieplichten worden in onderdeel 6.1 van deze module uitgewerkt.

< Terug naar de inhoudsopgave

Het beginsel van doelbinding (artikel 5 lid 1 sub b AVG)

Er moet sprake zijn van één of meer duidelijk bepaalde, uitdrukkelijk omschreven en gerechtvaardigde doeleinden voor het verwerken van de persoonsgegevens.
Wanneer de gegevens later voor een ander doel worden gebruikt dan waarvoor de persoonsgegevens aanvankelijk zijn verzameld, dan moet dat nieuwe doel verenigbaar zijn met het oorspronkelijke verzameldoel. Alleen in dat geval is er géén aparte grondslag uit de AVG vereist voor het nieuwe doel om de persoonsgegevens te verwerken.

Of een doel verenigbaar is, is afhankelijk van de omstandigheden van het geval, dit kan dus per situatie verschillen. Het hangt af van de aard van de persoonsgegevens (gewone of bijzondere persoonsgegevens); de gevolgen voor de betrokkene van de nieuwe verwerking; zijn de gegevens van de betrokkene zelf verkregen of van iemand anders (in verband met de verwachtingen bij de betrokkene hierover), het bestaan van passende technische waarborgen.

Het beginsel van minimale gegevensverwerking/dataminimalisatie (artikel 5 lid 1 sub c AVG)

Het beginsel van dataminimalisatie brengt met zich mee dat de zorgorganisatie niet meer persoonsgegevens mag verwerken dan strikt noodzakelijk is voor het doel.
Hieruit volgt ook dat de persoonsgegevens zo snel mogelijk moeten worden gewist wanneer het bewaren niet langer noodzakelijk is voor het betreffende doel en er géén sprake is van bewaartermijn op grond van de wet.

Het beginsel van juistheid van persoonsgegevens (artikel 5 lid 1 sub d AVG)

Alle redelijke maatregelen moeten worden genomen om ervoor te zorgen dat onjuiste persoonsgegevens worden gerectificeerd of gewist. Wanneer wordt gewerkt met onjuiste of achterhaalde gegevens, kan dat vervelende gevolgen hebben voor de betrokkene. De verwerkingsverantwoordelijke heeft een vergaande inspanningsverplichting om de juistheid van de persoonsgegevens te borgen. Dit beginsel is nader uitgewerkt in het recht van rectificatie (artikel 16 AVG) en het recht van gegevenswissing (artikel 17 AVG).

Aandachtspunt: actieve houding
Uit het 'juistheidbeginsel' vloeit voor de verwerkingsverantwoordelijke een zelfstandige plicht voort om actief zorg te dragen voor de juistheid van de persoonsgegevens die hij onder zich heeft. Het is onjuist en boetewaardig (artikel 83 lid 5 sub a) om als verwerkingsverantwoordelijke passief te wachten tot betrokkenen klagen over onjuiste of achterhaalde persoonsgegevens.

< Terug naar de inhoudsopgave

Het beginsel van opslagbeperking (artikel 5 lid 1 sub e AVG)

Persoonsgegevens mogen niet langer bewaard worden dan noodzakelijk is voor het doel van de verwerking. De AVG noemt geen expliciete termijnen in jaren, maanden of weken, maar verlangt van de verwerkingsverantwoordelijke dat deze gezien zijn beoogde verwerkingen zelf concrete termijnen vaststelt voor het wissen van gegevens of periodieke toetsing daarvan.

Diverse wetgeving (zoals de Wgbo, de Wet Bopz of de Algemene wet inzake rijksbelastingen) verplichten de verwerkingsverantwoordelijke om bepaalde gegevens te bewaren gedurende een bepaalde termijn (dit is een wettelijke bewaartermijn). Deze bewaartermijn is gerechtvaardigd op basis van de AVG-grondslag wettelijke plicht (artikel 6 lid 1 sub c AVG). Zie onder andere vraag 35 in module 2. Wanneer er géén bewaartermijn is opgenomen in een (zorgspecifieke) wet zoals de Wgbo of de Wlz, dan geldt de hoofdregel: niet langer bewaren dan voor het doel van de verwerking noodzakelijk is.

Het beginsel van integriteit en vertrouwelijkheid (artikel 5 lid 1 sub f AVG)

Persoonsgegevens moeten worden verwerkt op een manier die een passende beveiliging en vertrouwelijkheid van die gegevens waarborgt, ook ter voorkoming van ongeoorloofde toegang tot of het ongeoorloofde gebruik van persoonsgegevens en de apparatuur die voor de verwerking wordt gebruikt. Ter borging van dit beginsel moet de verwerkingsverantwoordelijke technische en organisatorische beveiligingsmaatregelen nemen. Dit beginsel wordt nader uitgewerkt in artikel 32 AVG, met daaraan gekoppeld de datalekmeldplicht uit artikelen 33 en 34 AVG.

3. Wanneer voldoet een zorgorganisatie aan het rechtmatigheidsbeginsel?

Er is alleen sprake van een rechtmatige gegevensverwerking als aan ten minste een van de onderstaande grondslagen is voldaan wanneer het gaat om gewone persoonsgegevens. Gaat het om bijzondere persoonsgegevens (zoals gegevens over de gezondheid), dan moet er naast een grondslag ook sprake zijn van een uitzonderingsgrond (noodzakelijk voor een goede behandeling van de betrokkene of voor het beheer van de instelling of voorziening) of de betrokkene moet uitdrukkelijke toestemming geven. Een belangrijk aandachtspunt bij het verwerken van bijzondere persoonsgegevens is het medisch beroepsgeheim (de geheimhoudingsplicht) van de zorgprofessional. Het medisch beroepsgeheim mag slechts onder bepaalde voorwaarden worden doorbroken, waarna verdere verwerking van persoonsgegevens mag plaatsvinden. De doorbreking van het medisch beroepsgeheim komt specifiek in module 2 aan de orde.

Klik hier voor het overkoepelend stappenplan hoe om te gaan met een privacyvraagstuk.

< Terug naar de inhoudsopgave

Grondslag 1 De betrokkene heeft ondubbelzinnige toestemming (artikel 4 onderdeel 11 AVG) gegeven voor de gegevensverwerking.

Gewone persoonsgegevens: ondubbelzinnige toestemming

Toestemming moet worden gegeven door een duidelijke actieve handeling. Bijvoorbeeld via een schriftelijke verklaring, met elektronische middelen (zoals het online plaatsen van vinkje in een vakje) of een mondelinge verklaring.
Ongeacht de gekozen methode dient altijd duidelijk te blijken dat de betrokkene vrijelijk, specifiek, geïnformeerd en ondubbelzinnig met de verwerking van zijn persoonsgegevens heeft ingestemd.

Gezondheidsgegevens: strenger toestemmingsvereiste → uitdrukkelijke toestemming

Indien toestemming dient te worden gevraagd in het kader van de verwerking van bijzondere persoonsgegevens, waaronder gezondheidsgegevens, dan moet sprake zijn van toestemming die uitdrukkelijk moet worden gegeven (artikel 9 AVG en artikel 22 UAVG).
Waar het geven van toestemming voor de verwerking van gewone persoonsgegevens kan worden afgeleid uit een handeling, een activiteit moet deze gegeven toestemming bij gezondheidsgegevens heel duidelijk, zonder twijfel, blijken uit woord, schrift of gedrag.

Uitdrukkelijk heeft betrekking op de manier waarop de toestemming tot uitdrukking wordt gebracht. Er moet sprake zijn van een uitdrukkelijke verklaring van toestemming. Een schriftelijke verklaring ligt dan voor de hand, maar dat hoeft niet.[3]

Zie ook vraag 7 in module 2 en vraag 6, 7 en 8 in module 4.

3 In de digitale of online context bijvoorbeeld kan een betrokkene de vereiste verklaring verstrekken door het invullen van een elektronisch formulier, door het versturen van een e-mail, door het uploaden van een gescand document waarop de handtekening van de betrokkene staat, of door middel van een elektronische handtekening. In theorie kan het gebruik van mondelinge verklaring ook voldoende zijn om geldige uitdrukkelijke toestemming te verkrijgen, het kan echter voor de verwerkingsverantwoordelijke moeilijk te bewijzen zijn dat bij het opnemen van de verklaring voldaan is aan alle voorwaarden voor geldige uitdrukkelijke toestemming. (Groep gegevensbescherming artikel 29, Richtsnoeren inzake toestemming overeenkomstig Verordening 2016/679, pagina 21).

< Terug naar de inhoudsopgave

Grondslag 2 De verwerking is noodzakelijk voor de uitvoering van een overeenkomst of precontractuele maatregelen daaraan voorafgaand.

In het kader van de zorg- en dienstverleningsovereenkomst zal gegevensuitwisseling plaatsvinden die daarvoor noodzakelijk is. Bijvoorbeeld het delen van informatie uit het ondersteuningsplan tussen collega's in de zorgorganisatie in het belang van de zorg- en dienstverlening aan de cliënt. (Zie meer hierover in module 2).

Gegevensuitwisseling zal voorafgaand aan het sluiten van deze overeenkomst ook al vaak essentieel zijn. Bijvoorbeeld om te bepalen of de zorgorganisatie kan voldoen aan de zorgvraag van de toekomstige cliënt. Ook in deze situatie is onderhavige grondslag van toepassing.

Aandachtspunt
Kijk kritisch naar welke gegevens onder deze grondslag geschaard kunnen worden. Als (bepaalde) gegevens niet noodzakelijk zijn voor de uitvoering van een overeenkomst dan moet de verwerking op een andere grondslag plaatsvinden. Is er geen andere grondslag dan mag de verwerking niet plaatvinden.

Grondslag 3 De verwerking is noodzakelijk om te voldoen aan een wettelijke verplichting waaraan de verwerkingsverantwoordelijke moet voldoen.

Hier kan onder meer gedacht worden aan de dossierplicht die is neergelegd in diverse wetten voor het aanleggen van een cliëntdossier. Zoals in de Wgbo, de Wlz en de Jeugdwet.
Een andere wettelijke verplichting is dat het BSN van een cliënt moet worden uitgewisseld met andere organisaties onder bepaalde omstandigheden. Maar let op: het BSN mag alleen voor de doeleinden genoemd in de wet worden verwerkt.

Aandachtspunt
Soms staat niet expliciet in een wet dat een organisatie verplicht is om persoonsgegevens te verwerken. De verwerking van persoonsgegevens kan ook zijn basis vinden in een ruimer geformuleerde wettelijke zorgplicht. In dat geval is het aan de organisatie (de verwerkingsverantwoordelijke) om goed te bepalen of de verwerking echt noodzakelijk is om aan de (impliciete) wettelijke verplichting te voldoen. Bij deze beoordeling heeft de verwerkingsverantwoordelijke een grotere eigen verantwoordelijkheid.

< Terug naar de inhoudsopgave

Grondslag 4 De verwerking is noodzakelijk voor de bescherming van vitale belangen van de betrokkene of van iemand anders.

Denk hier aan de situatie dat iemand onwel is geworden waarop direct medisch handelen noodzakelijk is en daarvoor in het cliëntdossier gekeken moet worden. Er kan niet gewacht worden totdat de betrokkene (cliënt) of iemand anders ((wettelijk) vertegenwoordiger) over deze inzage een beslissing kan nemen.

Grondslag 5 De verwerking is noodzakelijk voor de vervulling van een taak van algemeen belang of van een taak in het kader van de uitoefening van het openbaar gezag.

Hier gaat het om een publieke taak van de overheid (overheden) die expliciet kan zijn neergelegd in een wet of kan worden afgeleid uit een samenstel van wettelijke regels. Voor het uitvoeren van deze publieke taak hoeft niet altijd sprake te zijn van een bestuursorgaan, dit mogen ook andere organisaties zijn mits dit uit wetgeving blijkt. De wetten in het sociaal domein zijn hier een voorbeeld van. In artikel 2.6.4. Wmo 2015 en artikel 2.11 Jeugdwet is bepaald dat gemeenten de uitvoering van hun taken mogen uitbesteden aan derden. Dit betekent dat deze derden vervolgens op grond van deze bepalingen persoonsgegevens mogen verwerken.

Een ander voorbeeld bij deze grondslag betreft het verkrijgen van onderzoeksgegevens van zorgorganisaties door de IGJ in het kader van een calamiteitenonderzoek (artikel 11 lid 2 Wkkgz en artikel 8.6 en 8.19 Uitvoeringsbesluit Wkkgz).

Grondslag 6 De verwerking is noodzakelijk voor de behartiging van het gerechtvaardigd belang van een organisatie of van een derde. De uitwisseling mag niet plaatsvinden als de belangen van de betrokkene zwaarder wegen.

Voor een beroep op gerechtvaardigd belang voor het mogen verwerken van persoonsgegevens moet zijn voldaan aan de volgende drie criteria:

1. Er moet sprake zijn van een gerechtvaardigd belang. Het belang moet rechtmatig, duidelijk verwoord en ook echt aanwezig zijn. Een voorbeeld is een gegevensverwerking welke aantoonbaar noodzakelijk is om bedrijfsactiviteiten te kunnen verrichten, zoals een personeels- en cliëntenadministratie in een zorgorganisatie.
2. Er moet een afweging worden gemaakt tussen de belangen van de verwerkingsverantwoordelijke en de betrokkene. Als de belangen van de betrokkene zwaarder wegen dan het belang van de verwerkingsverantwoordelijke is een beroep op gerechtvaardigd belang niet mogelijk. Kan er na deze belangenafweging wél een beroep op gerechtvaardigd belang worden gedaan dan moeten er door de verwerkingsverantwoordelijke maatregelen worden getroffen die ervoor zorgen

< Terug naar de inhoudsopgave

dat de rechten en vrijheden van betrokkene niet worden beperkt. Een maatregel is om gegevens niet langer te bewaren dan voor het doel noodzakelijk is.

3. De verwerking moet worden getoetst aan het proportionaliteits- en subsidiariteitsbeginsel.

4 Wat houdt het proportionaliteits- en subsidiariteitsbeginsel in?

Als een beroep wordt gedaan op een van de grondslagen genoemd in 2 t/m 6 moet vervolgens de vraag worden beantwoord of de gegevensverwerking voldoet aan het proportionaliteits- én subsidiariteitsbeginsel. Dit is een extra toets om de belangen van de betrokkenen te waarborgen. Deze toets is niet vereist als de betrokkene zijn/haar toestemming heeft gegeven voor de gegevensverwerking.

Proportionaliteit
Wordt met de verstrekking van de gegevens het gestelde doel bereikt? Staat dit doel in verhouding met het feit dat daarvoor persoonsgegevens moeten worden verwerkt? Om tot gegevensverwerking te mogen overgaan dient hier het noodzakelijke antwoord **ja** te zijn.

Subsidiariteit
Kan het doel van het verstrekken van de gegevens ook op een andere manier worden bereikt die minder/geen inbreuk maakt op de privacy van de betrokkene?
Om tot gegevensverwerking te mogen overgaan dient hier het noodzakelijke antwoord **nee** te zijn.

Aandachtspunt
Het is van belang de grondslag te kiezen die het meest geschikt is. Dit brengt enerzijds met zich mee dat veelal géén toestemming hoeft te worden gevraagd (in geval van toepasbaarheid van een en andere grondslag) maar anderzijds ook dat als om toestemming gevraagd wordt en deze wordt op een later moment ingetrokken, niet alsnog een beroep kan worden gedaan op de grondslag gerechtvaardigd belang als terugvalmogelijkheid.

5 Moet een zorgorganisatie kunnen aantonen dat voldaan wordt aan deze beginselen?

Ja, er is een verantwoordingsplicht voor alle beginselen (artikel 5 lid 2 AVG). De zorgorganisatie (de verwerkingsverantwoordelijke) moet kunnen aantonen dat de hierboven genoemde beginselen worden nageleefd. Dit betekent dat de zorgorganisatie beleid moet opstellen om de naleving te borgen in de zorgorganisatie en in het geval verwerkers worden ingeschakeld aan hen verplichtingen worden opgelegd zodat de naleving ook in relatie tot de verwerkers is geborgd.

< Terug naar de inhoudsopgave

De AVG legt de bal voor het voldoen aan deze beginselen expliciet neer bij de verwerkingsverantwoordelijke. Deze moet erop toezien dat de beginselen uit artikel 5 AVG worden nageleefd én moet in staat zijn om deze naleving te kunnen aantonen. Deze verantwoordingsplicht introduceert ook een omgekeerde bewijslastverdeling. Dit betekent dat als de verwerkingsverantwoordelijke niet kan aantonen dat hij aan de beginselen heeft voldaan, er sprake is van een boetewaardige overtreding van de AVG.

6 Welke rechten heeft de betrokkene op grond van de AVG? (artikel 12-22 AVG)

De bescherming van privacy is een grondrecht (artikel 10 Grondwet). De betrokkene wiens persoonsgegevens worden verwerkt, heeft dan ook een aantal sterke rechten ten aanzien van de verwerkingsverantwoordelijke (en ook ten aanzien van de verwerkers). De betrokkene kan zijn privacyrechten bij de zorgorganisatie inroepen. Voor de zorgorganisatie betekent dit dat er rekening moet houden met de situatie dat de betrokkene (cliënt of (wettelijk) vertegenwoordiger) zich op een van deze rechten bij de zorgorganisatie beroept.

6.1 Recht op transparante informatie over de verwerkingen (artikelen 13 en 14 AVG)

De betrokkene heeft het recht om te weten of, en zo ja welke persoonsgegevens de zorgorganisatie verwerkt en waarom zij dat doet: de informatieplicht (transparantiebeginsel).

Zorgorganisaties hebben een actieve informatieplicht. Dat betekent dat de zorgorganisatie verplicht is om nieuwe en bestaande cliënten duidelijk te informeren over wat er met hun persoonsgegevens gebeurt en waarom.

Dit brengt het volgende met zich mee:

a. Zodra de zorgorganisatie de persoonsgegevens van de betrokkene verkrijgt, moet zij de betrokkene op een duidelijke en toegankelijke wijze informeren over de verwerking van deze persoonsgegevens. Om welke informatie dit gaat komt terug in 6.1.1.
b. Als de zorgorganisatie de persoonsgegevens van de betrokkene van iemand anders krijgt dan van de betrokkene (bijvoorbeeld van de huisarts), laat zij dit binnen een redelijke termijn aan de betrokkene weten. Hoofdregel is dat de betrokkene uiterlijk binnen een maand na de verkrijging door de zorgorganisatie moet worden geïnformeerd dat zijn persoonsgegevens worden gebruikt. Om welke informatie dit gaat komt terug in 6.1.2.

< Terug naar de inhoudsopgave

Aandachtspunt 1
De informatie moet bovendien in "beknopte, transparante, begrijpelijke en gemakkelijk toegankelijke vorm en in duidelijke en eenvoudige taal" worden verstrekt (artikel 12 lid 1 AVG). Dat betekent dat zorgorganisaties de informatie moeten aanpassen aan het niveau van de doelgroepen (cliënten van verschillend niveau en ook (wettelijk) vertegenwoordigers). In de praktijk is een online privacyreglement (plaatsen op de website van de zorgorganisatie) de meest handige manier om hieraan te voldoen. De VGN heeft een model ontwikkeld die zorgorganisaties hiervoor kunnen gebruiken.
De zorgorganisatie kan haar privacyreglement ook aan cliënten overhandigen en mondeling toelichten of per post toesturen aan cliënten die geen toegang hebben tot het internet. Een andere manier om een privacyverklaring over te brengen is bijvoorbeeld een animatiefilmpje toegesneden op betrokkenen of een factsheet met pictogrammen.

Om de betrokkene vroegtijdig te informeren over zijn of haar gegevensverwerking is het raadzaam om ook in de zorg- en dienstverleningsovereenkomst en in de e-mailhandtekening (voor extern mailen) een verwijzing op te nemen naar het privacyreglement.

Aandachtspunt 2
Het is mogelijk om een ander vorm, dan de hierboven genoemde, te kiezen waarmee de zorgorganisatie aan haar informatieplicht voldoet. De AVG bevat hier geen bepalingen over.

< Terug naar de inhoudsopgave

De zorgorganisatie heeft deze informatieplicht niet (artikel 13 lid 4 en artikel 14 lid 5 sub a t/m d AVG):

- als de **betrokkene al weet** dat de zorgorganisatie over zijn persoonsgegevens beschikt omdat zij deze gegevens van de betrokkene zelf heeft verkregen (artikel 13 lid 4 AVG);
- als de zorgorganisatie de persoonsgegevens **buiten de betrokkene om** heeft verkregen **maar de betrokkene hier van weet** (artikel 14 lid 5 sub a AVG);
- als de zorgorganisatie de persoonsgegevens **buiten de betrokkene om** heeft verkregen, maar het onmogelijk blijkt of een **onevenredige inspanning** oplevert voor de zorgorganisatie om de informatie aan de betrokkene te verstrekken (sub b);
- als de zorgorganisatie de persoonsgegevens **buiten de betrokkene om** heeft verkregen, maar in de wet is voorgeschreven dat de zorgorganisatie de persoonsgegevens mag verkrijgen en in die **wet** de **gerechtvaardigde belangen** van de betrokkene zijn gewaarborgd (sub c);
- als de zorgorganisatie de persoonsgegevens **buiten de betrokkene om** heeft verkregen, maar de persoonsgegevens van de betrokkene vertrouwelijk moeten blijven in verband met een **beroepsgeheim** (sub d).

Toelichting op deze laaste uitzondering:
Wanneer de zorgorganisatie (verwerkingsverantwoordelijke) gehouden is aan een beroepsgeheim, zoals het medisch beroepsgeheim, gaat dit boven de informatieplicht uit artikel 14 AVG. Bijvoorbeeld wanneer de zorgorganisatie een dossier krijgt van zijn cliënt met daarin persoonsgegevens van derden. De zorgorganisatie is dan niet gehouden deze derden te informeren over deze verkrijging, aangezien dit in strijd zou zijn met zijn beroepsgeheim ten aanzien van zijn cliënt. Zie ook vraag 16 van module 2.

6.1.1 Welke informatie moet de zorgorganisatie verstrekken aan de betrokkene wanneer de persoonsgegevens van de betrokkene zijn verkregen? (artikel 13 AVG)

Als de persoonsgegevens van de betrokkene zelf zijn verkregen, bijvoorbeeld bij de intake, dan moet de zorgorganisatie onderstaande informatie op het moment van verkrijging van deze persoonsgegevens aan de betrokkene verstrekken:

- identiteit (volledige of statutaire naam van) en contactgegevens (adres, telefoonnummer, e-mail en sociale media) van de zorgorganisatie of de vertegenwoordiger daarvan;
- contactgegevens (telefoonnummer en e-mail) van de functionaris voor gegevensbescherming (indien aangesteld);
- de verwerkingsdoeleinden (bijv. zorgverlening, dossierbeheer, voldoen aan een wettelijke verplichting) waarvoor de per-

< Terug naar de inhoudsopgave

soonsgegevens zijn bestemd en de grondslag(en) voor verwerking (o.g.v. artikel 6 AVG);
- de gerechtvaardigde belangen waarop een verwerking is gebaseerd, indien de zorgorganisatie een beroep op de grondslag gerechtvaardigd belang doet (artikel 6 lid 1 sub f AVG);
- aan welke (categorieën van) partij(en) de gegevens worden verstrekt (bijvoorbeeld aan CIZ, zorgkantoor of gemeente);
- of gegevens worden doorgegeven aan een derde land (niet EU) en zo ja, welke waarborgen er dan zijn getroffen;
- de bewaartermijn gedurende welke de persoonsgegevens worden opgeslagen of de criteria om de bewaartermijn te bepalen;
- de rechten van betrokkene (inzage en afschrift, rectificatie, gegevenswissing, beperking, overdraagbaarheid en bezwaar);
- wanneer de verwerking is gebaseerd op toestemming (artikel 6 lid 1 sub a AVG), de betrokkene het recht heeft zijn toestemming ten allen tijde in te trekken en dat een dergelijke intrekking geen terugwerkende kracht heeft;
- dat betrokkene een klacht bij de Autoriteit Persoonsgegevens kan indienen (artikel 77 AVG);
- of verstrekking van gegevens een wettelijk of contractuele verplichting is en wat de gevolgen zijn indien de gegevens niet worden verstrekt;
- of sprake is van geautomatiseerde besluitvorming en zo ja, wat de onderliggende logica is en welke gevolgen er zijn voor de betrokkene;
- de zorgorganisatie moet aan betrokkene melden als zij van plan is de persoonsgegevens ook voor andere doelen te gebruiken. Deze doelen moeten verenigbaar zijn met het doel van de verkrijging (artikel 5 lid 1 sub b AVG, doelbinding).

6.1.2 Welke informatie moet de zorgorganisatie verstrekken wanneer persoonsgegevens niet van de betrokkene zijn verkregen? (artikel 14 AVG)

Wanneer de zorgorganisatie persoonsgegevens verzamelt die niet van betrokkene zijn verkregen, dan moet in beginsel dezelfde informatie worden verstrekt als wanneer de zorgorganisatie de persoonsgegevens van de betrokkene heeft gekregen (zie 6.1.1). Met als extra vereiste dat de zorgorganisatie de **bron** waaruit persoonsgegevens zijn verkregen moet **toevoegen**. Als de bron van de informatie niet kan worden vastgesteld, bijvoorbeeld omdat de informatie uit verschillende bronnen is samengesteld, dient de zorgorganisatie algemene informatie over de herkomst te verstrekken.

6.2 Recht op inzage en afschrift van de persoonsgegevens (artikel 15 AVG)

De betrokkene heeft het recht om zijn persoonsgegevens, die de zorgorganisatie van de betrokkene verwerkt, in te zien. De betrokkene heeft ook het recht op een afschrift (kopie) van die gegevens.
Voor een afschrift van de persoonsgegevens brengt een zorgorganisatie in beginsel geen kosten in rekening. Tenzij de betrokkene verzoekt om meerdere kopieën van dezelfde persoonsgegevens. In dat geval kan de zorgorganisatie op basis van administratieve kosten daarvoor een redelijke vergoeding vragen. Zie voor specifieke FAQ's over inzage en afschrift in cliëntdossier door betrokkene (minderjarig en meerderjarig) module 2.

< Terug naar de inhoudsopgave

6.2.1 Moet er altijd inzage en afschrift aan de betrokkene worden gegeven?

Nee, de volgende uitzonderingen gelden:

- de betrokkene heeft geen recht op informatie over anderen;
- de zorgorganisatie verleent geen (of gedeeltelijk) inzage en/of verstrekt geen (of gedeeltelijk) afschrift uit het cliëntdossier als de persoonlijke levenssfeer van een ander daardoor wordt geschaad;
- de betrokkene heeft geen recht op inzage in de persoonlijke werkaantekeningen van een zorgprofessional. Deze maken géén onderdeel uit van het cliëntdossier.

Zie voor specifieke FAQ's over inzage en afschrift in cliëntdossier door betrokkene (minderjarig en meerderjarig) module 2.

6.3 Recht op rectificatie van de gegevens als deze niet kloppen (artikel 16 AVG)

De betrokkene heeft het recht om de zorgorganisatie te vragen zijn persoonsgegevens te verbeteren als deze niet meer kloppen of aan te vullen als deze niet volledig zijn. Ook mag de betrokkene de zorgorganisatie vragen om een verklaring aan zijn cliëntdossier toe te voegen. Het recht op rectificatie betreft feitelijke gegevens en gaat niet over verklaringen van bevindingen die medewerkers in een cliëntdossier hebben opgenomen.

6.4 Recht op gegevenswissing (recht op vergetelheid) (artikel 17 AVG)

De betrokkene heeft het recht om vergeten te worden. Dit betekent dat de betrokkene de zorgaanbieder mag vragen zijn persoonsgegevens te wissen, verwijderen of vernietigen als:

- de zorgorganisatie de persoonsgegevens van de betrokkene niet langer nodig heeft voor het doel waarvoor deze zijn verwerkt;
- de betrokkene zijn toestemming voor verwerking intrekt en er geen andere juridische grond voor verwerking aanwezig is;
- de zorgorganisatie de persoonsgegevens van de betrokkene onterecht heeft verwerkt;
- er sprake is van een wettelijke bepaling die de zorgorganisatie verplicht tot het wissen of verwijderen van de persoonsgegevens van de betrokkene;
- de betrokkene gegrond bezwaar heeft gemaakt tegen de gegevensverwerking.

Zie vraag 6.5 over het recht op vergetelheid in relatie tot gegevens over de gezondheid.

< Terug naar de inhoudsopgave

6.5 Moet een zorgorganisatie altijd voldoen aan een verzoek van betrokkene tot het wissen van gegevens?

Nee, in het geval het gegevens over de gezondheid van de betrokkene betreft hoeft de zorgorganisatie niet te verwijderen, wissen of vernietigen:

- als er een wet is die een afwijkende bewaartermijn kent. Tijdens die bewaartermijn mag de zorgorganisatie de gegevens niet vernietigen;
- als iemand anders (een derde) een aanmerkelijk belang heeft bij het bewaren van de gegevens van de betrokkene;
- als dit ervoor zou zorgen dat de zorgprofessional van de betrokkene zijn werk niet meer goed kan doen (in strijd met 'het goed hulpverlenerschap' genoemd in de Wgbo).

6.6 Recht op beperking van de verwerking (artikel 18 AVG)

De betrokkene mag de zorgorganisatie vragen tijdelijk zijn persoonsgegevens niet te gebruiken zolang een bepaald probleem of bezwaar dat gaat over de verwerking van deze persoonsgegevens nog niet is opgelost. Het recht op beperking van de verwerking geldt in situaties die voldoen aan één van de volgende criteria:

- de gegevens zijn mogelijk onjuist;
- de verwerking is onrechtmatig (er wordt dus in strijd gehandeld met artikel 6 AVG);
- de gegevens zijn niet meer nodig;
- de betrokkene maakt bezwaar.

6.7 Recht op overdraagbaarheid van gegevens (dataportabiliteit) (artikel 20 AVG)

De betrokkene mag de zorgorganisatie verzoeken zijn persoonsgegevens aan hem te verstrekken op een manier die het voor de betrokkene makkelijk maakt om zijn gegevens te hergebruiken en door te geven aan een andere (zorg)organisatie.

Maar dit recht geldt enkel:

- voor de persoonsgegevens die door de betrokkene zelf zijn verstrekt;
- én de betrokkene voor de verwerking toestemming heeft verleend of verwerking kon plaatsvinden ter uitvoering van een overeenkomst;
- én de verwerking geautomatiseerd plaatsvindt.
  Het recht op dataportabiliteit geldt niet voor niet-geautomatiseerde (papieren) bestanden.

< Terug naar de inhoudsopgave

6.8 Recht van bezwaar (artikel 21 AVG)

De betrokkene mag bezwaar maken tegen de gegevensverwerking door de zorgorganisatie op grond van een gerechtvaardigd eigen belang of een taak van algemeen belang.

Wanneer een verwerkingsverantwoordelijke zich heeft beroepen op de grondslag taak van algemeen belang (artikel 6 lid 1 punt e AVG) of gerechtvaardigd belang (artikel 6 lid 1 sub f AVG) moet hij een belangenafweging verrichten ten aanzien van de privacy van de betrokkenen. Een betrokkene kan echter in een specifieke situatie anders tegen zo'n afweging aankijken. Het recht van bezwaar geeft de betrokkene de mogelijkheid van de verwerkingsverantwoordelijke te verlangen dat deze de belangenafweging nogmaals maakt met inachtneming van de specifieke situatie van de betrokkene.

Geen bezwaar (door betrokkene) is mogelijk als de betrokkene toestemming heeft gegeven voor de verwerking. De betrokkene kan wel zijn toestemming intrekken waarna de verwerking moet worden gestaakt.

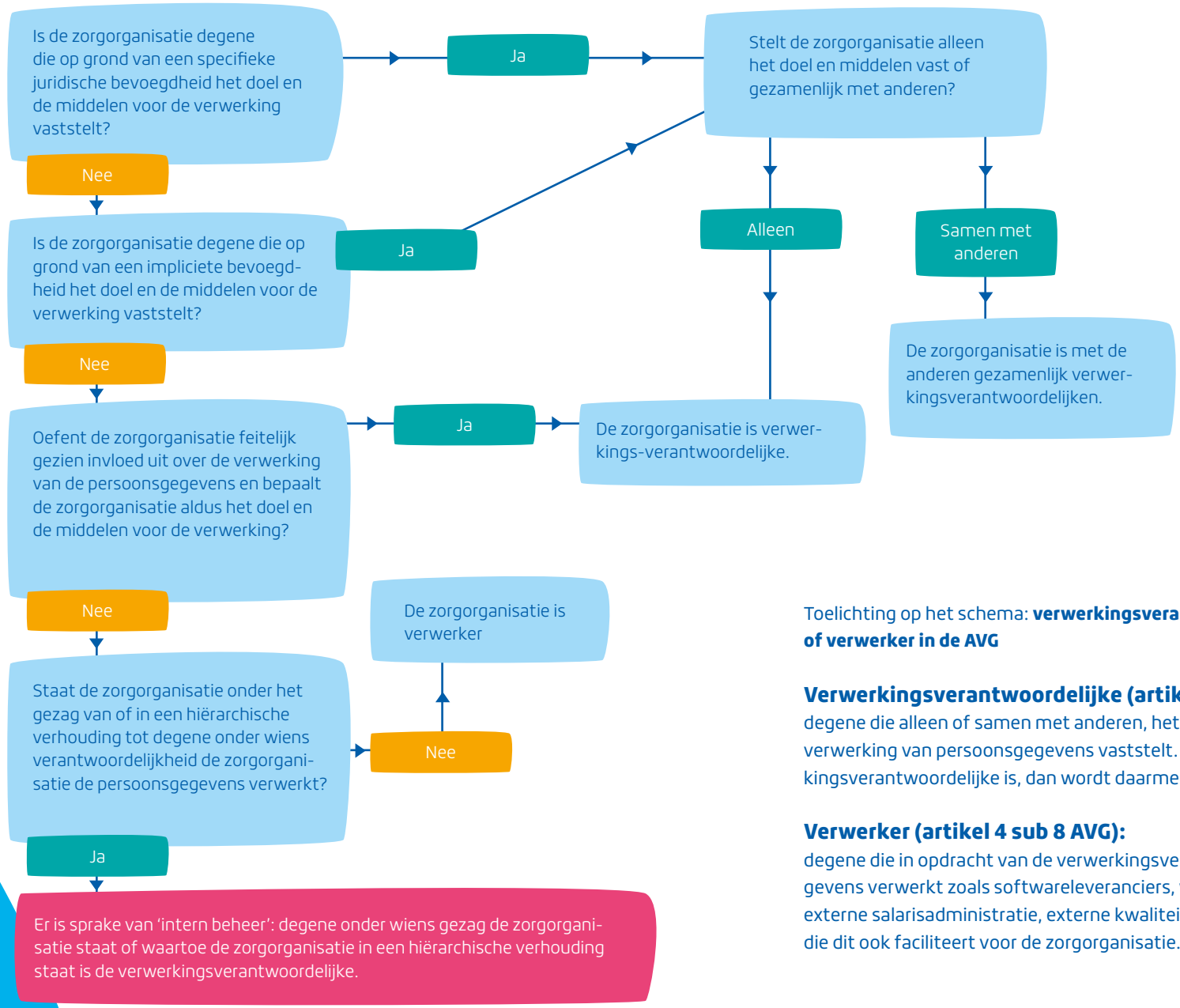
De verwerkingsverantwoordelijke en de verwerker

7 Stroomschema verwerkingsverantwoordelijke of verwerker[4]

Om te bepalen of een zorgorganisatie verwerkingsverantwoordelijke of verwerker is, kan het stroomschema op de volgende bladzijde doorlopen worden.

4 Schema is overgenomen uit de Handleiding Algemene verordening gegevensbescherming en Uitvoeringswet Algemene verordening gegevensbescherming van het Ministerie van Justitie en Veiligheid, januari 2018.

Stroomschema verwerkingsverantwoordelijke of verwerker



Toelichting op het schema: **verwerkingsverantwoordelijke of verwerker in de AVG**

Verwerkingsverantwoordelijke (artikel 4 sub 7 AVG):
degene die alleen of samen met anderen, het doel van en de middelen voor de verwerking van persoonsgegevens vaststelt. Als de zorgorganisatie verwerkingsverantwoordelijke is, dan wordt daarmee de Raad van Bestuur bedoeld.

Verwerker (artikel 4 sub 8 AVG):
degene die in opdracht van de verwerkingsverantwoordelijke persoonsgegevens verwerkt zoals softwareleveranciers, website hosts, clouddiensten, externe salarisadministratie, externe kwaliteitsauditor, leverancier van het ECD die dit ook faciliteert voor de zorgorganisatie.

< Terug naar de inhoudsopgave

8. Welke verplichtingen heeft een verwerkingsverantwoordelijke?

Volgens de AVG rusten er op de verwerkingsverantwoordelijke twee hoofdverplichtingen. Enerzijds moet de verwerkingsverantwoordelijke de plichten uit de AVG naleven en anderzijds moet de verwerkingsverantwoordelijke deze naleving kunnen aantonen. Dit wordt ook wel het accountability-principe genoemd.

Op welke manier de verwerkingsverantwoordelijke aan deze verplichtingen concreet invulling moet geven, meldt de AVG niet. Wel volgt uit de AVG dat de verwerkingsverantwoordelijk verplicht is passende technische en organisatorische maatregelen te nemen om te waarborgen en te kunnen aantonen dat elke verwerking van persoonsgegevens overeenkomstig de AVG wordt uitgevoerd. Deze maatregelen moeten worden geëvalueerd en indien nodig geactualiseerd.

De **vuistregel** is, naarmate de verwerking van persoonsgegevens een hoger risico voor de betrokkene met zich meebrengt, hoe meer maatregelen de verwerkingsverantwoordelijke moet nemen ter bescherming van de persoonsgegevens.
De betekenis van elke verplichting worden hierna toegelicht. Het is van belang om onderstaande verplichtingen goed eigen te maken in de zorgorganisatie (privacy awareness) en hierop beleid te ontwikkelen.

< Terug naar de inhoudsopgave

De verplichtingen voor de verwerkingsverantwoordelijke in één oogopslag:

1. De verwerkingsverantwoordelijke is verplicht een **register** bij te houden van de verwerkingsactiviteiten die onder zijn verantwoordelijkheid hebben plaatsgevonden;
2. Onder bepaalde omstandigheden ben je verplicht een **functionaris voor gegevensbescherming** aan te stellen;
3. Voorafgaand aan risicovolle verwerkingsactiviteiten moet de verwerkingsverantwoordelijke een **gegevens** de **beschermingseffectbeoordeling** uitvoeren;
4. Onder bepaalde omstandigheden moet de verwerkingsverantwoordelijke de **Autoriteit Persoonsgegevens raadplegen**, voorafgaand aan een nieuwe risicovolle verwerkingsactiviteit;
5. Bij het inrichten van verwerkingen moet de verwerkingsverantwoordelijke rekening houden met het **principe van privacy door ontwerp en standaardinstellingen.** Dit wordt ook wel privacy by design en privacy by default genoemd;
6. Met het oog op de bescherming van persoonsgegevens dient verwerkingsverantwoordelijke **passende beveiligingsmaatregelen** te nemen;
7. In het geval van een **datalek** moet de verwerkingsverantwoordelijke melding doen bij de Autoriteit Persoonsgegevens en onder bepaalde omstandigheden moet de verwerkingsverantwoordelijke ook de betrokkene informeren;
8. De verwerkingsverantwoordelijke moet **afspraken maken met zijn verwerkers.** Wanneer de verwerkingsverantwoordelijke een verwerker inschakelt (artikel 28 AVG) moet deze afdoende garanties bieden dat ook zijn verwerkingen met passende waarborgen zijn omkleed.

8.1 Verplichting 1 Verwerkingsregister

Opstellen en bijhouden van verwerkingsregister (artikel 30 AVG)

Het verwerkingsregister is één van de nieuwe verplichtingen onder de AVG. Met het verwerkingsregister dient de zorgorganisatie duidelijk in kaart brengen welke gegevens zij verwerkt en voor welke doeleinden. Met andere woorden, het register geeft inzicht in de verwerkingsactiviteiten. Zowel een verwerkingsverantwoordelijke als een verwerker moet een register van verwerkingsactiviteiten bijhouden.

< Terug naar de inhoudsopgave

Zorgorganisaties voor de gehandicaptenzorg zijn verplicht om een verwerkingsregister op te stellen en bij te houden:

1. Het bijhouden van een verwerkingsregister is verplicht als een zorgorganisatie meer dan 250 medewerkers heeft. Dit zal voor het overgrote deel van de VGN-leden het geval zijn.
2. Voor zorgorganisaties met minder dan 250 medewerkers, is het bijhouden van een verwerkingsregister ook verplicht:

- als verwerkingen met een hoog risico voor betrokkenen worden uitgevoerd;
- als de verwerking van persoonsgegevens van cliënten structureel is[5];
- als een zorgorganisatie persoonsgegevens verwerkt die vallen onder de categorie bijzondere persoonsgegevens, zoals gegevens over de gezondheid van cliënten[6].

Wanneer de Autoriteit Persoonsgegevens daarom vraagt zijn zorgorganisaties verplicht om dit register te verstrekken.

8.1.1 Wat moet er in het register van verwerkingsactiviteiten staan?

Het register van verwerkingsactiviteiten bevat de belangrijkste informatie over de persoonsgegevens die de zorgorganisatie verwerkt. Het is nadrukkelijk niet de bedoeling dat verwerkingen van persoonsgegevens in het register worden opgenomen. De zorgorganisatie mag zelf weten hoe het register wordt opgesteld, als het maar schriftelijk is (hieronder wordt ook een elektronische vorm verstaan).

Wel schrijft de AVG voor welke informatie het register moet bevatten:

- de naam en contactgegevens van de zorgorganisatie als verwerkingsverantwoordelijke, eventuele gezamenlijke verwerkingsverantwoordelijken en in voorkomende geval van de vertegenwoordiger van de verwerkingsverantwoordelijke;
- de contactgegevens van de functionaris voor gegevensbescherming (indien aangesteld);
- de verwerkingsdoeleinden. In de gehandicaptenzorg is een verwerkingsdoel bijvoorbeeld het verzamelen en uitwisselen van cliëntgegevens (gewone persoonsgegevens en gezondheidsgegevens) om goede zorg te kunnen bieden in het kader van de zorg- en dienstverleningsovereenkomst (zie vraag 2 in module 2);
- een beschrijving van de categorieën van betrokkenen en van de categorieën van persoonsgegevens. In de gehandicaptensector zijn betrokkenen (toekomstige) cliënten, maar vaak ook de wettelijk vertegenwoordigers, schriftelijk gemachtigden, of de belangenbehartigers door wie de cliënten worden vertegenwoordigd. Categorieën van (bijzondere)

5 Dit zal veelal het geval zijn.
6 Idem.

< Terug naar de inhoudsopgave

persoonsgegevens zijn bijvoorbeeld NAW-gegevens, telefoonnummers, maar ook gegevens over de beperking of de medische voorgeschiedenis;
- de categorieën van ontvangers aan wie de persoonsgegevens zijn of zullen worden verstrekt, zoals medewerkers in de zorgorganisatie, maar ook andere zorgorganisaties zoals de tandarts of paramedici. Of verstrekking van gegevens aan externe organisaties zoals het CIZ, een gemeente of het zorgkantoor;
- wanneer de gegevens worden gedeeld met een land of internationale organisatie buiten de EU dan moet dit worden aangeven in het verwerkingsregister (denk bijvoorbeeld aan de situatie dat een zorgorganisatie gebruik maakt van clouddiensten);
- indien mogelijk, de beoogde termijnen hoe lang de verschillende categorieën van gegevens moeten worden bewaard. De bewaartermijnen in de gehandicaptenzorg vloeien naast de AVG onder andere voort uit verschillende zorgwetten;
- indien mogelijk, een algemene beschrijving van de technische en organisatorische beveiligingsmaatregelen, encryptie, logische toegangscontrole, pseudonimisering.

Aandachtspunt 1: volledig en actueel
Het register van verwerkingsactiviteiten moet altijd een volledig en actueel overzicht van de hierboven genoemde informatie bevatten. Wanneer de zorgorganisatie bijvoorbeeld nieuwe categorieën van persoonsgegevens gaat verzamelen, dan moeten deze in het register worden toegevoegd.

Aandachtspunt 2: rol voor functionaris voor gegevensbescherming in het bijhouden van registers
De verwerkingsverantwoordelijke of de verwerker kan de functionaris voor gegevensbescherming de taak opleggen om het register van verwerkingsactiviteiten bij te houden; dit onder verantwoordelijkheid van de verwerkingsverantwoordelijke of de verwerker.

Aandachtspunt 3: toegang verlenen
De zorgorganisatie moet het verwerkingsregister ter beschikken stellen aan de Autoriteit Persoonsgegevens, als zij daarom vraagt. Ook dient de functionaris voor gegevensbescherming, wanneer de zorgorganisatie deze heeft aangesteld, toegang te krijgen tot het register.

< Terug naar de inhoudsopgave

8.2 Verplichting 2 Functionaris Gegevensbescherming

Functionaris voor gegevensbescherming (artikelen 37-39 AVG)

De functionaris voor gegevensbescherming (FG) is een onafhankelijk en deskundig persoon met als taak intern toezicht houden en adviseren over de toepassing en naleving van de AVG en andere toepasselijke regelgeving binnen de zorgorganisatie. De FG kan zowel in dienst zijn van de organisatie als een externe persoon zijn. De FG heeft geen bevoegdheden tot opleggen van formele sancties. De FG niet eindverantwoordelijk als er binnen de zorgorganisatie overtredingen van de AVG plaatsvinden. De naleving van de AVG is een verantwoordelijkheid van de verwerkingsverantwoordelijke of de verwerker. De FG heeft een geheimhoudingsplicht.

8.2.1 Is het voor zorgorganisaties in de gehandicaptenzorg verplicht om een functionaris gegevensbescherming aan te stellen?

Op grond van artikel 37 van de AVG is een FG in drie situaties verplicht. Zorgorganisaties in de gehandicaptenzorg vallen onder de situatie die wordt genoemd in artikel 37 lid 1 sub c AVG. Dit brengt met zich mee dat zorgorganisaties verplicht zijn een FG te benoemen als ze op grote schaal bijzondere persoonsgegevens verwerken en dit een kernactiviteit is. De AVG laat echter in het midden wat een verwerking 'op grote schaal' inhoudt.

Visie Autoriteit Persoonsgegevens over grootschalige verwerking

In mei 2018 heeft de Autoriteit Persoonsgegevens (AP) het begrip 'grootschalig' uitgelegd voor ziekenhuizen, huisartsenposten en zorggroepen.[7] In december 2018 heeft de AP vervolgens uitleg gegeven voor alle overige zorgaanbieders, waaronder leden van de VGN. [8]

De AP stelt dat er sprake is van grootschalige verwerking van persoonsgegevens als van meer dan 10.000 patiënten gegevens worden verwerkt in één informatiesysteem. [9]

7 Het bericht van de AP vindt u hier: www.autoriteitpersoonsgegevens.nl/nl/nieuws/ap-geeft-uitleg-over-grootschalige-gegevensverwerking-de-zorg.

8 Het bericht van de AP vindt u hier: www.autoriteitpersoonsgegevens.nl/nl/nieuws/uitleg-begrip-'grootschalig'-verduidelijkt-voor-alle-zorgaanbieders.

9 De interpretatie van de AP riep de nodige vragen op. De VGN heeft samen met Actiz, NVZ, NFU en GGZ Nederland (verenigd in BoZ) aanvullende vragen gesteld, zie: https://www.vgn.nl/artikel/27315. De volledige reactie van de AP vindt u hier: https://www.vgn.nl/artikel/27431.

< Terug naar de inhoudsopgave

De AP geeft aan dat het uitgangspunt in de interpretatie de omvang van de zorgorganisatie is. Dit tegen de achtergrond van de wens van de Tweede Kamer om kleinere instellingen te ontzien van de verplichting om een FG aan te stellen. De AP is daarbij redelijkerwijs uitgegaan van een grens van 10.000 cliënten die bij een zorgorganisatie zijn ingeschreven of door een zorgorganisatie jaarlijks worden behandeld. Overstijgt het aantal - ingeschreven of jaarlijks behandelde - cliënten bij een zorgorganisatie de grens van 10.000, dan beschouwt de AP dat als een grote zorginstelling.

De AP benadrukt dat cliënten die op een wachtlijst staan, cliënten die 'uit-zorg' zijn en (wettelijk) vertegenwoordigers niet meegerekend worden bij de grens van 10.000 cliënten. Zouden deze gegevens ook meetellen, dan zouden ook kleinere instellingen al gauw onder de FG verplichting vallen en dat was niet de bedoeling van de Tweede Kamer. [10]

Advies
De Autoriteit Persoonsgegevens noemt 10.000 cliënten in één informatiesysteem als getal vanaf wanneer sprake is van een grootschalige gegevensverwerking. De meeste zorgorganisaties in de gehandicaptenzorg bereiken de grens van 10.000 cliënten niet en zouden daarmee op grond van de interpretatie van de Autoriteit Persoonsgegevens van het begrip 'grootschalige verwerking' niet verplicht zijn om een FG aan te stellen.

Het advies is dit getal niet als uitgangspunt te nemen, maar uit te gaan van het feit dat de AVG risico-gestuurde wetgeving is. Dit betekent dat de zorgorganisatie bij elke gegevensverwerking moet nagaan welke risico's de verwerking met zich mee kan brengen voor de betrokkenen en voor de zorgorganisatie, zeker gezien het feit dat sprake is van verwerking van bijzondere persoonsgegevens. Het is derhalve raadzaam een FG aan te stellen (ongeacht het aantal cliënten). De FG kan voor een zorgorganisatie als 'geweten' op het gebied van privacy optreden en helpen de organisatie AVG-proof te maken. Het voorgaande sluit ook aan bij wat de Autoriteit Persoonsgegevens in haar visie heeft aangegeven, namelijk dat het de verantwoordelijkheid blijft van de verwerkingsverantwoordelijken en verwerkers zelf om, met inachtneming van het juridisch kader en op basis van de aanwezige risico's van de verwerking, te beoordelen of zij verplicht zijn een FG aan te stellen.

Aandachtspunt 1
De zorgorganisatie kan een FG voor een bepaald aantal uren extern inhuren of gezamenlijk met een collega zorgorganisatie delen, zodat de kosten beperkt blijven.

10 De volledige reactie van de AP vindt u hier: www.vgn.nl/artikel/27431

< Terug naar de inhoudsopgave

Aandachtspunt 2
Organisaties moeten hun functionaris gegevensbescherming met een (nieuw) webformulier aanmelden bij de Autoriteit Persoonsgegevens. Organisaties die hun FG vóór 25 mei 2018 hebben aangemeld, moeten dat opnieuw doen. FG-aanmeldingen die niet via het online aanmeldingsformulier zijn gedaan, zijn na 25 mei 2018 vervallen.

8.2.2 Aan welke eisen moet een FG in de gehandicaptenzorg voldoen? (artikel 37 lid 5 AVG)

De FG heeft een zorgplicht om op een professionele en deskundige manier zijn taken te vervullen. De AVG formuleert deze zorgplicht als het hebben van professionele kwaliteiten en deskundigheid op het gebied van gegevensbescherming zowel wat betreft wetgeving als de praktijk.

Voor de gehandicaptenzorg betekent dit dat de FG naast kennis van de AVG en UAVG, ook kennis moet hebben van specifieke zorgwetgeving op het gebied van privacy. Daarnaast moet de FG:

- kennis hebben van de gehandicaptensector en zorgorganisatie waarvoor hij werkt;
- verstand hebben van de gegevensverwerkingen die de zorgorganisatie uitvoert;
- verstand hebben van IT en beveiliging van gegevens;
- in staat zijn om binnen de zorgorganisatie over (het belang van) de beveiliging van persoonsgegevens te adviseren

8.2.3 Welke positie heeft de FG binnen de zorgorganisatie (artikel 38 AVG)

De FG vervult een belangrijke rol en moet daarin worden gepositioneerd en gefaciliteerd:

- De verwerkingsverantwoordelijke en de verwerker moeten ervoor zorgen dat de FG naar behoren en tijdig wordt betrokken bij alle aangelegenheden die verband houden met de verwerking en bescherming van de persoonsgegevens van de zorgorganisatie.
- De verwerkingsverantwoordelijke en de verwerker moeten de FG ondersteunen bij de invulling van zijn taken, door hem toegang te geven tot persoonsgegevens en verwerkingsactiviteiten.
- Daarnaast moet de FG kunnen beschikken over voldoende middelen voor het vervullen van zijn taken, zoals voldoende steun vanuit het management, voldoende tijd, financiële middelen en faciliteiten en zo nodig ondersteunend personeel.
- Ook moet de FG toegang hebben tot de (bijzondere) persoonsgegevens en de verwerkingsactiviteiten van de zorgorganisatie. De bekendheid en bereikbaarheid van de FG moet goed geregeld zijn in de zorgorganisatie ook voor betrokkenen. Zijn gegevens moeten ook worden opgenomen in het privacyreglement van de zorgorganisatie (wanneer de

< Terug naar de inhoudsopgave

zorgorganisatie gebruik maakt van een privacyreglement) of op een andere manier goed vindbaar zijn, zoals op de website van de zorgorganisatie.

- De FG moet onafhankelijk kunnen opereren en mag dus geen instructies krijgen van de zorgorganisatie voor de uitvoering van zijn taken. De FG brengt rechtstreeks verslag uit aan de hoogste leidinggevende van de zorgorganisatie: dit is de Raad van Bestuur. Een FG heeft dezelfde ontslagbescherming als leden van een ondernemingsraad. Dat betekent dat de FG niet kan worden ontslagen voor de uitvoering van zijn/haar taken als FG.

De FG is met betrekking tot de uitvoering van zijn taken **gehouden tot geheimhouding en vertrouwelijkheid.**

De FG mag **geen conflicterende belangen hebben.** Het is niet aan te raden om bijvoorbeeld een manager cliëntenadministratie of een regiodirecteur wonen en dagbesteding te benoemen als FG, omdat deze personen te nauw betrokken zijn bij de verwerking van (bijzondere) persoonsgegevens.

8.2.4 Welke taken heeft een FG? (artikel 39 AVG)

Een FG heeft de volgende taken op grond van de AVG en de Guidelines FG:

1. Creëren van privacy-bewustzijn in de zorgorganisatie:
   - Het informeren en adviseren van de zorgorganisatie over de verplichtingen op grond van AVG, UAVG en zorgspecifieke wetgeving (denk aan: fungeren als sparringpartner voor management en zorgorganisatie op het gebied gegevensbeveiliging). Een belangrijk voorbeeld is het advies van de FG bij de gegevensbeschermingseffectbeoordeling (artikel 35 lid 2 AVG);
   - Bewust maken en opleiden van het medewerkers (bijvoorbeeld door het geven van interne trainingen, aanbieden van e-learning en verstrekken van informatiemateriaal;
2. Actief betrokken bij de wijze waarop in de zorgorganisatie wordt omgegaan met persoonsgegevens.
3. Overige toezichtstaken:
   - De FG houdt toezicht op de naleving van de privacywetgeving binnen de zorgorganisatie en het eigen interne gegevensverwerkingsbeleid;

< Terug naar de inhoudsopgave

- De FG voert interne audits uit;
- Samenwerken met de Autoriteit Persoonsgegevens.

De FG treedt naar de AP op als eerste aanspreekpunt voor alle aangelegenheden aangaande persoonsgegevens.

8.3 Verplichting 3 Gegevensbeschermingseffectbeoordeling (artikel 35 AVG)

Een gegevensbeschermingseffectbeoordeling, ook wel data protection impact assessment (DPIA) genoemd, is een proces dat de verwerkingsverantwoordelijke, die het doel van en de middelen voor de gegevensverwerking vaststelt, doorloopt om de risico's van de verwerking van persoonsgegevens in kaart te brengen en aan de hand daarvan maatregelen te nemen om de gesignaleerde risico's aan te verkleinen of te voorkomen. De DPIA stimuleert de zorgorganisatie om op tijd na te denken over de invloed die een verwerking heeft op de privacy van betrokkenen, op welke wijze de persoonsgegevens normconform kunnen worden verwerkt en of er ook een aanpak mogelijk is die minder gevolgen heeft voor de privacy van betrokkenen.

8.3.1 Wat houdt een DPIA in?

Een DPIA moet in ieder geval het volgende inhouden:

- een beschrijving van de beoogde verwerkingen en de verwerkingsdoeleinden;
- een beoordeling van de noodzaak en de evenredigheid van de verwerkingen;
- een beoordeling van de risico's voor de rechten en vrijheden van betrokkenen;
- de beoogde maatregelen om de risico's aan te pakken en aan te tonen dat aan de AVG is voldaan.

De DPIA dient vervolgens te leiden tot een rapport waarin de bovengenoemde punten zijn verwerkt, tot welke oordelen dit heeft geleid en wat de beoogde maatregelen in de zin van waarborgen, veiligheidsmaatregelen en mechanismen om risico's weg te nemen of te beperken.

De resultaten van de DPIA moeten meegenomen worden bij het vaststellen van de maatregelen om de belangen van betrokkene te beschermen en om aan te tonen dat zorgorganisatie de AVG bij haar verwerkingsactiviteit naleeft. Wanneer een zorgorganisatie de hoge risico's voor betrokkenen niet met redelijke maatregelen kan beperken, moet de voorgenomen verwerking, voordat deze van start gaat, voor worden gelegd aan de Autoriteit Persoonsgegevens.

< Terug naar de inhoudsopgave

Aandachtspunt 1
Gesprekken met medewerkers kunnen een belangrijk onderdeel zijn van een DPIA. Daarin kunnen de volgende vragen worden gesteld: welke persoonsgegevens gaan er verwerkt worden en waarom? Zijn alle gegevens die worden gebruikt ook noodzakelijk? Wie heeft er toegang tot de gegevens? Waar worden gegevens opgeslagen en zijn ze op de juiste wijze beveiligd? Met wie worden gegevens uitgewisseld, en hoe is er dan voor gezorgd dat zij er zorgvuldig mee omgaan?
Soms kan het ook wenselijk zijn de betrokkenen hun mening te vragen over de voorgenomen verwerking.

Aandachtspunt 2
In het DPIA rapport worden geen persoonsgegevens opgenomen.

8.3.2 Wanneer is het uitvoeren van een DPIA in de gehandicaptenzorg verplicht?

Op grond van de AVG is een verwerkingsverantwoordelijke verplicht om een DPIA uit te voeren vanuit het perspectief van een zorgvuldige omgang met persoonsgegevens als de verwerking waarschijnlijk een hoog risico inhoudt voor de rechten en vrijheden van betrokkenen.

Wanneer is er sprake van zo'n risico? Daar zijn geen harde regels voor: de verwerkingsverantwoordelijke moet dat steeds zelf beoordelen. Ga bij het nemen van de beslissing of een DPIA moet worden uitgevoerd uit het van het feit dat de AVG risico-gestuurde wetgeving is wat betekent dat de zorgorganisatie bij elke gegevensverwerking in beeld moet hebben welke risico's de verwerking voor de betrokkene en de zorgorganisatie kan hebben. Het is en blijft de verantwoordelijkheid van de verwerkingsverantwoordelijke (en verwerker) om op grond van de beginselen en uitgangspunten van de AVG (het juridisch kader) met inachtneming van de aanwezige risico's, te beoordelen welke beslissing moet worden gemaakt.

Om verwerkingsverantwoordelijken daarbij een handje te helpen, heeft de Artikel 29 Werkgroep[11] in 2017 een richtlijn opgesteld. Voor de gehandicaptenzorg geldt dat als de verwerking van persoonsgegevens aan **twee van de drie onderstaande criteria** voldoet, ervan uitgaan moet worden dat de zorgorganisatie een **DPIA** moet **uitvoeren**:

1. Er worden gevoelige gegevens of gegevens van zeer persoonlijke aard verwerkt (bijvoorbeeld medische dossiers);
2. Het gaat om gegevens van kwetsbare betrokkenen (zoals mensen met een (verstandelijke) beperking);
3. Er worden op grote schaal bijzondere persoonsgegevens verwerkt.

11 De voormalige artikel 29 Werkgroep was een adviesorgaan bestaande uit vertegenwoordigers van de Autoriteit Persoonsgegevens van alle EU-lidstaten. Op 25 mei 2018 is de European Data Protection Board (EDPB) opgericht als opvolger van de artikel 29 Werkgroep. De EDPB bestaat uit alle voorzitters van de privacytoezichthouders van de EU.

< Terug naar de inhoudsopgave

Wanneer er een verandering optreedt in de risico's van de verwerkingen, moet de verwerkingsverantwoordelijke of de verwerker zijn verwerkingen opnieuw toetsen op de nakoming van de uitkomsten van de DPIA. Bijvoorbeeld bij de invoering van een nieuw cliëntdossier. Zie daarnaast Guidelines DPIA.

8.3.3 Wie moet een DPIA uitvoeren?

De verwerkingsverantwoordelijk kan de DPIA zelf uitvoeren, maar kan dit ook laten doen door een eventuele verwerker of door een externe partij. Wat daarin de beste keus is, is afhankelijk van de mogelijkheden en het kennisniveau van de verwerkingsverantwoordelijke en de omvang en complexiteit van de verwerking.

De verwerkingsverantwoordelijke moet bij de DPIA het advies inwinnen van de FG en vervolgens het advies van de FG meenemen in het rapport en aangeven wat er mee is gedaan. De FG voert de DPIA niet zelf uit. De FG bekijkt tevens of de conclusies uit de DPIA correct zijn. Als de verwerkingsverantwoordelijke of de verwerker de adviezen van de FG niet overnemen, moeten zij dit toelichten in de DPIA.

8.4 Verplichting 4 Voorafgaande raadpleging (artikel 36 AVG)

Wanneer uit de gegevensbeschermingseffectbeoordeling blijkt dat een voorgenomen verwerking een hoog risico voor betrokkenen inhoudt en dat dit risico niet wordt weggenomen door het treffen van risicobeperkende maatregelen, dan moet de voorgenomen verwerking worden voorgelegd aan de Autoriteit Persoonsgegevens. De zorgorganisatie mag niet beginnen met een verwerkingsactiviteit zolang de Autoriteit Persoonsgegevens geen positief oordeel heeft uitgebracht.

8.4.1 Welke informatie moet de verwerkingsverantwoordelijke verstrekken aan de AP bij een voorafgaande raadpleging?

Een verzoek om een advies van de AP bij een verwerking met een hoog risico moet alle informatie bevatten waarmee de AP een beoordeling kan doen. Er zijn zes elementen die in ieder geval aan de AP moeten worden verstrekt:

1. wie de verwerkingsverantwoordelijke is en welke verwerker(s) betrokken is/zijn;
2. welke doelen de verwerking heeft en welke middelen daarvoor worden ingezet;
3. welke maatregelen en waarborgen de verwerkingsverantwoordelijke neemt om de privacyrechten van betrokkenen te beschermen;
4. de contactgegevens van de functionaris voor gegevensbescherming (indien aangesteld);

< Terug naar de inhoudsopgave

5. de uitkomst van de DPIA. Deze moet alle informatie bevatten over de verwerking en de risico's, plus de maatregelen die de verwerkingsverantwoordelijke zelf al had overwogen;
6. alle andere informatie waar de AP om vraagt.

8.4.2 Binnen welke termijn moet de AP reageren?

De AP moet binnen acht weken advies geven over de voorgenomen verwerking van persoonsgegevens van de zorgorganisatie. Het advies van de AP moet met name toelichten waarom de verwerking van persoonsgegevens een overtreding van de AVG zou betekenen en welke risico's daarbij centraal staan. Bij complexe zaken mag de AP de reactietermijn met maximaal zes weken verlengen.

8.5 Verplichting 5 Privacy by design, privacy by default (artikel 25 AVG)

Naast de algemene verplichting tot beveiliging van persoonsgegevens (artikel 24 AVG) kent de AVG een verplichting voor de verwerkingsverantwoordelijke om verwerkingen zo in te richten dat, zoveel mogelijk vanaf het begin, rekening wordt gehouden met privacy by design en privacy by default.

8.5.1 Wat is privacy by design?

De letterlijke vertaling van privacy by design is: gegevensbescherming door ontwerp. Privacy by design houdt in dat de verwerkingsverantwoordelijke al bij de ontwikkeling van nieuw beleid of het ontwerp van nieuwe (informatie)systemen waarmee persoonsgegevens worden verwerkt rekening houdt met privacy. De AVG verplicht de verwerkingsverantwoordelijke om al in het ontwerp waarborgen in te bouwen voor een optimale bescherming van de privacy van betrokkenen en technische en organisatorische privacy verhogende maatregelen te implementeren. De aandacht voor privacy blijft tijdens de gehele levensduur van het systeem bestaan. Het doel is de beveiliging van persoonsgegevens te optimaliseren. Dat kan al door na te denken over de noodzakelijkheid van het opslaan, welke gegevens zijn echt nodig en welke niet? Ook moet rekening worden gehouden met de hele levenscyclus van de data: opslag, wijziging en verwijdering.

Een belangrijk onderdeel van privacy by design is data-minimalisatie. In het ontwerp moet gewaarborgd worden dat er niet méér persoonsgegevens verwerkt worden dan strikt noodzakelijk voor het doel van de verwerking.

< Terug naar de inhoudsopgave

Aandachtspunt 1: wachtwoorden
Een belangrijk aandachtspunt is de veiligheid van wachtwoorden, bijvoorbeeld voor toegang tot het cliëntendossier. Let op dat moeilijk te onthouden en vaak wijzigende wachtwoorden in de praktijk kunnen leiden tot het opschrijven van wachtwoorden en ophangen bij de computer. Dit is uiteraard niet bevorderlijk voor het waarborgen van de privacy van persoonsgegevens van cliënten.

Aandachtspunt 2: kosten en kwaliteit ICT-systemen
Zoals altijd in de ICT is het beter een systeem vanaf het begin goed te ontwerpen dan het later te moeten wijzigen. Aanpassingen achteraf zijn duurder en leveren meestal systemen van mindere kwaliteit. Dat geldt ook voor systemen die worden gebruikt voor de verwerking van persoonsgegevens.

8.5.2 Wat is privacy by default?

De letterlijke vertaling van privacy by default is: gegevensbescherming door standaardinstellingen. Privacy by default kan gezien worden als onderdeel van privacy by design. Privacy by default vereist dat de standaardinstellingen zo zijn gekozen dat de privacy maximaal wordt geborgd. Er moet bijvoorbeeld voor gezorgd worden dat persoonsgegevens nooit standaard openbaar zichtbaar zijn. Het meest sprekende voorbeeld is waarschijnlijk een profiel op sociale media. Dit mag wel openbaar zijn, maar slechts als een gebruiker daar eerst zélf actief voor kiest. De sociale media-toepassing zal in de standaardinstellingen de gebruikersprofielen zoveel mogelijk moeten afschermen.

8.5.3 Op welke wijze kan een zorgorganisatie invulling geven aan privacy by design en privacy by default?

Welke maatregelen een zorgorganisatie kan nemen om invulling te geven aan het uitgangspunt van privacy by design en privacy by default (onderdeel van artikel 32 AVG) is afhankelijk van de concrete situatie, maar rekening moet worden met de volgende elementen:

- de stand van de techniek;
- de uitvoeringskosten;
- de aard, omvang, context en het doel van de verwerking;
- de risico's voor de betrokkenen.

Zie meer over beveiligingsmaatregelen vanaf Verplichting 6.

< Terug naar de inhoudsopgave

8.6 Verplichting 6 Beveiligingsmaatregelen (technisch en organisatorisch)

De AVG kent diverse verplichtingen voor de verwerkingsverantwoordelijke. Hoe daaraan voldaan moet worden, laat de AVG in het midden. Wel geeft dat AVG aan dat de verwerkingsverantwoordelijk verplicht is **passende technische en organisatorische maatregelen** te nemen om te waarborgen en te kunnen aantonen dat elke verwerking van persoonsgegevens overeenkomstig de AVG wordt uitgevoerd.

In artikel 24 lid 1 AVG wordt het niveau van de maatregelen met een open norm beschreven: de verwerkingsverantwoordelijke moet bij het nemen van de maatregelen rekening houden met de aard, de omvang, de context en het doel van de verwerking, evenals met de waarschijnlijkheid en ernst van de uiteenlopende risico's die de verwerking van persoonsgegevens voor de rechten en vrijheden van de betrokkene kunnen hebben.

De risico's van de verwerking van persoonsgegevens kunnen voor de betrokkenen sterk uiteenlopen. Objectief moet worden vastgesteld of er kan sprake zijn van een laag, gemiddeld of hoog risico. Bij een hoog risico is een voorafgaande DPIA nodig (artikel 35 AVG).

Voor het bepalen van passende maatregelen kan voor elk risico een maatregelen worden geformuleerd door gebruik te maken van gangbare normen zoals de NEN7510-2 of de ISO 27002. (Zie meer hierover in module 1)

8.6.1 Waar dient een zorgorganisatie rekening mee te houden bij het nemen van beveiligingsmaatregelen? (artikel 32 AVG)

Welke technische en organisatorische maatregelen de verwerkingsverantwoordelijke moet nemen om invulling te geven aan de verantwoordingsplicht op grond van de AVG is afhankelijk van de concrete situatie. Zorgorganisaties kunnen bij de besluitvorming rekening houden met de volgende elementen:

- de stand van de techniek;
- de uitvoeringskosten;
- de aard, omvang, context en het doel van de verwerking;
- de risico's voor de betrokkenen.

Deze elementen bepalen in hoeverre de maatregelen haalbaar zijn. Technische mogelijkheden zijn steeds in ontwikkeling, dit brengt met zich mee dat de gekozen technische maatregelen periodiek moeten worden herzien.

< Terug naar de inhoudsopgave

8.6.2 Wat zijn voorbeelden van technische maatregelen?

Technische maatregelen zijn maatregelen die zonder menselijk ingrijpen een beveiligings- of toegangsaspect afdwingen. Enkele voorbeelden van technische beveiligingsmaatregelen zijn:

- *Pseudonimisering en versleuteling van de persoonsgegevens*
  Pseudonimiseren is het verhullen van iemands identiteit voor derden. Een voorbeeld is het vervangen van de naam van een persoon door een cliëntnummer. De medische gegevens van deze persoon worden dan gekoppeld aan dit nummer. Omdat een koppeling kan worden gemaakt tussen de naam (het persoonsgegeven) en het nummer (pseudoniem) is en blijft de AVG van toepassing. Een pseudoniem is een persoonsgegeven, de AVG is daarop van toepassing.

- *Versleutelen (encryptie)* is het langs wiskundige weg omzetten van gegevens tot een onbruikbare reeks tekens zodanig dat zonder de sleutel de gegevens niet toegankelijk zijn. Versleutelde bestanden kunnen alleen worden geopend door degene die de unieke sleutel en/of het wachtwoord in zijn bezit heeft. Versleuteld opslaan moet voorkomen dat anderen ongewenst toegang hebben tot bestanden en is een methode om gegevens vertrouwelijk te versturen.
  Het versleutelen van bestanden kan heel handig zijn als zorgorganisaties vertrouwelijke informatie (bijvoorbeeld gegevens over de gezondheid van een cliënt) willen delen via een bijlage bij de e-mail of via bijvoorbeeld de cloud.

- *Een kwalitatieve goede inrichting van diensten en systemen*
  Deze IT-infrastructuur en IT-architectuur moet gericht zijn op een goede beschikbaarheid en veerkracht (omgang met storingen) en ontwikkeld zijn om persoonsgegevens vertrouwelijk en met integriteit (weerstand tegen ongewenste aanpassingen of wissingen) te kunnen behandelen. Zie ook privacy by design.

- *Voorkomen van verlies van gegevens bij een storing*
  De technische mogelijkheid om bij een incident te zorgen dat persoonsgegevens niet permanent verloren gaan is ook een belangrijke beveiligingsmaatregel. Als door een storing bijvoorbeeld medicatiegegevens van een cliënt niet meer beschikbaar zijn, kan dit ernstig nadelig zijn voor de betrokkene.

- *Controleprocedure*
  Op gezette tijdstippen testen, beoordelen en evalueren van de doeltreffendheid van de technische en organisatorische maatregelen ter beveiliging van de verwerking.

< Terug naar de inhoudsopgave

- Andere meer gedetailleerde voorbeelden van technische maatregelen zijn:
  - Persoonsgegevens alleen toegankelijk laten zijn via inlogfaciliteit;
  - Mfa (multifactor-authenticatie);
  - Firewalls;
  - Software tegen malware-aanvallen;
  - Up-to-date virusscanners;
  - Het periodiek maken van back-ups;
  - Software waarmee wordt geattendeerd op het dreigende verstrijken van een bewaartermijn;
  - Geen onbeveiligde externe harde schijven;
  - Toegang vanaf andere locatie alleen via VPN naar kantoornetwerk;
  - Medewerkers die uit dienst gaan, direct accounts en pasjes blokkeren.

8.6.3 Wat zijn organisatorische maatregelen?

Organisatorische maatregelen gaan over maatregelen met menselijk toezicht. Denk aan:

- Het goed regelen van de toegangsrechten tot de verschillende systemen of applicaties (autorisatiebeleid). Medewerkers mogen alleen toegang hebben tot de gegevens die zij in het kader van hun werkzaamheden nodig hebben. Dit is één van de belangrijkste organisatorische maatregelen.
- Geheimhouding door medewerkers die toegang hebben tot persoonsgegevens. Zie meer informatie hierover in module 2.
- Mochten zich beveiligingsproblemen voordoen dan moet de zorgorganisatie procedures en checklists hebben waarin beschreven is hoe gehandeld moet worden (continuïteitsbeleid).

Andere organisatorische maatregelen zijn:

- Een wachtwoordbeleid;
- Beveiliging van omgeving (toegankelijkheid, kasten op slot, clean desk policy);
- Locken van pc en laptops als medewerker van zijn plek is;
- Zorgvuldig gebruik van USB-sticks, externe harde schijven en andere gegevensdragers;
- Gedragscodes in de zorgorganisaties, zoals aanvaardbaar gebruik van ICT middelen;
- Screening van medewerkers als deze bepaalde risicovolle werkzaamheden gaat verrichten (integriteitsonderzoeken);
- Beleggen van verantwoordelijkheden voor processen en systemen in de zorgorganisatie bij medewerkers.

< Terug naar de inhoudsopgave

Belangrijk is om ook daadwerkelijk toezicht te houden op de naleving van de procedures en de regels over privacy. Die taak kan bijvoorbeeld bij een functionaris gegevensbescherming worden gelegd.

8.6.4 Gegevensbeschermingsbeleid

Het gegevensbeschermingsbeleid documenteert hoe een zorgorganisatie omgaat met gegevensbescherming, zowel technisch al organisatorisch. In dit beleid bepaalt de zorgorganisatie bijvoorbeeld welke technische en organisatorische maatregelen genomen moeten worden, hoe deze maatregelen vorm krijgen in de praktijk (processen, procedures et cetera) en belegt de zorgorganisatie de rollen en verantwoordelijkheden voor de uitvoer ervan. Gezien de aard van de gegevens (bijzondere persoonsgegeven) en de omvang van de verwerkingsactiviteiten is een dergelijk gegevensbeschermingsbeleid voor een zorgorganisatie vereist.

Dit beleid wordt geschreven voor de medewerkers van de zorgorganisatie. Het beleid kan gecombineerd worden met het verplichte beleid ten aanzien van gegevensbescherming door ontwerp (privacy by design) en gegevensbescherming door standaardinstellingen (privacy by default), beiden ingevolge artikel 25 AVG.

Zie ook vraag 5 van deze module.

8.7 Verplichting 7 Meldplicht datalek (artikelen 33 en 34 AVG)

Een datalek (inbreuk in verband met persoonsgegevens) is een daadwerkelijke inbreuk op de beveiliging waarbij persoonsgegevens per ongeluk of op onrechtmatige wijze in handen van onbevoegden zijn gekomen, voor onbevoegden toegankelijk waren, of zijn vernietigd, gewijzigd of verloren.

Voorbeelden van een datalek in de gehandicaptenzorg zijn: een hack van systemen, zoals het ECD waarbij persoonsgegevens worden buitgemaakt, of het verlies van een USB-stick of laptop met niet-versleutelde persoonsgegevens van cliënten. Ook een verkeerd verzonden e-mail met (bijzondere) persoonsgegevens naar een onbevoegd persoon is een datalek.

< Terug naar de inhoudsopgave

8.7.1 Moet een zorgorganisatie een datalek melden bij de AP?

Ja, de AVG kent de verplichting voor de verwerkingsverantwoordelijke een inbreuk in verband met persoonsgegevens (een datalek) te melden aan de Autoriteit Persoonsgegevens, behalve als het niet waarschijnlijk is dat de inbreuk een risico inhoudt voor de rechten en vrijheden van betrokkenen. Dan hoeft er niet te worden gemeld.

Of er een dergelijk risico is moet onder andere worden beoordeeld op basis van:

- de aard van de inbreuk (wat is er concreet gebeurd);
- de gevoeligheid en omvang van de persoonsgegevens;
- hoeveel betrokkenen het betreft;
- de mogelijke gevolgen van de inbreuk en hoe waarschijnlijk het is dat deze zullen optreden.

Voorgaande beoordeling vloeit (wederom) voort uit het vertrekpunt dat de AVG-risico gestuurd is. Het is de verantwoordelijkheid van verwerkingsverantwoordelijken (en verwerkers) telkens in beeld te krijgen welke risico's aan een gegevensverwerking kunnen kleven en op grond daarvan beslissingen te nemen.

Indien er wel moet worden gemeld dan moet de verwerkingsverantwoordelijke dit zonder onredelijke vertraging en, indien mogelijk, binnen 72 uur doen nadat de verwerkingsverantwoordelijke er kennis van heeft genomen (artikel 33 lid 1 AVG). De melding moet worden gedaan via het formulier op de website van de Autoriteit Persoonsgegevens te vinden op het meldloket.

Meer informatie staat in hoofdstuk II van de Guidelines meldplicht datalekken.

8.7.2 Welke informatie moet de zorgorganisatie verstrekken bij melding aan de AP?

Bij het doen van de melding voorziet de zorgorganisatie de Autoriteit Persoonsgegevens in ieder geval van de volgende informatie:

- de aard en omvang van de inbreuk;
  Voorbeelden van een "aard van de inbreuk" zijn: persoonsgegevens bij het oud papier gezet, persoonsgegevens per ongeluk gepubliceerd, persoonsgegevens verstuurd naar verkeerde ontvanger, gegevensdrager (laptop) met persoonsgegevens gestolen.
- waar mogelijk de categorieën van betrokkenen (cliënten of wettelijke vertegenwoordigers), de persoonsgegevensregisters

< Terug naar de inhoudsopgave

en, bij benadering, het aantal betrokkenen en persoonsgegevensregisters [12](naam-, adres-, telefoonnummerregisters);
- de naam en de contactgegevens van de functionaris voor gegevensbescherming of een ander contactpersoon waar meer informatie kan worden verkregen;
- de waarschijnlijke gevolgen van de inbreuk in verband met persoonsgegevens;
  Zoals bijvoorbeeld identiteitsfraude, verlies van vertrouwelijkheid van door het beroepsgeheim beschermde persoonsgegevens, dat betrokkenen hun rechten niet uitoefenen.
- de maatregelen die de zorgorganisatie heeft voorgesteld of genomen om de inbreuk in verband met persoonsgegevens aan te pakken, waaronder de maatregelen ter beperking van de eventuele nadelige gevolgen daarvan.

Aandachtspunt
Ingevolge artikel 33 lid 5 AVG moet de verwerkingsverantwoordelijke ieder datalek, ongeacht of het gemeld moet worden, documenteren (registreren) inclusief de gevolgen en de genomen maatregelen om dit in de toekomst te voorkomen.

8.7.3 Moet de betrokkene worden geïnformeerd over het datalek?

Ja, de AVG kent de verplichting voor de verwerkingsverantwoordelijke om een inbreuk in verband met persoonsgegevens onverwijld te melden aan de betrokkene, wanneer deze inbreuk waarschijnlijk **een hoog risico** inhoudt voor de rechten en vrijheden van de betrokkene (artikel 34 lid 1 AVG).

Om dit te bepalen dient een risicobeoordeling plaats te vinden: wat is er gebeurd?; welke gegevens betrof het; aantal betrokkenen; wat kunnen de risico's zijn; is het waarschijnlijk dat deze risico's zich zullen voordoen?

Van een hoog risico is sprake wanneer de te verwachten gevolgen van het datalek zich met grote waarschijnlijkheid voordoen. Negatieve gevolgen voor de rechten en vrijheden van betrokkenen kunnen bijvoorbeeld zijn: verlies van controle over hun persoonsgegevens (zoals wissing of rectificatie), identiteitsfraude of het ongedaanmaking van pseudonimisering.
Meer informatie staat in hoofdstuk III en IV van de Guidelines meldplicht datalekken.

12 Het persoonsregisters moet worden onderscheiden van het verwerkingsregister. In dit laatste is opgenomen welke verwerkingsactiviteiten een zorgorganisatie verricht, daarin staan geen persoonsgegevens.

< Terug naar de inhoudsopgave

8.7.4 Welke informatie moet de zorgorganisatie verstrekken aan de betrokkenen?

De betrokkene moet over het datalek van de verwerkingsverantwoordelijke dezelfde informatie krijgen als de Autoriteit Persoonsgegevens.

De aard van de inbreuk moet in duidelijke en eenvoudige taal worden omschreven en de mededeling moet tevens aanbevelingen bevatten waarmee de betrokkene zelf aan de slag kan en zoveel mogelijk de mogelijke negatieve gevolgen van de datalek kan beperken.

8.8 Verplichting 8 Verwerkersovereenkomst (artikel 28 lid 3 AVG)

Als de zorgorganisatie (verwerkingsverantwoordelijke) een verwerker inschakelt die persoonsgegevens verwerkt namens de verwerkingsverantwoordelijke, bijvoorbeeld een leverancier van een cliëntendossier, dan is de verwerkingsverantwoordelijke verplicht een verwerkersovereenkomst af te sluiten. De AVG eist dat de verwerkersovereenkomst schriftelijk of elektronisch wordt aangegaan (artikel 28 lid 9 AVG). De VGN heeft samen met ActiZ, NVZ, GGZ Nederland en de NFU (samen verenigd in Brancheorganisaties Zorg, BoZ) een model verwerkersovereenkomst opgesteld.

De verwerkersovereenkomst geeft de keten in het proces van verwerking tussen de verwerkingsverantwoordelijke, verwerkers en eventuele subverwerkers weer en geeft inzicht in de verdeling van verantwoordelijkheden en aansprakelijkheden. De verwerkersovereenkomst staat nooit op zichzelf en maakt onderdeel uit van de overeenkomst van opdracht of dienstverleningsovereenkomst tussen partijen. Het is van belang om goede afspraken te maken over onderlinge aansprakelijkheid. Een aandachtspunt hierbij is de verwerkers in de praktijk proberen hun aansprakelijkheid uit te sluiten of te beperken.

Klik hier voor het stroomschema verwerkingsverantwoordelijke of verwerker. Zie ook vraag 8.8.2.

8.8.1 Wat moet er in de verwerkersovereenkomst staan?

In artikel 28 AVG staan de bepalingen die minimaal in de verwerkersovereenkomst moeten staan:

a. Omschrijving van de verwerking door de verwerker
   In de overeenkomst moet worden aangegeven:
   - een omschrijving van de verwerking;
   - hoe lang de verwerking duurt;
   - wat de aard is en het doel van de verwerking;

< Terug naar de inhoudsopgave

- het soort persoonsgegevens en de categorieën betrokken personen wiens persoonsgegevens worden verwerkt.

b. Toestemming voor uitbesteden aan subverwerkers
   - Als de verwerker handelingen met de persoonsgegevens uitbesteedt aan andere verwerkers (subverwerkers), dit zijn meestal onderaannemers of leveranciers van de verwerker, dan moet de zorgorganisatie daarvoor voorafgaande specifieke of algemene toestemming geven aan de verwerker.
   - Als er algemene toestemming wordt gegeven moet de verwerker wijzigingen van subverwerkers melden aan de zorgorganisatie en de zorgorganisatie de mogelijkheid geven bezwaar te maken.

c. Dezelfde verplichtingen opleggen aan subverwerkers
   - De verwerker moet ingehuurde subverwerkers dezelfde minimale verplichtingen opleggen als de in deze lijst opgesomde verplichtingen die de zorgorganisatie aan de verwerker moet opleggen.

d. Alleen handelen in opdracht van de zorgorganisatie
   - De verwerker mag alleen maar handelingen met de persoonsgegevens verrichten in opdracht van de zorgorganisatie. Dat wil zeggen: de verwerker mag alleen die handelingen verrichten die noodzakelijk zijn voor het uitvoeren van de diensten die de verwerker voor de zorgorganisatie verricht. De verwerker mag dus niet zelfstandig bepalen wat er met de persoonsgegevens gebeurt.

e. Beveiligen persoonsgegevens
   - Het beveiligen van de persoonsgegevens is één van de belangrijkste taken van de verwerker. In de verwerkersovereenkomst moet staan dat de verwerker passende technische en organisatorische maatregelen neemt om de persoonsgegevens te beveiligen. De AP stelt daarbij als eis dat de beveiligingsmaatregelen ook worden omschreven in de verwerkersovereenkomst.
     Denk daarbij ook aan bepalingen over datalekken.

f. Zorgen voor geheimhouding door medewerkers
   De verwerker moet ervoor zorgen dat de personen die de persoonsgegevens onder toezicht van de verwerker verwerken, verplicht zijn tot geheimhouding van die persoonsgegevens, ofwel door middel van afspraken met de verantwoordelijke ofwel op basis van een beroepsmatige geheimhoudingsplicht. Zie module 2.

g. De zorgorganisatie assisteren
   In de overeenkomst moet staan dat de verwerker de zorgorganisatie door middel van passende technische en organisatorische maatregelen, voor zover mogelijk, assisteert bij het beantwoorden van verzoeken van de personen om wiens gegevens het gaat, bij het beveiligen van de persoonsgegevens, het melden van datalekken, het uitvoeren van DPIA´s en (wanneer dat nodig is) voorafgaande raadpleging van de AP.

h. Locatie van de data
   De zorgorganisatie moet weten in welke landen zijn data worden opgeslagen. Dit is mede van belang met het oog op de

< Terug naar de inhoudsopgave

verplichtingen die gelden bij doorgifte van persoonsgegevens naar het buitenland.

i. Audits
De verwerkingsverantwoordelijke moet kunnen controleren of de verwerker zich houdt aan de gemaakte afspraken. Dit gebeurt vaak in de vorm van een audit (onderzoek) door de verantwoordelijke of door een onafhankelijke derde. In de verwerkersovereenkomst kunnen partijen hier nadere afspraken over maken.

j. Aansprakelijkheid
De verwerkingsverantwoordelijke kan worden aangesproken als iemand schade lijdt doordat de AVG niet wordt nageleefd. Dit geldt zelfs als de schade het gevolg is van nalatigheid van de verwerker, die in dat geval ook zelfstandig aansprakelijk is. Het is verstandig in de verwerkersovereenkomst heldere afspraken te maken over deze verdeling.

k. Persoonsgegevens weer overdragen of vernietigen.
Na het einde van de dienstverlening door de verwerker moet deze de persoonsgegevens wissen of de persoonsgegevens aan de zorgorganisatie teruggeven en bestaande kopieën verwijderen (zie ook vraag 33 module 1).

8.8.2 AVG-rolverdeling in de gehandicaptenzorg: verwerkingsverantwoordelijke of verwerker?

Bij het inschakelen van verwerkers door de verwerkingsverantwoordelijke is het belangrijkste uitgangspunt dat deze verwerkers voldoende garanties met betrekking tot het toepassen van passende technische en organisatorische maatregelen bieden zodat de verwerking aan de vereisten voldoet en de bescherming van de rechten van de betrokkene is gewaarborgd.

Van belang is om in de verwerkersovereenkomst zoveel mogelijk concrete afspraken vast te leggen zodat ook de verwerkingsverantwoordelijke beter in staat wordt gesteld zelf te bepalen of de beveiliging in zijn situatie voldoende is, of dat er aanvullende maatregelen (bij hem intern, of bij de verwerker) nodig zijn.

De verwerkingsverantwoordelijke is de zorgorganisatie die de opdracht heeft tot het verlenen van zorg, jeugdhulp of ondersteuning aan cliënten. Dit is de primaire opdracht van de zorgorganisatie én niet het verwerken van persoonsgegevens. Dit neemt niet weg dat het verwerken van persoonsgegevens een onderdeel is van de primaire opdracht. De zorgorganisatie bepaalt als verwerkingsverantwoordelijke welke gegevens worden verwerkt en het ‘hoe en waarom’ van de gegevensverwerking.

< Terug naar de inhoudsopgave

Een verwerker is degene die als primaire opdracht persoonsgegevens verwerkt, uitsluitend ten behoeve van en in opdracht van de verwerkingsverantwoordelijke. Denk bijvoorbeeld aan het bedrijf die het ECD van de zorgorganisatie faciliteert. De verwerker mag de persoonsgegevens niet voor eigen doeleinden gebruiken.

In de verwerkersovereenkomst worden afspraken vastgelegd over:

- het onderwerp en de duur van de verwerking;
- de aard en het doel van de verwerking;
- het soort persoonsgegevens en de categorieën van betrokkenen;
- de rechten en verplichtingen van de verwerkingsverantwoordelijke en de verwerker.

Klik hier voor het stroomschema verwerkingsverantwoordelijke of verwerker.

8.8.3 Is een onderaannemer een verwerkingsverantwoordelijke of een verwerker?

Een onderaannemer (zorgorganisatie) die door een andere zorgorganisatie wordt ingeschakeld is een verwerkingsverantwoordelijke. De onderaannemer wordt namelijk ingeschakeld om zorg- en/of dienstverlening te verrichten: dit is de primaire opdracht. Het feit dat door deze opdracht ook persoonsgegevens worden verwerkt, brengt niet met zich mee dat de onderaannemer daardoor een verwerker wordt. Dat zou anders zijn als de primaire opdracht aan de onderaannemer is het verwerken van persoonsgegevens.

Als een zorgorganisatie samen met een andere zorgorganisatie gezamenlijk het doel en middelen van de verwerking van persoonsgegevens bepaald, is sprake van een gezamenlijke verwerkingsverantwoordelijkheid (artikel 26 lid 1 AVG). Denk bijvoorbeeld aan het inrichten van een cliëntportaal door twee zorgorganisaties om daarin te rapporteren over cliënten waaraan zij beiden zorg verlenen (hoofdaannemer en onderaannemer).

De relatie tussen gezamenlijke verwerkingsverantwoordelijken is wezenlijk anders dan die van de verwerkingsverantwoordelijke en de verwerker (artikel 28 AVG). De verwerker is immers **niet** betrokken bij het vaststellen van de doelen en de middelen.

Zie vraag 21 in module 2 voor het antwoord op de vraag of een onderaannemer cliëntgegevens mag ontvangen.

< Terug naar de inhoudsopgave

Onderling afspraken maken

De gezamenlijke verwerkingsverantwoordelijken moeten dan vervolgens op grond van artikel 26 lid 1 AVG in onderling overleg vaststellen wie welke verantwoordelijkheden op zich neemt ten aanzien van de verplichtingen uit de AVG. Het gaat dan met name om het faciliteren van de rechten van betrokkenen en het voldoen aan de informatieplichten aan betrokkenen. De AVG stelt geen formele eisen aan hoe de verantwoordelijkheden worden vastgelegd in een onderlinge regeling. Vanuit de verantwoordingsplicht (artikel 5 lid 2 AVG) is het desondanks aan te raden de verantwoordelijkheidsverdeling (al dan niet elektronisch) schriftelijk vast te leggen.

Dit hoeft *niet* in een aparte overeenkomst. De afspraken kunnen ook worden opgenomen in een schriftelijke regeling of een bijlage zijn van een samenwerkingsovereenkomst of onderaannemingsovereenkomst. De VGN heeft een modelonderaannemingsovereenkomst ontwikkeld waar zorgaanbieders gebruik van kunnen maken.

9 Verplichtingen verwerker

Op de verwerker rust de verplichting om de verwerkingsverantwoordelijke te helpen bij het uitvoeren van sommige van zijn of haar verplichtingen en anderzijds moet de verwerker ook zelfstandig voldoen aan de volgende verplichtingen op grond van de AVG:

- De verwerker dient deskundig en betrouwbaar te zijn. Om aan deze eis te voldoen kan de verwerker zich aansluiten bij goedgekeurde gedragscodes of certificeringsmechanismes (bijvoorbeeld ISO certificering 27001);
- De verwerker dient aantoonbaar in overeenstemming te werken met de van toepassing zijnde NEN normen voor de zorg (zoals NEN 7510, 7512, en 7513). In aanvulling op deze normen heeft het NEN in samenspraak met het zorgveld de veldnorm NTA 7516 ontwikkeld, die zich specifiek richt op het beveiligd versturen van mail en beveiligd chatten;
- Afspraken met de verwerkingsverantwoordelijke over de wijze waarop de verwerker persoonsgegevens verwerkt moeten vastgelegd worden in een verwerkersovereenkomst;
- De verwerker kan zelf andere subverwerkers inschakelen voor het verwerken van persoonsgegevens die de verwerkingsverantwoordelijke heeft opgedragen aan de verwerker. Aan het inschakelen van subverwerkers zijn verschillende eisen verbonden;
- Net zoals de verwerkingsverantwoordelijke heeft de verwerker een registerplicht;
- Onder bepaalde omstandigheden moet een functionaris voor gegevensbescherming aangesteld worden;
- De verwerker draagt zorg voor passende beveiligingsmaatregelen voor de gegevensverwerking die de verwerker in opdracht van de verwerkingsverantwoordelijke uitvoert;
- De verwerker heeft ook een meldplicht bij een datalek.

< Terug naar de inhoudsopgave

10 Toezicht en handhaving door de Autoriteit Persoonsgegevens

Aan het niet nakomen van de AVG-verplichtingen door de zorgorganisatie zijn consequenties verbonden. Betrokkenen kunnen de zorgorganisatie aansprakelijk stellen en schadevergoeding eisen. De Autoriteit Persoonsgegevens is belast met het toezicht op de naleving en handhaving van privacywetgeving. Als blijkt dat een organisatie de regels uit de AVG niet naleeft, riskeert zij in het uiterste geval een boete van maximaal 20 miljoen euro of 4% van de wereldwijde omzet als dit meer is. Naast het opleggen van deze boetes is de Autoriteit Persoonsgegevens bevoegd om een last onder dwangsom op te leggen of bestuursdwang toe te passen.

Last onder dwangsom betekent dat wanneer een zorgorganisatie een overtreding in de zin van de AVG begaat zij deze overtreding binnen een bepaalde termijn moet herstellen (last). Als dat niet gebeurt dan moet de zorgorganisatie per een bepaald tijdsvlak (dag, week, maand) een boete (dwangsom) betalen. Daarnaast heeft de Autoriteit Persoonsgegevens de mogelijkheid om zelf een eind te maken aan de overtreding als de zorg organisatie dit niet doet binnen een bepaald tijdvak, dit heet een last onder bestuursdwang.

10.1 Wat kan een betrokkene doen bij overtreding van de AVG?

Een betrokkene heeft een aantal mogelijkheden in handen om op te treden tegen een schending van zijn rechten onder de AVG. Een betrokkene kan bijvoorbeeld getroffen worden als zijn persoonsgegevens op straat komen te liggen. Zeker wanneer het gaat om gevoelige informatie, zoals een medisch dossier, kan dit een grote inbreuk zijn op het privéleven van deze persoon met alle gevolgen van dien.

- Een betrokkene kan een klacht indienen bij de AP (artikel 77 lid 1 AVG).
- Een betrokkene kan een procedure starten tegen de AP (artikel 78 lid 1 AVG).
  Wanneer de klacht door de toezichthouder niet in behandeling wordt genomen, de betrokkene niet tijdig verneemt hoe de behandeling van de klacht verloopt of wanneer de betrokkene het niet eens is met het besluit van de AP, dan kan de betrokkene naar de bestuursrechter stappen. De AVG vereist namelijk dat besluiten van toezichthouders kunnen worden getoetst door een onafhankelijke rechter. In Nederland betekent dit dat de rechter marginaal zal toetsen of de AP in redelijkheid het besluit had kunnen nemen. Ook kan bij de rechtbank een verzoek tot handhaving ingediend worden als de klacht niet opgepakt wordt.
- De betrokkene kan daarnaast ook een gerechtelijke procedure (civiele rechter) starten tegen de verwerkingsverantwoordelijke en de verwerker wanneer zijn rechten zijn geschonden (artikel 79 lid 1 AVG). Dat ook de verwerker aangesproken kan worden is nieuw onder de AVG. Als de verwerkingsverantwoordelijke of de verwerker een beslissing genomen heeft

< Terug naar de inhoudsopgave

over de rechten van de betrokkene (bijvoorbeeld over het recht op inzage, het recht op gegevenswissing en het recht op dataportabiliteit) en hij het daarmee niet eens is, dan kan hij tegen dit besluit beroep instellen. De rechter zal dan een beslissing nemen. Er kan bijvoorbeeld een verwerkingsverbod opgelegd worden of geoordeeld worden dat de betrokkene wél zijn recht mag uitoefenen.

- De betrokkene kan ook een schadeclaim (civielrechtelijk) indienen bij de rechter (artikel 82 lid 1 AVG). Als de betrokkene schade heeft geleden als gevolg van overtreding van de AVG, dan kan via de rechter een schadevergoeding gevorderd worden van de verwerkingsverantwoordelijke en/of de verwerker. Als geen sprake is van vermogensschade, dan dient de betrokkene een 'billijke vergoeding' te ontvangen. Hoe hoog deze billijke vergoeding wordt, zal nog moeten blijken. Deze schadeclaim staat los van de administratieve geldboete die de AP kan opleggen.

10.2 Waarvoor kan een verwerkingsverantwoordelijke of verwerker aansprakelijk worden gesteld?

De verwerkingsverantwoordelijke kan aansprakelijk worden gesteld voor:

- alle schade die wordt veroorzaakt door een verwerking die inbreuk maakt op de AVG, ongeacht of die door hemzelf of door een verwerker is veroorzaakt (artikel 82 lid 2 AVG).

De verwerker kan aansprakelijk worden gesteld voor:

- alle schade veroorzaakt door een specifiek tot hem gerichte AVG-verplichting, zoals het inschakelen van een sub-verwerker zonder toestemming van de verwerkingsverantwoordelijke (artikel 28 lid 2 AVG);
- het niet op orde hebben van zijn beveiliging (artikel 32 AVG).
- schade veroorzaakt door zijn handelen buiten de instructies van de verwerkingsverantwoordelijke (artikel 82 lid 2 AVG).
- overige contractuele afspraken die partijen in de verwerkersovereenkomst hebben gemaakt.

Een verwerkingsverantwoordelijke of verwerker kan slechts van zijn aansprakelijkheid worden vrijgesteld, als hij bewijst op geen enkele wijze verantwoordelijk te zijn voor het schadeveroorzakende feit. Dit heet ook wel omgekeerde bewijslast (artikel 82 lid 3 AVG).

< Terug naar de inhoudsopgave

10.3 Aansprakelijkheidsbepaling in verwerkersovereenkomst

Eén van de doelen van de AVG is om betrokkenen beter te beschermen. Deze kan op grond van de AVG schadevergoeding eisen van iedere partij (verwerkingsverantwoordelijke of verwerker) die inbreuk heeft gemaakt op de AVG als hij daardoor heeft geleden. De betrokkene kan voor het vorderen van schadevergoeding een gerechtelijke procedure starten tegen zowel de verwerkingsverantwoordelijke als de verwerker. Beide partijen zijn hoofdelijk aansprakelijk voor de geleden schade.

Onderling kunnen de verwerkingsverantwoordelijke en de verwerker deze schadevergoeding op elkaar verhalen. In een verwerkersovereenkomst kan hiertoe een aansprakelijkheidsbeperking worden opgenomen die geldt in geval van schending van privacywetgeving of de verwerkersovereenkomst, ten aanzien van schadevergoeding naar de andere partij toe.

Aansprakelijkheid van de verwerkingsverantwoordelijke of de verwerker naar betrokkenen toe kan niet op deze manier worden beperkt.

Aandachtspunt:
Het is niet mogelijk om álle aansprakelijkheid contractueel in een verwerkersovereenkomst uit te sluiten. In het geval van opzet of bewuste roekeloosheid, is er altijd aansprakelijkheid voor de daardoor ontstane schade.

11 Privacy awareness (bewustzijn) binnen de zorgorganisatie, hoe doe je dat?

Privacy awareness houdt in dat je als zorgorganisatie ervoor moet zorgen dat privacy in hoofd, hart en handen van de medewerkers komt. Met het oog op de verantwoordingsplicht moet een zorgorganisatie ook kunnen aantonen dat er voldoende is gedaan om dit te bewerkstelligen.

Als je als zorgorganisatie echt wilt voldoen aan de AVG, vereist dit dat alle medewerkers, bekend zijn met de basisprincipes van de AVG en zorgspecifieke wetgeving en hiernaar gaan handelen. Eigenlijk moet het de normale manier van werken worden en onderdeel van de organisatiecultuur. Het is daarbij van belang om naast de medewerkers van staf- en ondersteunende diensten, met name gerichte aandacht te besteden aan de medewerkers die werkzaam zijn in het primair proces. Het plaatsen van informatie op bijvoorbeeld het Intranet van de zorgorganisatie, met de aanname dat de medewerkers deze informatie zullen lezen en toepassen, is niet voldoende.

Om ervoor te zorgen dat medewerkers intrinsiek gemotiveerd raken om privacy centraal te zetten in hun dagelijkse praktijk, heeft de zorgorganisatie een effectieve boodschap nodig. Deze boodschap moet ertoe bijdragen dat medewerkers goed

< Terug naar de inhoudsopgave

kunnen begrijpen wat de waarde van privacy is en hoe een inbreuk op privacy betrokkenen kan schaden. Een grote uitdaging bij het communiceren over het belang van privacy is het voorkomen van het gebruik van ingewikkelde juridische taal, die ver van de medewerkers afstaat. De boodschap moet aansluiten bij de doelgroep; voor medewerkers in het primair proces betekent dit zoveel mogen moeilijke begrippen vermijden en gebruik maken van aansprekende voorbeelden uit de dagelijkse praktijk. Een uitdaging is om de medewerkers niet te bedelven onder te veel regels. Als de systemen van de zorgorganisatie, bijvoorbeeld het ECD, AVG-proof zijn, hoeven medewerkers niet alle regels te kennen, maar kunnen zij wel veilig werken.

Hieronder staan een aantal suggesties om de privacy awareness van de medewerkers te vergroten.

Deel kennis
Om medewerkers privacy bewust te maken, is een eerste vereiste dat ze de juiste kennis hebben. Medewerkers moeten weten waar privacy over gaat en wat ze moeten doen. Kennis van het privacybeleid van de zorgorganisatie moet dus niet alleen bekend zijn bij het management, stafdiensten of de functionaris voor gegevensbescherming.

- Wat is de AVG/ zorgspecifieke wetgeving en wat houden de basisprincipes in?
- Attendeer de medewerkers bij voorbeeld op de werkplaats van Vilans 'Juridische kennis: zo zit het!', waar toegankelijke informatie te vinden is over geheimhouding en privacy van gegevens. www.kennispleingehandicaptensector.nl/juridische-kennis
- Wat zijn de risico's als je je niet aan de privacywetgeving houdt?
- Wat moet je als medewerker doen bij een datalek?
- Stel een eenvoudige gedragscode op met de do's en dont's op het gebied van privacy.
- Maak duidelijk bij wie in de zorgorganisatie medewerkers terecht kunnen met hun vragen.

Organiseer trainingen voor de medewerkers
Om medewerkers privacy bewust te maken en te houden, is het organiseren van (jaarlijkse) trainingen een goede manier. Daarbij kan ook worden gedacht aan e-learning.
Gebruik in de trainingen zoveel mogelijk praktijksituaties om het onderwerp toegankelijk en levendig te maken

Stimuleer medewerkers om met elkaar in gesprek te gaan over privacy
Als de zorgorganisatie wil dat privacy bewust werken onderdeel van de organisatiecultuur wordt, is het essentieel om erover te blijven praten. Op die manier wordt het een vast onderdeel van de manier van werken. Bespreek bijvoorbeeld een

< Terug naar de inhoudsopgave

praktijkcasus aan de hand van vragen of stellingen en ondersteun medewerkers op deze manier met nadenken over de privacyregels en het toepassen hiervan.

Bespreek en deel met collega organisaties in de gehandicaptenzorg hoe zij het thema privacy op de kaart zetten. Zoek collega organisaties op en maak gebruik van elkaars goede voorbeelden op dit gebied.

12 Hoe kan een zorgorganisatie omgaan met het opnemen van namen van medewerkers in een cliëntendossier?

De cliënt heeft het recht om te weten wie zijn zorgprofessional is. Het is in de praktijk gangbaar dat de namen van betrokken zorgprofessionals in het cliëntdossier worden opgenomen. Bijvoorbeeld in een verslag of in een cliëntrapportage. Indien er sprake is van een incident in het kader van de Wkkgz, dan is de zorgaanbieder verplicht om de namen van betrokkenen bij dit incident (waaronder namen van medewerkers) op te nemen in het dossier.[13]

Tegelijkertijd is een zorgorganisatie verplicht om zich als een goed werkgever richting haar medewerkers te gedragen.[14] Dat betekent onder meer dat zorgprofessionals recht hebben op een veilige werkplek, waaronder veilige werkprocessen. De zorgorganisatie als werkgever moet hieraan invulling geven door te onderzoeken welke risico's kleven aan (nieuwe) verplichtingen uit wet- en regelgeving en hoe vervolgens aan de verplichtingen vorm kan worden gegeven, waarbij gevaren en risico's voor de werknemer zoveel mogelijk worden voorkomen of beperkt.[15]

Er kan echter spanning ontstaan tussen het opnemen van namen van medewerkers in het cliëntdossier en de veiligheid van medewerkers. Uit wet- en regelgeving blijkt niet of de verplichting uit de Wkkgz of het überhaupt opnemen van namen in het cliëntdossier voorrang heeft ten aanzien van de veiligheid van medewerkers op grond van de Arbowet. Dat betekent dat zorgorganisaties hier zelf een afweging in zullen moeten maken. Op verzoek van de VGN zal dit punt in de evaluatie van de Wkkgz in 2021 mee worden meegenomen. Tot die tijd adviseren wij zorgorganisaties de namen wel op te nemen in het cliëntdossier, maar dit achterwege te laten wanneer dit arbeidsrechtelijke bezwaren met zich meebrengt die zo zwaar wegen dat het achterwege laten

13 Art. 10 lid 3 Wkkgz.
14 Art. 7: 611 BW jo. art. 3 lid 1 sub b Arbeidsomstandighedenwet.
15 Idem.

< Terug naar de inhoudsopgave

van het opnemen van de namen in het cliëntdossier verantwoord kan worden op grond van ‘de zorg van een goed werkgever’. Dit zal een afweging per individuele situatie zijn. We benadrukken dat de cliënt altijd (dus ook als de namen niet opgenomen zijn in het cliëntdossier) het recht heeft om de namen van medewerkers die bij zijn zorg zijn betrokken te weten, wanneer hij daarom vraagt.

Module 4

Wettelijk kader op hoofdlijnen

Module 4 - Wettelijk kader op hoofdlijnen

Inleiding en doel

Deze module beschrijft het wettelijk kader van de privacywetgeving in de gehandicaptenzorg met daarin de belangrijkste aspecten uit de Algemene Verordening Gegevensbescherming (AVG) en de Uitvoeringswet AVG (UAVG). Daarnaast wordt ingegaan op de verhouding tussen de AVG, UAVG en zorgspecifieke wetgeving zoals de Wet langdurige zorg (Wlz), de Jeugdwet (Jw), de Wet maatschappelijke ondersteuning 2015 (Wmo 2015) en de Wet op de geneeskundige behandelingsovereenkomst (Wgbo).

Concreet bezien bestaat deze module uit twee onderdelen. Deel A geeft een beschrijving van het wettelijk kader; deel B gaat in op de bouwstenen waarop de AVG is gestoeld. Met behulp van FAQ's en stroomschema's worden hulpmiddelen aangeboden om de materie praktisch eigen te kunnen maken.

Deel A Wettelijk kader

1 Geschiedenis privacywetgeving: in het kort

Privacywetgeving is niet nieuw. Tot de jaren tachtig van de vorige eeuw was de bescherming van het individu tegen inbreuken op zijn persoonlijke levenssfeer gefragmenteerd neergelegd in het recht. Zoals bijvoorbeeld het briefgeheim in artikel 13 Grondwet, de Archiefwet maar ook de eed van Hippocrates welke artsen afleggen. Met de komst van computers, waardoor het mogelijk werd op grote schaal persoonsgegevens te kunnen verwerken, ontstond de behoefte aan een rechtskader op dit onderwerp. Dat startte in 1981 met het Verdrag over Gegevensbescherming waarin deelnemende landen zich verplichten hun wetgeving in lijn te brengen met dit Verdrag. In Nederland is vervolgens in 1989 de Wet persoonsregistraties in werking getreden. Op Europees niveau verscheen in 1995 de Privacyrichtlijn. Het kenmerk van een Europese richtlijn is dat deze moet worden omgezet in nationale wetgeving. Lidstaten zijn verplicht om het resultaat van een richtlijn te behalen, maar de wijze waarop dat resultaat mag worden bereikt, bepalen de lidstaten zelf. Dit leidde in 2001 tot de Wet bescherming persoonsgegevens (Wbp).

1.1 Algemene Verordening Gegevensbescherming en UAVG

Sinds 25 mei 2018 is de AVG van kracht en vervangt daarmee de Wbp. Vanaf deze datum geldt in de Europese Unie overal dezelfde regels op het gebied van privacy. De AVG regelt de privacy voor natuurlijke personen en kent verplichtingen voor overheden en bedrijven hoe zij moeten omgaan met de persoonsgegevens van deze individuen. De AVG heeft rechtstreekse werking, er hoeft geen omzetting zoals bij een richtlijn naar nationale wetgeving plaats te vinden. Wel is het zo dat de AVG

< Terug naar de inhoudsopgave

op een aantal punten de nationale wetgever de ruimte heeft gelaten voor nationale keuzes bij de uitvoering van de AVG. De Nederlandse wetgever heeft derhalve de Uitvoeringswet AVG (UAVG) opgesteld (ook sinds 25 mei 2018 van kracht).

> Door de Nederlandse wetgever is ervoor gekozen om daar waar ruimte is op grond van de AVG het regime van de Wbp te handhaven. Dit noemt men een beleidsneutrale invulling. Gekeken is of en in hoeverre het bestaande nationale recht, de Wbp en bestaande nationale beleidskeuzes kunnen worden gehandhaafd onder de AVG.

De UAVG moet in samenhang met de AVG worden gelezen. Daar waar de AVG ruimte laat voor nationale regelingen of opdraagt tot het treffen van een regeling, komt de UAVG in beeld. De belangrijkste gebieden waar de UAVG een rol speelt zijn: het toepassingsbereik van AVG; de rol, positie en bevoegdheden van de nationale toezichthouder (de Autoriteit Persoonsgegevens); regelingen rondom het gebruik van bijzondere categorieën van persoonsgegevens; regelingen omtrent (de uitzonderingen op) de rechten van de betrokkenen; en regelingen voor specifieke verwerkingssituaties (zoals in relatie tot de vrijheid van meningsuiting).

De bescherming van persoonsgegevens is in verschillende wet- en regelgeving neergelegd. Naast de AVG, de UAVG zijn er ook in zorgspecifieke wetgeving regels over de bescherming van persoonsgegevens neergelegd, zoals de Wlz en de Wgbo. Dit geeft de complexiteit van het onderwerp privacy aan, omdat meerdere wetten tegelijkertijd van toepassing kunnen zijn. Deze module geeft hier meer inzicht in.

1.2 AVG en Wbp: is er iets veranderd?

De wetgever heeft bij de UAVG gekozen voor aansluiting bij het regime van de Wbp waar de AVG ruimte liet. De AVG en Wbp kennen niet veel structurele verschillen. In de kern gelden dezelfde regels omtrent de bescherming van persoonsgegevens. Zoals het mogen verwerken van persoonsgegevens als daarvoor een grondslag aanwezig is. Een grondslag kan zijn de toestemming van de betrokkene of een wettelijke verplichting. Een wettelijke verplichting in de gehandicaptenzorg is bijvoorbeeld het verstrekken van persoonsgegevens in het kader van het in rekening brengen van tarieven door de zorgorganisatie aan het zorgkantoor op grond van artikel in 9.1.2 lid 1 sub f Wlz. En brengt de AVG, net zoals de Wbp, met zich mee dat bij elke gegevensverwerking sprake moet zijn van een gerechtvaardigd doel en dat niet meer gegevens mogen worden gebruikt dan voor dat doel noodzakelijk is. Verder kende de Wbp ook al regels over datalekken, bewaartermijnen en het opstellen bewerkersovereenkomsten (nu verwerkersovereenkomsten).

< Terug naar de inhoudsopgave

Niettemin bestaan er enkele verschillen, waarvan het goed is de meest relevante te benoemen. Waarbij wordt opgemerkt dat deze verschillen niet allemaal ingrijpend van aard zijn.

- De verwerkingsverantwoordelijke moet naar de betrokkene toe, ten opzichte van de Wbp, transparanter zijn en steeds duidelijk maken welke persoonsgegevens worden verwerkt en waarom, waaronder de informatieplicht. De Wbp kende slechts een beperkte informatieplicht naar de betrokkene toe. De AVG heeft dit flink uitgebreid (artikel 13 AVG) op de hoeveelheid informatie die moet worden verstrekt; de vereisten waaraan de informatieplicht moet voldoen en passende maatregelen die het ontvangen van de informatie waarborgen. Een 'privacy reglement' is een middel om te voldoen aan de informatieplicht onder de AVG. De VGN heeft een model privacyreglement ontwikkeld. Klik hier voor een uitgebreide beschrijving van deze omvangrijke informatieplicht.
- In het verlengde hiervan kent de AVG als nieuwe verplichting dat de verwerkingsverantwoordelijke moet kunnen aantonen dat hij aan de AVG voldoet, dat hij compliant is (artikel 5 lid 2 AVG). Deze 'aantoonbaarheid' legt de verwerkingsverantwoordelijke onder andere de plicht op om een privacybeleid te formuleren.
- De AVG verplicht de organisatie een 'verwerkingsregister' op te stellen en bij te houden. Onder de Wbp diende een verwerking te worden gemeld bij de Autoriteit Persoonsgegevens. Deze melding is vervallen, maar het is wel verplicht om elke verwerking door een organisatie in een eigen verwerkingsregister op te nemen (artikel 30 AVG).
- Een versterking van de positie van de betrokkene (artikel 15 tot en met 23 AVG).
  Naast de reeds bestaande rechten tot inzage en correctie kent de AVG twee nieuwe rechten: "het recht op dataportabiliteit" en "het recht op vergetelheid".
  Het recht op dataportabiliteit houdt in dat de verwerkingsverantwoordelijke ervoor moet zorgen dat betrokkenen hun gegevens makkelijk kunnen verkrijgen en vervolgens kunnen doorgeven aan een andere organisatie als ze dat willen.[1]
  Het recht op vergetelheid houdt in dat op verzoek van de betrokkene al zijn persoonsgegevens zonder onredelijke vertraging moeten worden verwijderd.
  Met recht op vergetelheid wordt niet enkele het recht op het verwijderen bedoeld maar ook de handeling die daarbij hoort. (De feitelijke handeling, het wissen, is gecombineerd met de waarde die het recht voor de betrokkenen kan hebben, zijn of haar vergetelheid.) Het moet niet zo zijn dat na een wissingsverzoek op het internet toch steeds bepaalde informatie boven water komt. Concreet betekent dit dat de zorgorganisatie de persoonsgegevens van de betrokkene

1 Dit recht geldt enkel:
- voor de persoonsgegevens die door de betrokkene zelf zijn verstrekt
- én de betrokkene voor de verwerking toestemming heeft verleend of verwerking kon plaatsvinden ter uitvoering van een overeenkomst;
- én de verwerking geautomatiseerd plaatsvindt.

Het recht op dataportabiliteit geldt niet voor niet-geautomatiseerde (papieren) bestanden.

< Terug naar de inhoudsopgave

moet verwijderen, maar ook dat de zorgorganisatie andere (zorg)organisaties moet verzoeken de persoonsgegevens van deze betrokkene te wissen in het geval de gegevens via de zorgorganisatie verkregen zijn.
Zie voor de uitgebreide beschrijving van de rechten van betrokkenen module 3.

- De verplichting tot het uitvoeren van een gegevensbeschermingseffectbeoordeling of Data Privacy Impact Assestment (DPIA) (artikel 35 AVG).
  De verwerkingsverantwoordelijke moet een DPIA uitvoeren wanneer de voorgenomen verwerking waarschijnlijk een hoog risico oplevert voor de personen van wie de gegevens worden verwerkt.
- Verplichting tot het aanstellen van een Functionaris Gegevensbescherming (FG) afhankelijk van wat er verwerkt wordt (artikel 37 AVG).
- De verplichting voor de verwerkingsverantwoordelijke voor privacy by design en privacy by default (artikel 25 AVG). By design: dit houdt in om bij de ontwerpfase van nieuwe producten en diensten op zowel technisch als organisatorisch gebied rekening te houden met de privacy. By default: standaardinstellingen moeten privacy vriendelijk zijn. Dus een vinkje voor het aanmelden voor nieuwsbrief mag niet als standaard zijn ingevuld.
- Er gelden zwaardere sancties als wordt nagelaten om datalekken te melden. De AVG kent verder aan de Autoriteit Persoonsgegevens de mogelijkheid toe hoge(re) boetes op te leggen (artikel 83 AVG) bij het niet naleven van de verplichtingen in de AVG. Op grond van de Wbp konden boetes oplopen tot € 820.000 of tot 10% van de jaaromzet van een organisatie. Onder de AVG is de boetebevoegdheid van de Autoriteit Persoonsgegevens uitgebreid. Er kunnen boetes worden opgelegd die kunnen oplopen tot het maximum van € 20.000.000, -- of 4% van de omzet van een onderneming, als dit hoger is.
- Een verwerker kan nu ook aansprakelijk worden gesteld voor schade aan een betrokkene als tijdens de verwerking niet voldaan is aan de specifieke AVG-verplichtingen voor verwerkers of als in strijd wordt gehandeld met rechtmatige instructies van verwerkingsverantwoordelijke (artikel 82 lid 2 AVG). Onder de Wbp was van deze aansprakelijkheidstelling voor een (toen nog) bewerker geen sprake.

2 Relevante definities AVG

De hierna beschreven definities zijn de belangrijkste begrippen uit de AVG. Het kennisnemen van deze begrippen zorgt voor een basiskennis van de AVG en draagt bij aan het beoordelen van privacyvraagstukken.

< Terug naar de inhoudsopgave

Persoonsgegevens (artikel 4.1 AVG):

Alle informatie over een geïdentificeerde of identificeerbare natuurlijke persoon (de betrokkene).

Betrokkene in de gehandicaptenzorg is degene van wie de zorgorganisatie persoonsgegevens verwerkt. Dat kan een (toekomstige) cliënt zijn, maar soms is dit (ook) de wettelijk vertegenwoordiger, schriftelijk gemachtigde of de belangenbehartiger door wie de cliënt wordt vertegenwoordigd. Van deze personen hebben zorgorganisaties persoonsgegevens nodig, zoals contactgegevens.
Zie ook vraag 5 in module 2, wie geeft wanneer toestemming?

Verwerking (artikel 4.2 AVG):

Elke bewerking of elk geheel van bewerkingen van persoonsgegevens, al dan niet geautomatiseerd, zoals het verzamelen, vastleggen, ordenen, structureren, opslaan, bijwerken of wijzigen, opvragen, raadplegen, gebruiken, verstrekken door middel van oorzending, verspreiden of op andere wijze ter beschikking stellen, samenbrengen of combineren, en ook het afschermen, wissen of vernietigen van gegevens.[2]

Betrokkenen in de gehandicaptenzorg kunnen zijn:

- Zorgvrager (= toekomstig cliënt);
- Cliënt;
- Wettelijk vertegenwoordiger: de persoon die een zorgvrager/cliënt vertegenwoordigt als deze handelings- en/of wilsonbekwaam is. Dit zijn de ouder(s) of voogd(en) bij minderjarigheid en de curator, mentor of bewindvoerder bij meerderjarigheid;
- Schriftelijk gemachtigde ingeval van meerderjarigheid: de persoon die de zorgvrager/cliënt in een schriftelijke opdracht heeft aangewezen en die hem vertegenwoordigt en bijstaat in de behartiging van zijn of haar belangen op het moment dat zorgvrager/cliënt wilsonbekwaam is;

2 Puur mondelinge overdracht van gegevens is geen verwerking van persoonsgegevens. Echter, in de meeste gevallen worden de uitkomsten van dergelijke gesprekken vastgelegd, waardoor er vaak alsnog een verwerking van persoonsgegevens plaatsvindt. Een begeleider bijvoorbeeld die met een collega mondeling de situatie van een cliënt bespreekt verwerkt geen persoonsgegevens, maar als bijvoorbeeld een plan van aanpak vervolgens wordt vastgelegd in een cliëntsysteem, dan is dat wel een verwerking van persoonsgegevens.

< Terug naar de inhoudsopgave

- Belangenhartiger ingeval van meerderjarigheid: de echtgenoot, geregistreerd partner, levensgezel, ouder, kind, broer of zuster in de situatie zoals bedoeld in artikel 7:465 lid 3 BW (Wet op de geneeskundige behandelingsovereenkomst).

Voor de leesbaarheid wordt in deze handreiking gesproken over (wettelijk) vertegenwoordiger bij het aanduiden van de wettelijk vertegenwoordiger, de schriftelijk gemachtigde en de belangenbehartiger tezamen.

Verwerkingsverantwoordelijke (artikel 4.7 AVG):

Degene die alleen of samen met anderen, het doel van en de middelen voor de verwerking van persoonsgegevens vaststelt. Als de zorgorganisatie verwerkingsverantwoordelijke is, dan wordt daarmee de Raad van Bestuur bedoeld.

Klik hier voor het stroomschema verwerkingsverantwoordelijke of verwerker. Zie ook vraag 8.8.2 in module 3.

Verwerker (artikel 4.8 AVG):

Degene die in opdracht van de verwerkingsverantwoordelijke persoonsgegevens verwerkt, zoals softwareleveranciers, website hosts, clouddiensten, externe salarisadministratie, externe kwaliteitsauditor, leverancier van het ECD die dit ook faciliteert voor de zorgorganisatie.

Klik hier voor het stroomschema verwerkingsverantwoordelijke of verwerker. Zie ook vraag 8.8.2 in module 3.

Subverwerker (artikel 28 lid 2 en 4 AVG):

Een partij die namens de verwerker persoonsgegevens verwerkt voor de verwerkingsverantwoordelijke. Bijvoorbeeld in het geval het bedrijf dat zorgdraagt voor het ECD van de zorgorganisatie een deel van haar werkzaamheden uitbesteedt aan een ander.

Bestand (artikel 4.6 AVG):

Een gestructureerd geheel van persoonsgegevens die volgens bepaalde criteria toegankelijk zijn, ongeacht of dit geheel gecentraliseerd of gedecentraliseerd is dan wel op functionele of geografische gronden is verspreid.

< Terug naar de inhoudsopgave

Een abstracte definitie die in samenhang met artikel 2 lid 1 AVG (en overweging 15 van de AVG) moet worden gelezen om te concluderen dat onder bestand de niet-geautomatiseerde gegevensverwerking wordt verstaan oftewel het archief met papieren dossiers.
Om te verduidelijken:
In artikel 2 is bepaald dat de AVG van toepassing is op:

1. een geheel of gedeeltelijk geautomatiseerde verwerking van persoonsgegevens.
   Geautomatiseerde verwerking: elke bewerking die wordt uitgevoerd met behulp van computers, smartphones, tablets, servers, databases etc.
2. of wanneer persoonsgegevens zijn opgenomen in een bestand of daartoe bestemd zijn.
   Bestand: een gestructureerde verzameling persoonsgegevens die via een bepaalde logica toegankelijk is. Zoals een archiefkast of een geordende verzameling naamkaartjes.

Aandachtspunt:
Het element 'gestructureerd geheel' in artikel 4.6 is essentieel om te kunnen beoordelen of sprake is van een bestand dat onder de werkingssfeer van de AVG valt.
Gestructureerd geheel houdt in dat de gegevensverwerking op grond van meer dan één kenmerk een onderlinge samenhang vertoont. Deze samenhang kan blijken uit het feit dat de verwerking in de praktijk als een geheel wordt beschouwd, uit de aangebrachte structuur van de gegevensverwerking zelf of uit een raadpleegmethodiek. Daarbij maakt het niet uit waar het bestand zich fysiek bevindt, als sprake is van onderlinge samenhang is sprake van één bestand. Dus ook als een papieren archief zich op meerdere locaties bevindt dan kan dat als één bestand worden aangemerkt als de verschillende onderdelen van dit archief als één geheel kunnen worden beschouwd. Daarnaast is om te beoordelen of sprake is van één bestand of meerdere bestanden het doel of de doelen van de verwerking(en) en het feitelijk gebruik van de gegevens van belang.

Aandachtspunt:
Losse papieren op een bureau met daarin namen van personen maken geen onderdeel uit van een bestand, mits deze papieren geen relatie met de taken en werkzaamheden van de zorgorganisaties verband houden. Wanneer de losse papieren wél verband houden met de taken en werkzaamheden van de zorgorganisatie dan maken ze onderdeel uit van een bestand. In de meeste gevallen zal hier sprake van zijn.

< Terug naar de inhoudsopgave

Bijzondere categorieën van persoonsgegevens (artikel 9 lid 1 AVG):
Persoonsgegevens waaruit ras of etnische afkomst, politieke opvattingen, religieuze of levensbeschouwelijke overtuigingen of het lidmaatschap van een vakbond blijken, genetische gegevens, biometrische gegevens, gegevens over de gezondheid en ook gegevens met betrekking tot iemands seksueel gedrag of seksuele gerichtheid.

Gegevens over de gezondheid (artikel 4.15 AVG):
Gegevens die betrekking hebben op de fysieke of mentale gezondheid van een natuurlijk persoon, waaronder gegevens over verleende gezondheidsdiensten waarmee informatie over zijn gezondheidstoestand wordt gegeven.
Zoals bijvoorbeeld informatie over bijvoorbeeld iemands beperking, ziekterisico, medische voorgeschiedenis; informatie die voortkomt uit testen of onderzoeken aan het lichaam van een persoon (genetische testen, bloedonderzoeken etc.) maar ook een cliëntnummer als unieke identificatie van een natuurlijk persoon.

Zie vraag 6, 7 en 8 voor meer informatie over bijzondere persoonsgegevens.

Genetische gegevens (artikel 4.13 AVG):
Persoonsgegevens die verband houden met de overgeërfde of verworven genetische kenmerken van een natuurlijke persoon die unieke informatie verschaffen over de fysiologie of de gezondheid van die natuurlijke persoon en die met name voortkomen uit een analyse van een biologisch monster van die natuurlijke persoon. Het betreft hier DNA-analyses, RNA-analyses[3] of analyses van andere elementen waarmee soortgelijke informatie kan worden verkregen.

Biometrische gegevens (artikel 4.14 AVG):
Persoonsgegevens verkregen uit iemands fysieke, fysiologische of gedragsgerelateerde kenmerken die identificatie mogelijk maken, zoals irisscans of vingerafdrukken.

Profilering (artikel 4.4 AVG):
Het geautomatiseerd verwerken van persoonsgegevens om bepaalde persoonlijke aspecten van een natuurlijke persoon te beoordelen met het oog op het analyseren of voorspellen van zijn of haar beroepsprestaties; economische situatie; gezondheid; persoonlijke voorkeuren, interesses, betrouwbaarheid, gedrag, locatie of verplaatsingen. Deze definitie moet worden bezien in het licht van de rechten van betrokkenen.

3 DNA: desoxyribonucleïnezuur. RNA: ribonucleïnezuur.

< Terug naar de inhoudsopgave

Derde(n) (artikel 4.10 AVG):
Een natuurlijk persoon of rechtspersoon, een overheidsinstantie, een dienst of een ander orgaan die geen cliënt, geen betrokkene, geen verwerkingsverantwoordelijke, geen verwerker of persoon is die onder rechtstreeks gezag van de verwerkingsverantwoordelijke of de verwerker persoonsgegevens mag verwerken.
Met andere woorden onder een derde wordt verstaan degene die niet de betrokkene is, niet de verwerkingsverantwoordelijke is of de verwerker met inbegrip van degenen die onder het rechtstreeks gezag (van de verwerkingsverantwoordelijke of de verwerker) werken.

Toestemming van de betrokkene (artikel 4.11 AVG): Elke vrije, specifieke, geïnformeerde en ondubbelzinnige verklaring of actieve handeling waarmee een betrokkene accepteert dat zijn persoonsgegevens worden verwerkt. Deze toestemming mag niet voor verschillende interpretaties vatbaar zijn. Daarnaast moet deze toestemming aantoonbaar zijn verkregen, bijvoorbeeld door ondertekening van een verklaring.
Klik hier voor meer informatie over toestemming.

Datalek, inbreuk in verband met persoonsgegevens (artikel 4.12 AVG):
Een inbreuk op de beveiliging waarbij persoonsgegevens per ongeluk of op onrechtmatige wijze in handen van onbevoegden zijn gekomen, voor onbevoegden toegankelijk waren, of zijn vernietigd, gewijzigd of verloren.

3 Waar is de AVG van toepassing: het territoriale bereik?

De AVG is van toepassing op landen binnen de EU. Maar wat betekent dit concreet?
De AVG geldt voor:

1. Organisaties (verwerkingsverantwoordelijke of verwerker) die in de Europese Unie zijn gevestigd en persoonsgegevens verwerken;
   Gevestigd zijn - het hebben van een vestiging - in de Europese Unie betekent niet dat de eigenlijke verwerking dan ook in de EU moet plaatsvinden. Ook maakt het niet uit welke rechtsvorm een organisatie heeft.
2. Organisaties (en personen) die niét in de Europese Unie gevestigd zijn, maar wel gegevens verwerken van burgers in de EU.
   Om ervoor te zorgen dat betrokkenen die zich in de EU bevinden de bescherming hebben van de AVG, ook als de verwerkingsverantwoordelijke of verwerker niet in de EU is gevestigd, is de AVG van toepassing op deze organisaties (of personen) als de verwerking verband houdt met:
   - het aanbieden van goederen en diensten aan deze betrokkenen in de EU, ongeacht of een betaling is vereist (bijvoorbeeld een online webshop);

< Terug naar de inhoudsopgave

- het monitoren van gedrag van natuurlijke personen voor zover dit gedrag in de EU plaatsvindt. Of daarvan sprake is moet worden vastgesteld of natuurlijke personen bijvoorbeeld op het internet worden gevolgd voor het onder-meer het opstellen van profielen.

3. Een verwerkingsverantwoordelijke die niet in de EU is gevestigd, maar wel op een plaats waar krachtens het internationaal publiekrecht het recht van de lidstaat van toepassing is. Denk hierbij aan ambassades en consulaten.
   Klik hier voor meer informatie over doorgifte van persoonsgegevens naar een derde land.[4]

4 Privacy en sectorspecifieke zorgwetgeving

Naast de AVG zijn regels over de bescherming van persoonsgegevens ook te vinden in sectorspecifieke wetgeving. Voor de gehandicaptenzorg zijn dat onder meer de Wet op de geneeskundige behandelingsovereenkomst (Wgbo), de Wet Beroepen individuele gezondheidszorg (Wet Big), de Wet marktordening gezondheidszorg (Wmg), de Wet langdurige zorg (Wlz), de Zorgverzekeringswet (Zvw), de Wet maatschappelijke ondersteuning 2015 (Wmo 2015), de Jeugdwet, de Wet kwaliteit, klachten en geschillen zorg (Wkkgz), de Wet bijzondere opnemingen in psychiatrische ziekenhuizen (Wet Bopz)[5] en de Wet aanvullende bepalingen verwerking persoonsgegevens in de zorg (Wabvpz)[6]. In deze zorgwetten staan bepalingen over het omgaan met persoonsgegevens welke blijven bestaan naast de AVG. Als voorbeeld kunt u denken aan art. 5.2.1 tot en met art. 5.2.9 Wmo 2015. Hierin wordt beschreven in welke situatie onder welke voorwaarden persoonsgegevens mogen worden uitgewisseld. Hier kunt u een schema vinden over de uitwisseling van persoonsgegevens op grond van een 'zorgwet' met andere organisaties zoals gemeenten, het CIZ en zorgkantoren.

4.1 Elektronische gegevensuitwisseling in de zorg: Wet aanvullende bepalingen verwerking persoonsgegevens in de zorg (Wabvpz).

Voor het verschaffen van een zo volledig mogelijk beeld wordt kort stilgestaan bij een relatief recente ontwikkeling toegespitst op het gebied van elektronische verwerking van persoonsgegevens in de zorg.

Op 1 juli 2017 trad de Wet cliëntenrechten bij elektronische verwerking van gegevens in werking. Het is geen aparte wet, maar wekte wel deze indruk. De bepalingen van de Wet cliëntenrechten werden namelijk ondergebracht in de Wet gebruik BSN in de zorg. Omdat door deze toevoeging de Wet gebruik BSN in de zorg over meer onderwerpen gaat dan alleen het Burgerservicenummer werd de titel van deze wet vervolgens weer gewijzigd in de Wet aanvullende bepalingen verwerking persoonsgegevens in de zorg (Wabvpz).

4 Derde landen zijn alle landen buiten de EU, met uitzondering van de landen in de Europese Economische Ruimte (EER). Dit zijn Noorwegen, Liechtenstein en IJsland. Deze drie landen kennen een gelijkwaardig niveau van bescherming van persoonsgegevens.

5 De handreiking privacy zal geactualiseerd worden zodra de Wet Zorg en Dwang (Wzd) in werking treedt.

6 Dit was voorheen de Wet BSN in de zorg.

< Terug naar de inhoudsopgave

Werkingssfeer Wabvpz

De Wabvpz is van toepassing op de zorg of dienst die krachtens de Zorgverzekeringswet en de Wet langdurige zorg wordt verleend (artikel 1, sub b onderdeel 1Wabvpz) en heeft betrekking op de zorgaanbieder zoals omschreven in de Wkkgz (artikel 1 sub c Wabvpz).
De Wabvpz is niet van toepassing op ondersteuning in de zin van de Wmo 2015 en jeugdhulpverlening op grond van de Jeugdwet.

Hoe verhoudt Wabvpz zich tot de Wgbo en de AVG?

De Wgbo en de AVG kennen verplichtingen voor zorgaanbieders voor een zorgvuldige omgang met de persoonsgegevens (gezondheidsgegevens) van cliënten. Verplichtingen zoals het: aanleggen van een dossier; het verlenen van inzage; het verstrekken van gegevens aan anderen dan de cliënt of zijn (wettelijk) vertegenwoordiger en het zorgdragen voor een passend beveiligingsniveau. De Wabvpz voegt hier aanvullende rechten en waarborgen voor de cliënt aan toe in geval van een **elektronische gegevensuitwisseling** en **beschikbaarheid van gegevens via een elektronisch uitwisselingssysteem.**
De Wabvpz geldt in aanvulling op de AVG en zorgspecifieke wetgeving zoals de Wgbo.

> Definitie elektronisch uitwisselingssysteem (artikel 1, sub b onderdeel j Wabvpz):
> "Een systeem waarmee zorgaanbieders op elektronische wijze, dossiers, gedeelten van dossiers of gegevens uit dossiers voor andere zorgaanbieders raadpleegbaar kunnen maken, waaronder niet begrepen een systeem binnen een zorgaanbieder, voor het bijhouden van een elektronisch dossier."

Concreet:
Het betreft een elektronisch uitwisselingssysteem tussen zorgaanbieders onderling waarmee zorgaanbieders op elektronische wijze, dossiers, gedeelten van dossiers of gegevens uit dossiers voor andere zorgaanbieders raadpleegbaar kunnen maken. Een voorbeeld daarvan is het uitwisselen van medicatiegegevens tussen de voorschrijvend arts (zoals een AVG-arts) en de verstrekkende apotheek via het Landelijk Schakel Punt (LSP) of het digitaal uitwisselen van overdracht gegevens tussen een ziekenhuis en zorgorganisatie via een regionaal IT-netwerk.[7] Het eigen interne elektronisch cliëntendossier is geen uitwisselingssysteem in de zin van de Wabvpz.

7 Juridische factsheet Wet cliëntenrechten bij elektronische verwerking van gegevens, VWS.

< Terug naar de inhoudsopgave

De Wabvpz kent een gedeeltelijke inwerkingtreding. Op 1 juli 2017 zijn al enkele bepalingen van kracht geworden, per 1 juli 2020 treedt het andere deel in werking.

Geldend vanaf 1 juli 2017

1. Uitdrukkelijke toestemming van de cliënt aan zorgaanbieder voor het beschikbaar stellen van zijn gegevens via een elektronisch uitwisselingssysteem (artikel 15a lid 1 Wabvpz). De bedoeling hiervan is dat de cliënt vooraf actief bepaalt of hij wel of niet wil deelnemen aan elektronische uitwisseling van zijn gegevens.

Toestemmingsvereiste artikel 15a Wabvpz heeft alleen betrekking op het pull-verkeer:

Zorgaanbieder stelt (gegevens uit) het medisch dossier elektronisch beschikbaar voor latere raadpleging (voor een bepaald doel) door andere zorgaanbieders (bijvoorbeeld ziekenhuis, huisarts-huisartsenpost-apotheker, landelijk schakelpunt), zonder dat op het moment van het verlenen van toestemming bekend is wie de andere zorgaanbieder zal zijn. De initiatiefnemer is de ontvanger van de gegevens. Benadrukt wordt dat alleen zorgaanbieders die - nu of in de toekomst - betrokken zijn bij de behandelingsovereenkomst van de cliënt gegevens kunnen raadplegen/opvragen. Het gaat hier alleen om gegevens in het kader van de behandelingsovereenkomst.

Artikel 15a Wabvpz heeft geen betrekking op het push-verkeer: het versturen van informatie elektronisch naar andere zorgaanbieders die een behandelrelatie hebben met de betrokkenen. De verzender is hier de initiatiefnemer.

Wie kan toestemming geven in geval cliënt wilsonbekwaam is?
In artikel 15g Wabvpz is opgenomen dat in geval de cliënt niet in staat is tot een redelijke waardering van zijn belangen ter zake de toestemming wordt gegeven door de (wettelijk) vertegenwoordiger.

2. Informatieplicht
   - Zorgaanbieder moet de cliënt informeren over zijn rechten bij elektronische gegevensuitwisseling, hoe hij zijn rechten kan uitoefenen, hoe het elektronisch uitwisselingssysteem werkt, welke zorgaanbieders zijn aangesloten op het systeem en hoe de cliënt zijn toestemming kan intrekken (artikel 15c lid 1 Wabvpz).

< Terug naar de inhoudsopgave

- Zorgaanbieder moet cliënt informeren over het aansluiten van nieuwe categorieën van zorgaanbieders bij het elektronisch uitwisselingssysteem en/of als de werking van het elektronisch uitwisselingssysteem substantieel wordt gewijzigd. Cliënt moet erop gewezen worden dat hij zijn eerder verleende toestemming mag aanpassen of intrekken. De Wabvpz vereist dus niet dat steeds opnieuw om toestemming moet worden gevraagd bij aansluiten van nieuwe zorgaanbieders aan het elektronische uitwisselingssysteem en/of substantiële wijziging van het systeem zelf.

3. Een verbod voor zorgverzekeraars, bedrijfs- en verzekerings- en keuringartsen om de elektronische uitwisselingssystemen van zorgaanbieders te raadplegen (artikel 15f Wabvpz).

Vanaf 1 juli 2020 treden de volgende bepalingen in werking:

1. Gespecificeerde toestemming van cliënt voordat elektronische gegevensuitwisseling plaatsvindt. Dit houdt in dat de cliënt toestemming kan geven voor uitwisseling met alle of bepaalde categorieën van zorgaanbieders. Een cliënt kan bijvoorbeeld toestemming gegeven voor uitwisseling met apothekers en huisartsen, maar sluit bijvoorbeeld tandartsen uit.
2. Zorgaanbieder is verplicht een registratie bij te houden van de verleende gespecificeerde toestemmingen waarbij aantekening wordt gemaakt vanaf welk tijdstip de toestemming van kracht wordt. De zorgaanbieder mag deze registratie beschikbaar stellen via het uitwisselingssysteem.
3. Cliënt heeft recht op kosteloze elektronische inzage en afschrift van het eigen dossier.
4. Cliënt heeft recht op elektronisch afschrift van de logging (wie heeft op welke datum bepaalde informatie in het elektronisch uitwisselingssysteem beschikbaar gesteld).

Besluit elektronische gegevensverwerking zorgaanbieders en gehandicaptenzorg

Naast de bepalingen in de Wabvpz is bovengenoemd Besluit op 10 november 2017 in werking getreden. Hierin zijn specifieke functionele, technische en organisatorische eisen aan elektronische gegevensuitwisseling én zorginformatiesystemen, waaraan zorgaanbieders moeten voldoen, vastgelegd:

- Voldoen aan de NEN-normen 7510 - informatiebeveiliging in de zorg; 7512 - vertrouwensbasis voor gegevensuitwisseling; 7513 - logging van toegang tot cliëntendossier (artikel 3 t/m 5 Besluit).
- Als NEN-norm 7521 - uniforme en veilige gegevensuitwisseling tussen zorgprofessionals en zorgorganisaties rond de behandeling van een cliënt, is vastgesteld, zal ook hieraan moeten worden voldaan.
- Vastleggen van beleid, procedures en verantwoordelijkheden rondom gebruikte elektronische uitwisselingssystemen en interne zorginformatiesystemen (artikel 4 Besluit).

< Terug naar de inhoudsopgave

- Zorgaanbieders houden de laatste stand van de wetenschap en techniek bij met betrekking tot informatiebeveiliging en de bescherming van persoonsgegevens, en verantwoorden zich over de toepassing daarvan bij de inrichting en het gebruik van hun systemen (artikel 6 Besluit).

(Het besluit heeft de status van een Algemene Maatregel van Bestuur[8] wat betekent dat er snel kan worden ingespeeld op de actuele stand van de techniek.)

Aandachtspunt:
In aanvulling op NEN 7510 is in mei 2019 de veldnorm NTA 7516 Eisen voor veilige e-mail en chatapplicaties gepubliceerd. De NTA 7516 is niet opgenomen in het Besluit elektronische gegevensverwerking door zorgaanbieders. Op grond van de AVG bestaat echter een brede(re) verplichting voor de verwerkingsverantwoordelijke tot het treffen van passende technische en organisatorische (beveiligings)maatregelen bij de verwerking van persoonsgegevens. Dit brengt met zich mee om te handelen in lijn met de voor de zorgorganisatie relevante NEN-normen en de veldnorm NTA 7516.[9] Het onderwerp veilig mailen komt aan de orde in module 1.

Wabvpz en Wmo 2015, Jeugdwet

Zoals hierboven aangegeven is de Wabvpz en daarmee ook het Besluit van toepassing op zorgorganisaties die onder de Wlz vallen, maar niet op zorgorganisaties die ondersteuning (Wmo 2015) en/of jeugdhulpverlening (Jeugdwet) bieden. Dit betekent dat de genoemde NEN-normen niet op deze zorgaanbieders van toepassing zijn. In lagere regelgeving van de Wmo 2015 en Jeugdwet zijn echter wel bepalingen over de informatiebeveiliging van gegevens opgenomen:

Wmo 2015
In artikel 3 Uitvoeringsregeling Wmo 2015 is opgenomen dat de gegevensverwerking, bedoeld in artikel 5.2.9 lid 6 Wmo voldoet aan NEN-ISO-IEC 27001 en NEN-ISO-IEC 27002.
Dit betreft de situatie waarin het BSN wordt uitgewisseld of persoonsgegevens indien de betrokkene geen BSN heeft.

8 Een AMvB kan, anders dan een wet, in principe zonder medewerking van de Tweede en Eerste Kamer worden vastgesteld. Een ministerie kan de AMvB opstellen, waarna de Ministerraad daar een besluit over neemt. De regering moet over een AMvB wel eerst juridische advies vragen aan de Raad van State. Na vaststelling vindt publicatie plaats in het Staatsblad.

9 NEN 7510-1, p. 11 en 12 jo. NTA 7516 p. 4.

< Terug naar de inhoudsopgave

Jeugdwet
Een soortgelijke bepaling geldt voor de jeugdhulpverlening. In artikel 6 van de Regeling Jeugdwet is bepaald dat de beveiliging van gegevensverwerking voldoet aan NEN-ISO-IEC 27001 en NEN-ISO-IEC 27002 of daaraan gelijkwaardige normen. Het betreft het gebruik van het BSN en de situatie waarbij persoonsgegevens worden verwerkt als aan de jeugdige geen BSN is toegekend (artikel 7.2.1 en 7.2.4 Jeugdwet).

Aandachtspunt:
Beperk de verwerking van persoonsgegevens niet tot de hier bovengenoemde toepassingen. Zorgorganisaties hebben een brede(re) verplichting als verwerkingsverantwoordelijke op grond van de AVG tot het treffen van passende technische en organisatorische beveiligingsmaatregelen bij de verwerking van persoonsgegevens. Dit brengt met zich mee om te handelen in lijn met de relevante NEN-normen.

Aankomende wet- en regelgeving
Tot slot wordt voor de volledigheid gewezen op de Richtlijn Netwerk en Informatiebeveiliging (NIB-Richtlijn) 2016/1148 die tot doel heeft een hoog gemeenschappelijk niveau van netwerk- en informatiebeveiliging te waarborgen. Deze Richtlijn is in Nederland geïmplementeerd in de Wet beveiliging netwerk- en informatiesystemen.[10]

4.2 Verhouding AVG tot sectorspecifieke wetgeving

De AVG geeft algemene regels over de verwerking van persoonsgegevens. Daarnaast kennen onder andere de Wmo 2015, de Jeugdwet, de Wgbo, de Wlz, de Wet Bopz[11] en de Wabvpz (zie 4) ook nog vaak regels over het verwerken van persoonsgegevens. Zoals beschreven in onderdeel 1.1 heeft de wetgever in de UAVG geregeld dat de ruimte die de AVG biedt, ingevuld wordt met het regime dat onder de Wbp van toepassing was (de beleidsneutrale invulling). Dit betekent ten eerste dat de privacyregels in de zorgspecifieke wetgeving blijven bestaan naast de algemene regels in de AVG. Maar ook dat de zorgspecifieke wetgeving de AVG verder mag inkleuren. Mocht een conflict ontstaan tussen twee of meer zorgwetten dan gaat een bepaling uit de AVG voor. Een Europese Verordening heeft voorrang op nationale wetgeving. Zie overkoepelend stappenplan over het toepassen van zorgspecifieke wetgeving naast de AVG.

10 De wet was ten tijde van publicatie van deze Handreiking in behandeling bij de Eerste Kamer.
11 Voor de volledigheid wordt opgemerkt dat de Wet Bopz voorrang heeft op de bepalingen over privacy in de Wgbo.

< Terug naar de inhoudsopgave

Aandachtspunt:
Bij het verwerken van (bijzondere) persoonsgegevens is het medisch beroepsgeheim (de geheimhoudingsplicht) van de zorgprofessional relevant. Naast het feit dat voor het kunnen verwerken van bijzondere persoonsgegevens (gezondheidsgegevens) eerst sprake moet zijn van een uitzondering op het verwerkingsverbod (artikel 30 UAVG) dient de zorgprofessional zijn medisch beroepsgeheim in acht te nemen welke slechts onder bepaalde voorwaarden doorbroken kan worden, waarna verdere verwerking mag plaatsvinden. De doorbreking van het medisch beroepsgeheim komt specifiek in module 2 aan de orde.

5 Richtlijnen beroepsverenigingen/brancheorganisaties en privacy

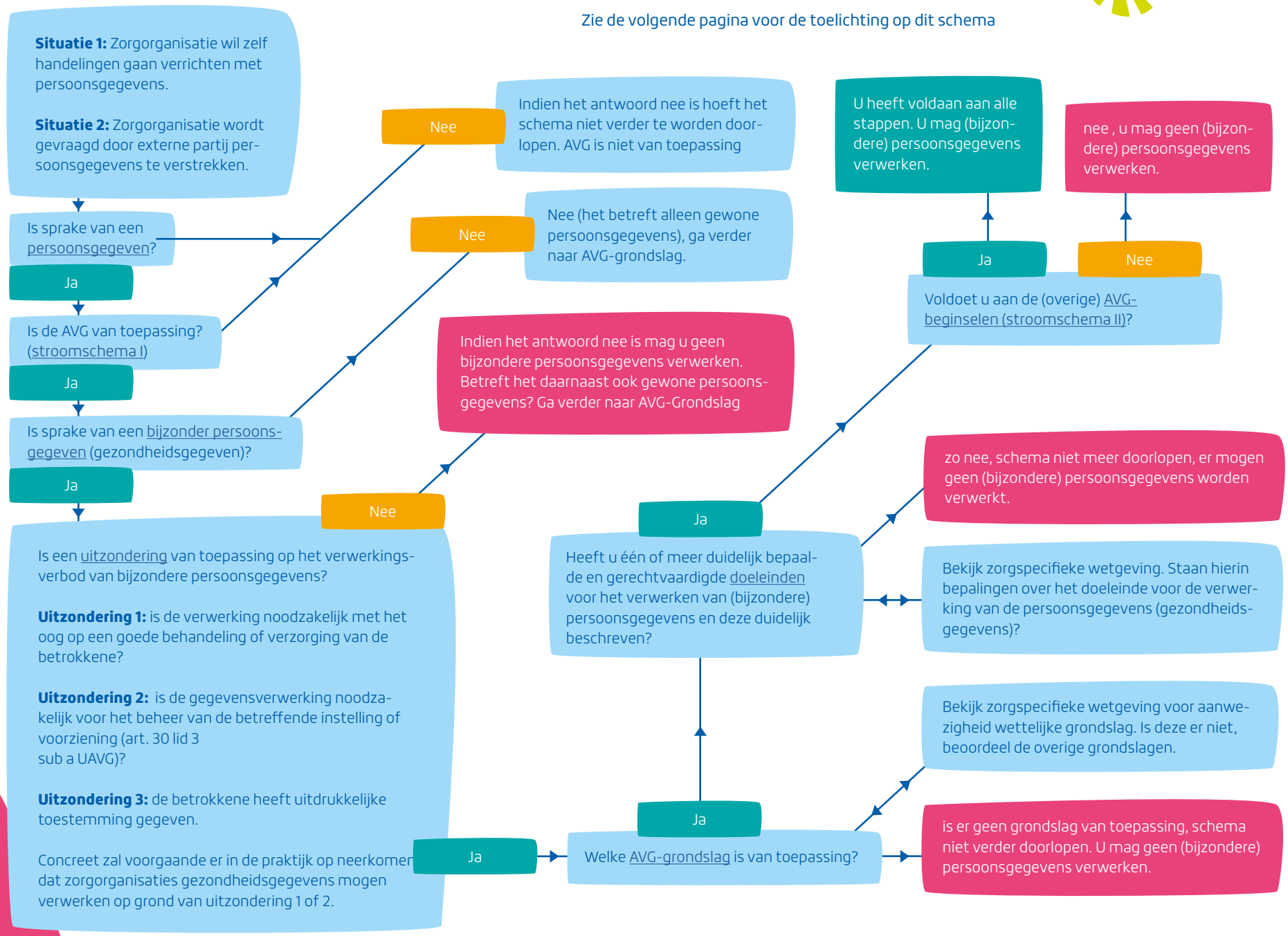
Diverse beroepsgroepen, zoals de KNMG, stellen richtlijnen op die een leidraad bieden voor het handelen van, in dit geval, de arts. Veel wettelijke bepalingen zijn algemeen geformuleerd en bevatten ruime begrippen zoals 'goede zorg' en 'de zorg van een goede hulpverlener' (zorgprofessional). Met een richtlijn wordt hieraan door de beroepsgroepen verder invulling gegeven.

Status richtlijnen
De civiele- en tuchtrechter kan de richtlijnen van beroepsgroepen gebruiken bij het toetsen van het handelen van de arts aan wettelijke (en tucht) normen. Ze hebben daarom betekenis voor de professionele standaard van de arts in het algemeen en gelden naast andere richtlijnen.

De VGN hanteert de Richtlijn Wgbo. Deze richtlijn stelt vast dat de VGN-leden bij hun zorg en ondersteuning aan cliënten handelen in overeenstemming met de Wgbo. Ook deze richtlijn kan de civiele- en tuchtrechter gebruiken bij een toets.

Het benoemen van deze richtlijnen in de Handreiking Privacy heeft te maken met het feit dat de Wgbo privacy-bepalingen kent zoals het recht op inzage, verwijdering en vernietiging van het medisch dossier en niet te vergeten de geheimhoudingsplicht, het medisch beroepsgeheim. Deze bepalingen gelden dus naast de AVG-bepalingen.Met dit stappenplan is getracht de wetgevingssystematiek omtrent privacy (begripsbepaling, uitzondering, beginselen, grondslagen) in een overzicht te vatten. Om hiermee een handvat te bieden bij het beoordelen van een privacyvraagstuk. Aangeraden wordt module 3 en module 4 erop na te slaan voor de context.

Zie de volgende pagina voor de toelichting op dit schema



< Terug naar de inhoudsopgave

Toelichting

Met dit stappenplan is getracht de wetgevingssystematiek omtrent privacy (begripsbepaling, uitzondering, beginselen, grondslagen) in een overzicht te vatten. Om hiermee een handvat te bieden bij het beoordelen van een privacyvraagstuk. Aangeraden wordt module 3 en module 4 erop na te slaan voor de context.

Aandachtspunt:
Bij het verwerken van (bijzondere) persoonsgegevens is het medisch beroepsgeheim (de geheimhoudingsplicht) van de zorgprofessional relevant. Naast het feit dat voor het verwerken van bijzondere persoonsgegevens (gezondheidsgegevens) eerst sprake moet zijn van een uitzondering op het verwerkingsverbod (artikel 30 UAVG) dient de zorgprofessional zijn medisch beroepsgeheim, in acht te nemen welke slechts onder bepaalde voorwaarden doorbroken kan worden, waarna verdere verwerking mag plaatsvinden. De doorbreking van het medisch beroepsgeheim komt specifiek in module 2 aan de orde. Bij het verwerken van (bijzondere) persoonsgegevens is het medisch beroepsgeheim (de geheimhoudingsplicht) van de zorgprofessional relevant. Naast het feit dat voor het verwerken van bijzondere persoonsgegevens (gezondheidsgegevens) eerst sprake moet zijn van een uitzondering op het verwerkingsverbod (artikel 30 UAVG) dient de zorgprofessional zijn medisch beroepsgeheim, in acht te nemen welke slechts onder bepaalde voorwaarden doorbroken kan worden, waarna verdere verwerking mag plaatsvinden. De doorbreking van het medisch beroepsgeheim komt specifiek in module 2 aan de orde.

B2 IS DE AVG VAN TOEPASSING?

FAQ'S EN STROOMSCHEMA I

1 Wat is een persoonsgegeven?

Persoonsgegevens zijn alle informatie waarmee een persoon geïdentificeerde of identificeerbaar is. Bijvoorbeeld naam, telefoonnummer, adres, e-mailadres, bankrekeningnummer. Maar ook gegevens die indirect iets over iemand zeggen kunnen een persoonsgegeven zijn. Bijvoorbeeld een postcode die op zichzelf staand nog niet tot een persoon leidt, maar door de combinatie met andere gegevens bijvoorbeeld een huisnummer of telefoonnummer is iemand identificeerbaar (zie ook vragen 2 en 3).

De AVG gaat niet over rechtspersonen, zoals een stichting, vereniging, B.V. of N.V. De AVG is wel van toepassing als deze organisaties persoonsgegevens verwerken van natuurlijke personen. Bijvoorbeeld een stichting die zorg en ondersteuning biedt aan mensen met een beperking. De stichting verwerkt persoonsgegevens van haar cliënten, op deze verwerking is de AVG van toepassing.

< Terug naar de inhoudsopgave

2 Wat betekent identificeerbaar?

Identificeerbaar betekent dat rekening moet worden gehouden met alle middelen waarvan redelijkerwijs te verwachten valt dat zij kunnen worden gebruikt om iemand direct of indirect (in combinatie met andere gegevens) te identificeren.

Dit betekent dat objectief moet worden gekeken naar de middelen die tot identificatie zou kunnen leiden. Zoals: de kosten, de tijd die nodig is voor identificatie, de beschikbare technologie op het tijdstip van verwerking en toekomstige technologische ontwikkelingen.

Niet alle gegevens zijn persoonsgegevens in de zin van de AVG. Dit wordt hierna beschreven.

3 Wat zijn géén persoonsgegevens in de zin van de AVG?

- Geanonimiseerde gegevens.
  Anonimiseren is het zodanig veranderen van persoonsgegevens dat ze niet meer terug te voeren zijn tot een persoon. Houd er rekening mee dat deze gegevens dan ook echt anoniem zijn en er geen mogelijkheden bestaan om iemand toch nog te kunnen identificeren.
  Let op: het anonimiseren van de persoonsgegevens is een verwerking van persoonsgegevens waarop de AVG van toepassing kan zijn.
- Gegevens van een overleden persoon.
  Gegevens van overleden personen zijn geen persoonsgegevens volgens de AVG, omdat personen volgens de wet dan geen natuurlijke personen meer zijn[12].
  Dit betekent echter niet dat het medisch beroepsgeheim van een hupverlener (zorgprofessional) eindigt met het overlijden van persoon. Dit blijft in stand op grond van de Wgbo en andere wettelijke bepalingen.
- Gegevens die op zichzelf staan.
  Zoals bijvoorbeeld enkel een postcode of IP-adres. Een IP-adres wordt pas een persoonsgegeven als men wettige middelen heeft om de persoon achter dit IP-adres te mogen achterhalen bijvoorbeeld op verzoek van de politie.
- Gegevens van iemand die worden gebruikt in de uitoefening van een zuiver persoonlijk of huishoudelijke activiteit (huiselijke kring).
  Voorbeelden van persoonlijke of huishoudelijke doelen zijn het bijhouden van persoonlijke adresbestanden, het mailen

12 Dit betekent niet vanzelfsprekend dat hiermee ook de privacy van de overleden persoon ophoudt te bestaan. Zie ABRvS 7 november 2012, nr. 201109485: de persoonlijke levenssfeer van een overledene is geschonden omdat de gegevens die over hem waren openbaargemaakt betrekking hadden op de tijd waarin de persoon nog leefde wat vervolgens ook gevolgen kan hebben voor de persoonlijke levenssfeer van de nabestaanden.

< Terug naar de inhoudsopgave

met vrienden en familie en het gebruik maken van sociale netwerken zolang dat geen enkel verband houdt met zakelijke (bedrijfsmatige) activiteiten. Met andere woorden, wanneer Facebook of Twitter door iemand voor persoonlijke doeleinden worden gebruikt, dan is de AVG daar niet op van toepassing.
- In geval er een onevenredige inspanning moet worden gedaan om iemand te kunnen identificeren (zie ook vraag 2).

4 Wat is pseudonimiseren?

Pseudonimiseren is het verhullen van iemands identiteit voor derden. Het is een beveiligingsmaatregel. Een voorbeeld is het vervangen van de naam van een persoon door een cliëntnummer. De medische gegevens van deze persoon worden dan gekoppeld aan dit nummer. Omdat een koppeling kan worden gemaakt tussen de naam (het persoonsgegeven) en het nummer (gepseudonimiseerd) is en blijft de AVG van toepassing.
Een pseudoniem is een persoonsgegeven, de AVG is daarop van toepassing.
Pseudonimiseren is dus niet hetzelfde als anonimiseren.

5 Is een bedrijfsnaam met de naam van een persoon een persoonsgegeven?

Een persoonsgegeven is alle informatie over een geïdentificeerde of identificeerbare persoon. Voor het beantwoorden van de vraag is dit laatste element relevant. Iemand is identificeerbaar als deze direct of indirect (in combinatie met andere gegevens) geïdentificeerd kan worden. Met een naamsvermelding in de bedrijfsnaam kan dat dus het geval zijn. Zoals bijvoorbeeld bij een eenmanszaak. Een bedrijfsnaam die met naam en achternaam in het KVK-register is opgenomen is herleidbaarheid naar een persoon. Dit betekent dat op het gebruiken van deze naam, door een andere dan de betrokkene zelf, de bepalingen uit de AVG van toepassing zijn. Bovenstaande geldt ook voor de naam in een e-mailadres van dat bedrijf, waarbij een persoon sneller herleidbaar zal zijn als de voor- en achternaam genoemd worden. Daarnaast kunnen ook andere gegevens, vanwege het kleinschalige karakter van de eenmanszaak, leiden tot een identificatie of identificeerbaarheid van een persoon, zoals bijvoorbeeld het adres van het bedrijf.

6 Wat zijn bijzondere persoonsgegevens?

In de gehandicaptenzorg worden gewone persoonsgegevens verwerkt, zoals naam, adres en geboortedatum maar betreffen het vooral gegevens over de gezondheid van een cliënt. Deze gegevens noemt de AVG bijzondere persoonsgegevens. Hiervoor gelden strengere eisen dan bij de gewone persoonsgegevens, bijvoorbeeld bij het verkrijgen van toestemming van de betrokkene.

< Terug naar de inhoudsopgave

7 Wat zijn gezondheidsgegevens in de gehandicaptenzorg?

Feitelijk gezien betreffen dit de gegevens over de zorg- en/of diensten en/of ondersteuning en/of jeugdhulp die een zorgprofessional aan een cliënt verleent. Deze gegevens geven informatie over de gezondheidstoestand van een cliënt. Het feit dat iemand cliënt is zegt iets over zijn gezondheidstoestand en is daarom een bijzonder persoonsgegeven.

Deze gegevens zijn van belang voor goede zorg en ondersteuning. In de gehandicaptenzorg is dat bijvoorbeeld het gespreksverslag van een cliënt met een persoonlijk begeleider, de behandelgegevens van een AVG-arts of orthopedagoog en het ondersteuningsplan.

8 Mogen zorgorganisaties gezondheidsgegevens verwerken?

Op deze vraag wordt een algemeen antwoord gegeven om inzicht te verkrijgen in de structuur van de AVG. Voor een concreet stappenplan klik hier.

De AVG zegt over de verwerking van bijzondere persoonsgegevens, waaronder gezondheidsgegevens, het volgende: **het is verboden om gezondheidsgegevens te verwerken (artikel 9 AVG).**

Waarom?
Dit verbod is ingegeven vanuit het feit dat deze persoonsgegevens naar hun aard bijzonder gevoelig zijn vanwege hun relatie met de grondrechten en fundamentele vrijheden van personen. Deze persoonsgegevens genieten specifieke bescherming doordat is geregeld dat het in beginsel verboden is deze bijzondere persoonsgegevens te verwerken.

Maar op dit verbod zijn uitzonderingen gemaakt. Er geldt namelijk een ontheffing verwerkingsverbod voor hulpverleners (zorgprofessionals) en instellingen of voorzieningen voor onder meer gezondheidszorg en maatschappelijke dienstverlening mits de gegevensverwerking (van gezondheidsgegevens) noodzakelijk is:

- voor een goede behandeling van de betrokkene;
- of voor het beheer van de instelling of voorziening.

Deze uitzondering is opgenomen in artikel 30 lid 3 sub a UAVG.
Onder beheer valt het waarborgen van de kwaliteit van de verleende zorg, intercollegiale toetsing door hulpverleners (zorgprofessional) onderling (kwaliteitsbeheer).

< Terug naar de inhoudsopgave

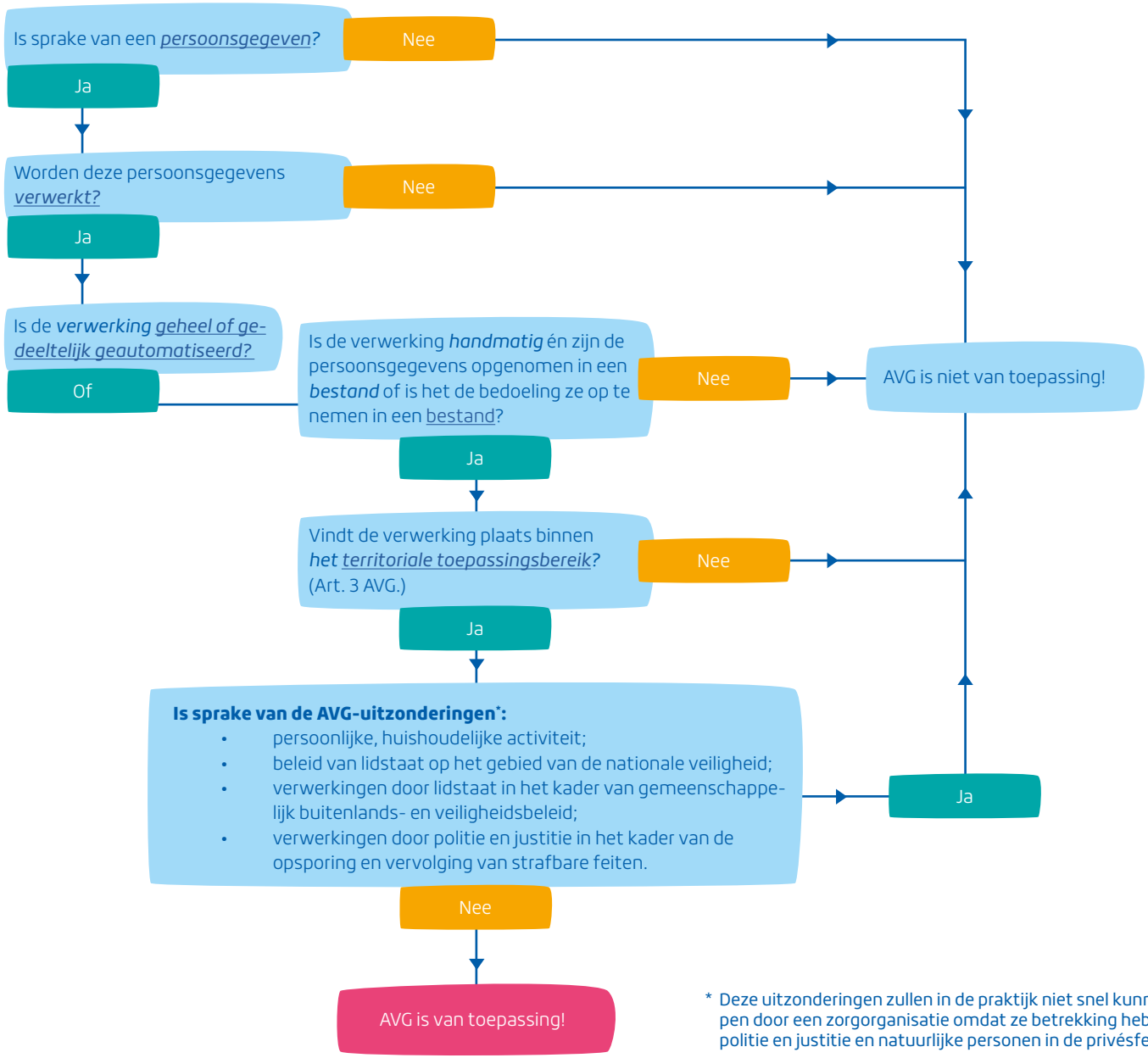
Dit betekent dat zorgorganisaties voor de gehandicaptenzorg gezondheidsgegevens mogen verwerken. Zouden zij deze verwerking niet kunnen verrichten dan is het voor hen ook niet mogelijk zorg- en dienstverlening te leveren.

Het verwerkingsverbod geldt daarnaast niet als de betrokkene uitdrukkelijke toestemming heeft verleend voor deze gegevensverwerking (artikel 9 lid 2 sub a en artikel 6 lid 1 sub a AVG.)

Zie ook vraag 2 in module 2.

Aandachtspunt
Het voorgaande neemt niet weg dat de feitelijke verwerking van bijzondere (en ook gewone) persoonsgegevens pas mag plaatsvinden als sprake is van een van de grondslagen in artikel 6 AVG én voldaan is aan de beginselen in artikel 5 AVG.
Een belangrijk aandachtspunt daarbij is dat bij het verwerken van bijzondere persoonsgegevens het medisch beroepsgeheim (de geheimhoudingsplicht) van de zorgprofessional relevant is. Dit medisch beroepsgeheim kan slechts onder bepaalde voorwaarden worden doorbroken, waarna een verdere verwerking van persoonsgegevens mag plaatsvinden. De doorbreking van het medisch beroepsgeheim komt specifiek in module 2 aan de orde.

< Terug naar de inhoudsopgave



* Deze uitzonderingen zullen in de praktijk niet snel kunnen worden ingeroepen door een zorgorganisatie omdat ze betrekking hebben op de overheid, politie en justitie en natuurlijke personen in de privésfeer.

< Terug naar de inhoudsopgave

B3 VOLDOE IK AAN DE AVG-BEGINSELEN (ARTIKEL 5 LID 1 EN 2 AVG)? BESCHRIJVING BEGINSELEN, STROOMSCHEMA II.

Bij de verwerking van persoonsgegevens moet worden voldaan aan alle hierna genoemde beginselen om AVG-proof te zijn. Deze worden kort aangestipt om vervolgens stapsgewijs in een stroomschema terug te komen. De beginselen worden genoemd in artikel 5 AVG waarvan het rechtmatigheidsbeginsel (artikel 5 lid 1 sub a) verder wordt uitgewerkt in artikel 6 AVG. Zoals eerder aangegeven heeft deze module de bedoeling om het wettelijk kader uit te leggen. In module 3 zijn de AVG-beginselen vanuit organisatieperspectief beschreven.

Beginsel van rechtmatigheid, behoorlijkheid en transparantie (artikel 5 lid 1 sub a AVG)

De betrokkene (de persoon) dient te weten dat zijn persoonsgegevens worden verwerkt en dat dit netjes gebeurt. Er is sprake van een rechtmatige verwerking in de zin van de AVG als aan één van hieronder staande voorwaarden is voldaan.

a. de betrokkene heeft toestemming gegeven voor de gegevensverwerking;
b. de verwerking is noodzakelijk voor de uitvoering van een overeenkomst of precontractuele maatregelen;
c. de verwerking is noodzakelijk om te voldoen aan een wettelijke verplichting;
d. de verwerking is noodzakelijk voor de bescherming van vitale belangen van de betrokkene of van iemand anders;
e. de verwerking is noodzakelijk voor de vervulling van een taak van algemeen belang;
f. de verwerking is noodzakelijk voor de behartiging van het gerechtvaardigd belang van de verwerkingsverantwoordelijke of het gerechtvaardigd belang van een derde, behalve wanneer de belangen of grondrechten en fundamentele vrijheden van de betrokkene zwaarder wegen.

Onderdeel b t/m f zijn noodzakelijkheidsvereisten.
Er moet bij deze grondslagen sprake zijn van een noodzaak tot het verwerken van persoonsgegevens. Dit betekent dat bij deze grondslagen, als extra waarborg, nog voldaan moet zijn aan het proportionaliteits- en subsidiariteitsbeginsel. Het proportionaliteitsbeginsel: kan met de gegevensverwerking het doel worden bereikt, staat het doel in verhouding tot verwerking van persoonsgegevens?
Subsidiariteitsbeginsel: kan het doel op een andere manier worden bereikt die minder of geen inbreuk maakt op de privacy?

Behoorlijkheid betekent dat er moet 'netjes' worden omgegaan met de persoonsgegevens binnen de zorgorganisatie. Dit heeft enerzijds betrekking op het nemen van beveiligingsmaatregelen en anderzijds op organisatorische en cultuurkenmerken van het omgaan met gegevens.

< Terug naar de inhoudsopgave

Transparantie → informatieverplichting (artikel 12, 13 en 14 AVG).
Organisaties zijn verplicht informatie te geven aan personen van wie zij persoonsgegevens gebruiken. Zij moeten deze personen informeren welke gegevens zij gebruiken en met welk doel. Informatie en communicatie in verband met de verwerking van die persoonsgegevens moet eenvoudig toegankelijk en begrijpelijk zijn en er moet duidelijke en eenvoudige taal worden gebruikt. Aan de informatieplicht wordt veelal invulling gegeven door gebruik te maken van een privacyreglement of statement. De VGN heeft hiervoor een model privacyreglement ontwikkeld.

Beginsel van doelbinding (artikel 5 lid 1 sub b AVG)
Er moet sprake zijn van één of meer duidelijk bepaalde, uitdrukkelijk omschreven en gerechtvaardigde doeleinden voor het verwerken van de persoonsgegevens.

Beginsel van minimale gegevensverwerking/dataminimalisatie (artikel 5 lid 1 sub c AVG)
De persoonsgegevens moeten toereikend, ter zake dienend en beperkt zijn tot wat noodzakelijk is om de doel(einden) te bereiken.

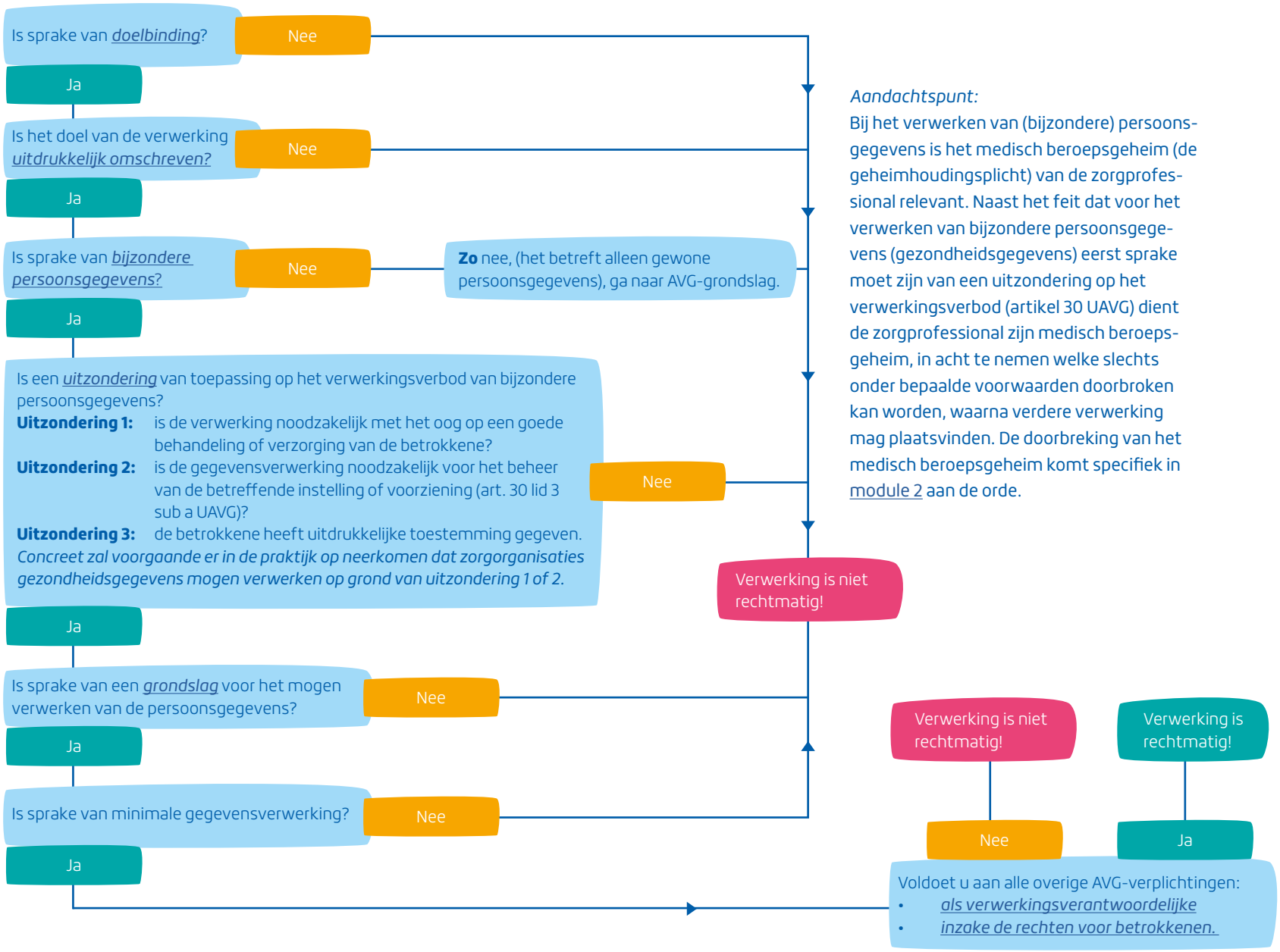
Beginsel van juistheid (artikel 5 lid 1 sub d AVG)
Alle redelijke maatregelen moeten worden genomen om ervoor te zorgen dat onjuiste persoonsgegevens worden gerectificeerd of gewist.

Beginsel van opslagbeperking (artikel 5 lid 1 sub e AVG)
Gegevens mogen niet langer bewaard worden dan noodzakelijk, er moeten termijnen worden bepaald voor het wissen van gegevens of periodieke toetsing daarvan.

Beginsel van integriteit en vertrouwelijkheid (artikel 5 lid 1 sub f AVG)
Persoonsgegevens moeten worden verwerkt op een manier die een passende beveiliging en vertrouwelijkheid van die gegevens waarborgt, ook ter voorkoming van ongeoorloofde toegang tot of het ongeoorloofde gebruik van persoonsgegevens en de apparatuur die voor de verwerking wordt gebruikt.

Tot slot: verantwoordingsplicht ten aanzien van deze beginselen (artikel 5 lid 2 AVG)
De organisatie (de verwerkingsverantwoordelijke) moet kunnen aantonen dat de hierboven genoemde beginselen worden nageleefd. Dit betekent dat de organisatie beleid opstelt om de naleving te borgen in de organisatie en in het geval verwerkers worden ingeschakeld aan hen verplichtingen worden opgelegd dat de naleving ook in relatie tot de verwerkers is geborgd.

< Terug naar de inhoudsopgave



Aandachtspunt:
Bij het verwerken van (bijzondere) persoonsgegevens is het medisch beroepsgeheim (de geheimhoudingsplicht) van de zorgprofessional relevant. Naast het feit dat voor het verwerken van bijzondere persoonsgegevens (gezondheidsgegevens) eerst sprake moet zijn van een uitzondering op het verwerkingsverbod (artikel 30 UAVG) dient de zorgprofessional zijn medisch beroepsgeheim, in acht te nemen welke slechts onder bepaalde voorwaarden doorbroken kan worden, waarna verdere verwerking mag plaatsvinden. De doorbreking van het medisch beroepsgeheim komt specifiek in module 2 aan de orde.

< Terug naar de inhoudsopgave

B4 WANNEER VERWERK IK PERSOONSGEGEVENS RECHTMATIG?

De gegevensverwerking moet rechtmatig zijn, dit is als beginsel opgenomen in artikel 5 lid 1 sub a AVG. Er is sprake van een rechtmatige gegevensverwerking als voldaan is aan minimaal één van de genoemde voorwaarden in artikel 6 AVG.

In de praktijk ook vaak terugkomend als de vraag: welke grondslag is van toepassing? Dat is dan ook de reden dat hierna over grondslagen wordt gesproken en niet over voorwaarden.

Grondslag 1 De betrokkene heeft ondubbelzinnige toestemming (artikel 4 onderdeel 11 AVG) gegeven voor de gegevensverwerking.

Gewone persoonsgegevens: ondubbelzinnige toestemming

Toestemming moet worden gegeven door een duidelijke actieve handeling. Bijvoorbeeld via een schriftelijke verklaring, met elektronische middelen (zoals het online plaatsen van vinkje in een vakje) of een mondelinge verklaring.
Ongeacht de gekozen methode dient altijd te duidelijk blijken dat de betrokkene vrijelijk, specifiek, geïnformeerd en ondubbelzinnig met de verwerking van zijn persoonsgegevens heeft ingestemd.

Gezondheidsgegevens: strenger toestemmingsvereiste → uitdrukkelijke toestemming

Indien toestemming dient te worden gevraagd in het kader van de verwerking van bijzondere persoonsgegevens, waaronder gezondheidsgegevens, dan moet sprake zijn van toestemming die uitdrukkelijk moet worden gegeven (artikel 9 AVG en artikel 22 UAVG).
Waar het geven van toestemming voor de verwerking van gewone persoonsgegevens kan worden afgeleid uit een handeling, een activiteit moet deze gegeven toestemming bij gezondheidsgegevens heel duidelijk, zonder twijfel, blijken uit woord, schrift of gedrag.

Uitdrukkelijk heeft betrekking op de manier waarop de toestemming tot uitdrukking wordt gebracht. Er moet sprake zijn van een uitdrukkelijke verklaring van toestemming. Een schriftelijke verklaring ligt dan voor de hand, maar dat hoeft niet.[13]

Zie ook vraag 7 in module 2.

13 In de digitale of online context bijvoorbeeld kan een betrokkene de vereiste verklaring verstrekken door het invullen van een elektronisch formulier, door het versturen van een e-mail, door het uploaden van een gescand document waarop de handtekening van de betrokkene staat, of door middel van een elektronische handtekening. In theorie kan het gebruik van mondelinge verklaring ook voldoende zijn om geldige uitdrukkelijke toestemming te verkrijgen, het kan echter voor de verwerkingsverantwoordelijke moeilijk te bewijzen zijn dat bij het opnemen van de verklaring voldaan is aan alle voorwaarden voor geldige uitdrukkelijke toestemming. (Groep gegevensbescherming artikel 29, Richtsnoeren inzake toestemming overeenkomstig Verordening 2016/679, pagina 21).

< Terug naar de inhoudsopgave

Grondslag 2 De verwerking is noodzakelijk voor de uitvoering van een overeenkomst of precontractuele maatregelen daaraan voorafgaand.

In het kader van de zorg- en dienstverleningsovereenkomst zal gegevensuitwisseling plaatsvinden die daarvoor noodzakelijk is. Bijvoorbeeld het delen van informatie uit het ondersteuningsplan tussen collega's in de zorgorganisatie in het belang van de zorg- en dienstverlening aan de cliënt. (Zie meer hierover module 2).

Gegevensuitwisseling zal voorafgaand aan het sluiten van deze overeenkomst ook al vaak essentieel zijn. Bijvoorbeeld om te bepalen of de zorgorganisatie kan voldoen aan de zorgvraag van de toekomstige cliënt. Ook in deze situatie is onderhavige grondslag van toepassing.

Grondslag 3 De verwerking is noodzakelijk om te voldoen aan een wettelijke verplichting waaraan de verwerkingsverantwoordelijke moet voldoen.

Hier kan onder meer gedacht worden aan de dossierplicht die is neergelegd in diverse wetten voor het aanleggen van een cliëntdossier. Zoals in de Wgbo, de Wlz en de Jeugdwet.
Een andere wettelijke verplichting is dat het BSN van een cliënt mag worden uitgewisseld met andere organisaties. Maar let op: het BSN mag alleen voor de doeleinden genoemd in de wet worden verwerkt.

Aandachtspunt 1
Soms staat niet expliciet in een wet dat een organisatie verplicht is om persoonsgegevens te verwerken. De verwerking van persoonsgegevens kan ook zijn basis vinden in een ruimer geformuleerde wettelijke zorgplicht. In dat geval is het aan de organisatie (de verwerkingsverantwoordelijke) om goed te bepalen of de verwerking echt noodzakelijk is om aan de (impliciete) wettelijke verplichting te voldoen. Bij deze beoordeling heeft de verwerkingsverantwoordelijke een grote eigen verantwoordelijkheid.

Grondslag 4 De verwerking is noodzakelijk voor de bescherming van vitale belangen van de betrokkene of van iemand anders.

Denk hier aan de situatie dat iemand onwel is geworden waarop direct medisch handelen noodzakelijk is en daarvoor in het cliëntdossier gekeken moet worden. Er kan niet gewacht worden totdat de betrokkene (cliënt) of iemand anders ((wettelijk) vertegenwoordiger) over deze inzage een beslissing kan nemen.

< Terug naar de inhoudsopgave

Grondslag 5 De verwerking is noodzakelijk voor de vervulling van een taak van algemeen belang of van een taak in het kader van de uitoefening van het openbaar gezag.

Hier gaat het om een publieke taak van de overheid (overheden) die expliciet kan zijn neergelegd in een wet of kan worden afgeleid uit een samenstel van wettelijke regels. Voor het uitvoeren van deze publieke taak hoeft niet altijd sprake te zijn van een bestuursorgaan, dit mogen ook andere organisaties zijn mits dit uit wetgeving blijkt. De wetten in het sociaal domein zijn hier een voorbeeld van. In artikel 2.6.4. Wmo 2015 en artikel 2.11 Jeugdwet is bepaald dat gemeenten de uitvoering van hun taken mogen uitbesteden aan derden. Dit betekent dat deze derden vervolgens op grond van deze bepalingen persoonsgegevens mogen verwerken.

Een ander voorbeeld bij deze grondslag betreft het verkrijgen van onderzoeksgegevens van zorgorganisaties door IGJ in het kader van een calamiteitenonderzoek (artikel 11 lid 2 Wkkgz en artikel 8.6 en 8.19 Uitvoeringsbesluit Wkkgz).

Grondslag 6 De verwerking is noodzakelijk voor de behartiging van het gerechtvaardigd belang van een organisatie of van een derde. De uitwisseling mag niet plaatsvinden als de belangen van de betrokkene zwaarder wegen.

Voor een beroep op gerechtvaardigd belang voor het mogen verwerken van persoonsgegevens moet zijn voldaan aan de volgende drie criteria:

1. sprake zijn van een gerechtvaardigd belang. Het belang moet rechtmatig, duidelijk verwoord en ook echt aanwezig zijn. Een voorbeeld is gegevensverwerking welke aantoonbaar noodzakelijk is om bedrijfsactiviteiten te kunnen verrichten, zoals een personeels- en cliëntenadministratie in een zorgorganisatie.
2. Er moet een afweging worden gemaakt tussen de belangen van de verwerkingsverantwoordelijke en de betrokkene. Als de belangen van de betrokkene zwaarder wegen dan het belang van de verwerkingsverantwoordelijke is een beroep op gerechtvaardigd belang niet mogelijk. Kan er na deze belangenafweging wél een beroep op gerechtvaardigd belang worden gedaan dan moeten er door de verwerkingsverantwoordelijke maatregelen worden getroffen die ervoor zorgen dat de rechten en vrijheden van betrokkene niet worden beperkt. Een maatregel is om gegevens niet langer te bewaren dan voor het doel noodzakelijk is.
3. De verwerking moet worden getoetst aan de proportionaliteit en subsidiariteit. (Zie het onderdeel hierna).

< Terug naar de inhoudsopgave

Toets op proportionaliteit en subsidiariteit vereist bij beroep op grondslag 2 t/m 6.

Als een beroep kan worden gedaan op een van de grondslagen genoemd in 2 t/m 6 dan dient vervolgens de vraag te worden beantwoord of de gegevensverwerking voldoet aan het proportionaliteits- én subsidiariteitsbeginsel.

Proportionaliteitsvereiste
Wordt met de verstrekking van de gegevens het gestelde doel bereikt? Staat dit doel in verhouding met het feit dat daarvoor persoonsgegevens moeten worden verwerkt? Om tot gegevensverwerking te mogen overgaan dient hier het noodzakelijke antwoord ja te zijn.

Subsidiariteitsvereiste
Kan het doel van het verstrekken van de gegevens ook op een andere manier worden bereikt die minder/geen inbreuk maakt op de privacy?
Om tot gegevensverwerking te mogen overgaan dient hier het noodzakelijke antwoord nee te zijn.

Aandachtspunt
Het is van belang de grondslag te kiezen die het meest geschikt is. Dit brengt enerzijds met zich mee dat dus niet overal toestemming voor hoeft te worden gevraagd (in geval van toepasbaarheid van een andere grondslag) maar anderzijds ook dat als om toestemming is gevraagd en deze wordt ingetrokken niet alsnog een beroep kan worden gedaan op de grondslag gerechtvaardigd belang als terugvalmogelijkheid.

Aandachtspunt: medisch beroepsgeheim
Een belangrijk aandachtspunt is dat bij het verwerken van bijzondere persoonsgegevens het medisch beroepsgeheim (de geheimhoudingsplicht) van de zorgprofessional relevant is. Dit medisch beroepsgeheim kan slechts onder bepaalde voorwaarden worden doorbroken, waarna verdere verwerking van persoonsgegevens mag plaatsvinden. De doorbreking van het medisch beroepsgeheim komt specifiek in module 2 aan de orde.

< Terug naar de inhoudsopgave

B5 DOORGIFTE VAN PERSOONSGEGEVENS NAAR DERDE LAND (NIET EU) STROOMSCHEMA III.

Binnen de Europese Unie kunnen persoonsgegevens vrij circuleren, mits de AVG-verplichtingen worden nageleefd. De AVG kent specifieke voorwaarden als sprake is van een doorgifte naar zogenaamde derde landen[14] en internationale organisaties. De bedoeling hiervan is dat het beschermingsniveau van de betrokkene door deze doorgifte niet wordt ondermijnd. In deze handreiking wordt bij dit item stilgestaan om een totaalbeeld te schetsen en met het oog op het vertrek van het Verenigd Koninkrijk uit de EU ("Brexit").

Het is toegestaan persoonsgegevens vanuit de EU (Nederland) aan een derde land te verstrekken, maar alleen als dat land voldoende bescherming, waarborgen biedt voor de betrokkene. Een doorgifte mag plaatsvinden op grond van:

1. Een adequaatheidsbesluit. Dit is een besluit dat wordt genomen door de Europese Commissie (artikel 45 AVG). De Europese Commissie beslist of in dat land sprake is van een vergelijkbaar niveau als de AVG.
   Het EU-VS privacyshield is zo'n adequaatheidsbeslissing. Met hier het verschil dat deze adequaatheidsbeslissing alleen geldt als het ontvangende bedrijf in de V.S. zich heeft gecertificeerd en zich houdt aan de principes in het privacyshield.
2. Een modelcontractbepaling die door de Europese Commissie is vastgesteld (artikel 46 lid 2 onder c AVG).
3. Goedgekeurde gedragscode (artikel 46 lid 2 sub e AVG) of via een certificeringsmechanisme (artikel 46 lid 2 sub f AVG).
4. Bindende bedrijfsvoorschriften. Dit zijn voorschriften die gelden binnen internationale organisaties (met vestigingen in derde landen). Binnen het concern moet men zich houden aan het privacybeleid.

Is het niet mogelijk een beroep te doen op een van deze waarborgen dan is doorgifte mogelijk op basis van specifieke uitzonderingen (artikel 49 AVG):

- De verwerkingsverantwoordelijke heeft de uitdrukkelijke toestemming van de betrokkene gekregen. Daarbij hoort ook de informatieplicht. De betrokkene moet worden ingelicht over deze doorgifte en wat daarvan de bedoeling is en welke beschermingsniveau in het desbetreffende derde land geldt. Let op: er is echt toestemming nodig. Het is onvoldoende als de betrokkene geen bewaar heeft gemaakt tegen doorgifte.
- De doorgifte is noodzakelijk voor de uitvoering van een overeenkomst tussen de betrokkene en de verwerkingsverant-

14 Derde landen zijn alle landen buiten de EU, met uitzondering van de landen in de Europese Economische Ruimte (EER). Dit zijn Noorwegen, Liechtenstein en IJsland. Deze drie landen kennen een gelijkwaardig niveau van bescherming van persoonsgegevens.

< Terug naar de inhoudsopgave

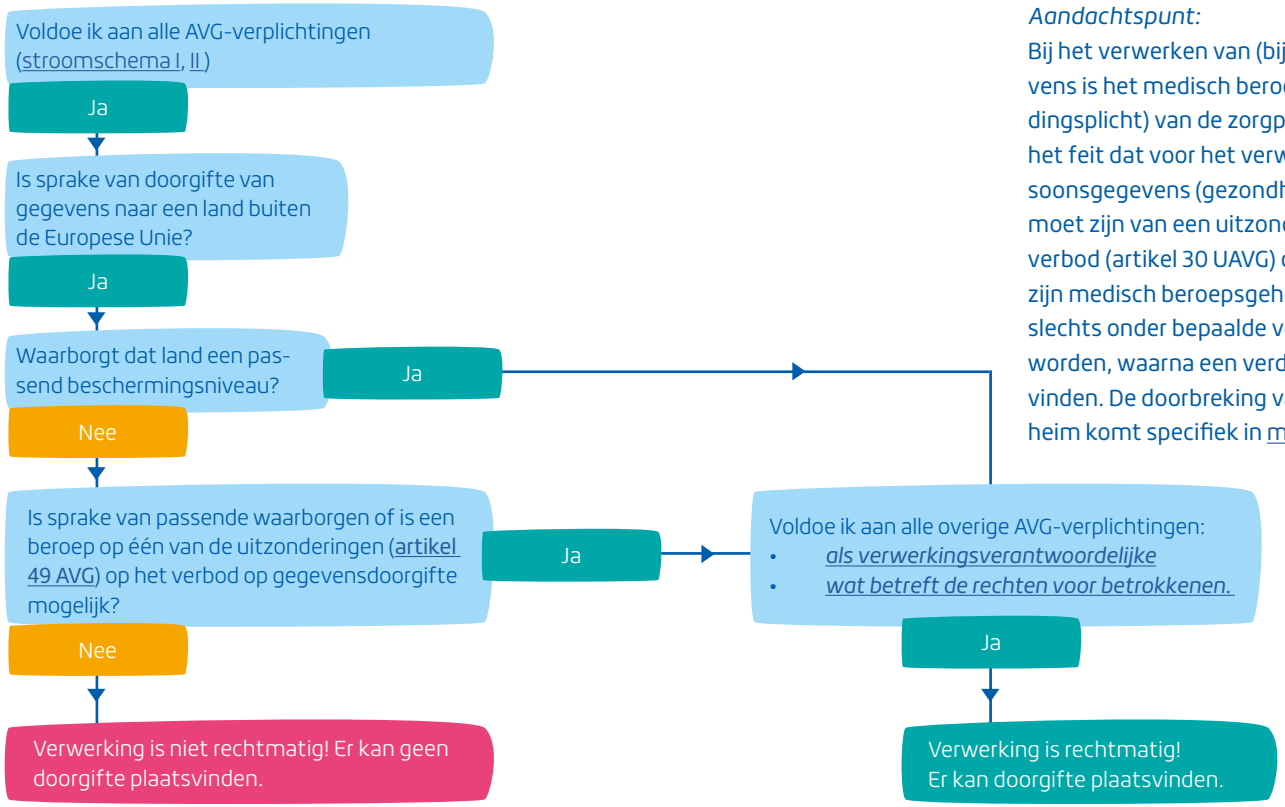
woordelijke of voor de uitvoering van op verzoek van de betrokkene genomen precontractuele maatregelen.
Bijvoorbeeld het reserveren van een vliegticket of het huren van een auto in het buitenland.

- De doorgifte is noodzakelijk voor de sluiting of de uitvoering van een overeenkomst in het belang van de betrokkene tussen de verwerkingsverantwoordelijke en een andere natuurlijke of rechtspersoon.
  Bijvoorbeeld: De herverzekering van een door de betrokkene in Nederland afgesloten verzekering bij een verzekeringsmaatschappij in een derde land.
- De doorgifte is noodzakelijk wegens gewichtige redenen van algemeen belang.
- De doorgifte is noodzakelijk voor de instelling, uitoefening of onderbouwing van een rechtsvordering.
  Bijvoorbeeld de doorgifte van persoonsgegevens aan een incassobureau in een derde land voorafgaand aan een mogelijke gerechtelijke procedure.
- De doorgifte is van vitaal belang voor de betrokkene of van andere personen, indien de betrokkene lichamelijk of juridisch niet in staat is zijn toestemming te geven. Bijvoorbeeld wanneer de betrokkene in het buitenland in het ziekenhuis terecht is gekomen. Het is dan noodzakelijk dat de zorgorganisatie de persoonsgegevens van de betrokkene zo snel mogelijk aan het ziekenhuis verstrekt.
- De doorgifte is verricht vanuit een bij wet ingesteld register dat bedoeld is om het publiek voor te lichten. Een voorbeeld is gegevens uit het Kadaster of Handelsregisters. Bron: Autoriteit Persoonsgegevens.

Concluderend voor de zorgorganisatie

Bezien vanuit de zorgorganisatie is het voorstelbaar dat persoonsgegevens worden verstrekt in het kader van een vitaal belang in het geval een cliënt met vakantie is en in het buitenland iets overkomt.

< Terug naar de inhoudsopgave



Aandachtspunt:
Bij het verwerken van (bijzondere) persoonsgegevens is het medisch beroepsgeheim (de geheimhoudingsplicht) van de zorgprofessional relevant. Naast het feit dat voor het verwerken van bijzondere persoonsgegevens (gezondheidsgegevens) eerst sprake moet zijn van een uitzondering op het verwerkingsverbod (artikel 30 UAVG) dient de zorgprofessional zijn medisch beroepsgeheim, in acht te nemen welke slechts onder bepaalde voorwaarden doorbroken kan worden, waarna een verdere verwerking mag plaatsvinden. De doorbreking van het medisch beroepsgeheim komt specifiek in module 2 aan de orde.

Bijlagen

Bijlage 1 Gegevensuitwisseling met andere organisaties

Inleiding en toelichting op het schema:
Deze bijlage bevat een overzicht van de belangrijkste uitwisselmomenten tussen zorgaanbieders en andere organisaties (niet zijnde zorgaanbieders/zorgorganisaties). Denk onder andere aan het verstrekken van (bijzondere) persoonsgegevens aan gemeentes, het CAK, zorgkantoren en zorgverzekeraars. Deze uitwisselmomenten kennen een wettelijke grondslag in de zin van artikel 6 lid 1 sub c en artikel 9 lid 2 sub a AVG. Dit betekent dat de verzochte (bijzondere) persoonsgegevens zonder toestemming van de betrokkene kunnen worden verstrekt. Een enkele keer wordt in dit schema wel gewezen op vereiste toestemming van de betrokkene gezien de gevoeligheid van de gegevens in relatie tot het doel waarvoor ze worden opgevraagd. Deze toestemming volgt dan uit de wettelijke bepaling.

In het schema zijn bepalingen uit de volgende wetten verwerkt: Wmo 2015, Wlz, Jw, Wlz, Zvw, Wmg, Wkkgz en het Burgerlijk Wetboek (Boek 1), ook lagere regelgeving is expliciet dan wel via een doorklik opgenomen. Het schema is niet uitputtend.

Tussen de wetten zijn er verschillen te bespeuren, waar in de ene wet duidelijk wordt aangegeven welke (bijzondere) persoonsgegevens moeten worden verstrekt, beschrijft een andere wet dit algemener bijvoorbeeld als: “persoonsgegevens, waaronder gezondheidsgegevens, noodzakelijk voor het uitvoeren van de doelen die in artikel (..) van deze wet staan” of dat de zorgaanbieder/zorgorganisatie “inlichtingen” dient te verstrekken waarbij die inlichtingen niet verder worden gespecificeerd.

Het blijft daarom van belang, ook tijdens het raadplegen van het schema, een eigen afweging te maken op grond van de beginselen van de AVG of tot verstrekking van de (bijzondere) persoonsgegevens kan worden overgegaan. Temeer een wettelijke grondslag niet altijd expliciet in een wet hoeft te staan maar ook kan voortvloeien uit de strekking van de wet (een ruimer geformuleerde wettelijke zorgplicht). De verwerkingsverantwoordelijke heeft dan een grotere eigen verantwoordelijkheid bij het beoordelen van de noodzakelijkheid van de gegevensverwerking bij het voldoen aan de wettelijke verplichting.

Beleidsregels zoals die onder andere door de NZa worden opgesteld zijn maken geen onderdeel uit van dit schema. In deze beleidsregels kunnen ook bepalingen staan over het gebruik van persoonsgegevens.

	Vragende, ontvangende organisatie	Gegevens	Doel	Wanneer	Toestemming	Verstrekken door
Art. 5.2.2	**Gemeente** **CAK** **SVB** **Toezichthoudende ambtenaren**	Persoonsgegevens, waaronder gezondheidsgegevens.	De persoonsgegevens voor zover noodzakelijk voor het uitvoeren van de doelen die in artikel 5.2.2 voor de gemeente, CAK, SVB en toezichthoudende ambtenaren worden genoemd: • verantwoording t.a.v. de maatwerkvoorziening • het innen van bijdragen • het verrichten van betalingen • of houden van toezicht.	Desgevraagd of uit eigen beweging.	Geen toestemming vereist.	Zorgaanbieder die maatwerkvoorziening aanbiedt.
Art. 5.2.5	**Gemeente**	Persoonsgegevens, waaronder gezondheidsgegevens.	Persoonsgegevens voor zover deze noodzakelijk zijn voor het toekennen van een (aanvullende) maatwerkvoorziening in het geval de persoon zorg ontvangt/heeft ontvangen op grond van Zvw en aanvullende of daarop aansluitende maatwerkvoorziening nodig heeft.	Desgevraagd of uit eigen beweging.	Uitdrukkelijke toestemming vereist.	Zorgaanbieder zoals bedoeld in de Zorgverzekeringswet.

	Vragende, ontvangende organisatie	Gegevens	Doel	Wanneer	Toestemming	Verstrekken door
Art. 5.2.6	**AMHK**	Inlichtingen[1].	Noodzakelijk om een situatie van huiselijk geweld of kindermishandeling te beëindigen of een redelijk vermoeden daarvan te onderzoeken.	Desgevraagd of uit eigen beweging.	Geen toestemming van cliënt vereist.	Derden die beroepshalve beschikken over inlichtingen. Zorgaanbieders en/of individuele zorgverleners.
Art. 5.3.6	**Een ander: denk aan onderzoeksinstituten, universiteiten etc.**	Inlichtingen [2] over de betrokkene of inzage in dossier.	Ten behoeve van statistiek of wetenschappelijk onderzoek op het gebied van de volksgezondheid, opgroei- en opvoedingsproblemen, psychische problemen en stoornissen, kinderbescherming of jeugdreclassering mits: a. onderzoek algemeen belang dient; b. onderzoek niet zonder die gegevens kan worden uitgevoerd; c. de betrokkene tegen verstrekking geen uitdrukkelijk bezwaar heeft gemaakt.	Desgevraagd.	Geen toestemming is vereist: • dit in redelijkheid niet mogelijk is en waarborgen zijn getroffen om schade aan de persoonlijke levenssfeer te voorkomen; • dit in redelijkheid niet kan worden verlangd en de verstrekte gegevens zodanig zijn verwerkt dat herleiding tot een individu redelijkerwijs wordt voorkomen. *Let op: als bovenstaande punten niet aan de orde zijn, dient om uitdrukkelijke toestemming te worden verzocht.*	Aanbieder (en college, derde, CAK of andere instantie, SVB, toezichthoudende ambtenaren, AMHK).

[1] De wetgever heeft niet nader geduid wat verstaan wordt onder Inlichtingen en welke (persoons)gegevens daartoe kunnen behoren.
[2] Idem.

Wmo 2015 Wettelijke grondslag (3/3)

	Vragende, ontvangende organisatie	Gegevens	Doel	Wanneer	Toestemming	Verstrekken door
Art. 5.4.1	**Zorgverzekeraars** *Aandachtspunt:* Wmo 2015 spreekt over zorgverzekeraars in de zin van de Zvw en daarmee worden ook de zorgkantoren bedoeld.	Gegevens zijnde geen persoonsgegevens. Het betreft geaggregeerde gegevens relevant voor het te voeren beleid en voor de uitvoering van beleid (zoals inkoop).[3]	Noodzakelijk zijn voor het vervullen van de wettelijke taken van gemeenten op grond van de Wmo 2015 en zorgverzekeraars op grond van de Zvw.	Desgevraagd of uit eigen beweging.	Geen toestemming.	Aanbieder.
Art. 3.4 Onverwijld melden calamiteit en geweld bij verstrekking van de voorziening	**Toezichthoudende ambtenaar**	Alle gegevens inclusief: persoonsgegevens, gezondheidsgegevens en andere bijzondere categorieën van persoonsgegevens en persoonsgegevens van strafrechtelijke aard.	Noodzakelijk voor het onderzoeken van de melding.	Uit eigen beweging.	Persoonsgegevens vallend onder geheimhoudingsplicht kunnen niet zonder toestemming van cliënt worden verstrekt. *Behalve* als cliënt hiertoe niet in staat is of dit noodzakelijk kan worden geacht ter bescherming van cliënten.	Aanbieder.
De financiële verantwoording door aanbieders wordt nader geregeld via de gemeentelijke verordeningen. Voor de volledigheid wordt gewezen op het Landelijk accountsprotocol Wmo 2015 en Jeugdwet[4] wat betreft de productieverantwoording.						

[3] Wmo 2015, Memorie van Toelichting, Tweede Kamer, vergaderjaar 2013–2014, 33 841, nr. 3, pagina 185.
[4] Let op: wordt jaarlijks opgesteld.

	Vragende, ontvangende organisatie	Gegevens	Doel	Wanneer	Toestemming	Verstrekken door
Art. 7.4.0 lid 1 en 2	**Gemeente**	Persoonsgegevens van jeugdige/ouders: • BSN van jeugdige • bijzondere categorieën persoonsgegevens (waaronder gezondheidsgegevens) • persoonsgegevens van strafrechtelijke aard. *Hierbij mag in beginsel door de opvragende instantie geen diagnose informatie of om een behandelplan worden verzocht.*	Noodzakelijk voor: a. de toeleiding naar, advisering over, bepaling van of het inzetten van een voorziening op het gebied van de jeugdhulp; b. het doen van verzoek tot onderzoek bij de raad voor de kinderbescherming of uitvoering van kinderbeschermings-maatregelen of jeugdreclassering; c. de bekostiging van preventie, jeugdhulp, kinderbeschermingsmaatregelen-jeugdreclassering of werkzaamheden m.b.t. gesloten jeugdhulpverlening; d. het verrichten van controle of fraudeonderzoek.	Desgevraagd of uit eigen beweging.	Geen toestemming vereist. *Let op: alleen die bijzondere gegevens die noodzakelijk zijn (lid 2).*	Jeugdhulpaanbieder.
Artikel 7.1.4.1 in relatie tot artikel 7.1.2.1, 7.1.4.2, 7.1.4.4, 7.2.5 Jeugdwet en artikel 7.3.1 Besluit Jeugdwet	**Verwijsindex risico jongeren**	Van jeugdige: BSN Heeft jeugdige geen BSN dan alle hierna genoemde persoonsgegevens: a. de familienaam b. de geboortedatum c. het geslacht.	Bij een redelijk vermoeden van de risico's die betrekking hebben op ontwikkelingsachterstand en opvoedingsproblemen (nader gedefinieerd in artikel 7.1.4.1).	Eigen beweging.	Geen toestemming vereist en zo nodig met doorbreking van de op grond van zijn ambt of beroep geldende plicht tot geheimhouding.	Meldingsbevoegde.*

*Meldingsbevoegde: functionaris die werkzaam is voor een instantie in een of meer van de domeinen jeugdhulp, jeugdgezondheidszorg, gezondheidszorg, onderwijs, maatschappelijke ondersteuning, werk en inkomen, of politie en justitie en waarmee ter uitvoering van de verwijsindex afspraken zijn gemaakt met het college, en de functionaris als zodanig heeft aangewezen (interne medewerker).
*Meldingsbevoegde: functionaris die niet werkzaam is voor een instantie en die behoort tot een bij AMvB aangewezen categorie van functionarissen die werkzaam is in een of meer van de genoemde domeinen en hierover afspraken heeft gemaakt met het college (externe functionaris).

	Vragende, ontvangende organisatie	Gegevens	Doel	Wanneer	Toestemming	Verstrekken door
Art. 7.4.2, 7.4.3 en 7.4.4 in relatie tot art. 7.5.2 en 7.5.3 Besluit Jeugdwet	**Gemeente en Ministers**	Persoonsgegevens, bijzondere persoonsgegevens (waaronder gezondheidsgegevens), persoonsgegevens van strafrechtelijke aard en het BSN. Bij incidentele[5] verstrekking: geen persoonsgegevens Bij structurele verstrekking: klik hier welke persoonsgegevens het betreft (artikel 7.5.3. Besluit Jeugdwet).	Noodzakelijk voor: a. het doelmatig en doeltreffend functioneren van de toegang tot de jeugdhulp, de uitvoering van kinderbeschermings-maatregelen en jeugdreclassering; b.het doelmatig en doeltreffend functioneren van de aanbieders van preventie, de jeugdhulpaanbieders, gecertificeerde instellingen en van de raad voor de kinderbescherming; c. de doelmatigheid en doeltreffendheid van het aanbod van preventie, jeugdhulp en gecertificeerde instellingen, en d. het waarborgen van de stelselverantwoordelijkheid.	Desgevraagd of uit eigen beweging. Kan structureel of incidentieel van aard zijn.	Geen toestemming vereist.	Jeugdhulpaanbieders, aanbieders van preventie, gecertificeerde instellingen, Raad voor de kinderbescherming.

[5] Met betrekking tot artikel 7.4.2 (het verstrekken van gegevens aan het Rijk) kan verstrekking een structureel of incidenteel karakter hebben. Een structurele uitvraag betreft gegevens die het Rijk nodig heeft in verband met haar stelselverantwoordelijkheid, maar ook een incidentele uitvraag is mogelijk. De(ze) gegevens die de gemeente nodig heeft ten behoeve van beleidsvorming en toegang tot jeugdhulp en in verband met haar stelselverantwoordelijkheid worden in eerste instantie op het niveau van de jeugdhulpaanbieder, de gecertificeerde instellingen, waaronder het Nidos, en de raad voor de kinderbescherming verwerkt. Dit artikel legt daarom aan deze instellingen de verplichting op om deze gegevens te leveren aan gemeente en Rijk en biedt daarmee tevens de basis voor gemeente en Rijk om deze met dat doel op te mogen vragen. Jeugdhulpaanbieders en gecertificeerde instellingen zijn gehouden deze gegevens kosteloos ter beschikking te stellen. (Jeugdwet, Memorie van Toelichting, pagina 181 via www.rijksoverheid.nl).

Jeugdwet Wettelijke grondslag (3/4)

	Vragende, ontvangende organisatie	Gegevens	Doel	Wanneer	Toestemming	Verstrekken door
Art. 4.1.8 Onverwijld melding van iedere calamiteit en geweld	**Toezichthoudende ambtenaren**	Gegevens: persoonsgegevens, gegevens over de gezondheid, andere bijzondere persoonsgegevens en persoonsgegevens van strafrechtelijke aard.	Noodzakelijk voor het onderzoeken van de melding.	Uit eigen beweging.	Geen toestemming vereist.	Jeugdhulpaanbieder en gecertificeerde instelling.
Art. 4.2.2	**Toezichthoudende ambtenaren**	Bevindingen (naar aanleiding van klacht).[6]	Het attenderen op structureel ernstige risicovolle situaties die niet langer mogen voortduren.[7]	Uit eigen beweging.	Geen toestemming vereist.	Klachtencommissie.
Art. 7.3.11 lid 4	**Gecertificeerde instelling ondertoezichtstelling**	Inlichtingen[8] inzake feiten en omstandigheden die de persoon van een onder toezicht gestelde minderjarige, diens verzorging en opvoeding of de persoon van een ouder of voogd betreffen.	Noodzakelijk kunnen worden geacht voor de uitvoering van de ondertoezichtstelling.	Desgevraagd of uit eigen beweging.	Geen toestemming vereist en indien nodig met doorbreking van de plicht tot geheimhouding op grond van een wettelijk voorschrift of op grond van hun ambt of beroep.	Derden[9] die beroepshalve beschikken over inlichtingen. Jeugdhulpverlener.

6 "Bij de behandeling van klachten kan aan de oppervlakte komen dat het gaat om een structurele situatie. Wanneer de klachtencommissie tot het oordeel komt dat de klacht betrekking heeft op een structureel ernstige situatie die niet langer mag voortduren, dient de klachtencommissie de jeugdhulpaanbieder of de gecertificeerde instelling van haar bevindingen op de hoogte te stellen. Als blijkt dat het management niet voornemens is adequaat te reageren en geen maatregelen neemt om de ernstige situatie te beëindigen, moet de klachtencommissie de betreffende situatie melden aan de met het toezicht belaste ambtenaar". (Jeugdwet, Memorie van Toelichting, pagina 144 via www.rijksoverheid.nl). De wetgever heeft niet nader geduid welke bevindingen (gegevens) het betreft.

7 Problemen in de organisatie van het zorgproces of in de samenwerking tussen verschillende hulpverleners met ernstige gevolgen voor cliënten.

8 De wetgever heeft niet nader geduid welke gegevens (persoonsgegevens, bijzondere persoonsgegevens) dit kunnen betreffen.

9 Het college kan de uitvoering van de Jeugdwet door derden (private organisaties zoals zorgaanbieders) laten verrichten.

	Vragende, ontvangende organisatie	Gegevens	Doel	Wanneer	Toestemming	Verstrekken door
Art. 7.3.12	**Een ander: denk aan onderzoeksinstituten of universiteiten**	Inlichtingen[10] over de betrokkene of inzage in dossier.	Ten behoeve van statistiek of wetenschappelijk onderzoek op het gebied van de volksgezondheid, opgroei- en opvoedingsproblemen, psychische problemen en stoornissen, kinderbescherming of jeugdreclassering mits: a. onderzoek algemeen belang dient b. onderzoek niet zonder die gegevens kan worden uitgevoerd; c. de betrokkene tegen verstrekking geen uitdrukkelijk bezwaar heeft gemaakt.	Desgevraagd.	Geen toestemming vereist: a. als dit in redelijkheid niet mogelijk is en waarborgen zijn getroffen om schade aan de persoonlijke levenssfeer te voorkomen; b. als dit in redelijkheid niet kan worden verlangd en de verstrekte gegevens zodanig zijn verwerkt dat herleiding tot een individu wordt redelijkerwijs voorkomen.	Jeugdhulpverlening.

[10] In de Memorie van Toelichting wordt met betrekking tot dit artikel gesproken over het verstrekken van inlichtingen of dossiergegevens. Hiertoe behoren ook (bijzondere) persoonsgegevens. De Jeugdwet sluit aan bij zorgwetgeving waaronder de Wgbo. (Memorie van Toelichting, pagina 43 t/m 45, 250, via www.rijksoverheid.nl. In artikel 7:458 BW (Wgbo) is opgenomen dat bescheiden beschikbaar kunnen worden gesteld voor onder andere wetenschappelijk onderzoek. Onder bescheiden worden patiëntgegevens verstaan, waaronder ook bijzondere persoonsgegevens.

	Vragende, ontvangende organisatie	Gegevens	Doel	Wanneer	Toestemming	Verstrekken door
Art. 7.4.0 lid 1 sub d Jeugdwet Art. 1, 5e streepje Regeling Jeugdwet Art. 6a.1, 6a3 t/m 6a.5 Regeling Jeugdwet Art. 6a. 7 lid 1 Regeling Jeugdwet Handreiking materiële controle VNG[11]	**Gemeente**	Persoonsgegevens, waaronder bijzondere persoonsgegevens.[12] Art. 6a.1, 6a3 t/m 6a.5 Regeling Jeugdwet Art. 6a. 7 lid 1 Regeling Jeugdwet Gemeenten hebben voor de formele controle geen (delen van) jeugdhulpverleningsdossiers of hulpverleningsplannen nodig en mogen dus ook voor die reden niet	Niet meer persoonsgegevens dan noodzakelijk voor de formele controle en de betaling van de declaratie.	Desgevraagd Uit eigen beweging.	Geen toestemming vereist.	Jeugdhulpaanbieder.

[11] Handreiking opgesteld door VNG inzake materiële controle Jeugdwet (inclusief formele controle en detailcontrole).

[12] De Verzamelwet VWS 2016 heeft geleid tot opname van artikel 7.4.0 van de Jeugdwet, waarmee duidelijker is aangegeven dat gemeentes persoonsgegevens van jeugdige of zijn ouders mogen verwerken, noodzakelijk voor de uitvoering van de wet. Dit op advies van destijds het CBP (nu Autoriteit Persoonsgegevens) dat niet duidelijk was of aanbieders (bijzondere) persoonsgegevens mogen verstrekken in het kader van financiële afwikkeling en controle van declaraties. Artikel 7.4.0 regelt daarom ook dat aanbieders, als zij over deze gegevens beschikken, deze aan de gemeenten moeten verstrekken. Bij ministeriele regeling, de Regeling Jeugdwet, is dit nader uitgewerkt met daarin regels voor zover het gaat om formele controle, materiële controle en fraudeonderzoek. (Bron: Regeling Jeugdwet, Toelichting, paragraaf 2, Staatscourant 2016, 44178.)Bij ministeriele regeling, de Regeling Jeugdwet, is dit nader uitgewerkt met daarin regels voor zover het gaat om formele controle, materiële controle en fraudeonderzoek. (Bron: Regeling Jeugdwet, Toelichting, paragraaf 2, Staatscourant 2016, 44178.)12

	Vragende, ontvangende organisatie	Gegevens	Doel	Wanneer	Toestemming	Verstrekken door
Art. 7.4.0 lid1 sub d Jeugdwet Art. 1 sub 4, 4e streepje Regeling Jeugdwet Art. 6a.7 lid 2 Regeling Jeugdwet Art. 6b.1 lid 1, lid 3 6b.2 t/m 6b.6 Regeling Jeugdwet Handreiking materiële controle VNG Landelijk accountsprotocol Wmo 2015 en Jeugdwet[13]	**Gemeente**	Persoonsgegevens, waaronder bijzondere persoonsgegevens.[14] Art. 1 sub 4, 4e streepje Regeling Jeugdwet Art. 6a.7 lid 2 Regeling Jeugdwet.	Voor zover noodzakelijk voor materiële controle.	Desgevraagd.[15]	Geen toestemming vereist.	Jeugdhulpaanbieder.

[13] Let op: wordt jaarlijks opgesteld.

[14] Idem als voetnoot 12: betreft de grondslag voor het mogen verwerken door gemeente van (bijzondere) persoonsgegevens en het verstrekken daarvan door de jeugdhulpaanbieder. Voor wat betreft de materiële controle (en fraudeonderzoek) in de Jeugdwet is zoveel mogelijk aangesloten bij hetgeen dat daarover in hoofdstuk 7 van de Regeling Zorgverzekering is opgenomen. (Bron: Regeling Jeugdwet, Toelichting, paragraaf 3.4, Staatscourant 2016, 44178.)en fraudeonderzoek. (Bron: Regeling Jeugdwet, Toelichting, paragraaf 2, Staatscourant 2016, 44178.)

[15] Art. 6b.3 Regeling Jeugdwet brengt met zich mee dat de materiële controle door de gemeente zo mogelijk wordt verricht zonder het opvragen van nadere persoonsgegevens bij de aanbieders of inzien daarvan bij de aanbieders. (Bron: Regeling Jeugdwet, Toelichting, artikelsgewijze toelichting (art. 6b.3) Staatscourant 2016, 44178, Staatscourant 2016, 44178.)

	Vragende, ontvangende organisatie	Gegevens	Doel	Wanneer	Toestemming	Verstrekken door
Art. 7.4.0 lid1 sub d Jeugdwet Art. 1, 4e streepje, sub e 4e streepje Regeling Jeugdwet Art. 6b.3, Art. 6b.5 t/m 6b.7 Regeling Jeugdwet	**Gemeente**	Persoonsgegevens[16], waaronder bijzondere persoonsgegevens.	Voor zover noodzakelijk voor verrichten werkzaamheden die uit detailcontrole voortvloeien. [17]	Desgevraagd.	Toestemming vereist. In geval van detailcontrole geschiedt het verwerken van persoonsgegevens door of onder verantwoordelijkheid van persoon met medisch beroepsgeheim of geheimhoudingsplicht (uit hoofde diens beroep of artikel 88 Wet Big).	Jeugdhulpaanbieder.

[16] Zie voetnoot 12.
[17] Niet meer persoonsgegevens dan voor het onderzoeksdoel en omstandigheden van het te onderzoeken geval noodzakelijk is. Bron: Regeling Jeugdwet, Toelichting, artikelsgewijze toelichting (art. 6b.5 lid 3), Staatscourant 2016, 44178.)

	Vragende, ontvangende organisatie	Gegevens	Doel	Wanneer	Toestemming	Verstrekken door
Art. 9.1.2 lid 1	**Wlz-uitvoerders** **CAK** **CIZ**	Persoonsgegevens, waaronder gezondheidsgegevens (inzage of afschrift). Klik hier (artikel 7.1 Regeling langdurige zorg) welke gegevens worden aangemerkt als persoonsgegevens welke voor de WLZ-uitvoerders noodzakelijk zijn om uitvoering te geven aan de wet, wat dus betekent dat de WLZ-uitvoerder hierom kan vragen.	Noodzakelijk voor: a. het nemen van indicatiebesluiten en het onderzoek CIZ daarvoor verricht b. het sluiten van schriftelijke overeenkomsten met zorgaanbieders c. de zorgplichten waaronder het opmaken van wachtlijsten d. de beoordeling van Wlz-uitvoerder of de zorg op verantwoorde wijze kan worden verleend zonder dat de verzekerde verblijft in een instelling of met een persoonsgebonden budget e. de zorglevering f. het in rekening brengen van tarieven voor geleverde prestaties en het daartoe ontvangen en verrichten van betalingen of vergoedingen aan zorgaanbieders van de geleverde prestaties, of vergoeding van zorgkosten aan een verzekerde g. de vaststellingen de inning van eigen bijdragen door het CAK h. het namens een Wlz-uitvoerder of het Zorginstituut verrichten van betalingen door CAK aan zorgaanbieders i. het verrichten van controle of fraudeonderzoek door Wlz-uitvoerders j. het uitoefenen van verhaalsrecht.	Desgevraagd of uit eigen beweging.	Geen toestemming vereist.	Zorgaanbieders (CAK, CIZ, Wlz-uitvoerders).
Art. 9.1.2 lid 2	**CIZ**	Persoonsgegevens, waaronder gezondheidsgegevens die **niet**[18] onder de doeleinden van lid 1 vallen.		Desgevraagd of uit eigen beweging.	Uitdrukkelijke toestemming cliënt of diens (wettelijk) vertegenwoordiger.	Zorgaanbieders (en CIZ).

[18] Het gaat hier om gegevens die dus niet noodzakelijk zijn voor de uitvoering van de taken in lid 1 van artikel 9.1.2. Het gaat om de situatie dat een zorgaanbieder zo snel mogelijk een indicatiebesluit kan ontvangen, dat hij nodig heeft om de zorgverlening te kunnen aanvangen. Dit als de verzekerde al weet naar welke zorgverlener hij zou willen, hiermee wordt tijdsverlies vermeden. Deze situatie kon niet worden bestempeld als noodzakelijk ter uitvoering van de wet, daarom uitdrukkelijke toestemming (bron MvT Wlz.).

Wlz Wettelijke grondslag (2/2)

	Vragende, ontvangende organisatie	Gegevens	Doel	Wanneer	Toestemming	Verstrekken door
Art. 9.1.2 lid 4 [19]	**Zorgaanbieder CIZ**	Persoonsgegevens, waaronder gezondheidsgegevens.	Om te voldoen aan verplichtingen in artikel 9.1.2 lid 1, 2 en 3.	Desgevraagd of uit eigen beweging.	Geen toestemming vereist.	Personen werkzaam voor zorgaanbieder (of CIZ).

Wlz Formele controle

	Vragende, ontvangende organisatie	Gegevens	Doel	Wanneer	Toestemming	Verstrekken door
Art. 9.1.2 lid 1, sub i Wlz jo art. 7.2 sub b Regeling langdurige zorg (en in relatie tot artikel 4.2.2 lid 2 sub f Wlz.) Regeling Controle en administratie Wlz-uitvoerder[20]	**Wlz-uitvoerder**	Verstrekken, ter inzage leggen of afschrift ter beschikking stellen van de persoonsgegevens waaronder gezondheidsgegevens. Zie voor overzicht van persoonsgegevens genoemd in art. 7.1 tot en met sub j Rlz.	Noodzakelijk voor het verrichten formele controle.	Desgevraagd Uit eigen beweging.	Geen toestemming vereist.	Zorgaanbieders.

[19] Dit lid regelt de geheimhoudingsplicht voor bijvoorbeeld een arts-AVG of arts die het CIZ adviseert bij de indicatiestelling (Wlz, Memorie van Toelichting, pagina 153).
[20] Let op: wordt jaarlijks vastgesteld.

Wlz Materiële controle

	Vragende, ontvangende organisatie	Gegevens	Doel	Wanneer	Toestemming	Verstrekken door
Art. 9.1.2 lid 1, sub i Wlz jo art. 7.2 sub a Regeling langdurige zorg (en in relatie tot artikel 4.2.2 lid 2 sub f Wlz.) Regeling Controle en administratie Wlz-uitvoerder[21] Protocol materiële controle[22]	**Wlz-uitvoerder**	Verstrekken, ter inzage leggen of afschrift ter beschikking stellen van de persoonsgegevens waaronder gezondheidsgegevens. Zie voor overzicht van de persoonsgegevens art. 7.1 Rlz Let op: sub k biedt ruimte om nog om andere dan genoemde persoonsgegevens te vragen.	Noodzakelijk voor het verrichten materiële controle.	Desgevraagd.	Geen toestemming vereist.	Zorgaanbieders..

Wlz Detail controle

	Vragende, ontvangende organisatie	Gegevens	Doel	Wanneer	Toestemming	Verstrekken door
Art. 9.1.2 lid 1, sub i Wlz jo art. 7.2 sub c Regeling langdurige zorg (en in relatie tot artikel 4.2.2 lid 2 sub f Wlz.) Regeling Controle en administratie Wlz-uitvoerder[23] Protocol materiële controle [24]	**Wlz-uitvoerder**	Verstrekken, ter inzage leggen of afschrift ter beschikking stellen van de persoonsgegevens waaronder gezondheidsgegevens.	Noodzakelijk voor onderzoek door de Wlz-uitvoerder naar bij de zorgaanbieder *berustende* persoonsgegevens m.b.t. eigen verzekerden ten behoeve van materiële controle. Betreft het cliëntdossier.[25]	Desgevraagd.	Detailcontrole: 1. toestemming vereist; 2. toestemming niet nodig mits protocol materiële controle wordt gevolgd. *In alle gevallen geldt: inbreuk op persoonlijke levenssfeer moet zo beperkt mogelijk zijn. Alleen de gegevens die in verhouding staan tot het onderzoeksdoel mogen worden verstrekt (proportionaliteit en subsidiariteit).*	Zorgaanbieders.

[21] Let op: de Regeling Controle en administratie Wlz-uitvoerder wordt jaarlijks vastgesteld.
[22] Te downloaden via www.zn.nl
[23] Let op: de Regeling Controle en administratie Wlz-uitvoerder wordt jaarlijks vastgesteld.(Wlz, Memorie van Toelichting, pagina 153).
[24] Te downloaden via www.zn.nl
[25] De verwerking van persoonsgegevens in het kader van detailcontrole geschiedt onder de verantwoordelijkheid van een medisch adviseur (artikel 7.8 lid 2 Regeling langdurige zorg).

	Vragende, ontvangende organisatie	Gegevens	Doel	Wanneer	Toestemming	Verstrekken door
Artikel 87 lid 1 en 3 (zorg in natura)	**Zorgverzekeraars of een door de zorgverzekeraar aangewezen persoon**	Persoonsgegevens van de verzekerde, waaronder gegevens over gezondheid (inzage in of afschrift van). In de Regeling Zorgverzekering in hoofdstuk 7 is uitgewerkt welke persoonsgegevens de zorgverzekeraar nodig heeft voor de uitvoering van zijn wettelijke taak. Dit betekent dat deze persoonsgegevens bij de zorgaanbieder kunnen worden opgevraagd.	Noodzakelijk voor de uitvoering zorgverzekering of Zvw.	Desgevraagd of uit eigen beweging.	Geen toestemming vereist.	Zorgaanbieder.

Zvw Wettelijke grondslag (2/2)

	Vragende, ontvangende organisatie	Gegevens	Doel	Wanneer	Toestemming	Verstrekken door
Artikel 88 lid 1 jo. art. 86 lid 4 en lid 5 Zvw.	**Zorgverzekeraars of een door de zorgverzekeraar aangewezen persoon.** **Zorginstituut** **NZa** **Minister** **Belastingen** **UWV** **SVB** **College B&W** **CAK**	Alle inlichtingen en gegevens, waaronder persoonsgegevens (inzage in of afschrift van). Bij de gegevensuitwisseling wordt, voor zover die personen en instanties tot gebruik van dat nummer bevoegd zijn, het BSN of, bij het ontbreken daarvan, het sociaal-fiscaalnummer gebruikt (artikel 86 lid 4 en 5 Zvw).[26] In de Regeling Zorgverzekering in hoofdstuk 7 is uitgewerkt welke persoonsgegevens de zorgverzekeraar nodig heeft voor uitvoering van zijn wettelijke taak. Dit betekent dat deze persoonsgegevens bij de zorgaanbieder kunnen worden opgevraagd.	Noodzakelijk voor de uitvoering zorgverzekering of Zvw.	Desgevraagd.	Geen toestemming vereist.	Een ieder.

[26] De wettelijke grondslag voor gebruik van het BSN in het kader van de Zvw is opgenomen in de Wabvpz. Deze wet is van toepassing op zorgaanbieders welke zorg aanbieden ingevolge de Zvw en Wlz. De wettelijke grondslag voor het gebruik van het BSN voor aanbieders op het gebied van de Jeugdwet en Wmo 2015 is opgenomen in deze wetten.

Zvw Formele controle

	Vragende, ontvangende organisatie	Gegevens	Doel	Wanneer	Toestemming	Verstrekken door
Art. 87 Zvw Art. 7.1 lid 2 jo art. 1 sub t Regeling zorgverzekering Nadere regel controle en administratie zorgverzekeraars [27]	**Zorgverzekeraars**	Verstrekken, ter inzage of ter afschrift ter beschikking stellen van persoonsgegevens, waaronder gezondheidsgegevens. Art. 7.2 tot en met h Regeling zorgverzekering	Te gebruiken voor formele, materiële controle (detailcontrole)	Formele controle: Uit eigen beweging. Materiële controle: Uit eigen beweging of desgevraagd.	Geen toestemming.	Zorgaanbieders.

Zvw Materiële controle

	Vragende, ontvangende organisatie	Gegevens	Doel	Wanneer	Toestemming	Verstrekken door
Art. 87 Zvw Art. 7.1 lid 2 jo art. 1 sub u Regeling zorgverzekering Protocol materiële controle[28] Nadere regel controle en administratie zorgverzekeraars[29]	**Zorgverzekeraars**	Verstrekken, ter inzage of ter afschrift ter beschikking stellen van persoonsgegevens, waaronder gezondheidsgegevens. Art. 7.2 Regeling zorgverzekering *Let op sub i in artikel 7.2 Regeling zorgverzekering: overige gegevens die noodzakelijk zijn.*[30]	Te gebruiken voor materiële	Desgevraagd.	Geen toestemming.	Zorgaanbieders.

27 Let op: wordt regelmatig opnieuw vastgesteld.
28 Te downloaden via www.zn.nl.
29 Let op: wordt regelmatig opnieuw vastgesteld.
30 Dit is bewust in de Regeling Zorgverzekering om geen twijfel te laten bestaan dat er een wettelijke grondslag is voor het verstrekken van gegevens die bijvoorbeeld uit het medisch dossier komen en dus ook de verplichting bestaat om deze gegevens te verstrekken.

Zvw Detail controle

	Vragende, ontvangende organisatie	Gegevens	Doel	Wanneer	Toestemming	Verstrekken door
Art. 87 Zvw Art. 7.8 lid 1, 2, 3 jo art. 1 sub x Regeling zorgverzekering Art. 7.2 Regeling zorgverzekering Protocol materiële controle[31] Nadere regel controle en administratie zorgverzekeraars[32] Protocol materiële controle[33]	**Zorgverzekeraars**	Verstrekken, ter inzage of ter afschrift ter beschikking stellen van persoonsgegevens, waaronder gezondheidsgegevens. Art. 7.2 Regeling zorgverzekering	Noodzakelijk voor onderzoek door de zorgverzekeraar naar bij de zorgaanbieder berustende persoonsgegevens met betrekking tot eigen verzekerden ten behoeve van materiële controle.	Desgevraagd.	Detailcontrole[34]: 1. toestemming vereist of 2. zonder toestemming mits protocol materiële controle wordt gevolgd. In alle gevallen geldt: Inbreuk op persoonlijke levenssfeer moet zo beperkt mogelijk zijn. Alleen de gegevens die in verhouding staan tot het onderzoeksdoel mogen worden verstrekt (proportionaliteit en subsidiariteit).	Zorgaanbieders.

[31] Te downloaden via www.zn.nl.
[32] Let op: wordt regelmatig opnieuw vastgesteld.
[33] Te downloaden via www.zn.nl.
[34] Verwerking van persoonsgegevens onder verantwoordelijkheid van medisch adviseur (artikel 7.8 lid 3 Regeling zorgverzekering).

Regeling zorgverzekering

	In de Regeling Zorgverzekering in hoofdstuk 7 is verder uitgewerkt welke persoonsgegevens uitgewisseld mogen worden. Enkele daarvan zijn hieronder uitgelicht.					
	Vragende, ontvangende organisatie	**Gegevens**	**Doel**	**Wanneer**	**Toestemming**	**Verstrekken door**
Art. 7.1 lid 1, 2 in relatie tot art. 7.2, 7.3 en 7.4	**Zorgverzekeraar of een door de zorgverzekeraar aangewezen persoon**	Persoonsgegevens zijn: a. naam, adres, postcode en woonplaats; b. polisnummer, burgerservicenummer, geslacht en geboortedatum; c. de prestatiebeschrijving van de aan de verzekerde geleverde prestatie; d. wanneer en in voorkomend geval ten gevolge van welke catastrofe als bedoeld in artikel 33, lid 1, onderdeel a van de Zvw, de prestatie is geleverd; e. het voor de geleverde prestatie in rekening gebrachte tarief; f. de gegevens die op grond van een declaratieregeling moeten worden verstrekt; g. de gegevens die noodzakelijk zijn om vast te stellen of de prestatie behoort tot het verzekerde pakket van die verzekerde en h. het bank- of girorekeningnummer; i. overige gegevens die noodzakelijk zijn voor het verrichten van materiële controle dan wel fraudeonderzoek.	Noodzakelijk voor de uitvoering van de zorgverzekering of Zvw (door de verzekeraar) Te gebruiken voor het verrichten van de materiële en formele controle.	Desgevraagd of uit eigen beweging: de gegevens van sub a t/m g verplicht aan te leveren (tenzij de regeling anders bepaald). Sub i (materiële controle): desgevraagd aanleveren. Sub h heeft betrekking op situatie dat zorgaanbieder rechtstreeks in rekening brengt bij verzekerde.	Geen toestemming vereist.	Zorgaanbieder.

	Vragende, ontvangende organisatie	Gegevens	Doel	Wanneer	Toestemming	Verstrekken door
Artikel 61 lid 1 in relatie tot artikel 60 en 65	**NZa of een door de NZa aangewezen persoon**	a. Gegevens en inlichtingen b. De boeken, bescheiden en andere gegevensdragers of de inhoud daarvan – zulks ter keuze van de vrager –beschikbaar te stellen. (Of kopieën, leesbare afdrukken, uittreksels) Persoonsgegevens in de Wmg worden onderscheiden in: a. identificerende persoonsgegevens: naam, adres, woonplaats, postadres; geboortedatum en geslacht; administratieve gegevens, zoals nummers van bank-, giro- en creditcard, gegevens uit de basisregistratie personen registratie ingevolge de Wet Big. b. medische persoonsgegevens: gegevens over gezondheid als bedoeld in artikel 4, onderdeel 15 AVG. c. strafrechtelijke persoonsgegevens: persoonsgegevens van strafrechtelijke aard als bedoeld in paragraaf 3.2. van de UAVG en persoonsgegevens betreffende onrechtmatig of hinderlijk gedrag in verband met een opgelegd verbod naar aanleiding van dat gedrag. In de Regeling categorieën persoonsgegevens (artikel 3) is opgenomen welke persoonsgegevens noodzakelijk zijn in het kader van artikel 61 lid 1.	Redelijkerwijs van belang voor uitvoering Wmg c.q. redelijkerwijs van belang kan zijn voor vaststelling feiten welke invloed kunnen uitoefenen uitvoeren van de wet.	Desgevraagd.	Geen toestemming vereist.	Een ieder.

Wmg Wettelijke grondslag (2/2)

	Vragende, ontvangende organisatie	Gegevens	Doel	Wanneer	Toestemming	Verstrekken door
Artikel 66 lid 1[35] in relatie tot artikel 60 en 65	**NZa** **Fiod-ECD**	a. Identificerende gegevens - naam, adres, woonplaats, postadres; - geboortedatum en geslacht; - administratieve gegevens, zoals nummers van bank-, giro- en creditcard, gegevens uit de basisregistratie personen en registratie ingevolge de Wet Big. b. medische persoonsgegevens gegevens over gezondheid als bedoeld in artikel 4, onderdeel 15 AVG. Zie Regeling categorieën persoonsgegevens Wmg (artikel 3) voor persoonsgegevens in kader van art. 66.	Toezicht op naleving en handhaving van artikel 35, 36, 38 Wmg[36] en uitvoering van de Wet op de economische delicten.	Desgevraagd.	Geen toestemming vereist.	Zorgaanbieders (en ziektekostenverzekeraars).
Artikel 68a lid 1 en 4 sub b. Zorg in Natura	**Ziektekostenverzekeraar of een door hen aangewezen persoon**	Persoonsgegevens, waaronder gegevens over de gezondheid (inzage in of afschrift van). In de Regeling persoonsgegevens vrijwillige ziektekostenverzekering Wmg (artikel 3) is opgenomen welke persoonsgegevens dit betreffen.	Noodzakelijk voor de uitvoering ziektekostenverzekering; Zvw, Wlz.	Desgevraagd.	Geen toestemming vereist.	Zorgaanbieder.

[35] Artikel 66 lid 2 bepaalt dat een zorgaanbieder geen medische gegevens aan anderen dan de NZa en Fiod-ECD hoeft te verstrekken ten behoeve van de uitvoering van artikel 35, 36 en 38 Wmg en WED.

[36] Deze artikelen hebben betrekking op voorkoming van zorgfraude (artikel 35), het inrichten van een administratie waaruit de geleverde prestaties blijken (artikel 36) en de informatieplicht van zorgaanbieders aan patiënten over hun tarieven (artikel 38)..

	Vragende, ontvangende organisatie	Gegevens	Doel	Wanneer	Toestemming	Verstrekken door
Art. 11 Onverwijld melden van calamiteit zorgverlening; geweld in de zorgrelatie; opzegging, ontbinding of niet voortzetting overeenkomst met hulpverlener wegens ernstig disfunctioneren.	**IGJ**	Persoonsgegevens, waaronder gezondheidsgegevens en andere bijzondere categorieën van persoonsgegevens en persoonsgegevens van strafrechtelijke aard.	Noodzakelijk voor het onderzoeken van melding.	Desgevraagd of uit eigen beweging.	Geen toestemming vereist.	Zorgaanbieder.

Met betrekking tot het doen van melding op grond van artikel 11 Wkkgz wordt u gewezen op de verdere vereisten neergelegd hoofdstuk 8 van het Uitvoeringsbesluit Wkkgz. Hierin staat beschreven aan welke vereisten een melding dient te voldoen en welke persoonsgegevens daarbij uitgewisseld moeten worden. Een aantal hebben wij er voor u uitgelicht.

	Vragende, ontvangende organisatie	Gegevens	Doel	Wanneer	Toestemming	Verstrekken door
Art. 8.1 lid 2 sub e en f	**IGJ**	Bij de melding wordt aangegeven of het gaat om een zorgverlener die is ingeschreven in een register als bedoeld in artikel 3 Wet Big en in voorkomend geval de naam, de contactgegevens en de geboortedatum van de betrokken cliënt.				
Art. 8.6	**IGJ**	Persoonsgegevens en, indien de Inspectie dit onder opgave van redenen verzoekt, gegevens over gezondheid, gegevens van strafrechtelijke aard en andere bijzondere categorieën van persoonsgegevens van de bij de gemelde feiten betrokken cliënt of cliënten en de betrokken zorgverleners.	Noodzakelijk voor het onderzoeken van de andere melding.	Desgevraagd.	Geen toestemming vereist.	Zorgaanbieder.
Art. 8.15 (andere melding zijnde geen verplichte melding) en artikel 8.19 lid 2. Zie hier informatie van IGJ over "andere meldingen".	**IGJ**	Persoonsgegevens van de bij de gemelde feiten betrokken cliënt of cliënten en de betrokken zorgverleners. Let op: hiertoe behoren geen bijzondere persoonsgegevens.	Noodzakelijk voor het onderzoeken van de andere melding.	Desgevraagd.	Geen toestemming vereist.	Zorgaanbieder.

	Vragende, ontvangende organisatie	Gegevens	Doel	Wanneer	Toestemming	Verstrekken door
Artikel 1:240	**Raad voor de kinderbescherming**	Gegevens[37] noodzakelijk voor het uitoefenen van de taken van de Raad voor de Kinderbescherming. Met artikel 1:240 BW heeft de wetgever een kan-bepaling beoogd. Dit betekent dat het niet verplicht is om gegevens aan de RvdK te verstrekken, maar het mag wel. Voor de hulpverlener (zorgprofessional) betekent dit dat gegevens pas mogen worden verstrekt als hij in conflict van plichten is komen te verkeren en op grond daarvan zijn beroepsgeheim mag schenden. Voordat hiertoe kan worden overgegaan moet zijn voldaan aan alle hierna genoemde criteria: 1. Is alles geprobeerd om toestemming te krijgen? 2. Als het beroepsgeheim niet wordt doorbroken, ontstaat er dan ernstige schade voor een ander of de cliënt zelf? 3. Is er gewetensnood ontstaan door het handhaven van het beroepsgeheim? 4. Is er geen andere manier om ernstige schade te voorkomen? 5. Zal het doorbreken van het beroepsgeheim vrijwel zeker leiden tot het voorkomen of beperken van ernstige schade? Als aan al deze criteria wordt voldaan mag het beroepsgeheim worden doorbroken op grond van conflict van plichten, zij het zo min mogelijk.		Desgevraagd of uit eigen beweging.	Geen toestemming vereist.	Hulpverlener die uit hoofde van zijn ambt of beroep een beroepsgeheim heeft.

[37] De wetgever heeft niet nader gespecificeerd welke gegevens dit kan betreffen en of daartoe ook (bijzondere) persoonsgegevens behoren.

Bijlage 2 toestemmingsformulier 1/3

Toestemmingsformulier voor gebruik van mijn persoonsgegevens, waaronder gezondheidsgegevens, door [*naam zorgorganisatie*].

Met dit formulier geef ik [*naam cliënt/(wettelijk) vertegenwoordiger*] toestemming om mijn [1] persoonsgegevens, waaronder gezondheidsgegevens, te gebruiken door [*naam zorgorganisatie*].

Doelen

Het kan gaan om het vastleggen van mijn persoonsgegevens in het cliëntdossier of bijvoorbeeld om het opvragen bij of verstrekken van mijn persoonsgegevens aan andere (zorg)organisaties en/of individuele zorgverleners. Mijn persoonsgegevens worden gebruikt voor het leveren van goede zorg en het kunnen waarborgen van de kwaliteit door [naam stichting].

Daarnaast kunnen foto's, filmpjes en/of geluidsopnames worden gemaakt waarop ik te zien en/of te horen ben en die [naam stichting] graag wil gebruiken. Foto's, filmpjes en/of geluidsopnames worden gebruikt om te laten zien welke sociale activiteiten er georganiseerd zijn of gaan worden. Dit kan naar familie en verwanten worden gestuurd, maar ook worden geplaatst op sociale mediakanalen. Het doel hiervan is het maatschappelijk inspireren en het vergroten van naamsbekendheid van [*naam stichting*].

Het toestemmingsformulier geeft voor beide doelen meerdere keuzemogelijkheden aan.

Waarvoor ik toestemming geef, heb ik hierna ingevuld.

A Toestemming voor het gebruiken van persoonsgegevens, waaronder gezondheidsgegevens, voor zorginhoudelijke doelen.

Gebruik van persoonsgegevens om goede zorg te kunnen leveren en kwaliteit te kunnen waarborgen door [*naam zorgorganisatie*] ten behoeve van:

- zorgondersteunende functies zoals: dossierbeheer, intercollegiale toetsing, intervisie, supervisie, opleiding, kwaliteitsbewaking, kwaliteitsbevordering en (wetenschappelijk) onderzoek. ☐ Ja ☐ Nee
- Onderaannemers waarvan [*naam zorgorganisatie*] gebruik maakt ☐ Ja ☐ Nee
- Individuele zorgverleners (huisarts, tandarts, fysiotherapeut) ☐ Ja ☐ Nee
- Ziekenhuis, medisch specialist ☐ Ja ☐ Nee
- Leveranciers medische hulpmiddelen (rolstoelbedrijf, thuiszorgwinkel, orthopedisch schoenmaker) ☐ Ja ☐ Nee
- Organisaties: CIZ, CAK, UWV [en.....] ☐ Ja ☐ Nee
- Onderwijsinstelling ☐ Ja ☐ Nee
- Werkvoorziening ☐ Ja ☐ Nee
- Taxibedrijf, vervoersbedrijf ☐ Ja ☐ Nee
- Mantelzorger(s) van de cliënt ☐ Ja ☐ Nee
- Anders, namelijk: ..... ☐ Ja ☐ Nee

[1] Wanneer de (wettelijk) vertegenwoordiger toestemming geeft dan worden hiermee de persoonsgegevens bedoeld van degene die hij vertegenwoordigt (de cliënt).

B Toestemming voor het gebruiken van persoonsgegevens, waaronder gezondheidsgegevens, verkregen tijdens sociale activiteiten die [*naam stichting*] graag wil delen met anderen via website of andere kanalen.

Foto's en film- en/of geluidsmateriaal voor maatschappelijke inspiratie en promotie van [*naam zorgorganisatie*].

Intern gebruik:

- Nieuwsbrief ☐ Ja ☐ Nee
- Prikbord ☐ Ja ☐ Nee
- Intranet ☐ Ja ☐ Nee
- Intern berichtenverkeer (chat-groepen) ☐ Ja ☐ Nee
- Anders, namelijk: ..... ☐ Ja ☐ Nee

Extern gebruik:

- Website ☐ Ja ☐ Nee
- Folders ☐ Ja ☐ Nee
- Banners ☐ Ja ☐ Nee
- Flyers ☐ Ja ☐ Nee
- Anders, namelijk: ..... ☐ Ja ☐ Nee

Foto's, geluid en filmmateriaal van activiteiten, feestjes en andere bijeenkomsten die op social media-accounts van [*naam zorgorganisatie*] kunnen worden geplaatst:

- Facebook ☐ Ja ☐ Nee
- LinkedIn ☐ Ja ☐ Nee
- WhatsApp ☐ Ja ☐ Nee
- Instagram ☐ Ja ☐ Nee
- Twitter ☐ Ja ☐ Nee
- YouTube ☐ Ja ☐ Nee
- Snapchat ☐ Ja ☐ Nee
- Anders, namelijk: ..... ☐ Ja ☐ Nee

Vink aan waarvoor wel of geen toestemming voor gegeven wordt.

Deze toestemming kan door mij op elk moment worden ingetrokken, vanaf dat moment worden de persoonsgegevens niet meer gebruikt.

Ondertekend en daarmee akkoord,

Naam cliënt:	Naam (wettelijk) vertegenwoordiger:
.....	.....
Handtekening:	Handtekening:
.....	.....
Datum:	Datum:
.....	.....

vgn vereniging gehandicaptenzorg nederland

< Terug naar de inhoudsopgave

Toelichting:

Het is van belang om te weten wie het toestemmingsformulier mag tekenen. Dit zal afhangen van de leeftijd van de cliënt en zijn of haar wilsbekwaamheid. Aan de hand van het lijstje hieronder wordt bepaald wie het toestemmingsformulier moet tekenen.

Bij in zorg nemen:

- Cliënt is jonger dan 16 jaar: **ouder en/of voogd.**
- Cliënt is 16 jaar of ouder en wilsbekwaam: **cliënt.**
- Cliënt is minderjarig en wilsonbekwaam ter zake: **ouder en/of voogd.**
- Cliënt is meerderjarig en wilsonbekwaam ter zake: **curator, mentor of schriftelijke gemachtigde.**

Tijdens de zorgverlening:

- Cliënt niet ouder dan 11 jaar: **ouder en/of voogd**.
- Cliënt 12 tot en met 15 jaar: **ouder en/of voogd én cliënt samen (mits deze wilsbekwaam is).**
- Cliënt is 16 jaar of ouder en wilsbekwaam: **cliënt zelf.**
- Cliënt is minderjarig en wilsonbekwaam ter zake: **ouders en/of voogd.**
- Cliënt is meerderjarig en wilsonbekwaam ter zake: **curator, mentor, schriftelijk gemachtigde of de belangenbehartiger als de eerst genoemde personen ontbreken. Dit kan dan zijn de echtgenoot, geregistreerd partner, levensgezel, een ouder, een kind, een broer of zus van de cliënt.**

Bijlage 3 - achtergrondinformatie

Privacy documenten VGN

VGN Privacyreglement

Verwerkersovereenkomst BoZ

FAQ AVG arbeidsrelatie BoZ (alleen voor leden van de VGN beschikbaar, op te vragen via: secretariaat@vgn.nl)

Informatie over privacy

www.autoriteitpersoonsgegevens.nl

www.hulpbijprivacy.nl#zorgverleners

www.jeugdconnect.nl

www.kennispleingehandicaptensector.nl/juridische-kennis

Bijlage 4 - Bronvermelding

< Terug naar de inhoudsopgave

Algemene Verordening Gegevensbescherming (AVG) inclusief Uitvoeringswet AVG
Tekst & Commentaar. Redactie: G.J. Zwenne, Wolters Kluwer, Deventer december 2018.

Sdu Commentaar AVG. Hoofdredactie: mr. drs. T.F.M. Hooghiemstra,
mr. dr. S. Nouwt, Sdu, Den Haag 2018.

Handleiding Algemene verordening gegevensbescherming en Uitvoeringswet
Algemene verordening, Ministerie van Justitie en Veiligheid, Den Haag 2018.

Kernregelgeving gebruik digitale patiëntengegevens, een korte introductie. R.P. Wijne,
Boom juridisch, Den Haag 2019.

KNMG-richtlijn, Omgaan met medische gegevens, KNMG, mei 2018.

NTA 7516, Medische informatica – Eisen voor veilige e-mail en chatapplicaties
(uitwisseling van ad-hocberichten met persoonlijke gezondheidsinformatie), NEN, mei 2019.

Tevens dank aan:
Amarant, Veelgestelde vragen AVG.

VGN Handreiking Privacy

< Terug naar de inhoudsopgave

Bescherming van persoonsgegevens van cliënten in de gehandicaptenzorg

Colofon

De handreiking privacy is een uitgave van de Vereniging Gehandicaptenzorg Nederland (VGN). De VGN is de brancheverenging van professionele zorgaanbieders in de gehandicaptenzorg.

Vereniging Gehandicaptenzorg Nederland (VGN)
Oudlaan 4 3515 GA Utrecht
Postbus 413 3500 AK Utrecht
T 030-27 39 300
info@vgn.nl
www.vgn.nl

De handreiking informeert zorgorganisaties in de gehandicaptenzorg over de privacywetgeving in relatie tot de zorg, ondersteuning en jeugdhulp die zij bieden. De handreiking is met grote zorgvuldigheid en met gebruikmaking van de meest actuele gegevens tot stand gekomen. Het is evenwel niet geheel uitgesloten dat de informatie uit deze handreiking onjuistheden of onvolkomenheden bevat. Bij het opstellen van deze handreiking is niet gestreefd naar volledigheid. Deze handreiking dient niet ter vervanging van juridisch advies. Bij twijfel over de stappen die u moet nemen bij een concreet privacyvraagstuk raden wij u aan zo nodig nader juridisch advies in te winnen. De VGN aanvaardt geen aansprakelijkheid voor directe of indirecte schade ontstaan door eventuele onjuistheden en/of onvolkomenheden.