Privacyreglement

Doel	Praktische uitwerking van de bepalingen van de Algemene Verordening Gegevensbescherming.
Doelgroep	Alle medewerkers, bewoners en bezoekers Beek & Bos
Versie	11
Opgesteld	6 oktober 2001
Laatst gewijzigd	April 2026
Evaluatie en actualisatie	April 2028
Verantwoordelijke	Bestuurder
Auteur	Beleidsmedewerker
Beoordelaar	Bestuurder

Inhoudsopgave

1 Inleiding

Op 25 mei 2018 is de Algemene Verordening Gegevensbescherming (hierna: AVG) in werking getreden. De AVG stelt het opstellen van een privacybeleid (gegevensbeschermingsbeleid) verplicht, als dat in verhouding staat tot de verwerkingsactiviteiten die een zorgaanbieder verricht. Dat is afhankelijk van de concrete omstandigheden zoals de aard, de omvang, de context en het doel van de gegevensverwerking. Zorgaanbieders verwerken bijzondere persoonsgegevens (gegevens met betrekking tot de gezondheid) en zijn daarom in principe verplicht dergelijk beleid op te stellen.

Het Privacyreglement is de uitwerking van AVG en sectorspecifieke wetten zoals de Wet op de geneeskundige behandelingsovereenkomst (Wgbo), de Wet Zorg en Dwang (Wzd), de Zorgverzekeringswet (Zvw), de Wet langdurige zorg (Wlz) en de Wet Maatschappelijke Ondersteuning 2015 (Wmo 2015).

Dit reglement is van toepassing op de verwerkingen (zowel op papier als elektronisch) van gegevens van cliënten die zorg ontvangen van Zorgcentrum Beek en Bos. De medewerkers en vrijwilligers worden hierbij buiten beschouwing gelaten.

2 Relatie met andere wetten

Algemene Verordening Gegevensbescherming (AVG)

De AVG is een Europese verordening die regels stelt voor gegevensverwerkingen en heeft als doel persoonsgegevens van natuurlijke personen te beschermen. Uit de AVG volgt dat het verboden is om bijzondere categorieën persoonsgegevens, zoals gezondheidsgegevens, te verwerken tenzij aan bijzondere (strengere) regels uit de AVG wordt voldaan. De bepalingen uit de AVG gelden voor alle Europese landen en hebben als doel de privacy van personen binnen de EU te beschermen in verband met de verwerking van persoonsgegevens en het vrije verkeer van die gegevens te waarborgen. De verordening laat op een aantal plaatsen ruimte aan de nationale wetgever om eigen regels in nationale wetgeving verder te regelen. Onder meer wat de verwerking van bijzondere persoonsgegevenscategorieën (“gevoelige gegevens”) betreft. Deels wordt dit geregeld in een (Nederlandse) uitvoeringswet. De AVG biedt de lidstaten ook ruimte om eigen regels voor de toepassing vast te stellen in sectorspecifieke wetten zoals met betrekking tot geneeskundige gezondheidszorg (Wgbo en Wzd) en met betrekking tot het sociaal domein (Wmo 2015).
Hieronder wordt aangegeven hoe de voor de gezondheidszorg belangrijkste wetten zich verhouden tot de AVG en tot elkaar.

Relatie met Wgbo

De Wgbo is een sectorspecifieke wet die de toepassing van de AVG met betrekking tot de verwerking van gezondheidsgegevens regelt; dit betekent dat specifieke privacybepalingen in de Wgbo naast die van de algemene bepalingen van de AVG gelden. Voorbeeld: als zorgaanbieder mag Beek en Bos alléén gegevens aan een derde verstrekken als dat mag op grond van de AVG én als er een grond is om het medisch beroepsgeheim te doorbreken.

Relatie met Wzd

Ook de Wzd is een sectorspecifieke wet die de toepassing van de AVG met betrekking tot de verwerking van gezondheidsgegevens regelt bij gedwongen zorgverlening. Dit betekent dat specifieke privacybepalingen in de Wzd naast de AVG gelden en voorrang krijgen ten opzichte van bepalingen die volgen uit de Wgbo. Bijvoorbeeld wat betreft de bewaar- en vernietigingsbepalingen in de Wzd en de bepalingen over gegevensverwerking in het Besluit zorg en dwang.

Relatie met de Zvw

De Zvw geeft ook bepalingen over privacy van de verzekerde/cliënt. Ook deze bepalingen gelden naast de bepalingen van de AVG. Een voorbeeld is het verplicht gebruik maken van het BSN door de

zorgverzekeraar en gegevensverstrekking aan derden maar ook de bevoegdheid van de zorgverzekeraar tot controle of de gedeclareerde zorg ook werkelijk door de zorgaanbieder geleverd is. Dit is echter geen vrijbrief voor ongelimiteerde gegevensverzoeken en/of -verstrekking; de zorgverzekeraar ontvangt slechts gegevens die noodzakelijk zijn voor zijn controle, niet meer en neemt bij materiële controles eventueel genoegen met inzage in gegevens waarover alleen de zorgaanbieder beschikt. De zorgverzekeraar moet zich bovendien houden aan de controlestappen in de Regeling zorgverzekering en de beleidsregels van het CBP (voorloper van de Autoriteit Persoonsgegevens) wat betreft de formele en materiële controles.

Relatie met de Wlz

De Wlz geeft bepalingen over privacy van cliënten. Een voorbeeld is het verplicht gebruik van het BSN en gegevensverstrekking aan derden in hoofdstuk 9 van de wet, maar ook de controle of de gedeclareerde zorg ook daadwerkelijk is geleverd. De Wlz geeft tevens “Wgbo-achtige” bepalingen en stelt bijzondere eisen aan het opstellen en de inhoud van een zorgplan met de cliënt. De Wlz is een specifieke wet ten opzichte van de Wgbo. De AVG blijft daarentegen naast de Wlz gelden. De afwijkende bepalingen in de Wzd gaan voor de Wlz.

Relatie met Wmo2015

De Wmo 2015 geeft bepalingen over privacy van de cliënt die een algemene- of maatwerkvoorziening krijgt, bijvoorbeeld begeleiding of beschermd wonen.

Relatie met Wkkgz

De Wet kwaliteit, klachten en geschillen zorg (Wkkgz) verplicht zorgaanbieders om goede zorg te leveren, incidenten te leren en een laagdrempelige klachten- en geschillenregeling te organiseren. Bij de uitvoering van deze verplichtingen worden (bijzondere) persoonsgegevens verwerkt, bijvoorbeeld bij de registratie en behandeling van klachten, de inzet van een klachtenfunctionaris, het voeren van correspondentie met cliënten/vertegenwoordigers en het opstellen van rapportages over incidenten en verbetermaatregelen. Deze gegevensverwerkingen moeten steeds voldoen aan de AVG (rechtmatigheid, doelbinding, minimale gegevensverwerking en passende beveiliging). Dat betekent onder meer dat alleen die persoonsgegevens worden verwerkt die noodzakelijk zijn voor een zorgvuldige afhandeling, dat toegang tot klachten- en incidentinformatie beperkt is tot degenen die dit voor hun taak nodig hebben, en dat gegevens niet langer worden bewaard dan nodig is (of dan wettelijk is voorgeschreven). Waar de Wkkgz aanvullende eisen stelt aan vastlegging, kwaliteitsbewaking en klachtenafhandeling, blijft het uitgangspunt dat medische en andere vertrouwelijke informatie niet verder wordt gedeeld dan noodzakelijk en dat betrokkenen transparant worden geïnformeerd over de verwerking van hun gegevens.

Relatie met NEN 7510

De NEN 7510 is de Nederlandse norm voor informatiebeveiliging in de zorg en geeft praktische invulling aan het inrichten, uitvoeren en verbeteren van passende technische en organisatorische beveiligingsmaatregelen. Daarmee ondersteunt de norm de naleving van de AVG, in het bijzonder de verplichting om persoonsgegevens passend te beveiligen (o.a. artikel 32 AVG) en om als organisatie aantoonbaar “in control” te zijn. Toepassing van NEN 7510 helpt om structureel risico’s te beoordelen en beheersmaatregelen vast te leggen en uit te voeren, zoals autorisatie- en toegangsbeheer, logging en monitoring, veilige werkplekken en mobiele apparatuur, beheer van leveranciers/verwerkers, back-up en herstel, en het melden en afhandelen van beveiligingsincidenten en datalekken. In dit privacyreglement is de zorgvuldige omgang met persoonsgegevens uitgewerkt; NEN 7510 beschrijft het kader waarbinnen de bijbehorende informatiebeveiligingsprocessen en -maatregelen worden georganiseerd, geborgd en periodiek geëvalueerd.

Relatie met de Cyberbeveiligingswet (Cbw)

De Cyberbeveiligingswet (Cbw) is de Nederlandse implementatie van de Europese NIS2-richtlijn en is gericht op het verhogen van de digitale weerbaarheid van organisaties die maatschappelijk of economisch belangrijke diensten leveren, waaronder (delen van) de zorgsector. Waar dit privacyreglement de verwerking van (bijzondere) persoonsgegevens en de naleving van de AVG beschrijft, richt de Cyberbeveiligingswet zich primair op het beheersen van cyberbeveiligingsrisico's rond netwerk- en informatiesystemen en de continuïteit van dienstverlening. De wet kent onder meer een zorgplicht (passende technische en organisatorische beveiligingsmaatregelen op basis van risicobeoordeling), een registratieplicht en een meldplicht voor significante cyberincidenten. In de praktijk kunnen incidenten overlappen: een cyberincident kan óók een datalek zijn. In dat geval kunnen zowel meldingen onder de Cyberbeveiligingswet (richting het aangewezen meldpunt/toezichthouder) als onder de AVG (richting Autoriteit Persoonsgegevens en eventueel betrokkenen) aan de orde zijn. Daarom worden de procedures voor incidentmanagement, informatiebeveiliging en datalekafhandeling op elkaar afgestemd, zodat tijdig kan worden beoordeeld welke meldplichten gelden, welke informatie moet worden vastgelegd en welke maatregelen nodig zijn om schade te beperken en herhaling te voorkomen.

3 Privacyreglement

3.1 Definities

Autoriteit Persoonsgegevens (AP): de toezichthoudende autoriteit, de onafhankelijke instantie die erover waakt dat persoonsgegevens zorgvuldig en veilig worden verwerkt en zo nodig sancties kan opleggen als dat niet gebeurt.

Bestand: elk gestructureerd geheel van persoonsgegevens die volgens bepaalde criteria toegankelijk zijn.

Betrokkene: degene op wie een persoonsgegeven betrekking heeft.

Bijzondere categorieën persoonsgegevens: persoonsgegevens waaruit ras of etnische afkomst, politieke opvattingen, religieuze of levensbeschouwelijke overtuigingen, of het lidmaatschap van een vakbond blijken, en genetische gegevens, biometrische gegevens met het oog op de unieke identificatie van een persoon, of gegevens over gezondheid, of gegevens met betrekking tot iemands seksueel gedrag of seksuele gerichtheid.

Derde: elke persoon of instantie die geen betrokkene, verwerkingsverantwoordelijke, verwerker, of een persoon is die onder rechtstreeks gezag van de verwerkingsverantwoordelijke of de verwerker gemachtigd is persoonsgegevens te verwerken.

Datalek: de toegang tot of vernietiging, wijziging of vrijkomen van persoonsgegevens zonder dat dit de bedoeling is van de verwerker. Of zonder dat dit wettelijk is toegestaan.

Gezondheidsgegevens: gegevens over de lichamelijke of geestelijke gezondheid van een persoon, waaronder gegevens over verleende gezondheidsdiensten waarmee informatie over zijn gezondheidstoestand wordt gegeven;

Inbreuk in verband met persoonsgegevens: een inbreuk op de beveiliging die per ongeluk of op onrechtmatige wijze leidt tot de vernietiging, het verlies, de wijziging of de ongeoorloofde verstrekking van of de ongeoorloofde toegang tot doorgezonden, opgeslagen of anderszins verwerkte gegevens.

Persoonsgegevens: alle informatie over een geïdentificeerde of identificeerbare natuurlijke persoon („de betrokkene"); als identificeerbaar wordt beschouwd een natuurlijke persoon die direct of indirect kan worden geïdentificeerd, met name aan de hand van een identificator zoals een naam, een identificatienummer, locatiegegevens, een online identificator of van een of meer elementen die kenmerkend zijn voor de fysieke, fysiologische, genetische, psychische, economische, culturele of sociale identiteit van die natuurlijke persoon.

Profilering: elke vorm van geautomatiseerde verwerking van persoonsgegevens waarbij aan de hand van persoonsgegevens bepaalde persoonlijke aspecten van een natuurlijke persoon worden geëvalueerd, met name met de bedoeling zijn beroepsprestaties, economische situatie, gezondheid, persoonlijke voorkeuren, interesses, betrouwbaarheid, gedrag, locatie of verplaatsingen te analyseren of te voorspellen.

Pseudonimisering: het verwerken van persoonsgegevens op zodanige wijze dat de persoonsgegevens niet meer aan een specifieke betrokkenen kunnen worden gekoppeld zonder dat aanvullende gegevens worden gebruikt, mits deze aanvullende gegevens apart worden bewaard en technische en organisatorische maatregelen worden genomen om ervoor te zorgen dat de persoonsgegevens niet aan een geïdentificeerde of identificeerbare natuurlijke persoon worden gekoppeld.

Toestemming van de betrokkene: door betrokkene, op goede informatie berustende, specifieke, in vrijheid en ondubbelzinnig gegeven toestemming waarbij betrokkene hem betreffende verwerking van persoonsgegevens aanvaardt. Dat kan door middel van een schriftelijke of mondelinge verklaring of een ondubbelzinnige actieve handeling (zoals het elektronisch aanvinken van een hokje).

Verzoek: beroep dat een betrokkene doet richting de verwerker op één van zijn rechten m.b.t. persoonsgegevens.

Verwerker: degene die in opdracht van en voor de verwerkingsverantwoordelijke persoonsgegevens verwerkt (bijvoorbeeld een externe hostingsfirma, software-leverancier, kwaliteitsauditor of een extern salarisadministratiekantoor).

Verwerking van persoonsgegevens: alle handelingen met betrekking tot persoonsgegevens, waaronder in ieder geval het verzamelen, vastleggen, ordenen, bewaren, bijwerken, wijzigen, opvragen, raadplegen, gebruiken, verstrekken door middel van doorzending, verspreiding of in een andere vorm beschikbaar stellen, samenbrengen, met elkaar in verband brengen, alsmede het afschermen, uitwissen of vernietigen van gegevens.

Verwerkingsverantwoordelijke: degene die, alleen of samen met anderen, het doel van en de middelen voor de verwerking van persoonsgegevens vaststelt; meestal de bestuurder van de zorgaanbieder.

Zorgaanbieder: Zorgcentrum Beek en Bos.

3.2 Verwerking van persoonsgegevens in overeenstemming met de AVG

3.2.1 Beginselen inzake persoonsgegevensverwerking

De zorgaanbieder is verantwoordelijk voor de naleving van onderstaande beginselen bij de verwerking van persoonsgegevens en moet de naleving van deze beginselen kunnen aantonen ("verantwoordingsplicht").

Binnen Zorgcentrum Beek en Bos worden persoonsgegevens alleen verwerkt:

- op een wijze die ten aanzien van de betrokkene rechtmatig, behoorlijk en transparant is;
- voor welbepaalde, uitdrukkelijk omschreven en gerechtvaardigde doeleinden en mogen vervolgens niet verder op een met die doeleinden onverenigbare wijze worden verwerkt; de verdere verwerking met het oog op archivering in het algemeen belang, wetenschappelijk of historisch onderzoek of statistische doeleinden wordt niet als onverenigbaar met de oorspronkelijke doeleinden beschouwd ("doelbinding");
- voor zover zij toereikend zijn, ter zake dienend en beperkt tot wat noodzakelijk is voor de doeleinden waarvoor zij worden verwerkt ("minimale gegevensverwerking" ook wel "dataminimalisatie");
- indien de persoonsgegevens juist zijn en zo nodig worden geactualiseerd. Alle redelijke maatregelen moeten worden genomen om de persoonsgegevens die, gelet op de doeleinden waarvoor zij worden verwerkt, onjuist zijn, onverwijld te wissen of te rectificeren ("juistheid")
- en bewaard in een vorm die het mogelijk maakt de betrokkenen niet langer te identificeren dan voor de doeleinden waarvoor de persoonsgegevens worden verwerkt noodzakelijk is; persoonsgegevens mogen voor langere perioden worden opgeslagen voor zover de persoonsgegevens louter met het oog op archivering in het algemeen belang, wetenschappelijk of historisch onderzoek of statistische doeleinden worden verwerkt mits de bij deze verordening vereiste passende technische en organisatorische maatregelen worden

getroffen om de rechten en vrijheden van de betrokkene te beschermen ("opslagbeperking");
- door het nemen van passende technische of organisatorische maatregelen op een dusdanige manier dat een passende beveiliging ervan gewaarborgd is, en dat zij onder meer beschermd zijn tegen ongeoorloofde of onrechtmatige verwerking en tegen onopzettelijk verlies, vernietiging of beschadiging ("integriteit en vertrouwelijkheid").

3.2.2 Rechtmatigheid van de verwerking (verwerkingsgrondslag)

De verwerking is alleen rechtmatig indien en voor zover aan ten minste één van de onderstaande voorwaarden, rechtsgrond voor de verwerking, is voldaan:

- de betrokkene heeft toestemming gegeven voor de verwerking van zijn persoonsgegevens voor één of meer specifieke doeleinden; de zorgaanbieder moet de toestemming kunnen aantonen en betrokkenen heeft het recht de toestemming te allen tijde in te trekken;
- de gegevensverwerking is noodzakelijk voor de uitvoering van een overeenkomst waarbij de betrokkene partij is, bijvoorbeeld de behandelingsovereenkomst;
- de gegevensverwerking is noodzakelijk om een wettelijke verplichting na te komen, bijvoorbeeld de dossierplicht in de Wgbo of gegevensuitwisseling in het kader van de Wzd;
- de gegevensverwerking is noodzakelijk ter bescherming van de vitale belangen van de betrokkene of een ander natuurlijk persoon;
- de gegevensverwerking is noodzakelijk voor de goede vervulling van een taak van algemeen belang, of van een taak in het kader van de uitoefening van het openbaar gezag dat aan de verwerkingsverantwoordelijke is opgedragen dat ook elders in een wet is vastgelegd met eventuele nadere bepalingen;
- de gegevensverwerking is noodzakelijk voor de behartiging van de gerechtvaardigde belangen van de verwerkingsverantwoordelijke of van een derde én de belangen, grondrechten of fundamentele vrijheden van degene van wie de gegevens worden verwerkt prevaleren niet.

3.2.3 Voorwaarden voor het verwerken van gezondheidsgegevens

Gezondheidsgegevens zijn één van de categorieën bijzondere persoonsgegevens. Het is in de AVG verboden bijzondere categorieën persoonsgegevens te verwerken, tenzij voldaan wordt aan één van de onderstaande voorwaarden:

- Als de verwerking noodzakelijk is voor doeleinden van preventieve of arbeidsgeneeskunde, voor de beoordeling van de arbeidsgeschiktheid van de werknemer, medische diagnosen, het verstrekken van gezondheidszorg of sociale diensten of behandelingen dan wel het beheren van gezondheidszorgstelsels en -diensten of sociale stelsels en diensten, voor zover dit is toegestaan in nationale wetgeving.
- Zo mogen gegevens over gezondheid worden verwerkt met het doel gezondheidszorg te leveren, onder de verantwoordelijkheid van een beroepsbeoefenaar die aan het beroepsgeheim gebonden is of door een ander persoon die op grond van de wet of overeenkomst tot geheimhouding is gehouden.

Let op: naast de opheffing van het verbod om bijzondere gezondheidsgegevens te verwerken zoals hierboven genoemd, moet ook nog een verwerkingsgrondslag aanwezig zijn om dergelijke gegevens te verwerken (zie ook 3.2.2).

3.2.4 Gegevensverwerking door verwerker

- De zorgaanbieder kan de verwerking (extern) uitbesteden aan een verwerker en legt dan in een verwerkersovereenkomst de verplichtingen uit de AVG op aan de verwerker. De zorgaanbieder doet uitsluitend een beroep op verwerkers die afdoende garanties met betrekking tot het toepassen van passende technische en organisatorische maatregelen bieden opdat de verwerking aan de vereisten van deze verordening voldoet en de bescherming van de rechten van de betrokkene is gewaarborgd.
- De verwerking door een verwerker wordt geregeld in een (verwerkers)overeenkomst die de verwerker ten aanzien van de zorgaanbieder bindt en waarin het onderwerp, de duur van de verwerking, de aard en het doel van de verwerking, het soort persoonsgegevens en de categorieën van betrokkenen en de rechten en verplichtingen van de zorgaanbieder worden omschreven. Een dergelijke overeenkomst dient te voldoen aan de eisen die de AVG daaraan stelt.
- De verwerker en eenieder die onder het gezag van de zorgaanbieder of van de verwerker handelt en toegang heeft tot persoonsgegevens, verwerkt deze uitsluitend in opdracht van de zorgaanbieder, tenzij hij door wet- of regelgeving tot verwerking gehouden is.

3.2.5 Aansprakelijkheid verwerkingsverantwoordelijke en/of verwerker

- De zorgaanbieder (verwerkingsverantwoordelijke) is verantwoordelijk en aansprakelijk voor schade die voortvloeit uit het toerekenbaar tekortschieten of niet voldoende naleven van de AVG, waaronder het wel/niet naleven van de beveiligingseisen.
- De verwerker, waaraan de zorgaanbieder (een deel van) gegevensverwerking heeft uitbesteed, kan daarnaast zelfstandig aansprakelijk zijn voor schade of een deel van de schade die voortvloeit uit zijn werkzaamheden. Hoe die aansprakelijkheid wordt verdeeld, wordt beoordeeld door de schadeverzekeraar of de rechter. Van belang is dat de zorgaanbieder goede afspraken maakt met de verwerker en deze vastlegt in een verwerkersovereenkomst.

3.2.6 Wanneer mogen andere bijzondere gegevens dan de gezondheidsgegevens worden verwerkt?

Andere bijzondere gegevens, bijvoorbeeld gegevens met betrekking tot ras/etniciteit of godsdienst/ levensovertuiging mogen alleen als aanvulling op gezondheidsgegevens worden verwerkt als dat nodig is voor een goede behandeling of verzorging van de betrokkene en dus niet systematisch bij iedereen. Bijvoorbeeld voor de inschakeling van een tolk/vertaler als dat voor de uitleg van de behandeling aan cliënt nodig is.

3.2.7 Geheimhoudingsplicht en verstrekking aan derden

- Persoonsgegevens verkregen in de uitoefening van een beroep in de gezondheidszorg vallen onder de geheimhoudingsplicht van de hulpverlener. Deze geheimhoudingsplicht is o.a. vastgelegd in de Wgbo en de wet BIG en in verschillende beroepscodes.
- Bij de verstrekking van gegevens aan derden wordt de wet nageleefd.

3.2.8 Wanneer mogen gegevens aan een ander worden verstrekt voor wetenschappelijk onderzoek en statistiek op het gebied van de volksgezondheid?

De gegevensverwerking met het oog op archivering in het algemeen belang, wetenschappelijk of historisch onderzoek of statistische doeleinden is onderworpen aan passende waarborgen in overeenstemming met de AVG voor de rechten en vrijheden van de betrokkene. De waarborgen zorgen ervoor dat er technische en organisatorische maatregelen zijn getroffen om de inachtneming van het beginsel van minimale gegevensverwerking te garanderen. Deze maatregelen kunnen pseudonimisering of anonimisering omvatten, mits aldus die doeleinden in kwestie kunnen worden

verwezenlijkt. Wanneer die doeleinden kunnen worden verwezenlijkt door verdere verwerking die de identificatie van betrokkenen niet of niet langer toelaat, moeten zij aldus worden verwezenlijkt. Tevens kan er in nationale wetgeving worden afgeweken van bepaalde rechten van betrokkenen uit de AVG voor zover die rechten de verwezenlijking van de specifieke doeleinden onmogelijk dreigen te maken of ernstig dreigen te belemmeren, en dergelijke afwijkingen noodzakelijk zijn om die doeleinden te bereiken.

De Wgbo geeft onderstaande afwijkende bepalingen voor wetenschappelijk onderzoek op het gebied van gezondheidszorg. Het uitgangspunt is dat voor het verstrekken van niet geanonimiseerde gegevens toestemming van de cliënt is vereist. In afwijking van dit uitgangspunt kan ook zonder toestemming van de cliënt ten behoeve van statistiek of wetenschappelijk onderzoek op het gebied van de volksgezondheid aan een ander desgevraagd inlichtingen over de cliënt of inzage in de bescheiden, worden verstrekt indien:

1. het vragen van toestemming in redelijkheid niet mogelijk is en bij de uitvoering van het onderzoek zodanige waarborgen gelden, dat de persoonlijke levenssfeer van de cliënt niet onevenredig wordt geschaad, of
2. het vragen van toestemming, gelet op de aard en het doel van het onderzoek, in redelijkheid niet kan worden verlangd en de hulpverlener ervoor zorgt dat gegevens in zodanige vorm worden verstrekt dat herleiding tot individuele natuurlijke personen redelijkerwijs wordt voorkomen.

Verder moet:

a) het onderzoek een algemeen belang dienen;
b) aangetoond zijn dat het onderzoek niet zonder de gegevens kan worden uitgevoerd; en
c) de betrokken cliënt tegen een verstrekking niet uitdrukkelijk bezwaar hebben gemaakt.

Belangrijk om te beseffen is dat bovenstaande voorwaarden cumulatief werken; verstrekking is pas mogelijk indien aan alle voorwaarden is voldaan.

3.2.9 Afspraken met de onderzoeker

De zorgaanbieder (verwerkingsverantwoordelijke) en de onderzoeker maken schriftelijke afspraken over de maatregelen die de onderzoeker neemt om de privacy van betrokkenen te beschermen.

3.2.10 Bewaren van persoonsgegevens

De zorgaanbieder dient de papieren en elektronische persoonsgegevens op een veilige wijze te bewaren, die in overeenstemming is met de geldende wet- en regelgeving. Persoonsgegevens worden niet langer bewaard dan noodzakelijk is om de doelen te bereiken waarvoor de gegevens worden verwerkt, tenzij de gegevens worden geanonimiseerd of indien het noodzakelijk is voor de uitoefening van het recht op vrijheid van meningsuiting en van informatie, voor de nakoming van een wettelijke verplichting, voor de uitvoering van een taak in het algemeen belang of in het kader van de uitoefening van het openbaar gezag dat aan de verwerkingsverantwoordelijke is verleend, om redenen van algemeen belang op het vlak van volksgezondheid, met het oog op archivering in het algemeen belang, wetenschappelijk of historisch onderzoek of statistische doeleinden of voor de vaststelling, uitoefening of onderbouwing van een rechtsvordering.

De zorgaanbieder stelt vast hoelang de vastgelegde/geregistreerde persoonsgegevens bewaard blijven in overeenstemming met de geldende wet- en regelgeving. Voor gezondheidsgegevens die binnen de zorgrelatie worden verwerkt, zoals het dossier van de cliënt, gelden verschillende bewaartermijnen.

3.3 Rechten van de betrokkenen (zie ook de Verzoekenprocedure)

3.3.1 Voorwaarden met betrekking tot de uitvoering van de rechten van de betrokkenen

1. Het verstrekken van de in deze paragraaf 3.3 bedoelde informatie, het verstrekken van de communicatie en het treffen van de maatregelen geschieden kosteloos. Indien het verzoek kennelijk ongegrond of buitensporig is, met name vanwege het repetitieve karakter, mag de zorgaanbieder:
    a) een redelijke vergoeding aanrekenen in het licht van de administratieve kosten waarmee het verstrekken van de gevraagde informatie of communicatie en het treffen van de gevraagde maatregelen gepaard gaan; ofwel
    b) weigeren gevolg te geven aan het verzoek.

   Het is aan de zorgaanbieder om de kennelijk ongegronde of buitensporige aard van het verzoek aan te tonen.
2. De zorgaanbieder verstrekt de betrokkene onverwijld en in ieder geval binnen een maand na ontvangst van het verzoek krachtens deze paragraaf informatie over het gevolg dat aan het verzoek is gegeven. Afhankelijk van de complexiteit van het verzoek en van het aantal verzoeken kan die termijn indien nodig met nog eens twee maanden worden verlengd. De zorgaanbieder stelt de betrokkene binnen één maand, na ontvangst van het verzoek, in kennis van een dergelijke verlenging. Wanneer de betrokkene zijn verzoek elektronisch indient, wordt de informatie indien mogelijk elektronisch verstrekt, tenzij de betrokkene anderszins verzoekt.
3. Het verzoek tot uitvoering van de rechten van betrokkenen kan gericht worden aan de medewerker privacy en informatiebeveiliging. Zie 3.6.4 voor de contactgegevens.

3.3.2 Te verstrekken informatie

1. Als de zorgaanbieder gegevens bij de betrokkene zelf opvraagt om te verwerken, informeert hij de betrokkene in een beknopte, transparante, begrijpelijke en gemakkelijk toegankelijke vorm, voorafgaand aan het verkrijgen van zijn persoonsgegevens, over:
   a) de identiteit en de contactgegevens van de zorgaanbieder;
   b) de verwerkingsdoelen waarvoor de gegevens zijn bestemd, alsook de rechtsgrond voor de verwerking;
   c) in voorkomend geval, de ontvangers of categorieën van ontvangers van de persoonsgegevens.
2. Daarnaast dient onderstaande aanvullende informatie te worden verstrekt om behoorlijke en transparante verwerking te waarborgen:
   a) de periode gedurende welke de persoonsgegevens zullen worden opgeslagen of indien dat niet mogelijk is, de criteria ter bepaling van die termijn;
   b) de mogelijkheden die de betrokkene heeft om een verzoek om inzage, rectificatie of wissen van de persoonsgegevens of beperking van de hem betreffende verwerking, alsmede het recht tegen de verwerking bezwaar te maken en het recht op gegevensoverdraagbaarheid;
   c) Indien de gegevensverwerking op toestemming is gebaseerd, dient de betrokkene geïnformeerd te worden over het recht om te allen tijde die toestemming in te trekken, zonder dat dit afbreuk doet aan de rechtmatigheid van de verwerking op basis van de toestemming voor de intrekking daarvan.
   d) het recht een klacht in te dienen bij de Autoriteit Persoonsgegevens en op welke wijze de betrokkene deze rechten kan inroepen.
   e) of de verstrekking van persoonsgegevens een wettelijke of contractuele verplichting is dan wel een noodzakelijke voorwaarde om een overeenkomst te sluiten en of de betrokkene verplicht is de persoonsgegevens te verstrekken en wat de mogelijke gevolgen zijn wanneer deze gegevens niet worden verstrekt.
3. Wanneer de zorgaanbieder voornemens heeft de persoonsgegevens verder te verwerken voor

een ander doel dan waarvoor de persoonsgegevens zijn verzameld, verstrekt de zorgaanbieder de betrokkene vóór die verdere verwerking informatie over dat andere doel en alle relevante verdere informatie als bedoeld in het tweede lid van deze bepaling.

4. De leden 1, 2 en 3 van dit artikel zijn niet van toepassing wanneer en voor zover de betrokkene reeds over de informatie beschikt.

3.3.3 Te verstrekken informatie wanneer de persoonsgegevens niet van de betrokkene zijn verkregen

1. Wanneer persoonsgegevens niet van de betrokkene zijn verkregen, verstrekt de zorgaanbieder de betrokkene alle informatie conform hierboven (artikel 3.3.1) onder lid 1 en 2 en bovendien de betrokken categorieën van persoonsgegevens alsmede de bron waar de persoonsgegevens vandaan komen.
2. De zorgaanbieder verstrekt de in het eerste lid van dit artikel bedoelde informatie:
    a) binnen een redelijke termijn, maar uiterlijk binnen één maand na de verkrijging van de persoonsgegevens, afhankelijk van de concrete omstandigheden waarin de persoonsgegevens worden verwerkt;
    b) indien de persoonsgegevens zullen worden gebruikt voor communicatie met de betrokkene, uiterlijk op het moment van het eerste contact met de betrokkene; of
    c) indien verstrekking van de gegevens aan een andere ontvanger wordt overwogen, uiterlijk op het tijdstip waarop de persoonsgegevens voor het eerst worden verstrekt.
    d) Wanneer de zorgaanbieder voornemens heeft om de persoonsgegevens verder te verwerken voor een ander doel dan dat waarvoor de persoonsgegevens zijn verkregen, verstrekt de zorgaanbieder de betrokkene vóór die verdere verwerking informatie over dat andere doel en alle relevante verdere informatie als bedoeld in het eerste lid van dit artikel.
3. De zorgaanbieder hoeft de betrokkene niet te informeren over de hiervoor genoemde informatie indien:
    a) de betrokkene al over de informatie beschikt;
    b) het informeren van betrokkene onmogelijk blijkt of een onevenredige inspanning kost. In het bijzonder bij verwerking met het oog op archivering in het algemeen belang, wetenschappelijk of historisch onderzoek of statistische doeleinden, behoudens de in artikel 89, lid 1, bedoelde voorwaarden en waarborgen, of voor zover de in lid 1 van dit artikel bedoelde verplichting de verwezenlijking van de doeleinden van die verwerking onmogelijk dreigt te maken of ernstig in het gedrang dreigt te brengen. In dergelijke gevallen neemt de zorgaanbieder passende maatregelen om de rechten, de vrijheden en de gerechtvaardigde belangen van de betrokkene te beschermen, waaronder het openbaar maken van de informatie;
    c) het verkrijgen of verstrekken van informatie (zoals hiervoor genoemd) op grond van wet- en regelgeving verplicht is voor de zorgaanbieder en die wet- en regelgeving voorziet in passende maatregelen om de gerechtvaardigde belangen van de betrokkene te beschermen; of
    d) de persoonsgegevens vertrouwelijk moeten blijven uit hoofde van een beroepsgeheim in het kader van wet- en regelgeving, waaronder een statutaire geheimhoudingsplicht.

3.3.4 Inzage en afschrift/kopie

1. De betrokkene heeft het recht op inzage en een kopie van de op zijn persoon betrekking hebbende verwerkte gegevens. De inzage of afschrift verstrekking vindt plaats voor zover daarbij de persoonlijke levenssfeer van een ander niet wordt geschaad. Bijvoorbeeld: informatie over of verstrekt door derden (niet-professionals), zoals familie en naastbetrokkenen of omstanders, wordt niet zonder voorafgaande toestemming van die derde verstrekt.

2. Een wettelijk vertegenwoordiger van een wilsonbekwame volwassene, heeft recht op inzage in of afschrift van het dossier met dezelfde uitzondering voor informatie over of verstrekt door derden (de andere ouder, familie, naastbetrokkenen en omstanders) voor zover van die vertegenwoordigers toestemming voor de behandeling is vereist. De wettelijk vertegenwoordiger krijgt alleen die informatie die noodzakelijk is voor het uitoefenen van zijn taken als wettelijk vertegenwoordiger.
3. Indien de hulpverlener door inlichtingen over de cliënt dan wel inzage in of afschrift van de bescheiden aan de (wettelijk) vertegenwoordiger te verstrekken niet geacht kan worden de zorg van een goed hulpverlener in acht te nemen, laat hij zulks achterwege.
4. Indien de zorgaanbieder van mening is dat de gevraagde inzage en/of de kopieën moeten worden verstrekt, dient dat zo spoedig mogelijk plaats te vinden/te worden verstrekt, doch uiterlijk binnen één maand. Afhankelijk van de complexiteit van het verzoek/de verzoeken en van het aantal verzoeken kan die termijn indien nodig met nog eens twee maanden worden verlengd. De zorgaanbieder stelt de betrokkene binnen één maand, na ontvangst van het verzoek, in kennis van een dergelijke verlenging. Wanneer de betrokkene zijn verzoek elektronisch indient, wordt de informatie indien mogelijk elektronisch verstrekt, tenzij de betrokkene anderszins verzoekt.

3.3.5 Rectificatie (verbetering)of aanvulling van persoonsgegevens en beperking van de verwerking van persoonsgegevens

1. De betrokkene kan de zorgaanbieder vragen om rectificatie (verbetering) van hem of haar betreffende persoonsgegevens als die onjuist zijn of de zorgaanbieder verzoeken om vervolledigen van zijn persoonsgegevens, met in acht neming van het doel van de verwerking, onder meer door een eigen aanvullende verklaring toe te voegen aan zijn dossier.
2. De zorgaanbieder informeert de verzoeker onverwijld en ten laatste binnen één maand na ontvangst van een verzoek tot aanvulling, rectificatie of wissing (verwijdering) van gegevens of en op welke manier aan het verzoek wordt voldaan. De zorgaanbieder heeft de mogelijkheid om de termijn van één maand te verlengen met nog eens twee maanden afhankelijk van de complexiteit van het verzoek. In dat geval dient de betrokkene wel binnen één maand van die verlenging in kennis te worden gesteld.
3. Als de zorgaanbieder het verzoek van betrokkene afwijst, geeft hij daarvan schriftelijk de reden. De zorgaanbieder deelt een afwijzing van het verzoek onverwijld en uiterlijk binnen één maand ontvangst van het verzoek aan de verzoeker mee. Ook informeert de zorgaanbieder de verzoeker over de mogelijkheid om een klacht in te dienen bij de Autoriteit Persoonsgegevens en de mogelijkheid om beroep in te stellen bij de rechter.
4. De betrokkene kan de zorgaanbieder vragen om bepaalde gegevens voor bepaalde personen af te schermen en hen de toegang tot die gegevens te laten blokkeren.
5. Het verzoek van een cliënt en beslissing van de zorgaanbieder tot rectificatie (verbetering), wissing of aanvulling van gegevens blijft bewaard in het dossier van de cliënt.

3.3.6 Recht op gegevenswissing (vergetelheid)

1. De betrokkene heeft het recht van de zorgaanbieder zonder onredelijke vertraging wissing van hem betreffende persoonsgegevens te verkrijgen en de zorgaanbieder is verplicht persoonsgegevens zonder onredelijke vertraging te wissen wanneer een van de volgende gevallen van toepassing is:
    a) de persoonsgegevens zijn niet langer nodig voor de doeleinden waarvoor zij zijn verzameld of anderszins verwerkt;
    b) de betrokkene trekt de toestemming waarop de verwerking berust in en er geen andere rechtsgrond is voor de verwerking;
    c) de persoonsgegevens zijn onrechtmatig verwerkt;

d) op basis van een wettelijke verplichting, die op de zorgaanbieder rust, de persoonsgegevens moeten worden gewist.

2. De zorgaanbieder stelt iedere ontvanger aan wie persoonsgegevens zijn verstrekt, in kennis van de wissing (verwijdering) van persoonsgegevens tenzij dit onmogelijk blijkt of onevenredig veel inspanning vergt. De zorgaanbieder verstrekt de betrokkene informatie over deze ontvangers indien de betrokkene hierom verzoekt.
3. Wanneer de zorgaanbieder de persoonsgegevens openbaar heeft gemaakt en overeenkomstig lid 1 verplicht is de persoonsgegevens te wissen, neemt hij, rekening houdend met de beschikbare technologie en de uitvoeringskosten, redelijke maatregelen, waaronder technische maatregelen, om verwerkingsverantwoordelijken die de persoonsgegevens verwerken, ervan op de hoogte te stellen dat de betrokkene de verwerkingsverantwoordelijken heeft verzocht om iedere koppeling naar, of kopie of reproductie van die persoonsgegevens te wissen.
5. Indien het gezondheidsgegevens betreft, wist de zorgaanbieder de gegevens zonder onredelijke vertraging en verstrekt de betrokkene in ieder geval binnen een maand na ontvangst van het verzoek informatie over het gevolg dat aan het verzoek is gegeven. Afhankelijk van de complexiteit van de verzoeken en van het aantal verzoeken kan die termijn indien nodig met nog eens twee maanden worden verlengd. De zorgaanbieder stelt de betrokkene binnen één maand na ontvangst van het verzoek in kennis van een dergelijke verlenging.
6. Een verzoek tot gegevenswissing mag alleen worden geweigerd als:
    a) de wet zich tegen de vernietiging verzet;
    Bijvoorbeeld: de gegevens en bescheiden omtrent onvrijwillige zorg in het kader van de Wzd moeten vijf jaar na beëindiging van onvrijwillige zorg bewaard blijven;
    b) een derde een aanmerkelijk belang heeft bij bewaring van die gegevens. Bijvoorbeeld: een kind van een cliënt heeft een erfelijke ziekte;
    c) de cliënt heeft een procedure tegen de hulpverlener aangespannen of het is waarschijnlijk dat hij dit zal doen;
    d) in het dossier gegevens over (vermoedens van) mishandeling staan dan kunnen deze gegevens op grond van de Meldcode Huiselijk Geweld en Kindermishandeling alleen op verzoek van het de cliënt zelf worden vernietigd en uitsluitend als de cliënt wilsbekwaam ter zake kan worden geacht;
    e) de zorgaanbieder de gegevens nodig heeft voor de instelling, uitoefening of onderbouwing van een rechtsvordering;
    f) om redenen van algemeen belang op het gebied van volksgezondheid.
7. Het verzoek tot wissing van gezondheidsgegevens en de reactie daarop worden bewaard door de zorgaanbieder.

3.3.7 Recht van bezwaar

1. De betrokkene heeft te allen tijde het recht om vanwege met zijn specifieke situatie verband houdende redenen bezwaar te maken tegen de verwerking van hem betreffende persoonsgegevens op basis van de noodzakelijkheid voor de vervulling van een taak van algemeen belang of van een taak in het kader van de uitoefening van het openbaar gezag dat aan de zorgaanbieder is opgedragen of op basis van de noodzakelijkheid voor de behartiging van de gerechtvaardigde belangen van de zorgaanbieder of van een derde;
2. De zorgaanbieder beoordeelt onverwijld en in ieder geval binnen één maand na ontvangst van het bezwaar of het bezwaar gerechtvaardigd is. Indien het bezwaar gerechtvaardigd is, beëindigt hij onmiddellijk de verwerking, tenzij er sprake is van dwingende gerechtvaardigde gronden voor de verwerking die zwaarder wegen dan de belangen, vrijheden en rechten van de betrokkene of die verband houden met de instelling, uitoefening of onderbouwing van een rechtsvordering.

3.3.8 Recht op gegevensoverdraagbaarheid (dataportabiliteit)

1. De betrokkene heeft het recht de hem betreffende persoonsgegevens, die hij aan een zorgaanbieder heeft verstrekt, in een gestructureerde, gangbare en machineleesbare vorm te verkrijgen en heeft het recht die gegevens aan een andere verwerkingsverantwoordelijke (bijvoorbeeld andere zorgaanbieder) over te dragen, zonder daarbij te worden gehinderd door de zorgaanbieder aan wie de persoonsgegevens waren verstrekt, indien de verwerking berust op toestemming of op uitvoering van een overeenkomst en de verwerking geautomatiseerd wordt verricht.
2. Bij de uitoefening van het recht op gegevensoverdraagbaarheid heeft de betrokkene het recht dat de persoonsgegevens, indien dit technisch mogelijk is, rechtstreeks van de ene zorgaanbieder naar de andere worden doorgezonden.
3. Bij de uitoefening van dit recht mag dit geen afbreuk doen aan de rechten en vrijheden van anderen.

3.3 Vertegenwoordiging

1. Is de betrokkene wilsonbekwaam ter zake, dan treedt als vertegenwoordiger voor hem op:
    a) een (toegewezen) curator of mentor;
    b) indien er geen curator of mentor is, de persoon die de cliënt schriftelijk heeft gemachtigd;
    c) indien de persoonlijk gemachtigde ontbreekt of niet optreedt; de echtgenoot of levensgezel van de betrokkene;
    d) indien de echtgenoot of levensgezel ontbreekt of niet optreedt: een kind, broer of zus van de betrokkene.
2. In het uiterste geval treedt de zorgaanbieder op als goed hulpverlener; hij zorgt dat er zo snel mogelijk een wettelijk vertegenwoordiger voor betrokkene optreedt. Zo nodig, als familie of naaste dat niet kan of wil, verzoekt hij de rechter om een vertegenwoordiger te benoemen.

3.5. Veilige verwerking van persoonsgegevens

3.5.1 Verantwoordelijkheid van de verwerkingsverantwoordelijke[1]

1. Rekening houdend met de aard, de omvang, de context en het doel van de verwerking, alsook met de qua waarschijnlijkheid en ernst uiteenlopende risico's voor de rechten en vrijheden van natuurlijke personen, treft de zorgaanbieder passende technische en organisatorische maatregelen om te waarborgen en te kunnen aantonen dat de verwerking in overeenstemming met de AVG wordt uitgevoerd. Die maatregelen worden geëvalueerd en indien nodig geactualiseerd.
2. Wanneer zulks in verhouding staat tot de verwerkingsactiviteiten, omvatten de hierboven bedoelde maatregelen een passend gegevensbeschermingsbeleid dat door de zorgaanbieder wordt uitgevoerd.

3.5.2 Gegevensbescherming door ontwerp en standaardinstellingen (Privacy by design en default)

1. Rekening houdend met de stand van de techniek, de uitvoeringskosten, en de aard, de omvang, de context en het doel van de verwerking alsook met de qua waarschijnlijkheid en ernst uiteenlopende risico's voor de rechten en vrijheden van natuurlijke personen welke aan de verwerking zijn verbonden, treft de zorgaanbieder, zowel bij de bepaling van de verwerkingsmiddelen als bij de verwerking zelf, passende technische en organisatorische maatregelen, zoals pseudonimisering, die zijn opgesteld met als doel de

[1] Artikel 24 AVG.

gegevensbeschermingsbeginselen, zoals minimale gegevensverwerking, op een doeltreffende manier uit te voeren en de nodige waarborgen in de verwerking in te bouwen ter naleving van de voorschriften van deze verordening en ter bescherming van de rechten van de betrokkenen.

2. De zorgaanbieder treft passende technische en organisatorische maatregelen om ervoor te zorgen dat in beginsel alleen persoonsgegevens worden verwerkt die noodzakelijk zijn voor elk specifiek doel van de verwerking. Die verplichting geldt voor de hoeveelheid verzamelde persoonsgegevens, de mate waarin zij worden verwerkt, de termijn waarvoor zij worden opgeslagen en de toegankelijkheid daarvan. Deze maatregelen zorgen met name ervoor dat persoonsgegevens in beginsel niet zonder menselijke tussenkomst voor een onbeperkt aantal natuurlijke personen toegankelijk worden gemaakt.

   Praktische uitwerking:

   a) De zorgaanbieder past de voor de veilige verwerking van zorggegevens de normen van de NEN 7510, 7512 en 7513 toe.
   b) Voor de verstrekking van gegevens via e-mail wordt gebruik gemaakt van de beveiligde e-mailverbinding ZIVVER.
   c) De zorgaanbieder werkt volgens de ‘Richtsnoeren beveiliging persoonsgegevens’ van de Autoriteit Persoonsgegevens en de ‘Praktijkgids patiëntgegevens in de cloud’ van de Autoriteit Persoonsgegevens.

3.5.3 Gezamenlijke verwerkingsverantwoordelijken

Wanneer twee of meer verwerkingsverantwoordelijken gezamenlijk de doeleinden en middelen van de verwerking bepalen, zijn zij gezamenlijke verwerkingsverantwoordelijken. Een betrokkene kan zijn rechten uit de AVG met betrekking tot en jegens iedere verwerkingsverantwoordelijke uitoefenen.

3.5.4 Register van verwerkingen

1. Zorgaanbieder dient een register bij te houden van de verwerkingsactiviteiten die onder hun verantwoordelijkheid plaatsvinden. Dat register bevat in ieder geval de volgende gegevens:
   a) de naam en de contactgegevens van de zorgaanbieder en eventuele gezamenlijke verwerkingsverantwoordelijken;
   b) de verwerkingsdoeleinden;
   c) de grondslag van de verwerking;
   d) een beschrijving van de categorieën van betrokkenen en van de categorieën van persoonsgegevens;
   e) de categorieën van ontvangers aan wie de persoonsgegevens zijn of zullen worden verstrekt, onder meer ontvangers in derde landen of internationale organisaties;
   f) indien mogelijk, de beoogde termijnen waarbinnen de verschillende categorieën van gegevens moeten worden gewist;
   g) indien mogelijk, een algemene beschrijving van de technische en organisatorische beveiligingsmaatregelen.
2. De verwerker en, in voorkomend geval, de vertegenwoordiger van de verwerker houdt een register van alle categorieën van verwerkingsactiviteiten die zij ten behoeve van een verwerkingsverantwoordelijke hebben verricht. Dit register bevat de volgende gegevens:
   a) de naam en de contactgegevens van de verwerkers en van iedere verwerkingsverantwoordelijke voor rekening waarvan de verwerker handelt en, in voorkomend geval, van de vertegenwoordiger van de verwerkingsverantwoordelijke of de verwerker en van de functionaris voor gegevensbescherming;
   b) de categorieën van verwerkingen die voor rekening van iedere verwerkingsverantwoordelijke zijn uitgevoerd;

c) indien van toepassing, doorgiften van persoonsgegevens aan een derde land of een internationale organisatie, onder vermelding van dat derde land of die internationale organisatie en, in geval van de in artikel 49, eerste lid, tweede alinea, van de AVG bedoelde doorgiften, de documenten inzake de passende waarborgen;
d) indien mogelijk, een algemene beschrijving van de technische en organisatorische beveiligingsmaatregelen.

3. Het register is in schriftelijke vorm, waaronder in elektronische [digitale] vorm, opgesteld.
4. Desgevraagd stellen de verwerkingsverantwoordelijke of de verwerker het register ter beschikking van de Autoriteit Persoonsgegevens.

3.5.5 Medewerking verlenen aan/samenwerken met de Autoriteit Persoonsgegevens

De zorgaanbieder en de verwerker en, in voorkomend geval, hun vertegenwoordigers, werken desgevraagd samen met de Autoriteit Persoonsgegevens bij het vervullen van haar taken.

3.5.6 Beveiliging van de verwerking

1. Rekening houdend met de stand van de techniek, de uitvoeringskosten, alsook met de aard, de omvang, de context en de verwerkingsdoeleinden en de qua waarschijnlijkheid en ernst uiteenlopende risico's voor de rechten en vrijheden van personen, treffen de zorgaanbieder en de verwerker passende technische en organisatorische maatregelen om een op het risico afgestemd beveiligingsniveau te waarborgen, die, waar passend, onder meer het volgende omvatten:
   a) de pseudonimisering en versleuteling van persoonsgegevens;
   b) het vermogen om op permanente basis de vertrouwelijkheid, integriteit, beschikbaarheid en veerkracht van de verwerkingssystemen en diensten te garanderen;
   c) het vermogen om bij een fysiek of technisch incident de beschikbaarheid van en de toegang tot de persoonsgegevens tijdig te herstellen;
   d) een procedure voor het op gezette tijdstippen testen, beoordelen en evalueren van de doeltreffendheid van de technische en organisatorische maatregelen ter beveiliging van de verwerking.
2. Bij de beoordeling van het passende beveiligingsniveau wordt met name rekening gehouden met de verwerkingsrisico's, met name als gevolg van vernietiging, verlies, wijziging of ongeoorloofde verstrekking van of ongeoorloofde toegang tot doorgezonden, opgeslagen of anderszins verwerkte gegevens, hetzij per ongeluk hetzij onrechtmatig.
3. De zorgaanbieder en de verwerker treffen maatregelen om ervoor te zorgen dat iedere natuurlijke persoon die handelt onder het gezag van de zorgaanbieder of van de verwerker en toegang heeft tot persoonsgegevens, deze slechts in opdracht van de zorgaanbieder verwerkt, tenzij hij daartoe volgens wet- en regelgeving is gehouden.

3.5.7 Melding van een inbreuk in verband met persoonsgegevens aan de Autoriteit Persoonsgegevens (datalekken melden aan de AP) en datalekkenregister

1. Indien een inbreuk in verband met persoonsgegevens heeft plaatsgevonden, meldt de zorgaanbieder dit zonder onredelijke vertraging en, indien mogelijk, uiterlijk 72 uur nadat hij er kennis van heeft genomen, aan de Autoriteit Persoonsgegevens, tenzij het niet waarschijnlijk is dat de inbreuk in verband met persoonsgegevens een risico inhoudt voor de rechten en vrijheden van natuurlijke personen. Indien de melding aan de Autoriteit Persoonsgegevens niet binnen 72 uur plaatsvindt, wordt de vertraging toegelicht (gemotiveerd).
2. De verwerker informeert de zorgaanbieder zonder onredelijke vertraging zodra hij kennis heeft genomen van een inbreuk in verband met persoonsgegevens.
3. In de melding aan de Autoriteit Persoonsgegevens wordt ten minste het volgende omschreven of meegedeeld:

a) de aard van de inbreuk in verband met persoonsgegevens, waar mogelijk onder vermelding van de categorieën van betrokkenen en persoonsgegevensregisters in kwestie en, bij benadering, het aantal betrokkenen en persoonsgegevensregisters in kwestie;
b) een contactpunt waar meer informatie kan worden verkregen;
c) de waarschijnlijke gevolgen van de inbreuk in verband met persoonsgegevens;
d) de maatregelen die de zorgaanbieder heeft voorgesteld of genomen om de inbreuk in verband met persoonsgegevens aan te pakken, waaronder, in voorkomend geval, de maatregelen ter beperking van de eventuele nadelige gevolgen daarvan.

4. Indien en voor zover het niet mogelijk is om alle informatie gelijktijdig te verstrekken, kan de informatie zonder onredelijke vertraging in stappen worden verstrekt.
5. De zorgaanbieder houdt alle inbreuken in verband met persoonsgegevens bij in een overzicht, met inbegrip van de feiten omtrent die inbreuk, de gevolgen daarvan en de genomen corrigerende maatregelen. Die documentatie stelt de Autoriteit Persoonsgegevens in staat de naleving van dit artikel te controleren.

3.5.8 Melding van een inbreuk in verband met persoonsgegevens aan de betrokkenen (datalekken melden aan de betrokkene)

1. Wanneer de inbreuk in verband met persoonsgegevens waarschijnlijk een hoog risico inhoudt voor de rechten en vrijheden van natuurlijke personen, deelt de zorgaanbieder de betrokkene de inbreuk in verband met persoonsgegevens onverwijld mee.
2. De bedoelde mededeling aan de betrokkene bevat een omschrijving, in duidelijke en eenvoudige taal, van de aard van de inbreuk in verband met persoonsgegevens en ten minste de in het vorige artikel (3.5.7, derde lid, onder b), c) en d), bedoelde gegevens en maatregelen.
3. De mededeling aan de betrokkene is niet vereist wanneer een van de volgende voorwaarden is vervuld:
   a) de zorgaanbieder heeft passende technische en organisatorische beschermingsmaatregelen genomen en deze maatregelen zijn toegepast op de persoonsgegevens waarop de inbreuk in verband met persoonsgegevens betrekking heeft, met name die welke de persoonsgegevens onbegrijpelijk maken voor onbevoegden, zoals versleuteling;
   b) de zorgaanbieder heeft achteraf maatregelen genomen om ervoor te zorgen dat het hoge risico voor de rechten en vrijheden van betrokkenen zich waarschijnlijk niet meer zal voordoen;
   c) de mededeling zou onevenredige inspanningen vergen. In dat geval komt er in de plaats daarvan een openbare mededeling of een soortgelijke maatregel waarbij betrokkenen even doeltreffend worden geïnformeerd.
4. Indien de zorgaanbieder de inbreuk in verband met persoonsgegevens nog niet aan de betrokkene heeft gemeld, kan de Autoriteit Persoonsgegevens, na beraad over de kans dat de inbreuk in verband met persoonsgegevens een hoog risico met zich meebrengt, de zorgaanbieder daartoe verplichten of besluiten dat aan een van de in lid 3 van dit artikel, bedoelde voorwaarden is voldaan.

3.5.9 Gegevensbeschermingseffectbeoordeling (Data Protection Impact Assessment, DPIA)

1. Wanneer een soort verwerking, in het bijzonder een verwerking waarbij nieuwe technologieën worden gebruikt, gelet op de aard, de omvang, de context en de doeleinden daarvan waarschijnlijk een hoog risico inhoudt voor de rechten en vrijheden van natuurlijke personen voert de zorgaanbieder vóór de verwerking een beoordeling uit van het effect van de beoogde verwerkingsactiviteiten op de bescherming van persoonsgegevens. Eén beoordeling kan een reeks vergelijkbare verwerkingen bestrijken die vergelijkbare hoge risico's inhouden.
2. Een gegevensbeschermingseffectbeoordeling als bedoeld in het eerste lid is met name vereist in

de volgende gevallen:

a) indien sprake is de verwerking van persoonsgegevens met het oog op het nemen van besluiten met betrekking tot specifieke natuurlijke personen na een systematische en uitgebreide beoordeling van persoonlijke aspecten van natuurlijke personen, die is gebaseerd op geautomatiseerde verwerking, waaronder profilering, en waarop besluiten worden gebaseerd waaraan voor de natuurlijke persoon rechtsgevolgen zijn verbonden of die de natuurlijke persoon op vergelijkbare wijze wezenlijk treffen;
b) er sprake is van een grootschalige verwerking van bijzondere categorieën van persoonsgegevens, zoals gezondheidsgegevens;
c) er sprake is van stelselmatige en grootschalige monitoring van openbaar toegankelijke ruimten.

3. De beoordeling bevat ten minste:
   a) een systematische beschrijving van de beoogde verwerkingen en de verwerkingsdoeleinden;
   b) een beoordeling van de noodzaak en de evenredigheid van de verwerkingen met betrekking tot de doeleinden;
   c) een beoordeling van het eerste lid van dit artikel bedoelde risico's voor de rechten en vrijheden van betrokkenen; en
   d) de beoogde maatregelen om de risico's aan te pakken, waaronder waarborgen, veiligheidsmaatregelen en mechanismen om de bescherming van persoonsgegevens te garanderen en om aan te tonen dat aan deze verordening is voldaan, met inachtneming van de rechten en gerechtvaardigde belangen van de betrokkenen en andere personen in kwestie.
4. Bij het beoordelen van het effect van de door een zorgaanbieder of verwerker verrichte verwerkingen en met name ter wille van een gegevensbeschermingseffectbeoordeling, wordt de naleving van goedgekeurde gedragscodes naar behoren in aanmerking genomen.
5. De zorgaanbieder vraagt in voorkomend geval de betrokkenen of hun vertegenwoordigers naar hun mening over de voorgenomen verwerking, met inachtneming van de bescherming van commerciële of algemene belangen of de beveiliging van verwerkingen.
6. Indien nodig verricht de zorgaanbieder een toetsing om te beoordelen of de verwerking overeenkomstig de gegevensbeschermingseffectbeoordeling wordt uitgevoerd, zulks ten minste wanneer sprake is van een verandering van het risico dat de verwerkingen inhouden.

3.5.10 Voorafgaande raadpleging van de Autoriteit Persoonsgegevens

1. Wanneer uit een gegevensbeschermingseffectbeoordeling blijkt dat de verwerking een hoog risico zou opleveren indien de zorgaanbieder geen maatregelen neemt om het risico te beperken, raadpleegt de zorgaanbieder voorafgaand aan de verwerking de Autoriteit Persoonsgegevens.
2. Wanneer de Autoriteit Persoonsgegevens van oordeel is dat de bedoelde voorgenomen verwerking inbreuk zou maken op deze verordening, met name wanneer de zorgaanbieder het risico onvoldoende heeft onderkend of beperkt, geeft de Autoriteit Persoonsgegevens binnen maximaal acht weken na de ontvangst van het verzoek om raadpleging schriftelijk advies aan de zorgaanbieder en in voorkomend geval aan de verwerker, en mag zij al haar bevoegdheden uitoefenen. Die termijn kan, naargelang de complexiteit van de voorgenomen verwerking, met zes weken worden verlengd. Bij een dergelijke verlenging stelt de Autoriteit Persoonsgegevens de zorgaanbieder en, in voorkomend geval, de verwerker binnen een maand na ontvangst van het verzoek om raadpleging in kennis van onder meer de redenen voor de vertraging. Die termijnen kunnen worden opgeschort totdat de Autoriteit Persoonsgegevens informatie heeft verkregen waarom zij met het oog op de raadpleging heeft verzocht.

3. Bij de raadpleging verstrekt de zorgaanbieder de nodige informatie zoals benoemd in de AVG. In ieder geval dienen de volgende gegevens te worden verstrekt:
    a) indien van toepassing, de verantwoordelijkheden van de zorgaanbieder, bij de verwerking betrokken gezamenlijke verwerkingsverantwoordelijken en verwerkers, in het bijzonder ten aanzien van een verwerking binnen een concern;
    b) de doeleinden en middelen van de voorgenomen verwerking;
    c) de maatregelen en waarborgen die worden geboden ter bescherming van de rechten en vrijheden van betrokkenen uit hoofde van de AVG;
    d) de gegevenseffectbeoordeling ten aanzien van die verwerking;
    e) alle andere informatie waar de Autoriteit Persoonsgegevens om verzoekt.

3.6. Functionaris voor gegevensbescherming (FG)

3.6.1 Aanwijzing van een functionaris voor gegevensverwerking

1. Zorgcentrum Beek & Bos verwerkt bijzondere persoonsgegevens, maar niet op grote schaal. Daarom is het aanwijzen van een functionaris voor gegevensbescherming niet vereist;
2. Binnen zorgcentrum Beek & Bos vervult de beleidsmedewerker de rol van medewerker privacy en informatiebeveiliging;
3. Voor de medewerker privacy en informatiebeveiliging is een rolbeschrijving vastgesteld.

3.6.2 Bij een klacht

Bij een klacht over de naleving van dit reglement kan de betrokkene zich wenden tot:
De beleidsmedewerker, tevens medewerker privacy en informatiebeveiliging:

Carlien Vaes
0475-391700
cvaes@beekenbos.nl

De Autoriteit Persoonsgegevens
www.autoriteitpersoonsgegevens.nl

Voor andere klachten raadpleegt de betrokkene de klachtenregeling van de zorgaanbieder.

3.6.3 Slotbepaling

Dit reglement geldt per 25 mei 2018 en is voor medewerkers van Beek en Bos in te zien via de digitale Organisatiegids. Betrokkenen kunnen het reglement opvragen bij de medewerker privacy en informatiebeveiliging (zie 3.6.4 voor de contactgegevens).