



**Model privacyreglement
Thuiszorg Maasland
Januari 2018**

Inhoudsopgave

1. Inleiding	3
1.1 Waarom dit model?	3
2. Relatie met andere wetten	3
Algemene Verordening Gegevensbescherming (AVG)	3
3. Model Privacyreglement	4
3.1 Definities	4
3.2 Verwerking van persoonsgegevens van cliënten in overeenstemming met de AVG	5
3.2.1 Beginselen inzake persoonsgegevens verwerking	5
3.2.2 Rechtmatigheid van de verwerking	5
3.2.3 Voorwaarden voor het verwerken van gezondheidsgegevens	6
3.2.4 Gegevensverwerking door verwerker	7
3.2.5 Aansprakelijkheid verwerkingsverantwoordelijke en/of verwerker	7
3.2.6 Wanneer mogen andere bijzondere gegevens dan de gezondheidsgegevens worden verwerkt?	7
3.2.7 Geheimhoudingsplicht en verstrekking aan derden	7
3.2.8 Wanneer mogen gegevens aan een ander worden verstrekt voor wetenschappelijk onderzoek en statistiek op het gebied van de volksgezondheid?	8
3.2.9 Afspraken met de onderzoeker.....	8
3.2.10 Bewaren van persoonsgegevens	8
3.3 Rechten van de betrokkenen	9
3.3.1 Voorwaarden met betrekking tot de uitvoering van de rechten van de betrokkenen ..	9
3.3.1 Te verstrekken informatie	9
3.3.2 Te verstrekken informatie wanneer de persoonsgegevens niet van de betrokkene zijn verkregen	10
3.3.3 Inzage en afschrift/kopie	11
3.3.4 Rectificatie (verbetering)of aanvulling van persoonsgegevens en beperking van de verwerking van persoonsgegevens	12
3.3.5 Recht op gegevenswissing (vergetelheid)	12
3.3.6 Recht van bezwaar	13
3.3.6 Recht op gegevensoverdraagbaarheid (dataportabiliteit)	14
3.4 Vertegenwoordiging	15
3.5 Veilige verwerking van persoonsgegevens	16
3.5.1 Verantwoordelijkheid van de verwerkingsverantwoordelijke.....	16
3.5.2 Gegevensbescherming door ontwerp en standaardinstellingen (Privacy by design en default)	16
3.5.3 Gezamenlijke verwerkingsverantwoordelijken	17
3.5.4 Register van verwerkingen	17
3.5.5 Medewerking verlenen aan/samenwerken met de Autoriteit persoonsgegevens	18
3.5.6 Beveiliging van de verwerking	18
3.5.7 Melding van een inbreuk in verband met persoonsgegevens aan de Autoriteit Persoonsgegevens (datalekken melden aan de AP) en datalekkenregister	19
3.5.8 Melding van een inbreuk in verband met persoonsgegevens aan de betrokkenen (datalekken melden aan de betrokkene)	19
3.5.9 Gegevensbeschermingseffectbeoordeling (Data Protection Impact Assessment, DPIA)	20
3.5.10 Voorafgaande raadpleging van de Autoriteit Persoonsgegevens	21
3.6 Motivering niet aanstelling van een functionaris voor gegevensbescherming	22
Andere situaties	22
Motivatie	22
3.6.1 Bij een klacht	23

1. Inleiding

1.1 Waarom dit model?

Met dit model privacyreglement geeft Thuiszorg Maasland een voorbeeld voor een praktische en toegankelijke uitwerking van de vanaf 25 mei 2018 geldende privacyregels neergelegd in de Algemene Verordening Gegevensbescherming (hierna: AVG) en sectorspecifieke wetten.

De AVG stelt het opstellen van privacy beleid (gegevensbeschermingsbeleid) verplicht, als onderdeel van de verantwoordingsplicht, 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. Op verzoek van een betrokkene wordt het (schriftelijke) privacy beleid ter beschikking gesteld.

Met dit document wordt het bestaand model privacyreglement tot 2018 vervangen. Dit nieuwe model is gebaseerd op de AVG (die vanaf 25 mei 2018 van toepassing is) en nationale (sector)specifieke wetgeving. Het betreft een weergave op grote lijnen; voor bijzondere uitwerking van privacy onderwerpen wordt in de tekst verwezen naar andere documenten.

Binnen uw eigen document kunt u verwijzen naar aanvullende informatie over bijzondere privacy-onderwerpen die u binnen uw instelling hanteert; een overzicht van bijzondere documenten (en waar deze te vinden zijn), kunt u in een bijlage opnemen.

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 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.¹ De bepalingen uit de AVG gelden voor alle Europese landen gelijk 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. Anders dan bij een richtlijn heeft een verordening niet te worden omgezet in een nationale regeling. De verordening werkt dus rechtstreeks. 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 AVG waarvan in december 2017 nog geen definitieve versie van beschikbaar is.² De AVG biedt de lidstaten ook ruimte om eigen regels voor de toepassing vast te stellen in sectorspecifieke wetten.

¹ Artikel 9 AVG.² Op 13 december 2017 is de Uitvoeringswet aangeboden aan de Tweede Kamer. Het idee is dat op 25 mei 2018 ook deze Uitvoeringswet in werking moet treden. Echter dient de Parlementaire proces nog te worden doorlopen.

3. Model Privacyreglement

Dit reglement is van toepassing binnen Thuiszorg Maasland te Rotterdam en heeft betrekking op de verwerkingen van gegevens van cliënten die van Thuiszorg Maasland krijgen.

Dit reglement is van toepassing op zowel op papier als elektronische verwerking van gegevens.

3.1 Definities

Autoriteit Persoonsgegevens (AP): de toezichhoudende 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, meestal de cliënt, of zijn (wettelijk) vertegenwoordiger.

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.

Functionaris voor gegevensbescherming (FG): functionaris die door de zorgaanbieder moet of kan worden aangesteld voor het informeren en adviseren over en het toezicht houden op de toepassing en naleving van de AVG en andere gegevensbeschermingsbepalingen.

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. Onder een 'datalek' valt dus niet alleen het vrijkomen (lekken) van gegevens, maar ook onrechtmatige verwerking van 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.

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).

Verwerker: degene die in opdracht van en voor de verwerkingsverantwoordelijke persoonsgegevens verwerkt (bijvoorbeeld een externe hostingsfirma, saas-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: Thuiszorg Maasland

3.2 Verwerking van persoonsgegevens van cliënten in overeenstemming met de AVG

3.2.1 Beginselen inzake persoonsgegevens verwerking³

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").⁴

Binnen Thuiszorg Maasland 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 wordt⁵ 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 verwerkt⁶ 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 verwerking⁷

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

³ Let op: in de AVG wordt de rechtmatig van de verwerking van persoonsgegevens geregeld in artikel 6. Dat artikel staat echter na het artikel over de beginselen inzake de verwerking (zoals doelbinding, juistheid, etc.). Maar, als er geen grondslag is voor rechtmatige gegevensverwerking, mag er helemaal niet verwerkt worden en komt men dus niet toe aan de beginselen die moeten worden nageleefd bij de verwerking van persoonsgegevens.

⁴ De beginselen inzake verwerking de verwerking van persoonsgegevens en de verantwoordingsplicht volgen uit artikel 5 AVG.

⁵ Overeenkomstig artikel 89, eerste lid, AVG.

⁶ Overeenkomstig artikel 89, eerste lid, AVG.

⁷ Artikel 6 AVG.

- de betrokkene heeft toestemming⁸ 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;
- de gegevensverwerking noodzakelijk is ter bescherming van de vitale belangen van de betrokkene of een ander natuurlijk persoon⁹;
- de gegevensverwerking noodzakelijk is voor de goede vervulling van een taak van algemeen belang, dat elders in een wet is vastgelegd met eventuele nadere bepalingen;
- de gegevensverwerking noodzakelijk is voor de behartiging van de gerechtvaardigde belangen¹⁰ van de verwerkingsverantwoordelijke of van een derde én de belangen, grondrechten of fundamentele vrijheden van degene van wie de gegevens worden verwerkt niet prevaleren.

3.2.3 Voorwaarden voor het verwerken van gezondheidsgegevens¹¹

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 voorwaarden¹²:

- Als de verwerking noodzakelijk is voor doeleinden van preventieve of arbeidsgeneeskunde, voor de beoordeling van de arbeidsgeschiktheid van de werknemer, medische diagnoses, 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).¹³

⁸ Voor de voorwaarden die aan de toestemming zijn verbonden, zie definities. Wat betreft jeugdigen gelden de leeftijdsregimes uit de Wgbo en Jeugdwet wat betreft de toestemming.

⁹ De AVG geeft in overweging (46) aan dat de verwerking van persoonsgegevens ook als rechtmatig wordt beschouwd indien zij noodzakelijk is voor de bescherming dat voor het leven van de betrokkene of dat van een ander persoon essentieel is. Deze grond voor verwerking is slechts toegestaan als de verwerking kennelijk niet op een andere rechtsgrond kan worden gebaseerd.

¹⁰ In overweging (47) en (49) AVG: een gerechtvaardigd belang kan aanwezig zijn wanneer sprake is van een relevante en passende verhouding tussen de betrokkene en de verwerkingsverantwoordelijke, in situaties waarin de betrokkene een klant is of in dienst is van de verwerkingsverantwoordelijke. In elk geval is een zorgvuldige beoordeling geboden om te bepalen of er sprake is van een gerechtvaardigd belang. De belangen en de grondrechten van de betrokkene kunnen met name zwaarder wegen wanneer persoonsgegevens worden verwerkt in omstandigheden waarin de betrokkenen redelijkerwijs geen verdere verwerking verwachten. De verwerking van persoonsgegevens voor zover die strikt noodzakelijk en evenredig is met het oog op netwerk- en informatiebeveiliging vormt een gerechtvaardigd belang van de verwerkingsverantwoordelijke in kwestie.

¹¹ Artikel 9, tweede lid, AVG.

¹² Artikel 9 AVG.

¹³ Op grond van de AVG is het voor lidstaten toegestaan om andere voorwaarden, waaronder beperkingen, met betrekking tot de verwerking van gegevens over de gezondheidszorg te handhaven of in te voeren (overweging (53) AVG). Hierbij kan gedacht worden aan de bepalingen in de Wgbo met betrekking tot het beroepsgeheim. Dergelijke bepalingen zullen dan naast de bepalingen uit de AVG gelden. Dit betekent dat een zorgaanbieder slechts aan derden gegevens betreffende iemands gezondheid mag verstrekken als dat mag op grond van de AVG (o.a. de hierboven genoemde voorwaarden) én als er sprake is van een grond om het

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.¹⁴ 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.¹⁵

3.2.5 Aansprakelijkheid verwerkingsverantwoordelijke en/of verwerker

1. 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.
2. 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 elke cliënt. 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

1. Persoonsgegevens verkregen in de uitoefening van een beroep in de thuiszorg vallen onder de geheimhoudingsplicht van de hulpverlener. Deze geheimhoudingsplicht is o.a. vastgelegd in de Wgbo en/of Jeugdwet en de wet BIG en in verschillende beroepscode's.
2. Bij de verstrekking van gegevens aan derden wordt de wet nageleefd.

medisch beroepsgeheim te doorbreken.

¹⁴ Artikel 28 AVG.

¹⁵ Artikel 29 AVG.

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 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.¹⁶ 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 Wgbo¹⁷ geeft onderstaande afwijkende bepalingen voor wetenschappelijk onderzoek op het gebied van de gezondheidszorg. Het uitgangspunt is dat voor het verstrekken van niet geanonimiseerde¹⁸ 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 is¹⁹ 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

¹⁶ Artikel 89 AVG.

¹⁷ Artikel 7:457 en 7:458 BW (Wgbo).

¹⁸ Pseudonimisering is een beveiligingsmaatregel (versleuteling of apart opslaan van identificerende gegevens los van de inhoudelijke) die direct herleiden tot een natuurlijke persoon onmogelijk maakt, maar indirecte herleiding (bijvoorbeeld door koppeling aan andere reeds bekende gegevens) blijft mogelijk. Daarom blijven gepseudonimiseerde gegevens persoonsgegevens en blijven de AVG-bepalingen en die uit de sectorspecifieke wetten over privacy van toepassing. Zie ook overweging (29) AVG.

¹⁹ Bijvoorbeeld als het gaat om een historisch onderzoek naar Jaren geleden verzamelde gegevens over personen van wie de adressen niet meer te achterhalen zijn. *Kamerstukken II*, 21561, 20, p. 3.

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.²⁰ De zorgaanbieder stelt vast hoelang de vastgelegde/geregistreerde persoonsgegevens bewaard blijven in overeenstemming met de geldende wet- en regelgeving

3.3 Rechten van de betrokkenen

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.²¹

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.

3.3.1 Te verstrekken informatie²²

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 vorm²³, voorafgaand aan het verkrijgen van zijn persoonsgegevens, over:

- a) de identiteit en de contactgegevens van de zorgaanbieder;
- b) indien van toepassing de contactgegevens van de functionaris voor gegevensbescherming
- c) de verwerkingsdoelen waarvoor de gegevens zijn bestemd, alsook de rechtsgrond voor de verwerking;

²⁰ Artikel 17, derde lid, AVG (overweging 65).

²¹ Artikel 12 AVG.

²² Artikel 13 AVG. Let op: ook de Wgbo kent in artikel 7:448 BW een informatieplicht over behandelinhoudelijke zaken.

²³ En in duidelijke en eenvoudige taal. Zie hiervoor artikel 12, eerste lid, AVG.

d) 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 wissing 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 invoeren.

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.

3.3.2 Te verstrekken informatie wanneer de persoonsgegevens niet van de betrokkene zijn verkregen²⁴

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:

²⁴ Artikel 14 AVG.

- 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.

3.3.3 Inzage en afschrift/kopie²⁵

1. De betrokkene van twaalf jaar of ouder 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 jongeren onder de 16 jaar of 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. ²⁶ De vertegenwoordiger krijgt alleen die informatie die noodzakelijk is voor het uitoefenen van zijn taken als 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 achterwege²⁷. Bijvoorbeeld als een minderjarige bezwaar maakt tegen het verstrekken van (bepaalde) informatie aan de ouders of bij een vermoeden van kindermishandeling. In dat geval kan een ouder inzage in het dossier van de minderjarige worden geweigerd. Onder omstandigheden kan de hulpverlener in dat geval feitelijk worden belemmerd om de wettelijk vertegenwoordigers voldoende te informeren om hun toestemming voor de behandeling van de minderjarige te verkrijgen.
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

²⁵ Artikel 7:456, 7:457 BW (Wgbo).

²⁶ In de Wgbo wordt de minderjarigheidsgrens verlaagd van 18 jaar naar 16 jaar. Bij jongeren die de leeftijd van 16 jaar hebben bereikt, is toestemming van de ouders (wettelijk vertegenwoordigers) en het verstrekken van de nodige informatie om toestemming te geven daarom niet nodig, tenzij de betrokkene ter zake wilsonbekwaam is.

²⁷ Artikel 7:457, derde lid, BW (Wgbo).

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.²⁸

3.3.4 Rectificatie (verbetering) of aanvulling van persoonsgegevens en beperking van de verwerking van persoonsgegevens²⁹

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 vervollediging 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 schriftelijk³⁰ 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.

3.3.5 Recht op gegevenswissing (vergetelheid)³¹

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.³²
3. Wanneer de zorgaanbieder de persoonsgegevens openbaar heeft gemaakt en overeenkomstig lid 1 verplicht is de persoonsgegevens te wissen, neemt hij, rekening

²⁸ Artikel 12 AVG (algemene regels voor de uitoefening van de rechten van de betrokkene).

²⁹ Artikel 12 AVG e.v. AVG, artikel 16 AVG.

³⁰ De betrokkene dient schriftelijk of met andere middelen, met inbegrip van , indien dit passend is, elektronische middelen, de informatie te verstrekken.

³¹ Artikel 17 AVG in samenhang met artikel 12 lid 3 e.v. AVG.

³² Artikel 19 AVG.

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: het dossier aangelegd binnen een gedwongen behandeling moet vijf jaar na beëindiging van de BOPZ-behandeling of verblijf in het ziekenhuis bewaard blijven. Een verzoek van een cliënt tot vernietiging binnen vijf jaar kan niet worden gehonoreerd;

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) kindermishandeling staan dan kunnen deze gegevens op grond van de Meldcode Huiselijk Geweld en Kindermishandeling alleen op verzoek van het kind zelf worden vernietigd en uitsluitend als het kind de leeftijd van 16 jaar heeft bereikt en 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.³³

3.3.6 Recht van bezwaar³⁴

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.

³³ In dat geval kan bij een materiële controle aan de financier worden aangetoond dat het dossier, op verzoek van betrokkene, is vernietigd.

³⁴ Artikel 21 AVG.

3.3.6 Recht op gegevensoverdraagbaarheid (dataportabiliteit)³⁵

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.

³⁵ Artikel 20 AVG.

3.4 Vertegenwoordiging

1. Bij een jeugdige jonger dan twaalf jaar en bij een wilsonbekwame jeugdige van twaalf tot achttien jaar, oefent (oefenen) de ouder(s) met gezag of de voogd de rechten van de jeugdige uit, tenzij dit niet verenigbaar is met de zorg van een goed hulpverlener.³⁶
2. De ouder die geen gezag heeft krijgt desgevraagd belangrijke, algemene en feitelijke informatie³⁷ over de gezondheidstoestand van de jeugdige, tenzij:
 - a. de hulpverlener de informatie ook niet aan de ouder met gezag heeft verstrekt/ verstrekt;
 - b. niet in niet verenigbaar is met de zorg van een goed hulpverlener.
3. De wilsbekwame jeugdige van twaalf jaar of ouder oefent zelfstandig zijn rechten over zijn persoons- en gezondheidsgegevens uit.³⁸ Vernietiging van gegevens over (vermoedens van) kindermishandeling vindt uitsluitend plaats met toestemming van een wilsbekwame jeugdige van zestien jaar en ouder.
4. Is de betrokkene ouder dan achttien jaar en 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.
5. In het uiterste geval treedt de zorgaanbieder op als goed hulpverlener; hij zorgt er voor 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.

³⁶ Artikel 457 BW (Wgbo). Dit kan aan de orde zijn als de hulpverlener meent dat het niet in belang van de jeugdige is of als de jeugdige niet wil dat bepaalde informatie wordt verstrekt.

³⁷ Er mag slechts informatie worden verstrekt die feitelijk, globaal, belangrijk en doelgericht is.

3.5 Veilige verwerking van persoonsgegevens

3.5.1 Verantwoordelijkheid van de verwerkingsverantwoordelijke³⁹

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. Het aansluiten bij goedgekeurde gedragscodes of goedgekeurde certificeringsmechanismen kan worden gebruikt als element om aan te tonen dat de verplichtingen van de zorgaanbieder zijn nagekomen.

3.5.2 Gegevensbescherming door ontwerp en standaardinstellingen (Privacy by design en default)⁴⁰

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 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.
3. Een goedgekeurd certificeringsmechanisme kan worden gebruikt als element om aan te tonen dat aan de voorschriften is voldaan.
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.
 - c) De zorgaanbieder werkt volgens de 'Richtsnoeren beveiliging persoonsgegevens' van de Autoriteit Persoonsgegevens en de 'Praktijkgids patiëntgegevens in de cloud' van de Autoriteit Persoonsgegevens.
 - d) De identificerende gegevens zijn zoveel als mogelijk gescheiden opgeslagen van de inhoudelijke gegevens, gepseudonimiseerd of versleuteld.

³⁹ Artikel 24 AVG.

⁴⁰ Artikel 25 AVG.

- e) De standaardinstellingen zijn nee, tenzij (opt-in) in plaats van ja, mits (opt-out), tenzij de wetgeving opt-out toelaatbaar stelt.
- f) De zorgaanbieder hanteert per verwerking een autorisatieprotocol. Daarin staat welke gegevens door wie/welke (groepen) medewerkers verwerkt kunnen worden en waarom en welke bevoegdheden zij hebben ten aanzien van welke gegevens (inzage, toevoegen, wijzigen, verwijderen).

3.5.3 Gezamenlijke verwerkingsverantwoordelijken⁴¹

1. Wanneer twee of meer verwerkingsverantwoordelijken gezamenlijk de doeleinden en middelen van de verwerking bepalen, zijn zij gezamenlijke verwerkingsverantwoordelijken. Zij stellen op transparante wijze hun respectieve verantwoordelijkheden voor de nakoming van de verplichtingen uit hoofde van deze AVG vast, met name met betrekking tot de uitoefening van de rechten van de betrokkene en hun respectieve verplichtingen om de verplichte informatie te verstrekken, door middel van een onderlinge regeling. In de regeling kan een contactpunt voor betrokkenen worden aangewezen.
2. Uit de bedoelde regeling blijkt duidelijk welke rol de gezamenlijke verwerkingsverantwoordelijken respectievelijk vervullen, en wat hun respectieve verhouding met de betrokkenen is. De wezenlijke inhoud van de regeling wordt aan de betrokkene beschikbaar gesteld.
3. Ongeacht een dergelijke regeling kan een betrokkene zijn rechten uit de AVG met betrekking tot en jegens iedere verwerkingsverantwoordelijke uitoefenen.

3.5.4 Register van verwerkingen⁴²

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, en van de functionaris voor gegevensbescherming;
 - b) de verwerkingsdoeleinden;
 - c) een beschrijving van de categorieën van betrokkenen en van de categorieën van persoonsgegevens;
 - d) de categorieën van ontvangers aan wie de persoonsgegevens zijn of zullen worden verstrekt, onder meer ontvangers in derde landen of internationale organisaties;
 - e) indien van toepassing, doorgiften van persoonsgegevens aan een derde land of een internationale organisatie, met inbegrip van de vermelding van dat derde land of die internationale organisatie en, in geval van de in artikel 49, lid 1, tweede alinea, van de AVG bedoelde doorgiften, de documenten inzake de passende waarborgen;
 - 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;

⁴¹ Artikel 26 AVG.

⁴² Artikel 30 AVG.

- 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 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 persoonsgegevens⁴³

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 verwerking⁴⁴

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 verwerkingsystemen 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. Het aansluiten bij een goedgekeurde gedragscode of een goedgekeurd certificeringsmechanisme kan worden gebruikt als element om aan te tonen dat de in lid 1 van dit artikel bedoelde vereisten worden nageleefd.

4. 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.

⁴³ Artikel 31 AVG.

⁴⁴ Artikel 32 AVG.

3.5.7 Melding van een inbreuk in verband met persoonsgegevens aan de Autoriteit Persoonsgegevens (datalekken melden aan de AP) en datalekkenregister⁴⁵

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) de naam en de contactgegevens van de functionaris voor gegevensbescherming of een ander 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)⁴⁶

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;

⁴⁵ Artikel 33 AVG.

⁴⁶ Artikel 34 AVG.

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)⁴⁷

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.⁴⁸ Eén beoordeling kan een reeks vergelijkbare verwerkingen bestrijken die vergelijkbare hoge risico's inhouden.

2. Wanneer een functionaris voor gegevensbescherming is aangewezen, wint de zorgaanbieder bij het uitvoeren van een gegevensbeschermingseffectbeoordeling diens advies in.

3. Een gegevensbeschermingseffectbeoordeling als bedoeld in het eerste lid is met name vereist in de volgende gevallen⁴⁹:

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.

4. 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.

⁴⁷ Artikel 35 AVG.

⁴⁸ De Autoriteit Persoonsgegevens zal een lijst opstellen van het soort verwerkingen waarvoor een gegevensbeschermingseffectbeoordeling verplicht is. Een dergelijke lijst is nu nog niet beschikbaar. Artikel 35, vijfde lid, AVG.

⁴⁹ Overweging (91) AVG.

5. 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.
6. 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.
7. 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 Persoonsgegevens⁵⁰

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.⁵¹
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 contactgegevens van de functionaris voor gegevensbescherming;
 - e) de gegevenseffectbeoordeling ten aanzien van die verwerking;
 - f) alle andere informatie waar de Autoriteit Persoonsgegevens om verzoekt.

⁵⁰ Artikel 36 AVG.

⁵¹ Uit overweging (94) AVG volgt dat dit gaat om situaties waarbij de zorgaanbieder van mening is dat het niet mogelijk het risico te beperken door middel van maatregelen die met het oog op de beschikbare technologie en uitvoeringskosten redelijk zijn

3.6 Motivering niet aanstelling van een functionaris voor gegevensbescherming

Per 25 mei 2018 geldt de Algemene verordening gegevensbescherming (AVG). Vanaf dit moment kunnen organisaties verplicht zijn een functionaris voor de gegevensbescherming (FG) aan te stellen. Op grond van artikel 37 van de AVG is een FG in een van de drie volgende situaties:

1. Overheden en publieke organisaties

Ten eerste zijn overheidsinstanties en publieke organisaties altijd verplicht om een FG aan te stellen, ongeacht het type gegevens dat ze verwerken. Het kan gaan om de rijksoverheid, gemeenten en provincies, maar ook om bijvoorbeeld zorg- en onderwijsinstellingen (Bijvoorbeeld ziekenhuizen en scholen). Voor rechtbanken geldt de verplichte aanstelling van een FG niet.

2. Observatie

Ten tweede geldt de verplichting om een FG aan te stellen voor organisaties die vanuit hun kernactiviteiten op grote schaal individuen volgen. Relevant hierbij zijn onder meer het aantal mensen dat een organisatie volgt, de hoeveelheid gegevens die deze organisatie verwerkt en hoe lang de organisatie mensen volgt.

3. Bijzondere persoonsgegevens

Ten derde zijn organisaties verplicht een FG te benoemen als ze op grote schaal bijzondere persoonsgegevens verwerken en dit een kernactiviteit is. Bijzondere persoonsgegevens zijn bijvoorbeeld gegevens over iemands gezondheid, ras, politieke opvatting, geloofsovertuiging of strafrechtelijke verleden.

Andere situaties

EU-lidstaten kunnen ook andere situaties benoemen waarin een FG verplicht is. Het is nog niet bekend of dit in Nederland gaat gebeuren. Wanneer onduidelijk is of een organisatie verplicht is om een FG aan te stellen, moet de organisatie goed kunnen onderbouwen waarom ervoor gekozen is om dat wel of niet te doen. Bij twijfel kunt u contact opnemen met de Autoriteit Persoonsgegevens.

Motivatie

Op 5 maart te Rotterdam is Thuiszorg Maasland tot de conclusie gekomen om niet een Functionaris Gegevensbescherming aan te stellen. Hieronder volgt een uiteenzetting waarom Thuiszorg Maasland van mening is dat de organisatie geen FG hoeft aan te stellen. Dit document is opgesteld om de Autoriteit Persoonsgegevens inzicht te geven in de besluitvorming waarom niet een FG is aangesteld.

Allereerst is Thuiszorg Maasland geen overheid of publieke organisatie. Thuiszorg Maasland verleent zorg en is een private organisatie. Op basis van dit criterium behoeft daarom volgens Thuiszorg Maasland geen FG aangesteld te worden.

Ten tweede is het volgen van grote schaal individuen niet een kerntaak van Thuiszorg Maasland. Thuiszorg Maasland verleent maatwerk dat sluit op de wensen en behoeften van de klant. De gegevens die worden verwerkt voor de gebruikelijke werkzaamheden zijn zeer beperkt en is de duur van de gegevensverwerking heel kort. Op basis van dit criterium behoeft daarom volgens Thuiszorg Maasland geen FG aangesteld te worden. Tenslotte worden er binnen Thuiszorg Maasland enkel gegevens verwerkt die voor de gebruikelijke werkzaamheden nodig zijn en die ook wettelijk zijn vastgesteld. Samenvattend de bovenstaande redenen hebben geleid tot het besluit om geen FG aan te stellen voor Thuiszorg Maasland. Wel heeft Thuiszorg Maasland een veiligheidsconsulent aangesteld die wordt vervuld door de cliënten coördinator.

3.6.1 Bij een klacht

Bij een klacht over de naleving van dit reglement kan de betrokkene zich wenden tot:

De verwerkingsverantwoordelijke/zorgaanbieder U.Kay;

Contactgegevens service@thuiszorgmaasland.nl

De functionaris voor gegevensverwerking

Contactgegevens

De Autoriteit Persoonsgegevens

Contactgegevens

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

3.6.2 Wijzigingen en inzage van dit reglement

Dit reglement geldt per 25 mei 2018 en is op www.thuiszorgmaasland.nl in te zien.