PRIVACYREGLEMENT

ALGEMEEN

Voor u ligt het privacyreglement dat van toepassing is binnen De Gelderhorst in Ede.

In dit reglement kunt u lezen hoe wij binnen De Gelderhorst omgaan met uw persoonsgegevens. Ook leest u welke rechten u heeft met betrekking tot uw privacy en hoe u deze kunt uitoefenen. Op onze website hebben wij ook onze privacyverklaring gepubliceerd. U leest hier in een notendop welke gegevens De Gelderhorst verzamelt, voor welke doelen en hoe lang deze gegevens bewaard blijven.

TOEPASSELIJKHEID

Dit reglement ziet op de verwerking van persoonsgegevens van cliënten die wonen bij De Gelderhorst en cliënten die deelnemen aan de dagbesteding. Dit reglement is van toepassing op zowel op papier als elektronische verwerking van gegevens.

PRIVACYWETGEVING

Aangezien wij binnen de Gelderhorst veel en privacygevoelige persoonsgegevens verwerken, is het uiterst belangrijk dat de privacywetgeving en dit reglement worden nageleefd.

VRAGEN, OPMERKINGEN, KLACHTEN OVER PRIVACY

Voor vragen over dit reglement of andere privacy gerelateerde vragen, opmerkingen of bezwaren kunt u terecht bij:

De verwerkingsverantwoordelijke/zorgaanbieder
De Gelderhorst, Judith Reiff – de Groen (Bestuurder)
Willy Brandtlaan 40, 6716 RK te Ede

De functionaris voor gegevensbescherming
Paula Dingler FG
Willy Brandtlaan 40, 6716 RK te Ede
fg@gelderhorst.nl

De Autoriteit Persoonsgegevens
Postbus 93374
2509 AJ DEN HAAG
https://autoriteitpersoonsgegevens.nl/nl/zelf-doen/privacyrechten/klacht-indienen-bij-de-ap

In geval van andere klachten over de dienstverlening van De Gelderhorst raadpleegt de betrokkene de klachtenregeling van De Gelderhorst.

WIJZIGINGEN EN INZAGE

Dit reglement geldt per 30 juli 2018 en wordt op de website van De Gelderhorst gepubliceerd. Als het reglement inhoudelijk wijzigt, dan zullen wij dit kenbaar maken aan de medewerkers van De Gelderhorst via mail of via intranet. Onze cliënten informeren we via ons maandblad en/of per e-mail. Beperkte tekstuele aanpassingen worden niet kenbaar gemaakt. De meest recente versie staat altijd op de website. Raadpleeg dat dan ook regelmatig.

Privacyreglement - Inhoudsopgave

1. DEFINITIES

Anonimiseren
Het verwerken van persoonsgegevens op zodanige wijze dat de persoonsgegevens niet meer aan een specifieke betrokkene kunnen worden gekoppeld. Anders dan pseudonimiseren is anonimiseren onomkeerbaar. De AVG is niet van toepassing op anonieme gegevens.

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.

AVG
De Europese privacywetgeving die vanaf 25 mei 2018 geldt en die gaat over de verwerking van persoonsgegevens en waaraan De Gelderhorst gebonden is.

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 of de contactpersoon van de cliënt.

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. Binnen de Gelderhorst zal het vooral om gezondheidsgegevens gaan.

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 Gelderhorst is 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. In de volksmond wordt dit wel een ‘datalek’ genoemd. 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.

Voorbeelden: namen, adresgegevens, financiële gegevens, foto's, contactgegevens, gezondheidsgegevens.

Pseudonimisering
Het verwerken van persoonsgegevens op zodanige wijze dat de persoonsgegevens niet meer aan een specifieke betrokkene kan 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, software as a serviceleverancier, 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. In dit reglement is dat de zorgaanbieder.

Zorgaanbieder:
Stichting De Gelderhorst in Ede.

2. VERWERKING VAN PERSOONSGEGEVENS VAN CLIËNTEN IN OVEREENSTEMMING MET DE AVG

2.1 Basisbeginselen
De Gelderhorst als zorgaanbieder is verantwoordelijk voor de naleving van onderstaande beginselen bij de verwerking van persoonsgegevens. Dit betekent dat De Gelderhorst de naleving van deze beginselen moet kunnen aantonen ("verantwoordingsplicht").

Privacy is voor een zorgaanbieder uiterst belangrijk. Daarom houdt De Gelderhorst zich aan de AVG. Binnen De Gelderhorst worden persoonsgegevens alleen verwerkt:

- op een wijze die ten aanzien van de betrokkene rechtmatig, behoorlijk en transparant is. De AVG geeft aan wanneer wij persoonsgegevens mogen verwerken en ook op welke wijze wij aan onze transparantieverplichtingen kunnen voldoen;
- 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. Met andere woorden: gegevens worden verwijderd nadat ze niet meer nodig zijn (“opslagbeperking”);
- en beveiligd door het nemen van passende technische of organisatorische maatregelen zodat de persoonsgegevens beschermd zijn tegen ongeoorloofde of onrechtmatige verwerking en tegen onopzettelijk verlies, vernietiging of beschadiging (“integriteit en vertrouwelijkheid”).

2.2 Rechtmatigheid van de verwerking

In de AVG staat genoemd wanneer het verwerken van persoonsgegevens rechtmatig is. Dat is alleen het geval voor zover er aan ten minste een van de volgende gronden is voldaan:

- de betrokkene heeft **toestemming** gegeven voor de verwerking van zijn persoonsgegevens voor één of meer specifieke doeleinden. De Gelderhorst moet de toestemming kunnen aantonen en betrokkenen hebben het recht de toestemming te allen tijde in te trekken;
- de gegevensverwerking is noodzakelijk voor de **voorbereiding of uitvoering van een overeenkomst** waarbij de betrokkene partij is, bijvoorbeeld de zorgovereenkomst;
- de gegevensverwerking is noodzakelijk om een **wettelijke verplichting** na te komen, bijvoorbeeld de dossierplicht in de Wet op de geneeskundige behandelingsovereenkomst of gegevensverstrekking bij gedwongen opname en gedwongen behandeling op grond van de Wet Bijzondere opnemingen psychiatrische ziekenhuizen;
- de gegevensverwerking noodzakelijk is ter **bescherming van de vitale belangen** van de betrokkene of een ander natuurlijk persoon, zoals wanneer er acute zorg noodzakelijk is en er geen mogelijkheid of tijd is toestemming hiervoor te vragen;
- 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, zoals bij Gemeenten en andere overheden speelt;
- de gegevensverwerking noodzakelijk is voor de **behartiging van de gerechtvaardigde belangen van de Gelderhorst of van een derde** én de belangen, grondrechten of fundamentele vrijheden van degene van wie de gegevens worden verwerkt niet prevaleren. In dit geval moeten altijd de rechten tegen elkaar afgewogen worden. Je kunt hier denken aan gebruik van gegevens voor marketingdoeleinden.

2.3 Welke persoonsgegevens verwerken wij binnen De Gelderhorst?

Op onze website staat een contactformulier. Wij vragen hier om:

- **voor- en achternaam**
- **e-mailadres; en**
- **een bericht in het tekstvlak, waarin ook gevoelige informatie kan staan.**

Deze gegevens verwerken wij om contact op te nemen met de betrokkene.

Van onze cliënten vragen wij om of leggen wij vast:

- **Volledige naam;**
- **Geboortedatum:**
- **Bankrekeningnummer;**
- **BSN;**
- **Medische gegevens, zoals behandel- en medicijngegevens;**
- **Zorgverzekeringsgegevens;**
- **Overige gegevens van persoonlijke aard voor in een zorgdossier, zoals bepaalde voorkeuren of wensen ten aanzien van behandelingen en informatie over geloofsovertuiging.**

Deze informatie hebben wij nodig om onze cliënten van goede zorg te voorzien.

Ook kunnen wij beeldmateriaal verwerken waarop het **portret** van onze cliënt herkenbaar is. Dit kan gebeuren via onze camera die enkel filmt om de veiligheid van onze cliënten en medewerkers te waarborgen. Ook kunnen we foto's of video's maken voor intern gebruik of voor op sociale media. Hierover informeren wij onze cliënten via onze toestemmingsverklaring.

Van contactpersonen van onze cliënten vragen wij om:

- **NAW-gegevens;**
- **Contactgegevens als een telefoonnummer en e-mailadres.**

Wij verwerken deze gegevens zodat we contact met hen kunnen opnemen als dat nodig is.

2.4 Voorwaarden voor het verwerken van gezondheidsgegevens

Binnen De Gelderhorst verwerken we veel gegevens, ook gezondheidsgegevens. Gezondheidsgegevens zijn één van de categorieën bijzondere persoonsgegevens in de AVG. Hiermee wordt bedoeld dat deze gegevens extra privacygevoelig zijn. Niet voor niets verbiedt de de AVG de verwerking van deze categorieën persoonsgegevens. Dit verbod geldt niet wanneer wordt voldaan aan bepaalde, in de AVG genoemde voorwaarden.

Gezondheidsgegevens mogen bijvoorbeeld worden verwerkt 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, zoals een arts, of door een ander persoon die op grond van de wet of overeenkomst tot geheimhouding is gehouden.

Uiteraard moet er ook nog een grondslag zijn om deze gegevens te verwerken, zoals uitgelegd in paragraaf 2.2.

2.5 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 alleen verwerkt als dat nodig is voor een goede behandeling of verzorging van de betrokkene. Bijvoorbeeld voor de inschakeling van een tolk/vertaler als dat voor de uitleg van de behandeling aan een bepaalde cliënt nodig is. Dit zal De Gelderhorst per geval bekijken. Deze uitzondering geldt dus niet systematisch bij elke cliënt.

2.6 Gegevensverwerking door verwerker

De Gelderhorst kan de verwerking van persoonsgegevens uitbesteden aan een andere partij. Deze partij en eenieder die onder het gezag van De Gelderhorst of van deze partij handelt en toegang heeft tot persoonsgegevens, verwerkt deze uitsluitend in opdracht van De Gelderhorst tenzij hij door wet- of regelgeving tot verwerking gehouden is. Deze partij heet dan een verwerker.

De Gelderhorst mag uitsluitend een beroep doen op verwerkers die de privacy van de persoonsgegevens waar zij verantwoordelijke voor zijn, zoals van haar cliënten, waarborgen. De privacy is met name gewaarborgd als deze gegevens passend worden beveiligd.

Afspraken over de omgang met persoonsgegevens worden vastgelegd. Hoewel de AVG dit niet expliciet benoemt, gebeurt dit in een verwerkersovereenkomst. De AVG noemt wat er minimaal in deze overeenkomst moet staan. Hierin staan onder andere het onderwerp, de duur van de verwerking, de aard en het doel van de verwerking, het soort persoonsgegevens en de categorieën van betrokkenen, met welke partijen de gegevens worden gedeeld en de rechten en verplichtingen van beide partijen. En tot slot: de verwerker moet na beëindiging van de overeenkomst de persoonsgegevens vernietigen of weer overdragen aan de verwerkingsverantwoordelijke, in dit geval De Gelderhorst.

Het kan ook zijn dat de verwerker op zijn beurt weer een andere partij inschakelt om namens haar de gegevens te verwerken. Ook hier zal weer een verwerkersovereenkomst komen te liggen met rechten en verplichtingen die gelijk luiden als die tussen de Gelderhorst en de verwerker. En De Gelderhorst moet hier toestemming voor geven. De verwerker zelf blijft wel verantwoordelijk voor de verwerking.

De Gelderhorst heeft al verschillende verwerkersovereenkomsten gesloten, waaronder met Cormel IT Services B.V. Dit is de partij die QIC opslaat (het elektronisch cliëntendossier). Deze overeenkomst voldoet aan de eisen van de AVG en waarborgt de privacy van onze cliënten.

2.7 Aansprakelijkheid verwerkingsverantwoordelijke en/of verwerker

In het algemeen geldt dat de zorgaanbieder (verwerkingsverantwoordelijke) verantwoordelijk en aansprakelijk is 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 in de praktijk beoordeeld door de schadeverzekeraar of uiteindelijk door de rechter. Voor De Gelderhorst des te meer reden betrouwbare contractspartners te kiezen, goede afspraken te maken en deze ook vast te leggen in de verwerkersovereenkomsten.

2.8 Geheimhoudingsplicht en verstrekking aan derden

Binnen De Gelderhorst verwerken we veel gevoelige informatie.

Persoonsgegevens verkregen in de uitoefening van een beroep in de (geestelijke) gezondheidszorg vallen onder de geheimhoudingsplicht van de hulpverlener. Deze geheimhoudingsplicht is o.a. vastgelegd in verschillende wetten waaraan De Gelderhorst gebonden is en in verschillende beroepscodes. Deze afgeleide geheimhouding ziet op alle medewerkers die betrokken zijn bij de behandeling en alleen voor zover deze medewerkers de gegevens nodig hebben voor een goede uitoefening van haar taak.

Met medewerkers van of derden ingeschakeld door De Gelderhorst is bovendien nog een geheimhoudingsverplichting overeengekomen in de arbeids- of opdrachtovereenkomst.

Bij de verstrekking van gegevens aan derden wordt altijd de wetgeving nageleefd.

Voor de gezondheidzorg belangrijkste wetten wordt hieronder aangegeven hoe zij zich verhouden tot de AVG en tot elkaar.

- **Relatie met de Wet geneeskundige behandelingsovereenkomst (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 mogen we bijvoorbeeld alléén gegevens aan een derde verstrekken als dat mag op grond van de AVG én als we een grond hebben om het medisch beroepsgeheim te doorbreken.
- **Relatie met de Wet bijzondere opnemingen psychiatrische ziekenhuizen (Wet Bopz)**
  Ook de Wet Bopz 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 Wet Bopz naast de AVG gelden en als lex specialis voorrang krijgen ten opzichte van bepalingen die volgen uit de Wgbo. Een specifieke wet gaan namelijk doorgaans boven een algemene wet, zoals de AVG. Bijvoorbeeld wat betreft de bijzondere bepalingen op de dossierplicht van de hulpverlener en de bewaar- en vernietigingsbepalingen in de Wet Bopz en het Besluit patiëntendossier Bopz.
- **Relatie met de Zorgverzekeringswet (Zvw)**
  De Zvw geeft ook bepalingen over privacy van de verzekerde/cliënt die ambulante ggz-behandeling of ggz-behandeling met opname tot maximaal drie jaar krijgt. 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. Goed om te weten is wel dat ook hier strikte regels gelden. 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 ook nog 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 Wet langdurige zorg (Wlz)**
  De Wlz geeft bepalingen over privacy van cliënten die, na drie jaar ggz-behandeling met opname, deze vorm van behandeling nog steeds nodig hebben. Een voorbeeld is het

verplicht gebruik van het BSN en gegevensverstrekking aan derden, maar ook de controle of de gedeclareerde zorg ook daadwerkelijk is geleverd. De Wlz kent “Wgbo-achtige” bepalingen en stelt bijzondere eisen aan het opstellen en de inhoud van een zorgplan met de cliënt. De AVG geldt naast de Wlz. De Wlz is een specifieke wet ten opzichte van de Wgbo. De afwijkende bepalingen in de Wet Bopz gaan voor de Wlz in het geval een cliënt opgenomen met een Bopz-titel na drie jaar overgaat naar de Wlz.

- **Relatie met de Wet maatschappelijke ondersteuning (Wmo2015)**
  De Wmo 2015 geeft bepalingen over privacy van de cliënt die een algemene- of maatwerkvoorziening krijgt, bijvoorbeeld begeleiding of beschermd wonen. Een voorbeeld is de gegevensverstrekking, zonder toestemming van de betrokkene, aan Veilig Thuis. Binnen het domein van de Wmo 2015 wordt er veel in wijkteams gewerkt. Hulpverleners die geneeskundige behandeling verlenen in een dergelijk wijkteam, zijn gebonden aan het beroepsgeheim (het regime van de Wgbo en de Wet op de beroepen in de individuele gezondheidszorg (Wet BIG)) en mogen dus niet zonder toestemming worden gedeeld met medewerkers uit het team die maatschappelijke ondersteuning verlenen.
- **Relatie met de Wet aanvullende bepalingen verwerking persoonsgegevens in de zorg (Wbvo-z).**
  Deze wet regelt het gebruik van het burgerservicenummer, de elektronische uitwisseling van medische gegevens tussen zorgverleners (waaronder de beveiliging) en geeft cliënten het recht om hun dossier elektronisch in te mogen kijken of er een afschrift van te ontvangen. Deze wet is aanvullend op de AVG. De bepalingen gelden naast die van de AVG, maar als de AVG meer bescherming biedt dan geldt de AVG.
- **Relatie met het Besluit gebruik burgerservicenummer in de zorg.**
  Dit besluit geeft een gedetailleerde beschrijving van de Wet aanvullende bepalingen verwerking persoonsgegevens in de zorg en werkt deze uit. Ook hier geldt dat deze aanvullend geldt en dat de AVG voorrang heeft als de privacy dan beter beschermd wordt.

2.9 Afspraken met de onderzoeker

De Gelderhorst als verwerkingsverantwoordelijke en de onderzoeker maken schriftelijke afspraken over de maatregelen die de onderzoeker neemt om de privacy van betrokkenen te beschermen.

2.10 Bewaren van persoonsgegevens

De Gelderhorst bewaart de papieren en elektronische persoonsgegevens op een veilige wijze , geheel in lijn met de geldende wet- en regelgeving. Persoonsgegevens bewaren we niet langer dan noodzakelijk is om de doelen te bereiken waarvoor de gegevens worden verwerkt. Hier zijn uitzonderingen op die in de AVG genoemd zijn. Gegevens mogen langer bewaard worden:

- indien de gegevens worden geanonimiseerd;
- 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;
- in het kader van de uitoefening van het openbaar gezag dat aan de verwerkings-verantwoordelijke 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 Gelderhorst heeft beleid opgesteld ten aanzien van bewaartermijnen, mede aan de hand van enkele specifieke wettelijke bewaartermijnen. Indien het niet mogelijk is een specifieke termijn te noemen, dan zijn de criteria voor het vaststellen van de bewaartermijn vastgelegd.

Voor de gezondheidsgegevens die binnen de zorgrelatie met De Gelderhorst worden verwerkt, zoals het dossier van de cliënt, gelden verschillende bewaartermijnen. Deze zijn als volgt:

Dossiers
Wij bewaren de dossiers zolang dat nodig is voor het verlenen van onze zorg en zolang de wet ons verplicht om deze gegevens te bewaren. Medische patiëntendossiers moeten bijvoorbeeld meestal nog 15 jaar bewaard worden na het stoppen van de behandeling/het verblijf. Indien en voor zover uw dossier onder de Wet BOPZ valt, dan geldt een bewaartermijn van 5 jaar. Dit kan soms langer zijn als dat nodig is. Daarna zullen wij deze gegevens verwijderen.

Camerabeelden
Camerabeelden die wij bij De Gelderhorst hebben hangen voor de veiligheid van onze cliënten en medewerkers worden iedere 4 weken verwijderd.

Factuur- en betalingsgegevens
Alle financiële gegevens bewaren we 7 jaar na einde van het boekjaar waarin de gegevens voorkomen.

Personeelsgegevens
Gegevens van sollicitanten die niet worden aangenomen worden binnen vier weken na de procedure verwijderd. Dit met uitzondering van Dove sollicitanten waarvan de gegevens langer bewaard worden. Alle sollicitanten worden hiervan op de hoogte gesteld en kunnen instemmen met een langere of kortere termijn. Gegevens van medewerkers worden bewaard tot 7 jaren na uitdiensttreding.

3. RECHTEN VAN DE BETROKKENEN

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

Privacy is een grondrecht. Betrokkenen, zoals cliënten, hebben dan ook veel rechten ten aanzien van hun privacy. Zo kunnen zij een verzoek doen tot inzage (welke gegevens heeft De Gelderhorst van deze betrokkene), tot verwijdering (in bepaalde gevallen kan een betrokkene uit het systeem gehaald worden) of een verzoek tot rectificatie (als gegevens niet of niet langer juist zijn moeten ze worden aangepast).

Het verstrekken van de in dit hoofdstuk bedoelde informatie, het verstrekken van de communicatie en het treffen van de maatregelen zoals hieronder uitgelegd geschieden kosteloos. Indien het verzoek van een betrokkene kennelijk ongegrond of buitensporig is, met name wanneer iemand herhaaldelijke verzoeken indient, mag De Gelderhorst:

- 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
- weigeren gevolg te geven aan het verzoek. De reden van de weigering moet De Gelderhorst wel gemotiveerd mededelen aan de betrokkene.

Uitgangspunt is dat de betrokkenen veel rechten hebben en dat niet te gemakkelijk aan deze rechten voorbij mag worden gegaan. Daar staat tegenover dat er geen misbruik mag worden gemaakt van deze rechten. Het is aan De Gelderhorst om de kennelijk ongegronde of buitensporige aard van het verzoek aan te tonen.

3.2 Uitoefening van rechten betrokkenen

Betrokkenen kunnen de rechten zoals genoemd in dit hoofdstuk uitoefenen door een e-mail te sturen naar de functionaris voor gegevensbescherming van De Gelderhorst via fg@gelderhorst.nl.

De Gelderhorst moet de identiteit vaststellen van de verzoeker. Dit om te voorkomen dat privacygevoelige informatie onterecht worden gedeeld of gewist. Een betrokkene moet daarom een kopie van zijn of haar identiteitsbewijs met het verzoek meesturen. Ter bescherming van de privacy adviseert De Gelderhorst de pasfoto, de strook met nummers in het identiteitsbewijs, het documentnummer en het Burgerservicenummer (BSN) zwart te maken. Deze kopie wordt verwijderd na het vaststellen van de identiteit.

De Gelderhorst informeert de betrokkene onverwijld en uiterlijk binnen één maand na ontvangst van een verzoek tot inzage, aanvulling, rectificatie of wissing (verwijdering) van gegevens of andere verzoeken en op welke manier aan het verzoek wordt voldaan (gehoor geven of afwijzen). De Gelderhorst 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 moet de betrokkene wel binnen één maand van die verlenging in kennis worden gesteld.

Als De Gelderhorst het verzoek van betrokkene afwijst, geeft hij daarvan schriftelijk de reden. De Gelderhorst deelt een afwijzing van het verzoek onverwijld en uiterlijk binnen één maand ontvangst van het verzoek aan de betrokkene mee. Ook informeert De Gelderhorst de betrokkene over de mogelijkheid om een klacht in te dienen bij de Autoriteit Persoonsgegevens en de mogelijkheid om beroep in te stellen bij de rechter.

Wanneer de betrokkene zijn verzoek (bijvoorbeeld tot inzage) elektronisch indient, wordt de informatie indien mogelijk elektronisch verstrekt, tenzij de betrokkene anderszins verzoekt.

Verzoeken voor het uitoefenen van de rechten uit deze paragraaf moeten betrokkenen altijd schriftelijk indienen bij de functionaris voor gegevensbescherming.

3.3 Inzage en afschrift/kopie

De betrokkene heeft het recht op inzage en een kopie van de op zijn persoon betrekking hebbende verwerkte gegevens. De Gelderhorst moet wel altijd rekening houden met de privacy van anderen, die mag niet worden 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.

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 (familie, naastbetrokkenen en omstanders) voor zover van die vertegenwoordigers toestemming voor de behandeling is vereist. De vertegenwoordiger krijgt alleen die informatie die noodzakelijk is voor het uitoefenen van zijn taken als vertegenwoordiger.

Indien de hulpverlener door inlichtingen over de cliënt dan wel inzage in of afschrift van de documenten aan de (wettelijk) vertegenwoordiger te verstrekken niet geacht kan worden de zorg van een goed hulpverlener in acht te nemen, laat hij dat achterwege.

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

De betrokkene kan De Gelderhorst vragen om rectificatie (verbetering) van hem of haar betreffende persoonsgegevens als die onjuist. Ook kan de betrokkene De Gelderhorst verzoeken om aanvulling van zijn persoonsgegevens, met inachtneming van het doel van de verwerking, onder meer door een eigen aanvullende verklaring toe te voegen aan zijn of haar dossier.

De betrokkene kan De Gelderhorst ook vragen om bepaalde gegevens voor bepaalde personen af te schermen en hen de toegang tot die gegevens te laten blokkeren.

Het verzoek van een cliënt en beslissing van De Gelderhorst tot rectificatie (verbetering), wissing of aanvulling van gegevens blijft bewaard in het dossier van de cliënt.

3.5 Recht op gegevenswissing (vergetelheid)

De betrokkene heeft het recht van De Gelderhorst zonder onredelijke vertraging wissing van hem betreffende persoonsgegevens te verkrijgen en De Gelderhorst is verplicht persoonsgegevens zonder onredelijke vertraging te wissen wanneer een van de volgende gevallen van toepassing is:

- de persoonsgegevens zijn niet langer nodig voor de doeleinden waarvoor zij zijn verzameld of anderszins verwerkt;
- de betrokkene trekt de toestemming waarop de verwerking berust in en er geen andere rechtsgrond is voor de verwerking;
- de persoonsgegevens zijn onrechtmatig verwerkt;
- op basis van een wettelijke verplichting, die op De Gelderhorst rust, de persoonsgegevens moeten worden gewist.

De verplichting van De Gelderhorst eindigt niet bij het wissen van gegevens uit zijn systemen. De Gelderhorst stelt ook iedere ontvanger aan wie persoonsgegevens zijn verstrekt, in kennis van de wissing (verwijdering) van persoonsgegevens tenzij dit onmogelijk blijkt of onevenredig veel inspanning vergt. Daarbij verstrekt De Gelderhorst de betrokkene informatie over deze ontvangers indien de betrokkene hierom verzoekt.

Wanneer De Gelderhorst de persoonsgegevens openbaar heeft gemaakt en verplicht is de persoonsgegevens te wissen, neemt hij -mits mogelijk in verband met technologie en kosten-redelijke (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.

Een verzoek tot gegevenswissing dat voldoet aan de eerdergenoemde voorwaarden mag alleen worden geweigerd als:

- de wet zich tegen de vernietiging verzet;
- een derde een aanmerkelijk belang heeft bij bewaring van die gegevens. Bijvoorbeeld: een kind van een cliënt heeft een erfelijke ziekte;
- de cliënt heeft een procedure tegen de hulpverlener aangespannen of het is waarschijnlijk dat hij dit zal doen;
- De Gelderhorst de gegevens nodig heeft voor de instelling, uitoefening of onderbouwing van een rechtsvordering (bijvoorbeeld aansprakelijkheid, incasso etc);
- om redenen van algemeen belang op het gebied van volksgezondheid.

Het verzoek tot wissing van gezondheidsgegevens en de reactie daarop worden bewaard door De Gelderhorst.

3.6 Recht van bezwaar

De betrokkene heeft te allen tijde het recht om vanwege zijn specifieke situatie bezwaar te maken tegen de verwerking van hem betreffende persoonsgegevens. Dit kan wanneer de persoonsgegevens worden verwerkt op grond 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 Gelderhorst is opgedragen maar ook op basis van de noodzakelijkheid voor de behartiging van de gerechtvaardigde belangen van De Gelderhorst of van een derde. Dit kan dus niet als de gegevens verwerkt worden op grond van een overeenkomst.

De Gelderhorst 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 De Gelderhorst 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. Hier zal dus een belangenafweging plaats moeten vinden. De uitkomst hiervan moet De Gelderhorst gemotiveerd mededelen aan de betrokkene.

Als een betrokkene bezwaar maakt tegen het gebruik van zijn gegevens voor direct marketing doeleinden, dan zal De Gelderhorst dat bezwaar altijd inwilligen.

3.7 Recht op gegevensoverdraagbaarheid (dataportabiliteit)

Dit recht is nieuw onder de AVG en is in het leven geroepen om te voorkomen dat een betrokkene tegen zijn wil in diensten moet blijven afnemen van een partij, omdat deze zijn gegevens vast houdt.

De betrokkene heeft het recht de hem betreffende persoonsgegevens, die hij aan De Gelderhorst heeft verstrekt, in een gestructureerde, gangbare en machineleesbare vorm (zoals Excel) te verkrijgen en heeft het recht die gegevens aan een andere verwerkingsverantwoordelijke (bijvoorbeeld andere zorgaanbieder) over te dragen, zonder daarbij te worden gehinderd door degene aan wie de persoonsgegevens waren verstrekt, indien de verwerking berust op toestemming of op uitvoering van een overeenkomst en de verwerking *geautomatiseerd* wordt verricht.

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.

Ook hier geldt dat bij de uitoefening van dit recht geen afbreuk mag worden gedaan aan de privacy van anderen.

3.8 Te verstrekken informatie / Transparantieplicht

Betrokkenen hebben het recht op informatie. De Gelderhorst informeert hen daarom over de omgang met persoonsgegevens. De AVG verlangt dat dit in een beknopte, transparante, begrijpelijke (dus in begrijpelijke taal) en gemakkelijk toegankelijke vorm gebeurt en voorafgaand aan het verkrijgen van de persoonsgegevens, of kort daarna als dat niet anders kan.

De Gelderhorst voldoet hieraan door te informeren via dit privacyreglement en de privacyverklaring op haar website. Zij verwijst hier naar bij het aangaan van de (zorg)overeenkomst met cliënten. Ook informeert zij hierover in haar toestemmingsverklaringen.

In deze documenten staat onder andere:

- de identiteit en de contactgegevens van De Gelderhorst;
- de contactgegevens van de functionaris voor gegevensbescherming;
- de persoonsgegevens die De Gelderhorst verwerkt of de categorieën;
- de doelen voor het verwerken van de gegevens en de rechtsgrond (b.v. overeenkomst, toestemming etc.);
- de bronnen van de gegevens, als deze niet van de betrokkene zelf komen;
- de gerechtvaardigde belangen die De Gelderhorst heeft bij het verwerken van persoonsgegevens (wanneer dat een rechtsgrond is waar De Gelderhorst hier een beroep op doet);
- de ontvangers of categorieën van ontvangers van de persoonsgegevens;
- of De Gelderhorst de gegevens worden doorgegeven (bijvoorbeeld opgeslagen) in een organisatie die zich buiten de Europese Unie bevindt en welke waarborgen er worden genomen om de privacy te waarborgen.

Daarnaast verstrekt De Gelderhorst onderstaande aanvullende informatie om behoorlijke en transparante verwerking te waarborgen:

- de bewaartermijnen of indien dat niet mogelijk is, de criteria ter bepaling van die termijn;
- 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;
- indien de gegevensverwerking op toestemming is gebaseerd, informeert De Gelderhorst de betrokkene 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. Anders gezegd: tot het moment dat de toestemming ingetrokken werd mochten de gegevens worden verwerkt voor dat doel, daarna niet meer;
- het recht een klacht in te dienen bij de Autoriteit Persoonsgegevens en op welke wijze de betrokkene deze rechten kan inroepen.
- 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.

Het kan zijn dat De Gelderhorst de gegevens voor een ander doel wil verwerken dan waarvoor de gegevens zijn verzameld. In dat geval verstrekt De Gelderhorst de betrokkene vóór die verdere verwerking informatie over dat andere doel en alle relevante verdere informatie voor de verwerking.

Als de gegevens niet via de betrokkenen wordt verkregen, maar via een andere manier moet De Gelderhorst deze informatie binnen een redelijke termijn verstrekken. Dit moet uiterlijk binnen een maand na verkrijging van deze gegevens.

Deze informatieverplichting geldt niet indien:

- de betrokkene al over de informatie beschikt;
- 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, (…), of voor zover het informeren 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 Gelderhorst passende maatregelen om de rechten, de vrijheden en de gerechtvaardigde belangen van de betrokkene te beschermen, waaronder het openbaar maken van de informatie;
- het verkrijgen of verstrekken van informatie (zoals hiervoor genoemd) op grond van wet- en regelgeving verplicht is voor De Gelderhorst en die wet- en regelgeving voorziet in passende maatregelen om de gerechtvaardigde belangen van de betrokkene te beschermen; of
- de persoonsgegevens vertrouwelijk moeten blijven uit hoofde van een beroepsgeheim in het kader van wet- en regelgeving, waaronder een statutaire geheimhoudingsplicht.

4. VERTEGENWOORDIGING

De wilsbekwame cliënt oefent zelfstandig zijn rechten over zijn persoons- en gezondheidsgegevens uit. Is de betrokkene cliënt wilsonbekwaam ter zake, dan treedt als vertegenwoordiger voor hem op:

- een (toegewezen) curator of mentor;
- indien er geen curator of mentor is, de persoon die de cliënt schriftelijk heeft gemachtigd;
- indien de persoonlijk gemachtigde ontbreekt of niet optreedt: de echtgenoot of levensgezel van de cliënt;
- indien de echtgenoot of levensgezel ontbreekt of niet optreedt: een kind, broer of zus van de cliënt.

In het uiterste geval treedt De Gelderhorst 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.

5. VEILIGE VERWERKING VAN PERSOONSGEGEVENS

5.1 Verantwoordelijkheid van de verwerkingsverantwoordelijke

Passende beveiliging is cruciaal in geval van gevoelige gegevens als gezondheidsgegevens. Om die reden treft De Gelderhorst passende technische en organisatorische maatregelen om te waarborgen en te kunnen aantonen dat de verwerking in overeenstemming met de AVG wordt uitgevoerd.

De Gelderhorst mag bij het bepalen van deze maatregelen rekening houden 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 privacy van betrokkenen.

Wanneer de maatregelen in verhouding staan tot de verwerkingsactiviteiten, omvatten de hierboven bedoelde maatregelen een passend gegevensbeschermingsbeleid dat door de zorgaanbieder wordt uitgevoerd.

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

De Gelderhorst treft, 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.

De Gelderhorst 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.

Binnen De Gelderhorst hebben we onder meer de volgende maatregelen genomen:

- Onze website is beveiligd. Gegevens die betrokkenen daar achter laten zijn niet bereikbaar voor anderen;
- We hebben een verwerkersovereenkomst gesloten met de partij die gegevens in het elektronische cliëntendossier opslaat en onderhoudt;
- Onze systemen worden beheerd en onderhouden door een partij die wij zorgvuldig hebben geselecteerd en aan de strengste eisen voldoet. Met deze partij hebben wij duidelijke afspraken gemaakt over geheimhouding en beveiliging;
- We zorgen ervoor dat jullie, onze medewerkers, persoonsgegevens alleen raadplegen als dat noodzakelijk is voor het uitvoeren van jullie taken. Niet alle medewerkers hebben toegang tot deze gegevens (autorisatieprotocol);
- We hebben cameratoezicht;
- De verpleegafdeling is afgesloten met een codeslot;
- Wij passen de beveiligingsmaatregelen die die standaard zijn in de zorg (NEN7510);
- Voor de verstrekking van gegevens via e-mail wordt gebruik gemaakt van de beveiligde e-mailverbinding;
- We werkten volgens de ‘Richtsnoeren beveiliging persoonsgegevens’ en de ‘Praktijkgids patiëntgegevens in de cloud’ van de Autoriteit Persoonsgegevens;
- De identificerende gegevens zijn zoveel als mogelijk gescheiden opgeslagen van de inhoudelijke gegevens, gepseudonimiseerd of versleuteld.

De genomen maatregelen worden geëvalueerd en indien nodig geactualiseerd. De Gelderhorst zal rekening houden met de stand van de techniek die in haar branche geldt.

5.2 Gegevensbescherming door ontwerp en standaardinstellingen

Privacy staat centraal bij De Gelderhorst. Dit betekent dat de Gelderhorst bij alle nieuwe processen, doelen en systemen:

- de privacy instellingen zo privacyvriendelijk mogelijk instelt. De standaardinstellingen zijn dus nee, tenzij (opt-in) in plaats van ja, mits (opt-out), tenzij de wetgeving opt-out toelaatbaar stelt;
- privacy van het begin af aan mee wordt genomen in de processen, zodat er meteen rekening kan worden gehouden met de privacy risico’s en de instellingen.

5.3 Gezamenlijke verwerkingsverantwoordelijken

Het is niet altijd zo dat alleen een zorgaanbieder de doelen en middelen van de verwerking van persoonsgegevens vaststelt. Wanneer twee of meer verwerkingsverantwoordelijken dit gezamenlijk doen, zijn zij gezamenlijke verwerkingsverantwoordelijken. Zij stellen op transparante wijze hun beider verantwoordelijkheden voor de nakoming van de verplichtingen uit de AVG vast, met name:

- met betrekking tot de uitoefening van de rechten van de betrokkene;
- 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.

Uit de bedoelde regeling blijkt duidelijk welke rol de gezamenlijke verwerkingsverantwoordelijken respectievelijk vervullen, en wat hun beider verhouding met de betrokkenen is. De wezenlijke inhoud van de regeling wordt aan de betrokkene beschikbaar gesteld.

Ongeacht een dergelijke regeling kan een betrokkene zijn rechten uit de AVG met betrekking tot en jegens iedere verwerkingsverantwoordelijke uitoefenen.

5.4 Register van verwerkingen

De Gelderhorst is verplicht een register bij te houden van de verwerkingsactiviteiten die onder zijn verantwoordelijkheid plaatsvinden. In dit verwerkingsregister staan gegevens over de verwerkingen die binnen De Gelderhorst plaatsvinden, zoals de naam en contactgegevens van De Gelderhorst en van de functionaris voor gegevensbescherming, de verwerkingsdoeleinden, categorieën van persoonsgegevens, betrokkenen en ontvangers, bewaartermijnen, doorgifte naar derde landen en beveiligingsmaatregelen.

Het register is in schriftelijke vorm, waaronder in elektronische vorm, opgesteld en biedt een duidelijk overzicht van de datastromen binnen en buiten De Gelderhorst.

Dit register is in principe voor intern gebruik en onderdeel van de verantwoordingsplicht. De Autoriteit Persoonsgegevens kan in bepaalde gevallen inzage verzoeken in dit register. De Gelderhorst houdt dit register dan ook altijd up-to-date.

De verwerkers die De Gelderhorst inschakelt houden ook bij welke verwerkingen deze verwerkers ten behoeve van De Gelderhorst verricht.

5.5 Medewerking verlenen aan/samenwerken met de Autoriteit Persoonsgegevens

De Gelderhorst en de verwerker(s) werken desgevraagd samen met de Autoriteit Persoonsgegevens bij het vervullen van hun taken.

5.6 Beveiliging van de verwerking

Zoals al aan bod is gekomen, treft De Gelderhorst passende maatregelen om de persoonsgegevens te beveiligen. Deze maatregelen moeten zowel de gegevens goed beveiligen, maar ook de mogelijkheid bieden dat we in geval van een inbreuk in verband met persoonsgegevens over de gegevens kunnen beschikken en de toegang tot deze gegevens tijdig kunnen herstellen.

5.7 Melding van een inbreuk in verband met persoonsgegevens aan de Autoriteit Persoonsgegevens en datalekregister

Indien een inbreuk in verband met persoonsgegevens heeft plaatsgevonden, meldt De

Gelderhorst dit zonder onredelijke vertraging en, indien mogelijk, uiterlijk 72 uur nadat hij er kennis van heeft genomen, aan de Autoriteit Persoonsgegevens. De Gelderhorst hoeft dit niet te melden als het niet waarschijnlijk is dat de inbreuk een risico inhoudt voor de privacy.

Indien de melding aan de Autoriteit Persoonsgegevens niet binnen 72 uur plaatsvindt, wordt de vertraging toegelicht (gemotiveerd).

Het kan zijn dat de inbreuk plaatsvindt bij een van de verwerkers van De Gelderhorst. De verwerker informeert De Gelderhorst binnen de termijn die is overeengekomen in de verwerkersovereenkomst en altijd zonder onredelijke vertraging zodra hij kennis heeft genomen van een inbreuk.

In de melding aan de Autoriteit Persoonsgegevens geeft De Gelderhorst informatie over de aard van de inbreuk (bijvoorbeeld een hack of een gestolen laptop), gegevens over de Gelderhorst en onze functionaris voor gegevensbescherming, de waarschijnlijke gevolgen en de (voorgestelde) maatregelen om verdere nadelige gegevens te voorkomen.

Als het niet lukt al deze gegevens ineens te verstrekken, dan mag dat in stappen verstrekt worden. Als de melding maar wel tijdig wordt gedaan.

De Gelderhorst documenteert intern alle inbreuken, inclusief die inbreuken niet gemeld zijn aan de Autoriteit Persoonsgegevens met de reden waarom deze melding achterwege is gebleven. Die documentatie stelt de Autoriteit Persoonsgegevens in staat de naleving van dit artikel te controleren.

Binnen De Gelderhorst wordt via beleid en training aandacht besteed aan de veilige omgang met persoonsgegevens en het herkennen van inbreuken in verband met persoonsgegevens. De medewerkers van De Gelderhorst melden een inbreuk zonder uitzondering aan de functionaris voor gegevensbescherming. De functionaris voor gegevensbescherming beoordeelt deze inbreuk en stelt vast welke stappen er genomen moeten worden.

5.8 Melding van een inbreuk in verband met persoonsgegevens aan de betrokkene

Wanneer een inbreuk in verband met persoonsgegevens waarschijnlijk een hoog risico inhoudt voor de privacy van betrokkenen, informeert De Gelderhorst de betrokkenen onverwijld over deze inbreuk. Deze mededeling bevat een omschrijving, in duidelijke en eenvoudige taal, van de aard van het incident en de informatie zoals al eerdergenoemd (omvang, maatregelen, risico's).
Ook informeert De Gelderhorst waar de betrokkene heen kan met vragen hieromtrent.

De mededeling aan de betrokkene is niet vereist wanneer een van de volgende voorwaarden is vervuld:

- De Gelderhorst heeft passende technische en organisatorische beschermingsmaatregelen genomen en deze maatregelen zijn toegepast op de persoonsgegevens waarop het incident betrekking heeft, met name die welke de persoonsgegevens onbegrijpelijk maken voor onbevoegden, zoals versleuteling;
- De Gelderhorst heeft achteraf maatregelen genomen om ervoor te zorgen dat het hoge risico voor de privacy zich waarschijnlijk niet meer zal voordoen;
- 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 doeltreffen worden geïnformeerd.

Het kan voorkomen dat De Gelderhorst een inbreuk niet heeft gemeld aan een betrokkene omdat

hij van mening was dat deze melding niet nodig was. De Autoriteit Persoonsgegevens kan dan, na beraad over de kans dat het incident een hoog risico met zich meebrengt, De Gelderhorst daartoe verplichten of besluiten dat aan een van bovengenoemde voorwaarden is voldaan en dus geen melding hoeft te worden gedaan.

Aangezien De Gelderhorst met gevoelige gegevens, zoals gezondheidsgegevens, werkt zal een inbreuk al snel tot een risico voor de betrokkenen leiden. De Gelderhorst zal dus zeer terughoudend zijn in het achterwege laten van een melding.

5.9 Gegevensbeschermingseffectbeoordeling (DPIA)

In bepaalde gevallen kan een verwerking extra privacyrisico's met zich meebrengen. Dit kan met name gebeuren als er nieuwe technologieën worden gebruikt. Ook speelt dit sneller als er een n groot aantal gevoelige gegevens worden verwerkt. De AVG verplicht De Gelderhorst bij die verwerkingen, voordat de verwerking plaats vindt, een beoordeling uit te voeren van het effect van de beoogde verwerkingsactiviteiten op de bescherming van persoonsgegevens. In het Engels is dit instrument afgekort tot DPIA.

E én beoordeling kan een reeks vergelijkbare verwerkingen bestrijken die vergelijkbare hoge risico's inhouden.

Een DPIA is met name vereist in de volgende gevallen:

- 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;
- *er sprake is van een grootschalige verwerking van bijzondere categorieën van persoonsgegevens, zoals gezondheidsgegevens*;
- er sprake is van stelselmatige en grootschalige monitoring van openbaar toegankelijke ruimten.

Hoe ziet zo een DPIA er dan uit? Deze DPIA bevat ten minste:

- een systematische beschrijving van de beoogde verwerkingen en de verwerkingsdoeleinden;
- een beoordeling van de noodzaak en de evenredigheid van de verwerkingen met betrekking tot de doeleinden;
- een beoordeling van het eerste lid van dit artikel bedoelde risico's voor de privacy van betrokkenen; en
- 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.

Bij de beoordeling wordt de naleving van goedgekeurde gedragscodes naar behoren in aanmerking genomen.

De Gelderhorst wint advies in bij de functionaris voor gegevensbescherming bij het uitvoeren van de DPIA. De functionaris voor gegevensbescherming kan namelijk goed beoordelen wat de risico's inhouden en hoe De Gelderhorst deze zo goed mogelijk kan beperken.
Ook zal De Gelderhorst de betrokkenen of hun vertegenwoordigers naar hun mening over de

voorgenomen verwerking vragen. Uiteraard met inachtneming van de bescherming van commerciële of algemene belangen of de beveiliging van verwerkingen.

Het kan zijn dat De Gelderhorst het nodig vindt te toetsen of de verwerking uiteindelijk overeenkomstig de DPIA wordt uitgevoerd. Dit speelt met name wanneer sprake is van een verandering van het risico dat de verwerkingen inhouden. De Gelderhorst zal hier actief beleid op voeren.

5.10 Voorafgaande raadpleging van de Autoriteit Persoonsgegevens

Wanneer uit een DPIA blijkt dat de verwerking een hoog risico zou opleveren indien De Gelderhorst geen maatregelen neemt om het risico te beperken, raadpleegt De Gelderhorst de Autoriteit Persoonsgegevens voorafgaand aan de verwerking.

Als de Autoriteit Persoonsgegevens een (te) groot risico ziet, geeft de Autoriteit Persoonsgegevens binnen maximaal acht weken na ontvangst van het verzoek schriftelijk advies (of de verwerker). Deze termijn mag worden verlengd met zes weken, mits dit binnen een maand na de ontvangst gemotiveerd kenbaar wordt gemaakt. Wel kunnen de termijnen nog worden opgeschort als de Autoriteit Persoonsgegevens nog niet de informatie heeft verkregen die zij bij De Gelderhorst of bij diens verwerker heeft opgevraagd.

Deze informatie houdt in:

- indien van toepassing, de verantwoordelijkheden van De Gelderhorst, bij de verwerking betrokken gezamenlijke verwerkingsverantwoordelijken en verwerkers, in het bijzonder ten aanzien van een verwerking binnen een concern;
- de doeleinden en middelen van de voorgenomen verwerking;
- de maatregelen en waarborgen die worden geboden ter bescherming van de privacy van betrokkenen uit hoofde van de AVG;
- de contactgegevens van de functionaris voor gegevensbescherming;
- de DPIA ten aanzien van die verwerking;
- alle andere informatie waar de Autoriteit Persoonsgegevens om verzoekt.

6. FUNCTIONARIS VOOR GEGEVENSBESCHERMING (FG)

6.1 Aanwijzing van een functionaris voor gegevensverwerking

De AVG verplicht de zorgaanbieder en de verwerker een functionaris voor gegevensbescherming aan te wijzen wanneer de zorgaanbieder of de verwerker, hoofdzakelijk is belast met grootschalige verwerking van bijzondere categorieën van gegevens, namelijk voor zorgaanbieders: gezondheidsgegevens.

De functionaris voor gegevensbescherming is een interne toezichthouder. Hij wordt aangewezen op grond van zijn professionele kwaliteiten en, in het bijzonder, zijn deskundigheid op het gebied van de privacywetgeving en de praktijk en zijn vermogen de hieronder bedoelde taken te vervullen. De vereiste expertise en vaardigheden omvatten in ieder geval:

a) kennis van nationale en Europese privacywet- en regelgeving over gegevensbescherming;
b) begrip van de gegevensverwerkingen die de organisatie uitvoert;
c) begrip van IT en informatiebeveiliging;
d) kennis van de organisatie en de sector waarin die actief is;
e) vaardigheden om binnen de organisatie een cultuur van gegevensbescherming te ontwikkelen.

De functionaris voor gegevensbescherming kan een personeelslid van de zorgaanbieder of de verwerker zijn of kan de taken op grond van een dienstverleningsovereenkomst verrichten.

De Gelderhorst heeft Paula Dingler aangesteld als functionaris voor gegevensbescherming en haar aangemeld bij de Autoriteit Persoonsgegevens.

6.2 Positie van de functionaris voor gegevensbescherming

De Gelderhorst zorgt ervoor dat de functionaris voor gegevensbescherming naar behoren en tijdig wordt betrokken bij alle aangelegenheden die verband houden met de bescherming van persoonsgegevens.

Concreet heeft een functionaris voor gegevensbescherming onder meer het volgende nodig om de functie in te vullen:

a) de actieve steun vanuit het management;
b) voldoende tijd om de taken uit te voeren;
c) voldoende praktische ondersteuning (budget, faciliteiten en personeel);
d) heldere communicatie aan al het personeel over de benoeming van de functionaris voor gegevensbescherming;
e) scholing.

De Gelderhorst en de verwerker ondersteunen de functionaris voor gegevensbescherming bij de vervulling van hieronder bedoelde taken door hem toegang te verschaffen tot persoonsgegevens en verwerkingsactiviteiten en door hem de benodigde middelen ter beschikking te stellen voor het vervullen van deze taken en het in stand houden van zijn deskundigheid.

De functionaris voor gegevensbescherming werkt zelfstandig en onafhankelijk. De Gelderhorst zorgt er dan ook voor dat de functionaris voor gegevensbescherming geen instructies ontvangt met betrekking tot de uitvoering van die taken. De functionaris voor gegevensbescherming wordt niet ontslagen of gestraft voor de uitvoering van zijn taken en ondervindt geen nadeel van de uitoefening van zijn taak. De functionaris voor gegevensbescherming brengt rechtstreeks verslag uit aan het hoogte bestuur binnen De Gelderhorst.

Betrokkenen kunnen met de functionaris voor gegevensbescherming contact opnemen over alle aangelegenheden die verband houden met de verwerking van hun persoonsgegevens en met de uitoefening van hun rechten uit de AVG.

De functionaris voor gegevensbescherming is met betrekking tot de uitvoering van zijn taken tot geheimhouding of vertrouwelijkheid gehouden.

De functionaris voor gegevensbescherming kan andere taken en plichten vervullen. De Gelderhorst zorgt ervoor dat deze taken of plichten niet tot een belangenconflict leiden. Om belangenverstrengeling te voorkomen, mag de functionaris voor gegevensbescherming binnen de organisatie niet ook een functie hebben waarin hij het doel en de middelen van een gegevensverwerking bepaalt. Dit kan bijvoorbeeld zo zijn als de functionaris voor gegevensverwerking een managementpositie vervult, zoals hoofd financiën, strategie, marketing, IT of HRM.

6.3 Taken van de functionaris voor gegevensbescherming

De functionaris voor gegevensbescherming vervult ten minste de volgende taken:

- De Gelderhorst en de medewerkers die verwerken, informeren en adviseren over hun verplichtingen uit hoofde van de privacywetgeving (de AVG en andere gegevensbeschermingsbepalingen zoals uit

sectorspecifieke wet- en regelgeving);

- toezien op naleving van deze AVG, van andere gegevensbeschermingsbepalingen en van het beleid van De Gelderhorst met betrekking tot de bescherming van persoonsgegevens, met inbegrip van de toewijzing van verantwoordelijkheden, bewustmaking en opleiding van het bij de verwerking betrokken personeel en de betreffende audits;
- desgevraagd advies verstrekken met betrekking tot de DPIA en toezien op de uitvoering daarvan;
- met de Autoriteit Persoonsgegevens samenwerken;
- optreden als contactpunt voor de Autoriteit Persoonsgegevens inzake met verwerking verband houdende aangelegenheden, met inbegrip van de voorafgaande raadpleging, en, waar passend, overleg plegen over enige andere aangelegenheid.

De functionaris voor gegevensbescherming houdt bij de uitvoering van zijn taken naar behoren rekening met het aan verwerkingen verbonden risico, en met de aard, de omvang, de context en de verwerkingsdoeleinden.

Versie: December 2018