

Privacyreglement De Regenboog Groep 2018



Dit reglement is van toepassing binnen De Regenboog Groep in Amsterdam heeft betrekking op de verwerkingen van gegevens van deelnemers, bezoekers of cliënten die bij De Regenboog Groep gebruik maken van faciliteiten en/of diensten.

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

Inhoudsopgave:

- 1. Definities**
- 2. Verwerking van persoonsgegevens van cliënten in overeenstemming met de AVG**
 - 2.1 Beginselen inzake persoonsgegevens verwerking**
 - 2.2 Rechtmatigheid van de verwerking**
 - 2.3 Voorwaarden voor het verwerken van gezondheidsgegevens**
 - 2.4 Gegevensverwerking door verwerker**
 - 2.5 Aansprakelijkheid verwerkingsverantwoordelijke en / of verwerker**
 - 2.6 Wanneer mogen andere bijzondere gegevens dan de gezondheidsgegevens worden verwerkt?**
 - 2.7 Geheimhoudingsplicht en verstrekking aan derden**
 - 2.8 Wanneer mogen gegevens aan een ander worden verstrekt voor wetenschappelijk onderzoek en statistiek op het gebied van de gezondheid?**
 - 2.9 Afspraken met de onderzoeker**
 - 2.10 Bewaren van persoonsgegevens**
- 3. Rechten van betrokkenen**
 - 3.1 Voorwaarden met betrekking tot de uitvoering van de rechten van de betrokkenen**
 - 3.2 Te verstrekken informatie**
 - 3.3 Te verstrekken informatie wanneer de persoonsgegevens niet van de betrokkene zijn verkregen**
 - 3.4 Inzage en afschrift/kopie**
 - 3.5 Rectificatie (verbetering) of aanvulling van persoonsgegevens en beperking van de verwerking van persoonsgegevens**
 - 3.6 Recht op gegevenswissing (vergetelheid)**

- 3.7 Recht op bezwaar
- 3.8 Recht op gegevensoverdraagbaarheid (dataportabiliteit)
- 3.9 Vertegenwoordiging
- 4. **Veilige verwerking van persoonsgegevens**
 - 4.1 Verantwoordelijkheid van de verwerkingsverantwoordelijke
 - 4.2 Gegevensbescherming door ontwerp en standaardinstellingen (Privacy by design en default)
 - 4.3 Gezamenlijke verwerkingsverantwoordelijken
 - 4.4 Register van verwerkingen
 - 4.5 Medewerking verlenen aan/samenwerking met de Autoriteit Persoonsgegevens (AP)
 - 4.6 Beveiliging van de verwerking
 - 4.7 Melding van een inbreuk in verband met persoonsgegevens aan de Autoriteit Persoonsgegevens (datalekken melden aan de AP) en datalekregister
 - 4.8 Melding van een inbreuk in verband met persoonsgegevens aan de betrokkenen (datalekken melden aan de betrokkene)
 - 4.9 Gegevensbeschermingseffectbeoordeling (Data Protection Impact Assessment DPIA)
 - 4.10 Voorafgaande raadpleging van de AP
- 5. **Functionaris voor Gegevensbescherming (FG)**
 - 5.1 Aanwijzing en een functionaris voorgegevensverwerking
 - 5.2 Positie van de functionaris voor gegevensbescherming
 - 5.3 Taken van de functionaris voor gegevensbescherming
 - 5.4 Bij een klacht
 - 5.5 Wijzigingen en inzage van dit reglement
- 6. **Donateurs / Financiële supporters**
 - 6.1 (Financiële) supporters en werving
 - 6.2 Vrijwilligers
 - 6.3 De Regenboog Groep kwartaal magazine Meeleven
 - 6.4 Webwinkel (e-commerce)
 - 6.5 Contact met de Regenboog Groep
 - 6.6 Nieuwsbrieven
 - 6.7 Jongeren onder 16 jaar
 - 6.8 Wie ontvangt jouw persoonsgegevens (nog mee)?
 - 6.9 Hoe lang worden persoonsgegevens bewaard?
 - 6.10 Welke beveiligingsmaatregelen nemen wij?
 - 6.11 Keurmerken, gedragscode en waarborgen
 - 6.12 Gegevens inzien, aanpassen, overdragen, verwijderen, intrekken toestemming of bezwaar

Bijlage 1:

- 7. **Competentieprofiel Functionaris voor de Gegevensbescherming (FG)**
 - 7.1 Rollen en verantwoordelijkheden t.a.v. privacybescherming

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 DRG 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 (lekkens) 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 identicator 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 betrokkene 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 DRG.

DRG: De Regenboog Groep

2. Verwerking van persoonsgegevens van cliënten in overeenstemming met de AVG

2.1 Beginselen inzake persoonsgegevens verwerking¹

DRG is verantwoordelijk voor de naleving van onderstaande beginselen bij de verwerking van persoonsgegevens en moet de naleving van deze beginselen kunnen aantonen (“verantwoordingsplicht”).²

Binnen De Regenboog Groep 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 wordt³ 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 verwerkt⁴ 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”).

2.2 Rechtmatigheid van de verwerking⁵

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

- de betrokkene heeft toestemming⁶ gegeven voor de verwerking van zijn persoonsgegevens voor één of meer specifieke doeleinden; DRG 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

¹ 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.

² De beginselen inzake verwerking de verwerking van persoonsgegevens en de verantwoordingsplicht volgen uit artikel 5 AVG.

³ Overeenkomstig artikel 89, eerste lid, AVG.

⁴ Overeenkomstig artikel 89, eerste lid, AVG.

⁵ Artikel 6 AVG.

⁶ 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.

- waarbij de betrokkene partij is, bijvoorbeeld de behandelingsovereenkomst;
- de gegevensverwerking is noodzakelijk om een wettelijke verplichting na te komen, bijvoorbeeld de dossierplicht in de Wgbo of gegevensverstrekking bij gedwongen opname en gedwongen behandeling op grond van de Wet Bopz;
- de gegevensverwerking noodzakelijk is ter bescherming van de vitale belangen van de betrokkene of een ander natuurlijk persoon⁷;
- 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 belangen⁸ van de verwerkingsverantwoordelijke of van een derde én de belangen, grondrechten of fundamentele vrijheden van degene van wie de gegevens worden verwerkt niet prevaleren.

2.3 Voorwaarden voor het verwerken van gezondheidsgegevens⁹

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 voorwaarden¹⁰:

- 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).¹¹

2.4 Gegevensverwerking door verwerker

- DRG kan de verwerking (extern) uitbesteden aan een verwerker en legt dan in een verwerkersovereenkomst de verplichtingen uit de AVG op aan de verwerker.¹² DRG 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

⁷ 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.

⁸ 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.

⁹ Artikel 9, tweede lid, AVG.

¹⁰ Artikel 9 AVG.

¹¹ 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 medisch beroepsgeheim te doorbreken.

¹² Artikel 28 AVG.

die de verwerker ten aanzien van DRG 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 DRG worden omschreven. Een dergelijke overeenkomst dient te voldoen aan de eisen die de AVG daaraan stelt.¹³ GGZ Nederland heeft in BOZ-verband een dergelijke [model verwerkersovereenkomst](#)¹⁴ ontwikkeld.

- De verwerker en eenieder die onder het gezag van DRG of van de verwerker handelt en toegang heeft tot persoonsgegevens, verwerkt deze uitsluitend in opdracht van DRG, tenzij hij door wet- of regelgeving tot verwerking gehouden is.¹⁵

2.5 Aansprakelijkheid verwerkingsverantwoordelijke en/of verwerker

1. DRG (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.¹⁶
2. De verwerker, waaraan DRG (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 DRG goede afspraken maakt met de verwerker en deze vastlegt in een verwerkersovereenkomst.¹⁷

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

Andere bijzondere gegevens, bijvoorbeeld gegevens met betrekking tot ras/ethniciteit 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.

2.7 Geheimhoudingsplicht en verstrekking aan derden

1. 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 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 en dienen de handreikingen van GGZ Nederland ter ondersteuning. Handreikingen die hierin behulpzaam kunnen zijn: [Wegwijzer Beroepsgeheim in samenwerkingsverbanden](#) en [Handreiking Beroepsgeheim](#).

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.¹⁸ Tevens kan er in nationale wetgeving worden afgeweken van bepaalde rechten van betrokkenen uit de AVG voor zover die rechten de verwezenlijking van de

¹³ In artikel 28, derde lid, AVG worden eisen gesteld aan de verwerkersovereenkomst. Sub a geeft bijvoorbeeld aan dat persoonsgegevens uitsluitend mogen worden verwerkt op basis van schriftelijke instructies van de verwerkingsverantwoordelijke.

¹⁴ Bij het model verwerkersovereenkomst is ook een [inleiding](#) en [toelichting](#) beschikbaar.

¹⁵ Artikel 29 AVG.

¹⁶ Zie de [toelichting](#) bij het model verwerkersovereenkomst (BOZ).

¹⁷ Model [verwerkersovereenkomst](#), [inleiding](#) en [toelichting](#) (BOZ).

¹⁸ Artikel 89 AVG.

specifieke doeleinden onmogelijk dreigen te maken of ernstig dreigen te belemmeren, en dergelijke afwijkingen noodzakelijk zijn om die doeleinden te bereiken.

De Wgbo¹⁹ geeft onderstaande afwijkende bepalingen voor wetenschappelijk onderzoek op het gebied de van gezondheidszorg. Het uitgangspunt is dat voor het verstrekken van niet geanonimiseerde²⁰ 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 is²¹ 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.

2.9 Afspraken met de onderzoeker

DRG (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

DRG dient de papieren en elektronische persoonsgegevens op een veilige wijze te bewaren, die in overeenstemming is met de geldende wet- en regelgeving. Persoonsgegevens worden niet langer bewaard dan noodzakelijk is om de doelen te bereiken waarvoor de gegevens worden verwerkt, tenzij de gegevens worden geanonimiseerd of indien het noodzakelijk is voor de uitoefening van het recht op vrijheid van meningsuiting en van informatie, voor de nakoming van een wettelijke verplichting, voor de uitvoering van een taak in het algemeen belang of in het kader van de uitoefening van het openbaar gezag dat aan de verwerkingsverantwoordelijke is verleend, om redenen van algemeen belang op het vlak van volksgezondheid, met het oog op archivering in het algemeen belang, wetenschappelijk of historisch onderzoek of statistische doeleinden of voor de vaststelling, uitoefening of onderbouwing van een rechtsvordering.²²

DRG stelt vast hoelang de vastgelegde/geregistreerde persoonsgegevens bewaard blijven in overeenstemming met de geldende wet- en regelgeving. Indien nog geen specifieke termijn kan worden genoemd: de criteria voor het vaststellen van de bewaartermijn.

Voor gezondheidsgegevens die binnen de zorgrelatie worden verwerkt, zoals het dossier van de cliënt, gelden verschillende bewaartermijnen.

Voor een overzicht van geldende bewaartermijnen, zie de [Notitie bewaartermijnen](#) van GGZ Nederland.

¹⁹ Artikel 7:457 en 7:458 BW (Wgbo).

²⁰ 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.

²¹ 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.

²² Artikel 17, derde lid, AVG (overweging 65).

3. Rechten van de betrokkenen

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

1. Het verstrekken van de in deze paragraaf 3.1 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 DRG:
 - 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 DRG om de kennelijk ongegronde of buitensporige aard van het verzoek aan te tonen.²³
2. DRG 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. DRG 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. De betrokkene kan verzoeken schriftelijk indienen bij het bestuur via info@deregenboog.org

3.2 Te verstrekken informatie²⁴

1. Als DRG gegevens bij de betrokkene zelf opvraagt om te verwerken, informeert hij de betrokkene in een beknopte, transparante, begrijpelijke en gemakkelijk toegankelijke vorm²⁵, voorafgaand aan het verkrijgen van zijn persoonsgegevens, over:
 - a) de identiteit en de contactgegevens van DRG;
 - 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;
 - 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 inroepen.
 - e) of de verstrekking van persoonsgegevens een wettelijke of contractuele verplichting is dan wel een noodzakelijke voorwaarde om een overeenkomst te sluiten en of de betrokkene verplicht is de persoonsgegevens te verstrekken en wat de mogelijke gevolgen zijn wanneer deze gegevens niet worden verstrekt.

²³ Artikel 12 AVG.

²⁴ Artikel 13 AVG. Let op: ook de Wgbo kent in artikel 7:448 BW een informatieplicht over behandelinhoudelijke zaken.

²⁵ En in duidelijke en eenvoudige taal. Zie hiervoor artikel 12, eerste lid, AVG.

3. Wanneer DRG voornemens heeft de persoonsgegevens verder te verwerken voor een ander doel dan waarvoor de persoonsgegevens zijn verzameld, verstrekt DRG 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 Te verstrekken informatie wanneer de persoonsgegevens niet van de betrokkene zijn verkregen²⁶

1. Wanneer persoonsgegevens niet van de betrokkene zijn verkregen, verstrekt DRG de betrokkene alle informatie conform hierboven (artikel 3.2) onder lid 1 en 2 en bovendien de betrokken categorieën van persoonsgegevens alsmede de bron waar de persoonsgegevens vandaan komen.
2. DRG 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 DRG voornemens heeft om de persoonsgegevens verder te verwerken voor een ander doel dan dat waarvoor de persoonsgegevens zijn verkregen, verstrekt DRG 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. DRG hoeft de betrokkene niet te informeren over de hiervoor genoemde informatie indien:
 - a) de betrokkene al over de informatie beschikt;
 - b) het informeren van betrokkene onmogelijk blijkt of een onevenredige inspanning kost. In het bijzonder bij verwerking met het oog op archivering in het algemeen belang, wetenschappelijk of historisch onderzoek of statistische doeleinden, behoudens de in artikel 89, lid 1, bedoelde voorwaarden en waarborgen, of voor zover de in lid 1 van dit artikel bedoelde verplichting de verwezenlijking van de doeleinden van die verwerking onmogelijk dreigt te maken of ernstig in het gedrang dreigt te brengen. In dergelijke gevallen neemt DRG 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 DRG 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.

3.4 Inzage en afschrift/kopie²⁷

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

²⁶ Artikel 14 AVG.

²⁷ Artikel 7:456, 7:457 BW (Wgbo).

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.²⁸ 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 achterwege²⁹. 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 DRG 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. DRG 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.³⁰
5. De betrokkene kan verzoeken schriftelijk indienen bij het bestuur via info@deregenboog.org

3.5 Rectificatie (verbetering) of aanvulling van persoonsgegevens en beperking van de verwerking van persoonsgegevens³¹

1. De betrokkene kan DRG vragen om rectificatie (verbetering) van hem of haar betreffende persoonsgegevens als die onjuist zijn of DRG 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. < eventueel toevoegen van bepalingen bij wie op welke wijze de betrokkene verzoeken moet doen voor het uitoefenen van deze rechten >
3. DRG 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. DRG 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.
4. Als DRG het verzoek van betrokkene afwijst, geeft hij daarvan schriftelijk³² de reden. DRG deelt een afwijzing van het verzoek onverwijld en uiterlijk binnen één maand ontvangst van het verzoek aan de verzoeker mee. Ook informeert DRG 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.
5. De betrokkene kan DRG vragen om bepaalde gegevens voor bepaalde personen af te schermen en hen de toegang tot die gegevens te laten blokkeren.
6. Het verzoek van een cliënt en beslissing van DRG tot rectificatie (verbetering), wissing of aanvulling van gegevens blijft bewaard in het dossier van de cliënt.

²⁸ 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.

²⁹ Artikel 7:457, derde lid, BW (Wgbo).

³⁰ Artikel 12 AVG (algemene regels voor de uitoefening van de rechten van de betrokkene).

³¹ Artikel 12 AVG e.v. AVG, artikel 16 AVG.

³² De betrokkene dient schriftelijk of met andere middelen, met inbegrip van , indien dit passend is, elektronische middelen, de informatie te verstrekken.

3.6 Recht op gegevenswissing (vergetelheid)³³

1. De betrokkene heeft het recht van DRG zonder onredelijke vertraging wissing van hem betreffende persoonsgegevens te verkrijgen en DRG 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 DRG rust, de persoonsgegevens moeten worden gewist.
2. De betrokkene kan verzoeken schriftelijk indienen bij het bestuur via info@deregenboog.org
3. DRG 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. DRG verstrekt de betrokkene informatie over deze ontvangers indien de betrokkene hierom verzoekt.³⁴
4. Wanneer DRG de persoonsgegevens openbaar heeft gemaakt en overeenkomstig lid 1 verplicht is de persoonsgegevens te wissen, neemt hij, rekening houdend met de beschikbare technologie en de uitvoeringskosten, redelijke maatregelen, waaronder technische maatregelen, om verwerkingsverantwoordelijken die de persoonsgegevens verwerken, ervan op de hoogte te stellen dat de betrokkene de verwerkingsverantwoordelijken heeft verzocht om iedere koppeling naar, of kopie of reproductie van die persoonsgegevens te wissen.
6. Indien het gezondheidsgegevens betreft, wist DRG 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. DRG stelt de betrokkene binnen één maand na ontvangst van het verzoek in kennis van een dergelijke verlenging.
7. 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) DRG de gegevens nodig heeft voor de instelling, uitoefening of onderbouwing van een rechtsvordering;
 - f) om redenen van algemeen belang op het gebied van volksgezondheid.
8. Het verzoek tot wissing van gezondheidsgegevens en de reactie daarop worden bewaard door DRG.³⁵

³³ Artikel 17 AVG in samenhang met artikel 12 lid 3 e.v. AVG.

³⁴ Artikel 19 AVG.

³⁵ In dat geval kan bij een materiële controle aan de financier worden aangetoond dat het dossier, op verzoek van betrokkene, is vernietigd.

3.7 Recht van bezwaar³⁶

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 DRG is opgedragen of op basis van de noodzakelijkheid voor de behartiging van de gerechtvaardigde belangen van DRG of van een derde;
2. DRG beoordeelt onverwijld en in ieder geval binnen één maand na ontvangst van het bezwaar of het bezwaar gerechtvaardigd is. Indien het bezwaar gerechtvaardigd is, beëindigt hij onmiddellijk de verwerking, tenzij er sprake is van dwingende gerechtvaardigde gronden voor de verwerking die zwaarder wegen dan de belangen, vrijheden en rechten van de betrokkene of die verband houden met de instelling, uitoefening of onderbouwing van een rechtsvordering.

3.8 Recht op gegevensoverdraagbaarheid (dataportabiliteit)³⁷

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 DRG aan wie de persoonsgegevens waren verstrekt, indien de verwerking berust op toestemming of op uitvoering van een overeenkomst en de verwerking geautomatiseerd wordt verricht.
2. Bij de uitoefening van het recht op gegevensoverdraagbaarheid heeft de betrokkene het recht dat de persoonsgegevens, indien dit technisch mogelijk is, rechtstreeks van de ene zorgaanbieder naar de andere worden doorgezonden.
3. Bij de uitoefening van dit recht mag dit geen afbreuk doen aan de rechten en vrijheden van anderen.

3.9 Vertegenwoordiging

1. Bij een jeugdige jonger dan twaalf jaar en bij een wilsbekwame 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.³⁸
2. De ouder die geen gezag heeft krijgt desgevraagd belangrijke, algemene en feitelijke informatie³⁹ 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.⁴⁰ 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 wilsbekwaam 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.

³⁶ Artikel 21 AVG.

³⁷ Artikel 20 AVG.

³⁸ 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.

³⁹ Er mag slechts informatie worden verstrekt die feitelijk, globaal, belangrijk en doelgericht is.

5. In het uiterste geval treedt DRG 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.

4. Veilige verwerking van persoonsgegevens

4.1 Verantwoordelijkheid van de verwerkingsverantwoordelijke⁴¹

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

4.2 Gegevensbescherming door ontwerp en standaardinstellingen (Privacy by design en default)⁴²

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 DRG, 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. DRG 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) DRG 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 <evt. naam>.
- c) DRG 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.
- e) De standaardinstellingen zijn nee, tenzij (opt-in) in plaats van ja, mits (opt-out), tenzij

⁴¹ Artikel 24 AVG.

⁴² Artikel 25 AVG.

de wetgeving opt-out toelaatbaar stelt.

- f) DRG 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).

4.3 Gezamenlijke verwerkingsverantwoordelijken⁴³

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

4.4 Register van verwerkingen⁴⁴

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 DRG 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;
 - 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

⁴³ Artikel 26 AVG.

⁴⁴ Artikel 30 AVG.

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 .

4.5 Medewerking verlenen aan/samenwerken met de Autoriteit persoonsgegevens⁴⁵

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

4.6 Beveiliging van de verwerking⁴⁶

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 DRG 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. DRG en de verwerker treffen maatregelen om ervoor te zorgen dat iedere natuurlijke persoon die handelt onder het gezag van DRG of van de verwerker en toegang heeft tot persoonsgegevens, deze slechts in opdracht van DRG verwerkt, tenzij hij daartoe volgens wet- en regelgeving is gehouden.

4.7 Melding van een inbreuk in verband met persoonsgegevens aan de Autoriteit Persoonsgegevens (datalekken melden aan de AP) en datalekkenregister⁴⁷

1. Indien een inbreuk in verband met persoonsgegevens heeft plaatsgevonden, meldt DRG 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 DRG 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

⁴⁵ Artikel 31 AVG.

⁴⁶ Artikel 32 AVG.

⁴⁷ Artikel 33 AVG.

- 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 DRG 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. DRG 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.

4.8 Melding van een inbreuk in verband met persoonsgegevens aan de betrokkenen (datalekken melden aan de betrokkene)⁴⁸

1. Wanneer de inbreuk in verband met persoonsgegevens waarschijnlijk een hoog risico inhoudt voor de rechten en vrijheden van natuurlijke personen, deelt DRG 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 (4.7, 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) DRG 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) DRG heeft achteraf maatregelen genomen om ervoor te zorgen dat het hoge risico voor de rechten en vrijheden van betrokkenen zich waarschijnlijk niet meer zal voordoen;
 - c) de mededeling zou onevenredige inspanningen vergen. In dat geval komt er in de plaats daarvan een openbare mededeling of een soortgelijke maatregel waarbij betrokkenen even doeltreffend worden geïnformeerd.
4. Indien DRG 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, DRG daartoe verplichten of besluiten dat aan een van de in lid 3 van dit artikel, bedoelde voorwaarden is voldaan.

4.9 Gegevensbeschermingseffectbeoordeling (Data Protection Impact Assessment, DPIA)⁴⁹

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 DRG vóór de verwerking een beoordeling uit van het effect van de beoogde verwerkingsactiviteiten op de bescherming van persoonsgegevens.⁵⁰ Eén beoordeling kan een reeks vergelijkbare verwerkingen bestrijken die vergelijkbare hoge risico's inhouden.
2. Wanneer een functionaris voor gegevensbescherming is aangewezen, wint DRG bij het uitvoeren van een gegevensbeschermingseffectbeoordeling diens advies in.

⁴⁸ Artikel 34 AVG.

⁴⁹ Artikel 35 AVG

⁵⁰ 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.

3. Een gegevensbeschermingseffectbeoordeling als bedoeld in het eerste lid is met name vereist in de volgende gevallen⁵¹:
 - 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.
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. DRG 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 DRG 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.

4.10 Voorafgaande raadpleging van de Autoriteit Persoonsgegevens⁵²

1. Wanneer uit een gegevensbeschermingseffectbeoordeling blijkt dat de verwerking een hoog risico zou opleveren indien DRG geen maatregelen neemt om het risico te beperken, raadpleegt DRG voorafgaand aan de verwerking de Autoriteit Persoonsgegevens.⁵³
2. Wanneer de Autoriteit Persoonsgegevens van oordeel is dat de bedoelde voorgenomen verwerking inbreuk zou maken op deze verordening, met name wanneer DRG 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 DRG 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 DRG 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.

⁵¹ Overweging (91) AVG.

⁵² Artikel 36 AVG. DRG heeft een model functieomschrijving FG opgesteld.

⁵³ Uit overweging (94) AVG volgt dat dit gaat om situaties waarbij DRG 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. Bij de raadpleging verstrekt DRG 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 DRG, 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.

5. Functionaris voor gegevensbescherming (FG)

5.1 Aanwijzing van een functionaris voor gegevensverwerking⁵⁴

1. DRG en de verwerker wijst een functionaris voor gegevensbescherming aan wanneer DRG of de verwerker, hoofdzakelijk is belast met grootschalige verwerking van bijzondere categorieën van gegevens, namelijk voor zorgaanbieders: gezondheidsgegevens.
2. Een concern heeft de mogelijkheid om één functionaris voor gegevensbescherming benoemen, mits de functionaris voor gegevensbescherming vanuit elke vestiging makkelijk te contacteren is.
3. De functionaris voor gegevensbescherming wordt aangewezen op grond van zijn professionele kwaliteiten en, in het bijzonder, zijn deskundigheid op het gebied van de wetgeving en de praktijk inzake gegevensbescherming 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.
4. De functionaris voor gegevensbescherming kan een personeelslid van DRG of de verwerker zijn of kan de taken op grond van een dienstverleningsovereenkomst verrichten.
5. DRG of de verwerker maakt de contactgegevens van de functionaris voor gegevensbescherming bekend en deelt die mee aan de Autoriteit Persoonsgegevens. Binnen De Regenboog Groep is als functionaris voor gegevensbescherming werkzaam: L. Dijkmans fg@deregenboog.org

5.2 Positie van de functionaris voor gegevensbescherming

1. DRG en de verwerker zorgen 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 FG;
 - e) scholing.

⁵⁴ Artikel 37 AVG. Zie voor een model functieomschrijving functionaris voor gegevensbescherming [Privacyreglement De Regenboog Groep](#)

2. DRG 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.
3. DRG en de verwerker zorgen ervoor dat de functionaris voor gegevensbescherming geen instructies ontvangt met betrekking tot de uitvoering van die taken; de functionaris voor gegevensbescherming werkt zelfstandig en onafhankelijk. De functionaris voor gegevensbescherming wordt door DRG of de verwerker 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 de hoogste leidinggevende, raad van bestuur of directie, van DRG of de verwerker.
4. 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.
5. De functionaris voor gegevensbescherming is met betrekking tot de uitvoering van zijn taken tot geheimhouding of vertrouwelijkheid gehouden.
6. De functionaris voor gegevensbescherming kan andere taken en plichten vervullen. DRG of de verwerker zorgt ervoor dat deze taken of plichten niet tot een belangenconflict leiden. Om belangenverstremming te voorkomen, mag de functionaris voor gegevensverwerking 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.

5.3 Taken van de functionaris voor gegevensverwerking

1. De functionaris voor gegevensbescherming vervult ten minste de volgende taken:
 - a) DRG of de verwerker en de werknemers die verwerken, informeren en adviseren over hun verplichtingen uit hoofde van de privacywetgeving (de AVG en andere gegevensbeschermingsbepalingen zoals uit sectorspecifieke wet- en regelgeving);
 - b) toezien op naleving van deze AVG, van andere gegevensbeschermingsbepalingen en van het beleid van DRG of de verwerker 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;
 - c) desgevraagd advies verstrekken met betrekking tot de gegevensbeschermingseffectbeoordeling en toezien op de uitvoering daarvan;
 - d) met de Autoriteit Persoonsgegevens samenwerken;
 - e) 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.
2. 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.

5.4 Bij een klacht

Bij een klacht over de naleving van dit reglement kan de betrokkene zich wenden tot de Verwerkingsverantwoordelijke/zorgaanbieder van De Regenboog Groep:

Bestuur: H. Wijnands info@deregenboog.org

De functionaris voor gegevensverwerking: L. Dijkmans fg@deregenboog.org

Voor andere klachten raadpleegt de betrokkene de klachtenregeling.

5.5 Wijzigingen en inzage van dit reglement

Dit reglement geldt per 25 mei 2018 en is te vinden op de Website van De Regenboog Groep: www.deregenboog.org

6. Donateurs / Financiële Supporters

Stichting De Regenboog Groep, gevestigd in Amsterdam (hierna De Regenboog Groep), gebruikt jouw gegevens om je als supporter goed van dienst te kunnen zijn, en om je te informeren over onze acties en campagnes. De Regenboog Groep beschermt jouw gegevens daarbij zoals het hoort. Jouw (persoons)gegevens zijn en blijven van jou: we vertellen je graag wat we van je weten, waarom we dat nodig hebben om je van dienst te kunnen zijn, precies wat je van ons kunt verwachten en aan welke regels we ons houden. In dit privacy statement geven wij je informatie over het volgende:

- welke persoonsgegevens wij waarvoor gebruiken;
- wie ontvangt jouw persoonsgegevens (nog meer);
- hoe lang persoonsgegevens worden bewaard;
- welke beveiligingsmaatregelen wij nemen;
- welke rechten je hebt ten aanzien van jouw persoonsgegevens en hoe je met ons daarover in contact komt.

Welke persoonsgegevens gebruiken wij waarvoor?

6.1 (Financiële) Supporters en werving

De Regenboog Groep heeft financiële en niet-financiële supporters en vrijwilligers. De eerste groep steunt ons met voor ons onmisbare donaties. Met de tweede groep wordt bedoeld de supporters die ons op andere wijze steunen zoals bij onze (online) acties en petities (hierna acties) om bepaalde zaken aan de orde te brengen.

De Regenboog Groep is voor haar inkomsten, naast subsidies, ook afhankelijk van de donaties en de steun van haar supporters. De Regenboog Groep heeft dus een gerechtvaardigd belang om steeds nieuwe supporters te werven, een langdurige relatie met huidige supporters en vrijwilligers tot stand te brengen en te onderhouden en hen te informeren over acties van De Regenboog Groep of andere belanghebbende zaken. De Regenboog Groep benadert haar (potentiële)supporters daarom actief met verzoeken om donaties en steun.

De gegevens die worden vastgelegd in de supportersadministratie worden gebruikt voor het verwerken van donaties en andere vormen van steun en het periodiek verzoeken om ons (opnieuw) te steunen. Daarbij gebruiken wij naam, adres, woonplaats, telefoonnummer, e-mailadres (contactgegevens), geslacht, geboortedatum. Voor onze donateursadministratie en fondsenwervende programma's gebruiken we hiernaast banknummer, betaalhistorie en interessegebied.

6.2 Vrijwilligers

Voor de totstandkoming en uitvoering van een vrijwilligersovereenkomst en om onze vrijwilligers te informeren via telefoon, post, e-mail gebruikt De Regenboog Groep persoonsgegevens zoals contactgegevens, geslacht, geboortedatum en bankgegevens (in geval van vergoeden van bepaalde onkostenvergoedingen). Je kunt je als vrijwilliger niet afmelden voor het ontvangen van deze informatie, tenzij je je uitschrijft als vrijwilliger.

6.3 De Regenboog Groep kwartaal magazine Meeleven

Financieel supporters ontvangen het kwartaalblad Meeleven. Voor de bezorging gebruikt De Regenboog Groep je naam, adres, postcode en woonplaats. Om je te kunnen bereiken in verband hiermee verwerken wij ook je emailadres en je telefoonnummer.

6.4 Webwinkel (e-commerce)

Als je online een bestelling doet bij De Regenboog Groep hebben we je naam en adresgegevens nodig voor het kunnen afleveren van je aankopen en je e-mailadres en telefoonnummer om je van deze levering op de hoogte te houden. Als je iets aan iemand cadeau geeft vragen wij de hiervoor genoemde gegevens, maar ook je naam, adres, woonplaats, e-mailadres en telefoonnummer van degene die het cadeau krijgt.

Omdat wij een niet fysieke aankoop (zoals het doneren van sokken, een maaltijd of een schone spuit) als een gift zien, kunnen wij je telefonisch benaderen om meer te vertellen over het werk van De Regenboog Groep of verdere donatiemogelijkheden te bespreken. Dit kan, ook al sta je met je mobiele nummer in het Bel-me-niet Register ingeschreven, vanwege de financiële transactie. Stel je er geen prijs op om door De Regenboog Groep op de hoogte te worden gehouden of gebeld te worden? Dan kan je contact opnemen via geef@deregenboog.org, dan halen we je uit ons systeem.

6.5 Contact met De Regenboog Groep

Wij treden graag in contact met onze (potentiële) supporters en vrijwilligers. Wij kunnen je via verschillende kanalen bereiken waaronder via de telefoon, e-mail, social media en via onze medewerkers en wervers in het land. Ook staan wij voor je klaar om je van dienst te zijn, vragen te beantwoorden en problemen op te lossen.

Voor deze doelen gebruiken wij contactgegevens, donateurshistorie met betrekking tot De Regenboog Groep en voor zover van toepassing jouw vraag en alle overige persoonsgegevens die je aan ons verstrekt en die nodig zijn om jouw vraag te beantwoorden. Als je een vraag of klacht hebt, gebruiken we informatie ook om je op de hoogte te houden van je vraag of klacht maar ook om inzicht te krijgen in de aard van de vraag of klacht.

6.6 Nieuwsbrieven

Financiële supporters ontvangen standaard onze nieuwsbrieven en informatie over onze campagnes en overige activiteiten. Maar ook anderen kunnen zich daarvoor aanmelden. Voor dit doel gebruiken we je inschrijving voor de nieuwsbrief en je contactgegevens.

Je kunt je altijd afmelden voor nieuwsbrieven via de link onderaan de e-mail of per telefoon via 020 5317600 (tijdens kantooruren).

6.7 Jongeren onder 16 jaar

De Regenboog Groep wil geen gegevens verzamelen van jongeren onder de 16 jaar, zonder toestemming van ouders of voogd. Wij hebben onze processen hierop ook ingericht maar we kunnen vaak niet met zekerheid vaststellen of een bezoeker van onze website ouder dan 16 is. Wij raden ouders dan ook aan betrokken te zijn bij de online activiteiten van hun kinderen, om zo te voorkomen dat er gegevens over kinderen verzameld worden zonder ouderlijke toestemming. Als je vermoedt dat wij zonder die toestemming persoonlijke gegevens hebben verzameld over een minderjarige, neem dan contact met ons op, dan kunnen wij als het juist is deze gegevens verwijderen.

6.8 Wie ontvangt jouw persoonsgegevens (nog meer)?

De Regenboog Groep schakelt soms andere bedrijven in, zoals bijvoorbeeld fondswervingsbureaus voor telemarketing en straat- en huis-aan-huis-werving, bedrijven die

zorgdragen voor mailings, hosting van onze website(s), postbezorgers, ICT-bedrijven en drukkerijen.

De Regenboog Groep streeft er zoveel mogelijk naar persoonsgegevens binnen de Europese Economische Ruimte te (laten) verwerken. Wij zorgen er in ieder geval voor dat er voldoende vereiste technische en organisatorische maatregelen zijn getroffen om te verzekeren dat jouw persoonsgegevens veilig zijn en uitsluitend voor opgedragen doeleinden worden gebruikt. Soms zijn we wettelijk verplicht om persoonsgegevens aan derden te verstrekken; zoals de Belastingdienst. Verder zullen we alleen gegevens aan derden verstrekken als we daarvoor jouw toestemming hebben gekregen.

6.9 Hoe lang worden persoonsgegevens bewaard?

Vanzelfsprekend bewaart De Regenboog Groep persoonsgegevens in overeenstemming met de wet niet langer dan noodzakelijk is. Hoe lang een persoonsgegeven wordt bewaard is afhankelijk voor het doel waarvoor het gebruikt wordt.

Na afloop van de bewaartermijn worden jouw persoonsgegevens verwijderd of geanonimiseerd. Anonimiseren houdt in dat jouw persoonsgegevens worden ontdaan van alle mogelijk identificerende kenmerken. Wat overblijft zijn statistische gegevens die op geen enkele manier meer aan jouw persoon kunnen worden gekoppeld. Deze statistische gegevens zijn voor ons van belang omdat wij op basis daarvan inzicht kunnen krijgen in het gebruik dat van onze producten en diensten wordt gemaakt.

6.10 Welke beveiligingsmaatregelen nemen wij?

De Regenboog Groep gaat uiterst zorgvuldig om met jouw persoonsgegevens. Wij hebben adequate technische en organisatorische maatregelen genomen om jouw persoonsgegevens te beveiligen tegen verlies of onrechtmatig gebruik, hieronder valt onder andere een deugdelijk informatiebeveiligingsbeleid en beveiligde servers. De Regenboog Groep heeft maatregelen genomen om jouw persoonsgegevens te beveiligen, onder meer door het gebruik van beveiligingssoftware, virusscanners en firewalls. Onze donatiepagina beveiligt ook jouw betaalgegevens door het gebruik van Secure Sockets Layer (SSL). Hiermee wordt af luisteren van communicatie, inmenging of vervalsing van berichten voorkomen. Als je op een beveiligde pagina zoals ons donatieformulier bent, dan dient je browser je te melden dat je op een veilige site bent door een slotje weer te geven in de adresbalk van je browser.

Verder hebben alleen medewerkers van De Regenboog Groep toegang tot jouw persoonsgegevens als dat nodig is om een bepaalde taak te verrichten en hebben alle medewerkers zich verbonden aan absolute geheimhouding.

6.11 Keurmerken, gedragscode en waarborgen

De Regenboog Groep heeft het CBF-keur voor goede doelen.

De Regenboog Groep werkt alleen met partijen die Postfilter en het Bel-me-niet Register in acht nemen.

Welke rechten heb je ten aanzien van jouw persoonsgegevens en hoe kom je met ons daarover in contact?

6.12 Gegevens inzien, aanpassen, overdragen, verwijderen, intrekken toestemming of bezwaar

Je hebt het recht om je persoonsgegevens in te zien, te corrigeren of te verwijderen. Daarnaast heb je het recht om je eventuele toestemming voor de gegevensverwerking in te trekken of bezwaar te maken tegen de verwerking van jouw persoonsgegevens door De Regenboog Groep en heb je het recht op gegevensoverdraagbaarheid. Dat betekent dat je bij ons een verzoek kan indienen om de persoonsgegevens die wij van jou beschikken in een computerbestand naar jou of een andere organisatie te sturen. Je kunt een verzoek tot inzage, correctie, verwijdering, gegevensoverdraging van je persoonsgegevens of verzoek tot intrekking van je toestemming of bezwaar op de verwerking van jouw persoonsgegevens sturen naar info@deregenboog.org. Om er zeker van te zijn dat het verzoek tot inzage door jou is gedaan, vragen wij jou een kopie van je identiteitsbewijs met het verzoek mee te sturen. Maak in deze kopie je pasfoto, MRZ (machine readable zone, de strook met nummers onderaan het paspoort), paspoortnummer en Burgerservicenummer (BSN) zwart. Dit ter bescherming van je privacy. Je kunt dit eenvoudig doen door de ID-app van de overheid te gebruiken. We reageren zo snel mogelijk, bij voorkeur binnen vier weken, op jouw verzoek.

Natuurlijk helpen wij je graag verder als je vragen of klachten hebt over de verwerking van jouw persoonsgegevens. Mocht je er desondanks toch niet samen met ons uitkomen, dan hebt je op grond van de privacywetgeving ook het recht om een klacht in te dienen bij de Autoriteit Persoonsgegevens.

Bijlage 1:

7 Competentieprofiel Functionaris voor de Gegevensbescherming (FG)

Beroepsbeschrijving:

De FG wordt door een verantwoordelijke (natuurlijk of rechtspersoon of bestuursorgaan) benoemd als onafhankelijk intern toezichthouder vanuit de Wet bescherming persoonsgegevens.

Wettelijke verantwoordelijkheden: De FG houdt toezicht op en geeft advies over de verwerking van persoonsgegevens en heeft geheimhoudingsplicht.

Kerntaken die voortvloeien uit de wettelijke verantwoordelijkheden:

De FG is een interne toezichthouder die:

- Gegevensverwerkingen inventariseert;
- Een openbaar register van (niet van melding vrijgestelde) gegevensverwerkingen bijhoudt;
- Klachten afhandelt over het gebruik van persoonsgegevens;
- Een deskundig aanspreekpunt is voor betrokkenen mbt verwerking van persoonsgegevens;
- Voorlichting en informatie geeft aan medewerkers over het verwerken van persoonsgegevens.
- De verantwoordelijk en/of medewerkers adviseert over verwerking van persoonsgegevens.
- Toezicht instrumentarium op basis van wet en (interne)regelgeving mbt verwerking van persoonsgegevens ontwerpt en initieert.
- Optreedt als intermediair richting de Autoriteit Persoonsgegevens.
- Het geweten is van het bedrijf met betrekking tot privacy aspecten.

Contacten

Intern

- Verantwoordelijke (directeur, raad van bestuur, bestuursorgaan e.d.);
Managers/leidinggevende van afdelingen die werken met persoonsgegevens;
- Privacy officer
- Security officer
- Accountant

Extern

- AP (Autoriteit persoonsgegevens)
- Betrokkenen
- NGFG (Nederlandse Beroepsvereniging van Functionarissen voor Gegevensbescherming)

Vereiste kennis

De FG heeft:

- HBO of Academisch werk- en denkniveau;
- Heeft kennis van relevante wet – en regelgeving omtrent bescherming van persoonsgegevens in brede zin;
- Heeft kennis van Governance en Compliance;
- Heeft kennis van informatie- en communicatietechnologie.
- Heeft kennis van informatiebeveiliging
- Heeft kennis van de administratieve organisatie
- Heeft kennis van Privacy Impact Assessment (PIA)
- Heeft kennis van audits
- Heeft kennis van integriteit en ethiek op gebied van privacy vraagstukken
- Kan schakelen tussen verschillende kennisgebieden (multidisciplinair en o.a. juridische en ICT relevante zaken)
- Heeft kennis van de organisatie waar de FG voor werkzaam is.

Vaardigheden

De FG beschikt over de volgende vaardigheden:

- Analytisch vermogen
- Overtuigingskracht.
- Omgevingsbewust
- Proactief
- Doorzettingsvermogen
- Communiceren
- Integriteit
- Organisationsensitiviteit
- Onafhankelijkheid
- Resultaatgericht
- Luisteren
- Risicobeheersing
- Empathie

Professionele attitude

De FG:

- Kan zijn controlebevoegdheden integer hanteren
- Kan zich binnen de organisatie goed positioneren
- Onderhoudt geregeld contact met AP
- Is diplomatiek
- Houdt zijn kennis up to date aangaande wet- en regelgeving bescherming van persoonsgegevens en ICT
- Kan omgaan met belangenverstrengelingen.
- Is lid van de branchevereniging

Aandachtspunten

De FG kan keten denken en beïnvloeden. De FG is geloofwaardig en betrouwbaar.

7.1 Rollen en verantwoordelijkheden t.a.v. privacybescherming

Directie

De directeur stelt het privacyreglement vast. Hij is daarmee eindverantwoordelijk voor de juiste implementatie van het privacyreglement.

Management

Het management is verantwoordelijk voor het privacyreglement binnen zijn verantwoordelijkheidsgebied. Het management is concreet verantwoordelijk voor:

- Het implementeren van de beleidsuitgangspunten uit het privacyreglement (en de relevante maatregelen) binnen de afdeling en de processen en systemen waarvoor het verantwoording draagt;
- Het toezien op de uitvoering van het privacyreglement en alle daarvan afgeleide beleidsnotities, procedures en richtlijnen, zowel voor wat betreft de eigen medewerkers als voor derden die onder zijn verantwoordelijkheid werkzaam zijn;
- Het instellen van de uit het privacy af te leiden procedures en werkinstructies.

Het is dus van belang dat het management aandacht besteedt aan bewustwording. Het management is verantwoordelijk voor het creëren van een open cultuur waarin risico's worden gemeld en tijdig adequate actie wordt ondernomen.

Functionaris Gegevensbescherming (FG)

De FG is verantwoordelijk voor de uitvoering en de naleving van de relevante wet- en regelgeving op het gebied van privacybescherming, in het bijzonder de AVG.

De FG heeft de volgende verantwoordelijkheden:

- Organisatiebreed gevraagd en ongevraagd adviseren over de naleving van de AVG;
- actualiseren van het privacyreglement en andere privacy procedures, -richtlijnen etc;
- voorbereiding van besluitvorming over privacy gerelateerde zaken;
- informeren van de directeur en het MT over ontwikkelingen met betrekking tot de AVG en relevante regelgeving;
- aanwijzingen en advies geven aan medewerkers met betrekking tot verwerking van persoonsgegevens;
- advisering in verband met de uitoefening van rechten van betrokkenen, informeren van betrokkenen, privacy statement op de website, meldplicht datalekken, contracteren van nieuwe verwerkers en de met hen af te sluiten verwerkersovereenkomsten;
- desgevraagd advies verstrekken of assistentie verlenen bij de uitvoering van een PIA en de hieruit volgende verbeterpunten;
- contactpersoon voor de Autoriteit Persoonsgegevens.

Security Officer (SO)

De SO (= de Directie) is verantwoordelijk voor het voorbereiden en het uitvoeren van het beleid voor informatiebeveiliging en de technische maatregelen.

De SO heeft de volgende verantwoordelijkheden:

- optreden als informatiebeveiligingsadviseur (voor het management) bij nieuwe ICT-voorzieningen en bij ingrijpende veranderingen in de ICT-infrastructuur. Bij wijzigingen in systemen en applicaties ziet de SO toe op de informatiebeveiliging in proces van bouwen/realisatie van de geautomatiseerde verwerking;
- coördineren van de uitvoering van informatiebeveiligingsmaatregelen uit het

informatiebeveiligingsbeleid/-plan en het ondersteunen van projecten waarin informatiebeveiliging een grote rol speelt;

- in samenwerking met de FG: opstellen van een informatiebeveiligingsplan;
- adviseren van de informatiemanagers over afhandeling van incidenten en evaluatie van incidenten in samenwerking met de FG;
- zorgdragen voor het autorisatiebeheer binnen de systemen/applicaties.

Leidinggevenden, afdelingsmanagers

De leidinggevenden zijn verantwoordelijk voor de (informatie)veiligheid, de betrouwbaarheid van de informatieprocessen en systemen en het gebruik van persoonsregistraties binnen hun verantwoordelijkheidsgebied.

De leidinggevenden hebben ten aanzien van de verwerkingen van persoonsgegevens de volgende taken:

- Borgen dat het werkproces wordt uitgevoerd conform de AVG;
- Borgen van de zogenaamde integriteit (betrouwbaarheid, juistheid) van de gegevens;
- Signaleren van mogelijke wijzigingen in het werkproces waarin persoonsgegevens betrokken zijn en indien noodzakelijk advies vragen aan de FG om de wijzigingen in lijn met de AVG te houden.
- Stimuleren van de bewustwording voor een goede privacybescherming onder de medewerkers van de afdeling.

Medewerkers en vrijwilligers

Alle vaste en tijdelijke medewerkers en vrijwilligers dragen persoonlijke verantwoordelijkheid voor de beveiliging van de activiteiten die behoren tot hun eigen functie en taken. Zij betrachten zorgvuldigheid bij het omgaan met persoonsgegevens, vertrouwelijke informatie en houden zich aan de afspraken die gecommuniceerd zijn en/of vastgelegd zijn in reglementen en richtlijnen.

Tevens is de medewerker verantwoordelijk, al dan niet via de (eigen) manager, voor het melden van beveiligingsincidenten volgens de procesbeschrijving melden data-incidenten.