Privacyreglement januari 2018

RiskCare

Inhoudsopgave

1. Inleiding

1.1 Waarom dit model?

Met dit privacyreglement is opgesteld voor een praktische en toegankelijke uitwerking van de vanaf 25 mei 2018 geldende privacyregels neergelegd in de Algemene Verordening Gegevensbescherming (hierna: AVG) en sectorspecifieke wetten zoals de Wet op de geneeskundige behandelingsovereenkomst (Burgerlijk Wetboek boek 7, titel 7, Afd.5 / Wgbo) en de Wet Bijzondere opnemingen in psychiatrische ziekenhuizen (Wet Bopz), de Zorgverzekeringswet (Zvw), Wet langdurige zorg (Wlz), de Wet Maatschappelijke Ondersteuning 2015 (Wmo 2015) en de Jeugdwet (Jw).
Om dit privacyregelement niet te omvangrijk te maken, beperken wij ons tot het noemen van (artikelen in) de aangegeven wet- en regelgeving en het geven van voorbeelden.

De AVG stelt het opstellen van privacybeleid (gegevensbeschermingsbeleid) verplicht, als onderdeel van de verantwoordingsplicht, als dat in verhouding staat tot de verwerkingsactiviteiten die een zorgaanbieder verricht. Dat is afhankelijk van de concrete omstandigheden zoals de aard, de omvang, de context en het doel van de gegevensverwerking. Zorgaanbieders verwerken bijzondere persoonsgegevens (gegevens met betrekking tot de gezondheid) en zijn daarom in principe verplicht dergelijk beleid op te stellen. Op verzoek van een betrokkene wordt het (schriftelijke) privacybeleid ter beschikking gesteld.
Met het aanpassen van dit privacyreglement aan het beleid van en uitvoeringspraktijk van RiskCare, voldoen wij aan de verplichting om privacybeleid op te stellen.
Met dit document wordt het model privacyreglement uit 2015 vervangen. Dit nieuwe regelement is gebaseerd op de AVG (die vanaf 25 mei 2018 van toepassing is) en nationale (sector)specifieke wetgeving. Het betreft een weergave op grote lijnen; voor bijzondere uitwerking van privacyonderwerpen wordt in de tekst verwezen naar andere documenten.

2. Relatie met andere wetten

Algemene Verordening Gegevensbescherming (AVG)

De AVG is een Europese verordening die regels stelt voor gegevensverwerkingen en heeft als doel persoonsgegevens te beschermen. Uit de AVG volgt dat het verboden is om bijzondere categorieën persoonsgegevens, zoals gezondheidsgegevens, te verwerken tenzij aan bijzondere (strengere) regels uit de AVG wordt voldaan.[2] De bepalingen uit de AVG gelden voor alle Europese landen gelijk en hebben als doel de privacy van personen binnen de EU te beschermen in verband met de verwerking van persoonsgegevens en het vrije verkeer van die gegevens te waarborgen. Anders dan bij een richtlijn behoeft een verordening niet te worden omgezet in een nationale regeling. De verordening werkt dus rechtstreeks. De verordening laat op een aantal plaatsen ruimte aan de nationale wetgever om eigen regels in nationale wetgeving verder te regelen. Onder meer wat de verwerking van bijzondere persoonsgegevenscategorieën (“gevoelige gegevens”) betreft. Deels wordt dit geregeld in een (Nederlandse) uitvoeringswet AVG waarvan in december 2017 nog geen definitieve versie van beschikbaar is.[3] De AVG biedt de lidstaten ook ruimte om eigen regels voor de toepassing vast te stellen in sectorspecifieke wetten zoals met betrekking tot geneeskundige gezondheidszorg (Wgbo en Wet Bopz) en met betrekking tot het sociaal domein (Wmo 2015 en Jw).[4]
Voor de gezondheidzorg belangrijkste wetten wordt hieronder aangegeven hoe zij zich verhouden tot de AVG en tot elkaar.

Relatie met Wgbo[5]

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

Relatie met 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 specialist/voorrang krijgen ten opzichte van bepalingen die volgen uit de Wgbo. 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 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.[6] Dit is echter geen vrijbrief voor ongelimiteerde gegevensverzoeken en/of -verstrekking; de zorgverzekeraar ontvangt slechts gegevens die noodzakelijk zijn voor zijn controle, niet meer en neemt bij materiële controles eventueel genoegen met inzage in gegevens waarover alleen de zorgaanbieder beschikt. De zorgverzekeraar moet zich bovendien houden aan de controlestappen in de Regeling zorgverzekering en de beleidsregels van het CBP (voorloper van de Autoriteit Persoonsgegevens) wat betreft de formele en materiële controles.

Relatie met de Wlz
De Wlz geeft bepalingen over privacy van cliënten 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 in hoofdstuk 9 van de wet, maar ook de controle of de gedeclareerde zorg ook daadwerkelijk is geleverd.[9] De Wlz geeft tevens “Wgbo-achtige” bepalingen en stelt bijzondere eisen aan het opstellen en de inhoud van een zorgplan met de cliënt. De Wlz is een specifieke wet ten opzichte van de Wgbo. De AVG blijft daarentegen naast de Wlz gelden. De afwijkende bepalingen in de 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 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.[10] 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 Jeugdwet
De Jeugdwet geeft bepalingen over privacy van een jeugdige en ouders bij preventie, ondersteuning, hulp en zorg bij opgroei- en opvoedingsproblemen, psychische problemen en stoornissen. Een voorbeeld is de gegevensverstrekking aan derden[11] waarin de gezinsvoogd ingeval van een ondertoezichtstelling van de jeugdige vergaande bevoegdheden is toegekend;

2 Artikel 9 AVG.
3 Op 13 december 2017 is de Uitvoeringswet aangeboden aan de Tweede Kamer. Het idee is dat op 25 mei 2018 ook deze Uitvoeringswet in werking moet treden. Echter dient de Parlementaire proces nog te worden doorlopen.
4 Overweging (10) AVG.
5 Burgerlijk Wetboek boek 7, Titel 7, Afd. 5.
6 Artikel 87 Zvw, dat wordt uitgewerkt in hoofdstuk 7 Regeling zorgverzekering.

aan de gezinsvoogd moet op zijn verzoek gezondheidsgegevens over de jeugdige en ouders worden verstrekt.[12] Het gaat daarbij om de informatie die voor de gezinsvoogd noodzakelijk is om de bedreigingen in de ontwikkeling weg te nemen. De hulpverlener geeft antwoord voor zover hij daartoe, binnen zijn deskundigheidsterrein, in staat is.
Verder is in de Jeugdwet het volgende geregeld: meldingsbevoegdheid aan de verwijsindex risicojongeren, verplicht gebruik van het BSN van de jeugdige, dossierplicht van de jeugdhulpverlener en bepaalde gegevensverstrekking aan het CBS ten behoeve van de beleidsinformatie.[13]

De Jeugdwet verplicht tot het vaststellen en gebruiken van een meldcode kindermishandeling. (de Wmo 2015 regelt dat Veilig Thuis zonder toestemming van betrokkene(n) gezondheidsgegevens mag verwerken voor het onderzoeken van een melding van kindermishandeling en huiselijk geweld [14]).
GGZ Nederland heeft een model Meldcode huiselijk geweld en kindermishandeling voor de ggz opgesteld.
De Jeugdwet bepaalt [15] dat de nadere regels over toestemming, dossier en privacy in paragraaf 7.3 niet van toepassing zijn als de Wgbo van toepassing is. De regels voor toestemming, dossier en privacy in de Wgbo zijn van toepassing als er bij de verlening van jeugdhulp geneeskundige handelingen op basis van een behandelingsovereenkomst worden verricht of als er in dat kader door een Wgbo-hulpverlener of een BIG-professional handelingen worden verricht.

9 Artikel 9.1.2 Wlz, dat wordt uitgewerkt in hoofdstuk 7 Regeling langdurige zorg.
10 Voorheen: het Advies- en Meldpunt Huiselijk Geweld en Kindermishandeling (AMHK). Hoofdstuk 4 Wmo 2015.
11 Jeugdwet, hoofdstuk 7.
12 Artikel 7.3.11, vierde lid, Jeugdwet
13 Deze opsomming is niet uitputtend
14 Artikel 5.1.6 Wmo 2015.
15 Artikel 7.3.1, derde lid, Jeugdwet.

3. Privacyreglement RiskCare GGZ

Dit reglement is van toepassing binnen RiskCare GGZ, te Geleen en Tilburg en heeft betrekking op de verwerkingen van gegevens van cliënten die bij RiskCare onder behandeling zijn.
Dit reglement is van toepassing op zowel op papier als elektronische verwerking van gegevens.

3.1 Definities

Autoriteit Persoonsgegevens (AP): de toezichthoudende autoriteit, de onafhankelijke instantie die erover waakt dat persoonsgegevens zorgvuldig en veilig worden verwerkt en zo nodig sancties kan opleggen als dat niet gebeurt.
Bestand: elk gestructureerd geheel van persoonsgegevens die volgens bepaalde criteria toegankelijk zijn.
Betrokkene: degene op wie een persoonsgegeven betrekking heeft, meestal de cliënt, of zijn (wettelijk) vertegenwoordiger.
Bijzondere categorieën persoonsgegevens: persoonsgegevens waaruit ras of etnische afkomst, politieke opvattingen, religieuze of levensbeschouwelijke overtuigingen, of het lidmaatschap van een vakbond blijken, en genetische gegevens, biometrische gegevens met het oog op de unieke identificatie van een persoon, of gegevens over gezondheid, of gegevens met betrekking tot iemands seksueel gedrag of seksuele gerichtheid.
Derde: elke persoon of instantie die geen betrokkene, verwerkingsverantwoordelijke, verwerker, of een persoon is die onder rechtstreeks gezag van de verwerkingsverantwoordelijke of de verwerker gemachtigd is persoonsgegevens te verwerken.
Functionaris voor gegevensbescherming (FG): functionaris die door de zorgaanbieder moet of kan worden aangesteld voor het informeren en adviseren over en het toezicht houden op de toepassing en naleving van de AVG en andere gegevensbeschermingsbepalingen.
Gezondheidsgegevens: gegevens over de lichamelijke of geestelijke gezondheid van een persoon, waaronder gegevens over verleende gezondheidsdiensten waarmee informatie over zijn gezondheidstoestand wordt gegeven;
Inbreuk in verband met persoonsgegevens: een inbreuk op de beveiliging die per ongeluk of op onrechtmatige wijze leidt tot de vernietiging, het verlies, de wijziging of de ongeoorloofde verstrekking van of de ongeoorloofde toegang tot doorgezonden, opgeslagen of anderszins verwerkte gegevens. Onder een ‘datalek’ valt dus niet alleen het vrijkomen (lekken) van gegevens, maar ook onrechtmatige verwerking van gegevens.
Persoonsgegevens: alle informatie over een geïdentificeerde of identificeerbare natuurlijke persoon („de betrokkene”); als identificeerbaar wordt beschouwd een natuurlijke persoon die direct of indirect kan worden geïdentificeerd, met name aan de hand van een identificator zoals een naam, een identificatienummer, locatiegegevens, een online identificator of van een of meer elementen die kenmerkend zijn voor de fysieke, fysiologische, genetische, psychische, economische, culturele of sociale identiteit van die natuurlijke persoon.
Pseudonimisering: het verwerken van persoonsgegevens op zodanige wijze dat de persoonsgegevens niet meer aan een specifieke betrokkenen kunnen worden gekoppeld zonder dat aanvullende gegevens worden gebruikt, mits deze aanvullende gegevens apart worden bewaard en technische en organisatorische maatregelen worden genomen om ervoor te zorgen dat de persoonsgegevens niet aan een geïdentificeerde of identificeerbare natuurlijke persoon worden gekoppeld.
Toestemming van de betrokkene: door betrokkene, op goede informatie berustende, specifieke, in vrijheid en ondubbelzinnig gegeven toestemming waarbij betrokkene hem betreffende verwerking van persoonsgegevens aanvaardt. Dat kan door middel van een schriftelijke of mondelinge verklaring of een ondubbelzinnige actieve handeling (zoals het elektronisch aanvinken van een hokje).
Verwerker: degene die in opdracht van en voor de verwerkingsverantwoordelijke persoonsgegevens verwerkt (bijvoorbeeld een externe hostingsfirma, saas-leverancier, kwaliteitsauditor of een extern salarisadministratiekantoor).
Verwerking van persoonsgegevens: alle handelingen met betrekking tot persoonsgegevens, waaronder in ieder geval het verzamelen, vastleggen, ordenen, bewaren, bijwerken, wijzigen,

opvragen, raadplegen, gebruiken, verstrekken door middel van doorzending, verspreiding of in een andere vorm beschikbaar stellen, samenbrengen, met elkaar in verband brengen, alsmede het afschermen, uitwissen of vernietigen van gegevens.
Verwerkingsverantwoordelijke: degene die, alleen of samen met anderen, het doel van en de middelen voor de verwerking van persoonsgegevens vaststelt; meestal de bestuurder van de zorgaanbieder.
Zorgaanbieder: RiskCare

3.2 Verwerking van persoonsgegevens van cliënten in overeenstemming met de AVG

3.2.1 Beginselen inzake persoonsgegevens verwerking [16]

RiskCare is verantwoordelijk voor de naleving van onderstaande beginselen bij de verwerking van persoonsgegevens en moet de naleving van deze beginselen kunnen aantonen ("verantwoordingsplicht").[17]
Binnen RiskCare worden persoonsgegevens alleen verwerkt:

- op een wijze die ten aanzien van de betrokkene rechtmatig, behoorlijk en transparant is;
- voor welbepaalde, uitdrukkelijk omschreven en gerechtvaardigde doeleinden en mogen vervolgens niet verder op een met die doeleinden onverenigbare wijze worden verwerkt; de verdere verwerking met het oog op archivering in het algemeen belang, wetenschappelijk of historisch onderzoek of statistische doeleinden wordt [18] niet als onverenigbaar met de oorspronkelijke doeleinden beschouwd ("doelbinding");
- voor zover zij toereikend zijn, ter zake dienend en beperkt tot wat noodzakelijk is voor de doeleinden waarvoor zij worden verwerkt ("minimale gegevensverwerking" ook wel "dataminimalisatie");
- indien de persoonsgegevens juist zijn en zo nodig worden geactualiseerd. Alle redelijke maatregelen moeten worden genomen om de persoonsgegevens die, gelet op de doeleinden waarvoor zij worden verwerkt, onjuist zijn, onverwijld te wissen of te rectificeren ("juistheid")
- en bewaard in een vorm die het mogelijk maakt de betrokkenen niet langer te identificeren dan voor de doeleinden waarvoor de persoonsgegevens worden verwerkt noodzakelijk is; persoonsgegevens mogen voor langere perioden worden opgeslagen voor zover de persoonsgegevens louter met het oog op archivering in het algemeen belang, wetenschappelijk of historisch onderzoek of statistische doeleinden worden verwerkt [19] mits de bij deze verordening vereiste passende technische en organisatorische maatregelen worden getroffen om de rechten en vrijheden van de betrokkene te beschermen ("opslagbeperking");
- door het nemen van passende technische of organisatorische maatregelen op een dusdanige manier dat een passende beveiliging ervan gewaarborgd is, en dat zij onder meer beschermd zijn tegen ongeoorloofde of onrechtmatige verwerking en tegen onopzettelijk verlies, vernietiging of beschadiging ("integriteit en vertrouwelijkheid").

3.2.2 Rechtmatigheid van de verwerking [20]

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

- de betrokkene heeft toestemming [21] gegeven voor de verwerking van zijn persoonsgegevens voor één of meer specifieke doeleinden; de zorgaanbieder moet de toestemming kunnen aantonen en betrokkenen heeft het recht de toestemming te allen tijde in te trekken;
- de gegevensverwerking is noodzakelijk voor de uitvoering van een overeenkomst waarbij de betrokkene partij is, bijvoorbeeld de behandelingsovereenkomst;
- de gegevensverwerking is noodzakelijk om een wettelijke verplichting na te komen, bijvoorbeeld de dossierplicht in de Wgbo of 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 persoon [22];
- 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 belangen [23] van de verwerkingsverantwoordelijke of van een derde én de belangen, grondrechten of fundamentele vrijheden van degene van wie de gegevens worden verwerkt niet prevaleren;

3.2.3 Voorwaarden voor het verwerken van gezondheidsgegevens [24]

Gezondheidsgegevens zijn één van de categorieën bijzondere persoonsgegevens. Het is in de AVG verboden bijzondere categorieën persoonsgegevens te verwerken, tenzij voldaan wordt aan één van de onderstaande voorwaarden [25]:

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

Let op: naast de opheffing van het verbod om bijzondere gezondheidsgegevens te verwerken zoals hierboven genoemd, moet ook nog een verwerkingsgrondslag aanwezig zijn om dergelijke gegevens te verwerken (zie ook 3.2.2). [26]

---

16 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.

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

18 Overeenkomstig artikel 89, eerste lid, AVG.

19 Overeenkomstig artikel 89, eerste lid, AVG.

20 Artikel 6 AVG.

21 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.

22 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.

23 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.

24 Artikel 9, tweede lid, AVG.

25 Artikel 9 AVG.

26 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 verstreken 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.

3.2.4 Gegevensverwerking door verwerker

- RiskCare kan de verwerking (extern) uitbesteden aan een verwerker en legt dan in een verwerkersovereenkomst de verplichtingen uit de AVG op aan de verwerker.[27] RiskCare 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.[28]
- De verwerking door een verwerker wordt geregeld in een (verwerkers)overeenkomst die de verwerker ten aanzien van de zorgaanbieder bindt en waarin het onderwerp, de duur van de verwerking, de aard en het doel van de verwerking, het soort persoonsgegevens en de categorieën van betrokkenen en de rechten en verplichtingen van de zorgaanbieder worden omschreven. Een dergelijke overeenkomst dient te voldoen aan de eisen die de AVG daaraan stelt.[29]
- De verwerker en eenieder die onder het gezag van RiskCare of van de verwerker handelt en toegang heeft tot persoonsgegevens, verwerkt deze uitsluitend in opdracht van RiskCare, tenzij hij door wet- of regelgeving tot verwerking gehouden is.[31]

3.2.5 Aansprakelijkheid verwerkingsverantwoordelijke en/of verwerker

RiskCare (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.[32]

De verwerker, waaraan RiskCare (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 RiskCare goede afspraken heeft gemaakt met de verwerker en deze heeft vastlegt in een verwerkersovereenkomst.[33]

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

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

3.2.7 Geheimhoudingsplicht en verstrekking aan derden

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 beroepscodes.

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.

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

De gegevensverwerking met het oog op archivering in het algemeen belang, wetenschappelijk of historisch onderzoek of statistische doeleinden is onderworpen aan passende waarborgen in overeenstemming met de AVG voor de rechten en vrijheden van de betrokkene. De waarborgen zorgen ervoor dat er technische en organisatorische maatregelen zijn getroffen om de inachtneming van het beginsel van minimale gegevensverwerking te garanderen. Tevens kan er in nationale wetgeving worden afgeweken van bepaalde rechten van betrokkenen uit de AVG voor zover die rechten de verwezenlijking van de specifieke doeleinden onmogelijk dreigen te maken of ernstig dreigen te belemmeren, en dergelijke afwijkingen noodzakelijk zijn om die doeleinden te bereiken.

De Wgbo [35] geeft onderstaande afwijkende bepalingen voor wetenschappelijk onderzoek op het gebied de van gezondheidszorg. Het uitgangspunt is dat voor het verstrekken van niet geanonimiseerde [36] gegevens toestemming van de cliënt is vereist. In afwijking van dit uitgangspunt kan ook zonder toestemming van de cliënt ten behoeve van statistiek of

wetenschappelijk onderzoek op het gebied van de volksgezondheid aan een ander desgevraagd inlichtingen over de cliënt of inzage in de bescheiden, worden verstrekt indien:

1. het vragen van toestemming in redelijkheid niet mogelijk is [37] en bij de uitvoering van het onderzoek zodanige waarborgen gelden, dat de persoonlijke levenssfeer van de cliënt niet onevenredig wordt geschaad, of
2. het vragen van toestemming, gelet op de aard en het doel van het onderzoek, in redelijkheid niet kan worden verlangd en de hulpverlener ervoor zorgt dat gegevens in zodanige vorm worden verstrekt dat herleiding tot individuele natuurlijke personen redelijkerwijs wordt voorkomen.

Verder moet:

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

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

3.2.9 Afspraken met de onderzoeker

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

3.2.10 Bewaren van persoonsgegevens

RiskCare 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.[38]

Bij RiskCare worden de dossiers 15 jaar na afsluiting van de zorg bewaard.

---

27 Artikel 28 AVG.
28 Voor de selectie van Leveranciers die voldoen aan de AVG wordt een checklist opgesteld die via de website van GGZ Nederland beschikbaar zal komen.
29 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.
30 Bij het model verwerkersovereenkomst is ook een inleiding en toelichting beschikbaar.
31 Artikel 29 AVG.
32 Zie de toelichting bij het model verwerkersovereenkomst (BOZ).
33 Model verwerkersovereenkomst, inleiding en toelichting (BOZ).
34 Artikel 89 AVG.
35 Artikel 7:457 en 7:458 BW (Wgbo).
36 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.
37 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.
38 Artikel 17, derde lid, AVG (overweging 65).

3.3 Rechten van de betrokkenen

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

Het verstrekken van de in deze paragraaf 3.3 bedoelde informatie, het verstrekken van de communicatie en het treffen van de maatregelen geschieden kosteloos. Indien het verzoek kennelijk ongegrond of buitensporig is, met name vanwege het repetitieve karakter, mag RiskCare:

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 RiskCare om de kennelijk ongegronde of buitensporige aard van het verzoek aan te tonen.[39]

RiskCare verstrekt de betrokkene onverwijld en in ieder geval binnen een maand na ontvangst van het verzoek krachtens deze paragraaf informatie over het gevolg dat aan het verzoek is gegeven. Afhankelijk van de complexiteit van het verzoek en van het aantal verzoeken kan die termijn indien nodig met nog eens twee maanden worden verlengd. De zorgaanbieder stelt de betrokkene binnen één maand, na ontvangst van het verzoek, in kennis van een dergelijke verlenging. Wanneer de betrokkene zijn verzoek elektronisch indient, wordt de informatie indien mogelijk elektronisch verstrekt, tenzij de betrokkene anderszins verzoekt.

3.3.2 Te verstrekken informatie [40]

Als RiskCare gegevens bij de betrokkene zelf opvraagt om te verwerken, informeert hij de betrokkene in een beknopte, transparante, begrijpelijke en gemakkelijk toegankelijke vorm [41], voorafgaand aan het verkrijgen van zijn persoonsgegevens, over:
de verwerkingsdoelen waarvoor de gegevens zijn bestemd, alsook de rechtsgrond voor de verwerking;
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.

Wanneer RiskCare voornemens heeft de persoonsgegevens verder te verwerken voor een ander doel dan waarvoor de persoonsgegevens zijn verzameld, verstrekt RiskCare 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.

---

39 Artikel 12 AVG.
40 Artikel 13 AVG. Let op: ook de Wgbo kent in artikel 7:448 BW een informatieplicht over behandelinhoudelijke zaken.
41 En in duidelijke en eenvoudige taal. Zie hiervoor artikel 12, eerste lid, AVG

3.3.3 Te verstrekken informatie wanneer de persoonsgegevens niet van de betrokkene zijn verkregen [42]

42 Artikel 14 AVG.

Wanneer persoonsgegevens niet van de betrokkene zijn verkregen, verstrekt RiskCare de betrokkene alle informatie conform hierboven (artikel 3.3.1) onder lid 1 en 2 en bovendien de betrokken categorieën van persoonsgegevens alsmede de bron waar de persoonsgegevens vandaan komen.
RiskCare 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 RiskCare voornemens heeft om de persoonsgegevens verder te verwerken voor een ander doel dan dat waarvoor de persoonsgegevens zijn verkregen, verstrekt RiskCare 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.

RiskCare hoeft de betrokkene niet te informeren over de hiervoor genoemde informatie indien:

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

3.3.4 Inzage en afschrift/kopie[43]

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.
Een wettelijk vertegenwoordiger van jongeren onder de 16 jaar of van een wilsonbekwame volwassene, heeft recht op inzage in of afschrift van het dossier met dezelfde uitzondering voor informatie over of verstrekt door derden (de andere ouder, familie, naastbetrokkenen en omstanders) voor zover van die vertegenwoordigers toestemming voor de behandeling is vereist. [44] 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 bescheiden aan de (wettelijk) vertegenwoordiger te verstrekken niet geacht kan worden de zorg van een goed hulpverlener in acht te nemen, laat hij zulks achterwege[45]. 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.

1. Indien de zorgaanbieder van mening is dat de gevraagde inzage en/of de kopieën moeten worden verstrekt, dient dat zo spoedig mogelijk plaats te vinden/te worden verstrekt, doch uiterlijk binnen één maand. Afhankelijk van de complexiteit van het verzoek/de verzoeken en van het aantal verzoeken kan die termijn indien nodig met nog eens twee maanden worden verlengd. RiskCare 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.[46]

2. eventueel toevoegen van bepalingen bij wie op welke wijze de betrokkene verzoeken moet doen voor het uitoefenen van dit recht

3.3.5 Rectificatie (verbetering)of aanvulling van persoonsgegevens en beperking van de verwerking van persoonsgegevens[47]

De betrokkene kan de zorgaanbieder vragen om rectificatie (verbetering) van hem of haar betreffende persoonsgegevens als die onjuist zijn of RiskCare 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.
eventueel toevoegen van bepalingen bij wie op welke wijze de betrokkene verzoeken moet doen voor het uitoefenen van deze rechten
RiskCare 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. RiskCare 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.
- Als RiskCare het verzoek van betrokkene afwijst, geeft hij daarvan schriftelijk[48] de reden. RiskCare deelt een afwijzing van het verzoek onverwijld en uiterlijk binnen één maand ontvangst van het verzoek aan de verzoeker mee. Ook informeert RiskCare 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.
- De betrokkene kan RiskCare 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 RiskCare tot rectificatie (verbetering), wissing of aanvulling van gegevens blijft bewaard in het dossier van de cliënt.

43 Artikel 7:456, 7:457 BW (Wgbo).
44 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.
45 Artikel 7:457, derde lid, BW (Wgbo).
46 Artikel 12 AVG (algemene regels voor de uitoefening van de rechten van de betrokkene).
47 Artikel 12 AVG e.v. AVG, artikel 16 AVG.

3.3.6 Recht op gegevenswissing (vergetelheid)[49]

De betrokkene heeft het recht van RiskCare zonder onredelijke vertraging wissing van hem betreffende persoonsgegevens te verkrijgen en RiskCare 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 RiskCare rust, de persoonsgegevens moeten worden gewist.

De betrokkene dient dit schriftelijk de wissing aan te vragen bij de directie van RiskCare. RiskCare wist 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. RiskCare stelt de betrokkene binnen één maand na ontvangst van het verzoek in kennis van een dergelijke verlenging.
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.
b) Een verzoek van een cliënt tot vernietiging binnen vijf jaar kan niet worden gehonoreerd;
c) een derde een aanmerkelijk belang heeft bij bewaring van die gegevens. Bijvoorbeeld: een kind van een cliënt heeft een erfelijke ziekte;
d) de cliënt heeft een procedure tegen de hulpverlener aangespannen of het is waarschijnlijk dat hij dit zal doen;
e) 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;
f) de zorgaanbieder de gegevens nodig heeft voor de instelling, uitoefening of onderbouwing van een rechtsvordering;
g) om redenen van algemeen belang op het gebied van volksgezondheid.

Het verzoek tot wissing van gezondheidsgegevens en de reactie daarop worden bewaard door RiskCare.[52]

3.3.7 Recht van bezwaar [53]

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 RiskCare is opgedragen of op basis van de noodzakelijkheid voor de behartiging van de gerechtvaardigde belangen van RiskCare of van een derde;

48 De betrokkene dient schriftelijk of met andere middelen, met inbegrip van , indien dit passend is, elektronische middelen, de informatie te verstrekken.
49 Artikel 17 AVG in samenhang met artikel 12 lid 3 e.v. AVG.
51 Artikel 19 AVG.
52 In dat geval kan bij een materiële controle aan de financier worden aangetoond dat het dossier, op verzoek van betrokkene, is vernietigd.
53 Artikel 21 AVG.

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

3.3.8 Recht op gegevensoverdraagbaarheid (dataportabiliteit)[54]

De betrokkene heeft het recht de hem betreffende persoonsgegevens, die hij aan RiskCare 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.
Bij de uitoefening van het recht op gegevensoverdraagbaarheid heeft de betrokkene het recht dat de persoonsgegevens, indien dit technisch mogelijk is, rechtstreeks van RiskCare naar de andere zorgaanbieder worden doorgezonden.
Bij de uitoefening van dit recht mag dit geen afbreuk doen aan de rechten en vrijheden van anderen.

3.4 Vertegenwoordiging

Bij een jeugdige jonger dan twaalf jaar en bij een wilsonbekwame jeugdige van twaalf tot achttien jaar, oefent (oefenen) de ouder(s) met gezag of de voogd de rechten van de jeugdige uit, tenzij dit niet verenigbaar is met de zorg van een goed hulpverlener.[55]
De ouder die geen gezag heeft krijgt desgevraagd belangrijke, algemene en feitelijke informatie [56] over de gezondheidstoestand van de jeugdige, tenzij:

- de hulpverlener de informatie ook niet aan de ouder met gezag heeft verstrekt/ verstrekt;
- dit niet verenigbaar is met de zorg van een goed hulpverlener.

De wilsbekwame jeugdige van twaalf jaar of ouder oefent zelfstandig zijn rechten over zijn persoons- en gezondheidsgegevens uit. Vernietiging van gegevens over (vermoedens van) kindermishandeling vindt uitsluitend plaats met toestemming van een wilsbekwame jeugdige van zestien jaar en ouder.
Is de betrokkene ouder dan achttien jaar en 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 betrokkene;
- indien de echtgenoot of levensgezel ontbreekt of niet optreedt: een kind, broer of zus van de betrokkene.

In het uiterste geval treedt RiskCare 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.

3.5 Veilige verwerking van persoonsgegevens

3.5.1 Verantwoordelijkheid van de verwerkingsverantwoordelijke[58]

RiskCare heeft passende technische en organisatorische maatregelen getroffen om te waarborgen dat de verwerking in overeenstemming met de AVG wordt uitgevoerd. Die maatregelen worden geëvalueerd en indien nodig geactualiseerd.
RiskCare beschikt over gegevensbeschermingsmaatregelen.
RiskCare is ISO 9001 gecertificeerd. In het bijbehorende kwaliteitsysteem staan gedragcodes die de veiligheid van de gegevensverwerking beschrijven. Alle hulpverleners werken volgens de Wgbo.

3.5.2 Gegevensbescherming door ontwerp en standaardinstellingen (Privacy by design en default)[59]

Rekening houdend met de stand van de techniek, de uitvoeringskosten, en de aard, de omvang, de context en het doel van de verwerking alsook met de qua waarschijnlijkheid en ernst uiteenlopende risico's voor de rechten en vrijheden van natuurlijke personen welke aan de verwerking zijn verbonden, treft de zorgaanbieder, zowel bij de bepaling van de verwerkingsmiddelen als bij de verwerking zelf, passende technische en organisatorische maatregelen, zoals pseudonimisering, die zijn opgesteld met als doel de gegevensbeschermingsbeginselen, zoals minimale gegevensverwerking, op een doeltreffende manier uit te voeren en de nodige waarborgen in de verwerking in te bouwen ter naleving van de voorschriften van deze verordening en ter bescherming van de rechten van de betrokkenen.
RiskCare 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.
Het registratiesysteem CRS is gecertificeerd en voldoet aan de veiligheidseisen van de AVG.

3.5.3 Register van verwerkingen

RiskCare beschikt over een register van de verwerkingsactiviteiten die onder hun verantwoordelijkheid plaatsvinden. Dat register bevat de volgende gegevens:

a) de naam en de contactgegevens van de zorgaanbieder 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 beoogde termijnen waarbinnen de verschillende categorieën van gegevens moeten worden gewist;
e) Een algemene beschrijving van de technische en organisatorische beveiligingsmaatregelen.

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

54 Artikel 20 AVG.
55 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.
56 Er mag slechts informatie worden verstrekt die feitelijk, globaal, belangrijk en doelgericht is.
58 Artikel 24 AVG.
59 Artikel 25 AVG.

3.5.4 Medewerking verlenen aan/samenwerken met de Autoriteit persoonsgegevens[63]

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

3.5.5 Beveiliging van de verwerking[64]

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 RiskCare en de verwerker passende technische en organisatorische maatregelen om een op het risico afgestemd beveiligingsniveau te waarborgen, die, waar passend, onder meer het volgende omvatten:

a) de pseudonimisering en versleuteling van persoonsgegevens;
b) het vermogen om op permanente basis de vertrouwelijkheid, integriteit, beschikbaarheid en veerkracht van de verwerkingssystemen en diensten te garanderen;
c) het vermogen om bij een fysiek of technisch incident de beschikbaarheid van en de toegang tot de persoonsgegevens tijdig te herstellen;
d) een procedure voor het op gezette tijdstippen testen, beoordelen en evalueren van de doeltreffendheid van de technische en organisatorische maatregelen ter beveiliging van de verwerking.

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.
Het aansluiten bij een goedgekeurde gedragscode of een goedgekeurd certificeringsmechanisme.
RiskCare en de verwerker treffen maatregelen om ervoor te zorgen dat iedere natuurlijke persoon die handelt onder het gezag van de zorgaanbieder of van de verwerker en toegang heeft tot persoonsgegevens, deze slechts in opdracht van de zorgaanbieder verwerkt, tenzij hij daartoe volgens wet- en regelgeving is gehouden.

3.5.6 Melding van een inbreuk in verband met persoonsgegevens aan de Autoriteit Persoonsgegevens (datalekken melden aan de AP) en datalekkenregister[65]

Indien een inbreuk in verband met persoonsgegevens heeft plaatsgevonden, meldt RiskCare 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).
De verwerker informeert RiskCare zonder onredelijke vertraging zodra hij kennis heeft genomen van een inbreuk in verband met persoonsgegevens.
In de melding aan de Autoriteit Persoonsgegevens wordt ten minste het volgende omschreven of meegedeeld:

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

Indien en voor zover het niet mogelijk is om alle informatie gelijktijdig te verstrekken, kan de informatie zonder onredelijke vertraging in stappen worden verstrekt.

De zorgaanbieder houdt alle inbreuken in verband met persoonsgegevens bij in een overzicht, met inbegrip van de feiten omtrent die inbreuk, de gevolgen daarvan en de genomen corrigerende maatregelen. Die documentatie stelt de Autoriteit Persoonsgegevens in staat de naleving van dit artikel te controleren.

3.5.7 Melding van een inbreuk in verband met persoonsgegevens aan de betrokkenen (datalekken melden aan de betrokkene)[66]

Wanneer de inbreuk in verband met persoonsgegevens waarschijnlijk een hoog risico inhoudt voor de rechten en vrijheden van natuurlijke personen, deelt RiskCare de betrokkene de inbreuk in verband met persoonsgegevens onverwijld mee.
De bedoelde mededeling aan de betrokkene bevat een omschrijving, in duidelijke en eenvoudige taal, van de aard van de inbreuk in verband met persoonsgegevens en ten minste de in het vorige artikel (3.5.7, derde lid, onder b), c) en d), bedoelde gegevens en maatregelen.
De mededeling aan de betrokkene is niet vereist wanneer een van de volgende voorwaarden is vervuld:

a. RiskCare 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. RiskCare 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.

Indien de zorgaanbieder de inbreuk in verband met persoonsgegevens nog niet aan de betrokkene heeft gemeld, kan de Autoriteit Persoonsgegevens, na beraad over de kans dat de inbreuk in verband met persoonsgegevens een hoog risico met zich meebrengt, de zorgaanbieder daartoe verplichten of besluiten dat aan een van de in lid 3 van dit artikel, bedoelde voorwaarden is voldaan.

3.5.8 Gegevensbeschermingseffectbeoordeling (Data Protection Impact Assessment, DPIA)[67]

De aard, de omvang, de context en de doeleinden van de persoonsgegevens die RiskCare opslaat van zijn cliënten is van dien aard dat deze geen hoog risico zijn voor de rechten en vrijheden van natuurlijke personen. RiskCare heeft derhalve geen DPIA.

63 Artikel 31 AVG.
64 Artikel 32 AVG.
65 Artikel 33 AVG.
66 Artikel 34 AVG.
67 Artikel 35 AVG. GGZ Nederland heeft een model gegevensbeschermingseffectbeoordeling (DPIA) opgesteld met toelichting.

3.6 Functionaris voor gegevensbescherming (FG)

3.6.1 Aanwijzing van een functionaris voor gegevensverwerking

RiskCare heeft een functionaris voor gegevensbescherming.

3.6.2 Taken van de functionaris voor gegevensverwerking

De functionaris voor gegevensbescherming vervult ten minste de volgende taken:

a) RiskCare 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 gegevensbeschermings-bepalingen en van het beleid van RiskCare 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 gegevensbeschermingseffect-beoordeling 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.

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.

3.6.3 Bij een klacht

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

RiskCare
T.a.v dhr. G. Frings
Geleenbeeklaan 80
6166 GR Geleen
g.frings@amacura.nl

of

De Autoriteit Persoonsgegevens

Voor andere klachten raadpleegt de betrokkene de klachtenregeling van RiskCare.

3.6.4 Wijzigingen en inzage van dit reglement

Dit reglement geldt per 1-1-2018 en is opgeslagen in ons kwaliteitsysteem.