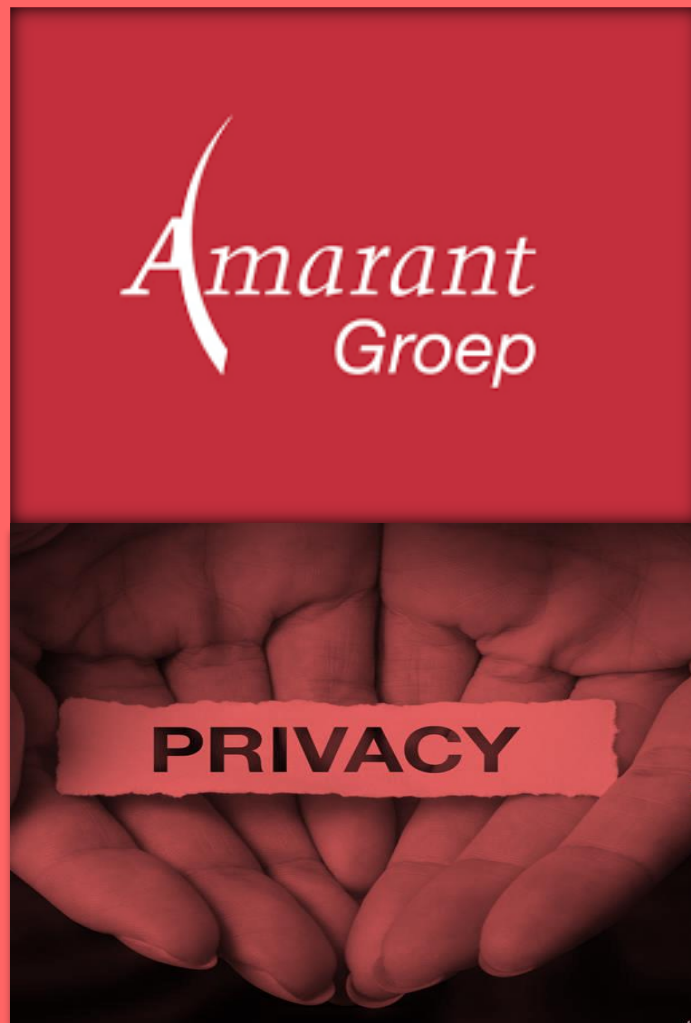


Zorg voor Privacy!

| Scriptie betreffende de gevolgen van de nieuwe privacywetgeving voor de zorginstelling Amarant Groep |



Incilay Göktas

Academie: Juridische Hogeschool Avans-Fontys

Afstudeerorganisatie: Amarant Groep

8 januari 2018, Tilburg

Het onderzoeksrapport:

Zorg voor Privacy!

**| Scriptie betreffende de gevolgen van de nieuwe privacywetgeving voor de
zorginstelling Amarant Groep |**

Classificatie: Intern

Opdrachtgever:
Organisatie: **Mw. W. van der Heijden
Amarant Groep
Bredaseweg 570
5036 NB Tilburg
klantenbureau@amarantgroep.nl
088 611 53 33**

Academie: **Juridische Hogeschool Avans-Fontys
Locatie Tilburg**

Coördinator: **Dhr. mr. B.C.M. Hooijdonk**

1^e Docent: **Dhr. mr. B.C.M. Hooijdonk**
2^e Docent: **Mw. mr. Y. Quispel**

Mentor: **Mw. W. van der Heijden**

Auteur/student: **Incilay Göktas**
Functie auteur/student: **Adviseren**
Studentnummer: **2057465**

Blok en thema: **E3-E4, afstuderen**

Periode: **September 2017 – Januari 2018**
Datum: **8 januari 2018**

Voorwoord

In opdracht van de stafmedewerker Wilma van der Heijden, van de afdeling Divisie Intensieve Behandeling van Idris, onderdeel van Amarant Groep, hierna te noemen Amarant Groep, verricht ik als opdrachtnemer, studente aan de Juridische Hogeschool Avans-Fontys te Tilburg, onderzoek naar de gevolgen van inwerkingtreding van de Algemene Verordening Gegevensbescherming voor Amarant Groep. In dit rapport geef ik de uitkomsten van mijn onderzoeksvragen door aan mijn opdrachtgever met de bedoeling om haar op de hoogte te houden van het huidige rechtssysteem. Dit onderzoeksrapport is een afsluiting van mijn studie en ik heb gekozen voor dit onderwerp omdat het zeer actueel en praktijkgericht is.

Ten slotte wil ik mijn opdrachtgever Wilma van der Heijden en mijn afstudeerdocent Bart Hooijdonk bedanken voor hun medewerking en begeleiding gedurende mijn afstudeerperiode en tevens de docente mevrouw Van Schaaijk van het vak methoden en technieken van onderzoek.

Incilay Göktas

Tilburg, januari 2018

Inhoudsopgave

Samenvatting

1 Inleiding

1.1 Aanleiding.....	8
1.2 Probleembeschrijving.....	8
1.3 Centrale vraag.....	8
1.4 Deelvragen.....	9
1.5 Doelstelling.....	9
1.6 Praktische en juridische kaders per hoofdstuk.....	9
1.7 Methoden van onderzoek en bronnen.....	9
1.8 Validiteit.....	11
1.9 Leeswijzer.....	11

2 Inleiding Algemene Verordening Gegevensbescherming

2.1 Vaststelling.....	12
2.2 Inwerkingtreding.....	12
2.3 Centraal doelstelling.....	12
2.4 Ontstaansgeschiedenis.....	13
2.5 Reikwijdte.....	14

3 Hoofdpijnen en juridische kaders Algemene Verordening Gegevensbescherming

3.1 Begrippen.....	15
3.2 Beginselen.....	15
3.3 Rechtsgrondslagen.....	15
3.4 Verwerking van persoonsgegevens.....	16
3.4.1 Bijzondere categorieën van persoonsgegevens.....	16
3.5 Rechten van de betrokkene.....	17
3.5.1 Inzagerecht.....	17
3.5.2 Rectificatierecht.....	18
3.5.3 Gegevenswissingsrecht.....	18
3.5.4 Gegevensoverdraagbaarheidsrecht.....	19
3.5.5 Profilerings.....	19
3.5.6 Beperkingen.....	19
3.6 Verplichtingen van de verwerkingsverantwoordelijke.....	19
3.6.1 Ontwerp en standaardinstellingen.....	20
3.6.2 Gegevensbeschermingseffectbeoordeling.....	21
3.6.3 Functionaris voor gegevensbescherming.....	21
3.6.4 Meldplicht voor datalekken.....	23
3.6.5 Bewerkingsovereenkomst.....	23
3.6.6 Register van de verwerkingsactiviteiten.....	24
3.7 Toezicht en handhaving.....	24
3.8 Sancties.....	25

4 Privacy in de praktijk van Amarant Groep

4.1 Sectorspecifieke wetten.....	26
4.2 Verwerkingsstappen in vogelvlucht.....	26
4.3 Kwaliteitshandboek.....	27
4.4 Algemene voorwaarden.....	27
4.4.1 Privacy en recht op inzage.....	27
4.4.2 Dossier.....	28
4.4.3 Persoonlijk plan en behandelplan.....	29
4.4.4 Samenwerking en coördinatie.....	31
4.5 Reglement verwerking persoonsgegevens.....	32
4.5.1 Bewerkingsovereenkomst.....	32

4.5.2 Informatieveiligheid.....	33
4.5.3 Bewaartermijn.....	34
4.5.4 Rechten van de cliënt.....	35
4.5.5 Functionaris voor gegevensbescherming.....	36
4.6 Reglement cliëntdossier.....	37
4.7 Reglement melding en afhandeling datalekken.....	38
4.8 Systemen.....	39
4.9 Geen beleid.....	39
4.9.1 Gegevensbeschermingseffectbeoordeling.....	40
4.9.2 Register van de verwerkingsactiviteiten.....	40

5 Conclusies en aanbevelingen

5.1 Conclusies.....	41
5.2 Aanbevelingen.....	43

Bronnen

Bijlagen

Samenvatting

Amarant Groep biedt ondersteuning, zorg en behandeling aan mensen met een beperking in iedere levensfase, variërend van lichte ondersteuning aan huis tot zeer intensieve specialistische zorg. Naast zorg en behandeling biedt zij kansen en mogelijkheden op het gebied van vrije tijd, dagbesteding, opleiding en werk. Bij het leveren van een goede zorg- en dienstverlening dient Amarant Groep ongetwijfeld te werken met veel persoonsgegevens van haar cliënten. Daarom is zij zich bewust van de privacynormen. Het huidige privacybeleid van Amarant Groep is echter nog niet geüpdatet waardoor het nog niet voldoet aan de toekomstige privacywetgeving.

Dit rapport betreft een onderzoek naar de gevolgen van de inwerkingtreding van de Algemene Verordening Gegevensbescherming voor Amarant Groep als zorginstelling. De Algemene Verordening Gegevensbescherming is op 25 mei 2016 in werking getreden en is per 25 mei 2018 van toepassing. De huidige nationale privacywetgeving, Wet bescherming persoonsgegevens, en de Europese privacyrichtlijn waar de Wet bescherming persoonsgegevens op gebaseerd is, vervallen en worden vervangen door de Algemene Verordening Gegevensbescherming, een Europese verordening.

De Europese Commissie, het Europees Parlement en de Raad van de Europese Unie willen het beschermingsniveau van persoonsgegevens verhogen door versterking en nadere omschrijving van de rechten van de betrokkenen en van de verplichtingen van degenen die persoonsgegevens verwerken. Daarnaast willen en kunnen zij niet langer accepteren dat het recht van de lidstaten is gefragmentariseerd, dat er rechtsonzekerheid is ontstaan en zorg bij de burgers over een tekortschietende bescherming van persoonsgegevens (bij online activiteiten). Daarom is er deze keer gekozen voor een verordening als instrument in plaats van een richtlijn, want een verordening is rechtstreeks toepasselijk in elke lidstaat en hoeft dus niet eerst omgezet te worden. De bestaande privacywetgeving heeft onder andere hierdoor burgers en hun persoonsgegevens onvoldoende kunnen beschermen.

De Algemene Verordening Gegevensbescherming brengt nieuwe rechten voor de betrokkenen en versterkt bestaande rechten van de betrokkenen op onderdelen. In het geval van Amarant Groep zijn haar cliënten de betrokkenen. Het gaat om het inzagerecht, het rectificatierecht, het gegevenswissingsrecht, het gegevensoverdraagbaarheidsrecht etc. van cliënten. In dit onderzoeksrapport komen deze rechten uitgebreid aan de orde. Daarnaast brengt deze Europese verordening verplichtingen met zich mee voor verwerkingsverantwoordelijken zoals Amarant Groep. Het gaat dan om verplichtingen zoals gegevensbescherming door ontwerp en door standaardinstellingen, gegevensbeschermingseffectbeoordeling, functionaris voor gegevensbescherming, meldplicht voor datalekken, bewerkingsovereenkomst, register van de verwerkingsactiviteiten etc. Ook deze verplichtingen worden uitvoerig besproken in dit onderzoeksrapport. Overigens worden overtredingen van de normen van de Europese verordening gesanctioneerd met zeer hoge boetes.

Amarant Groep als zorginstelling is een maatschappelijk betrokken organisatie en wenst voorop te lopen bij het vergaren van kennis over de toekomstige privacywetgeving alsmede bij het voldoen aan de eisen van die wetgeving. Aangezien Amarant Groep een zeer grote organisatie is in de regio Noord-Brabant, dient zij meer dan gewoonlijk rekening te houden met de privacy van haar vele cliënten. Dit onderzoeksrapport dient als handvat voor Amarant Groep waarin de huidige werkwijze van Amarant Groep wordt geanalyseerd en welke veranderingen op komt zijn, gezien de toekomstige privacywetgeving.

Tot slot worden er in dit onderzoeksrapport conclusies en aanbevelingen gegeven omtrent de Algemene Verordening Gegevensbescherming.

Lijst van afkorting

AP	Autoriteit Persoonsgegevens
Art	Artikel
AVG	Algemene Verordening Gegevensbescherming
Bopz	Wet bijzondere opnemingen in psychiatrische ziekenhuizen
BW	Burgerlijk Wetboek
ECD	Elektronisch Cliënten Dossier
FG	Functionaris voor gegevensbescherming
Handvest	Handvest van de grondrechten van de Europese Unie
PC2	Plancare2
VWEU	Verdrag betreffende de werking van de Europese Unie
Wbp	Wet bescherming persoonsgegevens
WGBO	Wet op de geneeskundige behandelingsovereenkomst
ZDO	Zorg- en dienstverleningsovereenkomst

1 Inleiding

Dit hoofdstuk bevat informatie over de opdrachtgever, de aanleiding van het onderzoeksrapport, de probleembeschrijving en het onderzoeksplan.

1.1 Aanleiding

Onlangs heeft Wilma van der Heijden, stafmedewerker van de Divisie Intensieve Behandeling van Idris, onderdeel van Amarant Groep, hierna te noemen Amarant Groep, gemeld dat Amarant Groep op de hoogte is van de Algemene Verordening Gegevensbescherming die met ingang van 25 mei 2018 geldt, maar dat Amarant Groep tot nu toe zich hierin onvoldoende heeft verdiept en benieuwd is hoe zij in de toekomst aan deze Europese verordening kan voldoen.

1.2 Probleembeschrijving

Op 25 mei 2018 is de Algemene Verordening Gegevensbescherming van kracht. De bedoeling van de Algemene Verordening Gegevensbescherming is dat de privacyrechten van personen verbeteren en er meer verantwoordelijkheden komen voor organisaties die persoonsgegevens verwerken.

De privacyproblematiek/privacywetgeving is een actueel onderwerp. De inwerkingtreding van de Algemene Verordening Gegevensbescherming heeft consequenties voor zowel publieke organisaties als organisaties in de private sector en dus ook voor zorginstellingen zoals Amarant Groep. Amarant Groep biedt ondersteuning, zorg en behandeling aan mensen met een beperking in iedere levensfase, variërend van lichte ondersteuning aan huis tot zeer intensieve specialistische zorg. Dat doet Amarant Groep in verbinding met de cliënt, zijn naasten en lokale cliëntenraden. Amarant Groep is gericht op in- en externe samenwerking wanneer dat in het belang is van de cliënt. Naast zorg en behandeling biedt Amarant Groep kansen en mogelijkheden op het gebied van vrije tijd, dagbesteding, opleiding en werk. Amarant Groep stimuleert en ondersteunt kwetsbare mensen om te leren, te groeien en sterker te worden.

Het is bij Amarant Groep gebruikelijk dat er een dossier aangemaakt wordt wanneer een cliënt wordt aangemeld bij het zogenaamde Klantenbureau van Amarant Groep. Dat is dus de eerste stap waar persoonsgegevens worden verwerkt. Vervolgens wordt er gekeken waar de cliënt past binnenin Amarant Groep. Er worden verslagen opgevraagd en zorgplannen opgemaakt. In de vervolgstappen komen onder andere voor: het doorsturen van het dossier naar de potentiële passende plaats/behandelaar en het opvragen van aanvullende verslagen bij de verwijzer. Als de partijen een behandelovereenkomst hebben gesloten, komt het dossier uiteindelijk ook in het zogenaamde PC2. Dat is een softwaretoepassing waarbij cliëntgegevens in digitale vorm bewaard en beschikbaar worden gemaakt. Dit zijn vele stappen in het begin waarbij men met persoonsgegevens werkt.

Vanuit Amarant Groep is er vraag naar een onderzoek naar de gevolgen van de Algemene Verordening Gegevensbescherming. Het moet voor Amarant Groep helder zijn hoe zij onder de nieuwe privacywetgeving moet omgaan met persoonsgegevens van haar cliënten, beveiliging daarvan en datalekken en wanneer een functionaris gegevensbescherming verplicht is. Het niet of niet geheel voldoen aan de nieuwe privacywetgeving is in strijd met de Algemene Verordening Gegevensbescherming en brengt sancties met zich mee.

1.3 Centrale vraag

Welke aanbevelingen kunnen aan de zorginstelling Amarant Groep worden gedaan bij de verwerking van persoonsgegevens van haar cliënten zodat zij voldoet aan de Algemene Verordening Gegevensbescherming die per 25 mei 2018 van toepassing is?

1.4 Deelvragen

1. Wat is de Algemene Verordening Gegevensbescherming (ontstaan, doel, vaststelling, inwerkingtreding en reikwijdte)?
2. Hoe luidt de nationale wet- en regelgeving met betrekking tot de verwerking van persoonsgegevens en wat zijn de belangrijkste veranderingen en nieuwe rechten/plichten na inwerkingtreding van de Algemene Verordening Gegevensbescherming?
3. Hoe werkt Amarant Groep momenteel in de praktijk met persoonsgegevens?
4. Welke stappen/maatregelen/middelen kan/moet Amarant Groep straks nemen in de praktijk?

1.5 Doelstelling

Op maandag 8 januari 2018 wordt er een onderzoeksrapport overhandigd aan de stafmedewerker Wilma van der Heijden van de Divisie Intensieve Behandeling van Idris, onderdeel van Amarant Groep. In het onderzoeksrapport wordt toegelicht wat de rechten en plichten en de consequenties daarvan zijn die de Algemene Verordening Gegevensbescherming met zich meebrengt. Daarnaast worden er aanbevelingen gedaan teneinde de verplichtingen voortvloeiend uit de Algemene Verordening Gegevensbescherming na te komen.

1.6 Praktische en juridische kaders per hoofdstuk

Hoofdstuk 1: Inleiding

Hoofdstuk 1 bevat, zoals nu wordt beschreven, informatie over de opdrachtgever, de aanleiding van het onderzoeksrapport, de probleembeschrijving en het onderzoeksplan.

Hoofdstuk 2: Inleiding Algemene Verordening Gegevensbescherming

Hoofdstuk 2 geeft een helder beeld van de inwerkingtreding, de rechtsgrondslagen en het doel van de Algemene Verordening Gegevensbescherming. In dit hoofdstuk wordt er uitgelegd wat deze Europese verordening inhoudt en wat het betekent voor de organisaties en personen, met name voor Amarant Groep als zorginstelling en haar cliënten. Ook wordt er ingegaan op het ontstaan, een stukje geschiedenis, van deze privacywetgeving.

Hoofdstuk 3: Hoofdpijnen en juridische kaders Algemene Verordening Gegevensbescherming

Hoofdstuk 3 is het juridisch hoofdstuk. In dit hoofdstuk wordt er gekeken naar de huidige/nationale wet- en regelgeving op het gebied van privacyrecht en wat de veranderingen en de nieuwe rechten/plichten zullen zijn in de toekomst nadat de Algemene Verordening Gegevensbescherming van toepassing is.

Hoofdstuk 4: Privacy in de praktijk van Amarant Groep

Hoofdstuk 4 is het praktijkgericht hoofdstuk. In dit hoofdstuk wordt ingegaan op hoe de verwerking van persoonsgegevens van cliënten momenteel eruitziet bij Amarant Groep en wordt er geschetst hoe dat in de toekomst dient te zijn, wil Amarant Groep voldoen aan de nieuwe privacywetgeving.

Hoofdstuk 5: Conclusies en aanbevelingen

Hoofdstuk 5 beschrijft de conclusies van dit onderzoek en aan de hand daarvan de concrete aanbevelingen aan Amarant Groep.

1.7 Methoden van onderzoek en bronnen

Bij de totstandkoming van dit onderzoeksrapport heb ik de wet- en regelgeving en de huidige situatie bij Amarant Groep geanalyseerd. Ik heb gebruik gemaakt van de tekst van de Algemene Verordening Gegevensbescherming, de EU-privacyrichtlijn, de Wet

bescherming persoonsgegevens, het Verdrag betreffende de Europese Unie, het Verdrag betreffende de werking van de Europese Unie, het Handvest van de grondrechten van de Europese Unie, de Wet op de geneeskundige behandelingsovereenkomst, de Wet bijzondere opnemingen in psychiatrische ziekenhuizen, literatuur en jurisprudentie. Daarnaast heb ik het boek 'Praktisch juridisch onderzoek' van Mw. Van Schaaijk geraadpleegd. Er is regelmatig contact geweest met de opdrachtgever, Wilma van der Heijden, stafmedewerker van de Divisie Intensieve Behandeling van Idris, onderdeel van Amarant Groep.

Hieronder wordt per deelvraag uiteengezet welke onderzoeksstrategieën, bronnen en methoden gebruikt zijn om de deelvragen te kunnen beantwoorden (deze drie vormen overigens de methodische verantwoording van dit onderzoek):

1. Wat is de Algemene Verordening Gegevensbescherming (ontstaan, doel, vaststelling, inwerkingtreding en reikwijdte)?

Hierbij gaat het om een onderzoek naar het recht. Om precies te zijn, gaat het om de historie en de theorie van het recht omtrent deze Europese verordening. Er is gebruik gemaakt van allerlei rechtsbronnen en literatuur. De hoofdlijnen van de Europese verordening Algemene Verordening Gegevensbescherming bestaande uit het ontstaan, de rechtsgrondslagen, het doel, de vaststelling, de inwerkingtreding en de reikwijdte worden besproken aan de hand van een onderzoek naar de wetsgeschiedenis. Het Europees Parlement en de Raad hebben ruim vier jaar onderhandeld over dit pakket voordat het kon worden vastgesteld in Brussel, maar in dit onderzoek wordt de wetgeschiedenis niet meer dan kort besproken en wordt de gedetailleerde parlementaire geschiedenis (en de bijbehorende documenten) buiten beschouwing gelaten. De intentie van deze deelvraag en de beantwoording daarvan is dan ook slechts het kort schetsen van het begin van deze nieuwe privacywetgeving. Het kort schetsen van de geschiedenis zorgt voor een beter en completer beeld van de Europese verordening. Bij de beantwoording van de eerste deelvraag is er daarom gebruik gemaakt van de literatuur, de tekst van deze Europese verordening en ten slotte de richtlijnen, verdragen en handvesten van de Europese Unie. Met literatuur wordt voornamelijk de artikelen uit juridische tijdschriften bedoeld. Hiertoe zijn de vindplaatsen en data van belang. Alsmede wordt er in dit onderzoeksrapport gebruik gemaakt van verwijzingen door middel van voetnoten en bronnenlijst.

2. Hoe luidt de nationale wet- en regelgeving met betrekking tot de verwerking van persoonsgegevens en wat zijn de belangrijkste veranderingen en nieuwe rechten/plichten na inwerkingtreding van de Algemene Verordening Gegevensbescherming?

Bij de tweede deelvraag worden de juridische kaders uiteengezet. Dat wordt gedaan door gebruik te maken van rechtsbronnen en vakliteratuur. De Europese verordening zelf is grondig geanalyseerd en er is gekeken naar in hoeverre deze invloed heeft op de opdrachtgever Amarant Groep als zorginstelling. Om de belangrijkste veranderingen en nieuwe rechten/plichten na de inwerkingtreding van de Europese verordening te kunnen toelichten, is er een vergelijking getrokken tussen de Europese verordening en de Nederlandse Wet bescherming persoonsgegevens die gebaseerd is op de Europese richtlijn. Daarnaast zijn verschillende wetten geraadpleegd, zoals: de Wet op de geneeskundige behandelingsovereenkomst en de Wet bijzondere opnemingen in psychiatrische ziekenhuizen. De bronnen zijn zorgvuldig geselecteerd. Zorgvuldig wil zeggen dat de gegevens recent en afkomstig zijn uit betrouwbare bronnen en deze toepasbaar zijn op de opdrachtgever Amarant Groep als zorginstelling. Er wordt in dit onderzoeksrapport gebruik gemaakt van verwijzingen door middel van voetnoten.

3. Hoe werkt Amarant Groep momenteel in de praktijk met persoonsgegevens?

De derde deelvraag vraagt om een beschrijving van de huidige werkwijze van Amarant Groep wanneer het neerkomt op het verwerken van persoonsgegevens. Om een dergelijke beschrijving te kunnen geven, zijn de werkinstructies en regelingen (o.a. het privacybeleid) van Amarant Groep bestudeerd en zijn er interviews gehouden/zijn er regelmatig gesprekken gevoerd met de gewenste medewerkers. Er zijn interviews gehouden met ten minste een stafmedewerker van de afdeling Divisie Intensieve Behandeling en met ad interim functionaris voor gegevensbescherming. In dit onderzoeksrapport wordt gebruik gemaakt van verwijzingen naar die interviews en de schriftelijke regelingen van Amarant Groep door middel van voetnoten.

4. Welke stappen/maatregelen/middelen kan/moet Amarant Groep straks nemen in de praktijk?

De laatste deelvraag betreft een toetsing van de werkwijze van Amarant Groep aan de nieuwe privacywetgeving. Na een dergelijke toetsing komen de aandachtspunten tevoorschijn en kunnen er conclusies worden getrokken en aanbevelingen worden gedaan aan Amarant Groep. Na het opvolgen van deze aanbevelingen zou Amarant Groep cliëntgegevens moeten verwerken conform de Europese verordening Algemene Verordening Gegevensbescherming. Hierbij zijn dus nogmaals de eerdergenoemde rechtsbronnen en vakliteratuur betrokken. Omdat Amarant Groep een zorginstelling is, is er voornamelijk gebruik gemaakt van vaktijdschriften op het gebied van gezondheidsrecht. Het gaat namelijk om privacyrecht binnenin het gezondheidsrecht. Bij het gebruik van bronnen is er een selectie gemaakt op betrouwbaarheid, recentheid en toepasbaarheid. Er wordt in dit onderzoeksrapport gebruik gemaakt van verwijzingen door middel van voetnoten en bronnenlijst.

1.8 Validiteit

Dit onderzoek is gebaseerd op feitelijke informatie, wet- en regelgeving, officiële bekendmakingen en jurisprudentie. Het onderzoeksrapport is controleerbaar door raadpleging van de bronnen en literatuurverwijzingen.

1.9 Leeswijzer

Dit onderzoeksrapport bestaat vijf hoofdstukken. De kern hoofdstukken zijn de hoofdstukken 2, 3 en 4.

Hoofdstuk 1: is de inleiding met negen paragrafen.

Hoofdstuk 2: bevat uitleg over de bedoeling van de Algemene Verordening Gegevensbescherming, een inleiding daarvan, introducerend naar het recht in de praktijk zoals uitgewerkt in de volgende hoofdstukken.

Hoofdstuk 3: licht de toekomstige privacywetgeving artikelsgewijs toe, vergelijkend met de huidige en de nationale privacywet- en regelgeving.

Hoofdstuk 4: betreft een analyse van hoe Amarant Groep op dit moment aan het werk is en een beschrijving van op welke wijze Amarant Groep binnenkort dient te werken.

Hoofdstuk 5: bevat conclusies en aanbevelingen.

Hierna vindt men de bronnenlijst en de bijlagen opgenomen.

2 Inleiding Algemene Verordening Gegevensbescherming

In dit hoofdstuk wordt als eerste een inleiding van de nieuwe privacywetgeving, de Algemene Verordening Gegevensbescherming, geschetst. Met een inleiding wordt ten minste het ontstaan, de vaststelling, de inwerkingtreding, het doel en de reikwijdte bedoeld.

2.1 Vaststelling

De Algemene Verordening Gegevensbescherming¹ (hierna: AVG) is op 27 april 2016 in Brussel vastgesteld. De AVG komt in de vorm van een verordening in plaats van de nu nog geldende Europese richtlijn, de EU-privacyrichtlijn². Samen met een richtlijn voor de gegevensbescherming op het gebied van de opsporing, de vervolging en de strafrechtstoepassing³ vormt de AVG de totale herziening van het gegevensbeschermingsrecht van de Europese Unie.

2.2 Inwerkingtreding

Op 4 mei 2016 is de AVG in het *Publicatieblad van de EU* bekendgemaakt en is het dus op 25 mei 2016 in werking getreden.⁴ De AVG geldt echter pas met ingang van 25 mei 2018⁵ omdat die uitgestelde gelding nodig is voor de lidstaten die ter uitvoering van de AVG veel wetgeving moeten vaststellen. Naast de vaststelling van wetgeving moet er ook wetgeving worden ingetrokken. Een Europese verordening is immers rechtstreeks toepasselijk. Daarom hoeft de AVG niet te worden omgezet, maar geïmplementeerd. In het geval van Nederland wordt de Wet bescherming persoonsgegevens (hierna: Wbp) ingetrokken en wordt er een Uitvoeringswet Algemene Verordening Gegevensbescherming vastgesteld.⁶

2.3 Centraaldoelstelling

De AVG heeft allereerst tot (hoofd)doel het beschermingsniveau van persoonsgegevens te verhogen door versterking van de rechten van de betrokkenen. Bescherming van persoonsgegevens is een grondrecht en verwerking van persoonsgegevens moet ten dienste staan van de mens.⁷ Het grondrecht heeft echter geen absolute gelding. Het moet volgens het evenredigheidsbeginsel worden afgewogen tegen andere grondrechten.⁸ In de volgende paragraaf komen ook nog andere (sub)doelstellingen naar voren.

¹ Verordening (EU) 2016/679 van het Europees Parlement en de Raad van 27 april 2016 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens en tot intrekking van Richtlijn 95/46/EG (algemene verordening gegevensbescherming; *PbEU* L 119).

² Richtlijn 95/46/EG van het Europees Parlement en de Raad van 24 oktober 1995 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens (*PbEG* L 281).

³ Richtlijn (EU) 2016/680 van het Europees Parlement en de Raad van 27 april 2016 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens door bevoegde autoriteiten met het oog op de voorkoming, het onderzoek, de opsporing en de vervolging van strafbare feiten of de tenuitvoerlegging van straffen en betreffende het vrije verkeer van die gegevens en tot intrekking van kaderbesluit 2008/977/JBZ van de Raad (*PbEU* L 119).

⁴ Art. 99 lid 1 AVG.

⁵ Art. 99 lid 2 AVG.

⁶ Zie voor de regels ter uitvoering van de verordening: www.internetconsultatie.nl (zoek op *Uitvoeringswet Algemene Verordening Gegevensbescherming*).

⁷ Art. 1 AVG.

⁸ H. de Vries & M. Goudsmit, 'Voorsorteren op de Algemene Verordening Gegevensbescherming. Twee stappen vooruit, één stap terug.', *Nederlands Juristenblad* 2016/1077.

2.4 Ontstaansgeschiedenis

De rechtsgrondslag voor de AVG kent twee aspecten. Allereerst is er een grondrechtelijk aspect. Het Handvest van de grondrechten van de Europese Unie (hierna: Handvest) garandeert eenieder het recht op bescherming van zijn persoonsgegevens.⁹ Behalve de formulering van het grondrecht zijn er ook enkele basisregels over gegevensbescherming opgenomen, bijvoorbeeld het beginsel van *eerlijke verwerking* van persoonsgegevens, het beginsel van *doelbinding* en de eis dat een verwerking moet berusten op *toestemming van de betrokkene* of een *andere gerechtvaardigde grondslag* verankert.¹⁰ Ten slotte moet er een *onafhankelijke autoriteit* toezien op de naleving van deze regels.¹¹

Het tweede aspect is een wetgevingsaspect en daarmee de eigenlijke rechtsgrondslag voor deze Europese verordening. Het Verdrag betreffende de werking van de Europese Unie (hierna: VWEU) regelt *dat het Europees Parlement en de Raad volgens de gewone wetgevingsprocedure de voorschriften vaststellen betreffende de bescherming van natuurlijke personen ten aanzien van de verwerking van persoonsgegevens door de instellingen en organen van de Europese Unie en door de lidstaten bij de uitoefening van activiteiten die binnen het toepassingsgebied van het recht van de Unie vallen, alsmede de voorschriften betreffende het vrije verkeer van gegevens*.¹²

De Europese Commissie heeft in 2012 gekozen voor de indiening van een ontwerpverordening in plaats van een ontwerprichtlijn. Het Europees Parlement en de Raad zijn de Europese Commissie in deze keuze gevolgd en hebben die keuze gemotiveerd.¹³ Hoewel de doelstellingen en beginselen van EU-privacyrichtlijn geldend blijven, heeft die richtlijn niet kunnen voorkomen dat het recht van de lidstaten is gefragmentariseerd, dat er rechtsonzekerheid is ontstaan en zorg bij de burgers over een tekortschietende bescherming van persoonsgegevens bij online activiteiten. Verschillen in de manier van bescherming tussen de lidstaten kunnen het vrije verkeer van gegevens in de Europese Unie belemmeren. Die verschillen kunnen de uitoefening van economische activiteiten in de Unie beïnvloeden, de mededinging verstoren en een beletsel vormen voor de uitoefening van de taak die de overheid uit hoofde van het Unierecht heeft. Ondanks de implementatie- en interpretatieverschillen moet er een eenvormige en gelijkwaardige bescherming van persoonsgegevens mogelijk zijn. Dat moet in combinatie met een versterking en nadere omschrijving van de rechten van betrokkenen en van de verplichtingen van degenen die gegevens verwerken. Tevens zijn gelijkwaardige bevoegdheden wat betreft toezicht en handhaving en vergelijkbare sancties voor overtredingen in alle lidstaten onontbeerlijk. Die doelstellingen kunnen het beste bereikt worden met een verordening, niet met een richtlijn. Een verordening is immers, zoals eerder vermeld in paragraaf 2.2 van dit onderzoeksrapport, van algemene strekking en rechtstreeks toepasselijk in elke lidstaat.¹⁴

De AVG is van toepassing op zeer veel terreinen. Het is ook van toepassing op terreinen die slechts deels door het Unierecht worden bestreken of die interfereren met het recht dat tot de bevoegdheidssfeer van de lidstaten behoort. Nagenoeg geen enkel beleidsterrein blijft verschoond van de verwerking van persoonsgegevens. Dat zorgt voor een gecompliceerde verhouding tussen de Europese en de nationale wetgevers. Daarom regelt de AVG expliciet dat de lidstaten bevoegd blijven om specifieke regels voor de verwerking van persoonsgegevens samenhangend met de specifieke rol van de overheid

⁹ Art. 8 lid 1 Handvest.

¹⁰ Art. 8 lid 2 Handvest.

¹¹ Art. 8 lid 3 Handvest.

¹² Art. 16 lid 2 VWEU.

¹³ R.o. 9 t/m 13 AVG.

¹⁴ Art. 288 VWEU.

te handhaven en zonodig vast te stellen.¹⁵ Te denken valt aan regels voor de verwerking van persoonsgegevens in het socialezekerheids- en belastingrecht.

2.5 Reikwijdte

De AVG is net als de EU-privacyrichtlijn *van toepassing op de geheel of gedeeltelijk geautomatiseerde verwerking van persoonsgegevens die in een (niet per se geautomatiseerd) bestand zijn opgenomen*.¹⁶ Op deze hoofdregel zijn er enkele uitzonderingen. De belangrijkste uitzondering is de volgende. De AVG is *niet van toepassing op de verwerking van persoonsgegevens die plaats vindt in het kader van een activiteit die buiten de werkingssfeer valt van het Unierecht*.¹⁷ Welke activiteiten dat zijn, staan in het Verdrag betreffende de Europese Unie.¹⁸ Daarin staan met name *defensie, handhaving van de openbare orde en nationale veiligheid* benoemd. Een andere belangrijke uitzondering is de gegevens die worden verwerkt *door de bevoegde autoriteiten met het oog op de voorkoming van, het onderzoek, de opsporing en de vervolging van strafbare feiten of de tenuitvoerlegging van straffen, met inbegrip van de bescherming tegen de voorkoming van gevaren voor de openbare veiligheid*.¹⁹ Deze zijn het onderwerp van een afzonderlijke richtlijn die gelijktijdig met de AVG is vastgesteld en die eerder in paragraaf 2.1 van dit onderzoeksrapport is genoemd.²⁰

Tot nu toe is de materiële reikwijdte besproken. De territoriale reikwijdte van de AVG is breed: de AVG is bovendien van toepassing op verantwoordelijkheden voor de verwerking van persoonsgegevens die zich buiten de Unie bevinden indien zij gegevens verwerken van betrokkenen die zich in de Europese Unie bevinden en die verwerking verband houdt met het aanbieden van goederen of diensten in de Europese Unie of wanneer de verwerking bestaat in het monitoren van het gedrag van die betrokkenen voor zover zij zich binnen de Europese Unie bevinden.²¹

¹⁵ Art. 6 lid 2 AVG.

¹⁶ Art. 2 lid 1 AVG.

¹⁷ Art. 2 lid 2 sub a AVG.

¹⁸ Art. 4 lid 2 Verdrag betreffende de Europese Unie.

¹⁹ Art. 2 lid 2 sub d AVG.

²⁰ Richtlijn (EU) 2016/680 van het Europees Parlement en de Raad van 27 april 2016 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens door bevoegde autoriteiten met het oog op de voorkoming, het onderzoek, de opsporing en de vervolging van strafbare feiten of de tenuitvoerlegging van straffen en betreffende het vrije verkeer van die gegevens en tot intrekking van kaderbesluit 2008/977/JBZ van de Raad (PbEU L 119).

²¹ Art. 3 lid 2 AVG.

3 Hoofddijnen en juridische kaders Algemene Verordening Gegevensbescherming

Dit hoofdstuk bevat informatie over de hoofddijnen en het juridisch kader van de toekomstige privacywetgeving. Deze zal invloed hebben op de werkwijze die binnen Amarant Groep moet worden gehanteerd. De belangrijkste artikelen uit de Europese verordening en de veranderingen worden toegelicht.

3.1 Begrippen

In de AVG zijn 26 definities van de in de AVG gebruikte begrippen gegeven.²² Die begrippen zijn voor het grootste deel overgenomen uit de EU-privacyrichtlijn. Er verandert inhoudelijk niet veel aan de centrale begrippen van het privacyrecht. De reikwijdte van het begrip ‘persoonsgegevens’ is echter min of meer verruimd.²³ In de rechtsoverweging wordt een zeer ruime uitleg gegeven van hetgeen onder de identificeerbaarheid van een persoon wordt verstaan. Een andere vernieuwing is de wijziging van het begrip ‘verantwoordelijke’ in ‘verwerkingsverantwoordelijke’. Betekenis van de begrippen is/blijft hetzelfde. Als laatste moet men nog wennen aan de term ‘verwerker’ omdat er in de Wbp in plaats daarvan de term ‘bewerker’ wordt gebruikt. Ook deze termen betekenen exact hetzelfde.

3.2 Beginselen

De AVG stelt dat persoonsgegevens moeten worden verwerkt in overeenstemming met een reeks beginselen. Het betreft achtereenvolgens de beginselen van *rechtmatigheid, behoorlijkheid en transparantie, van doelbinding, van minimale gegevensverwerking, van juistheid en van integriteit en vertrouwelijkheid*.²⁴ De inhoud van deze beginselen in de AVG stemt nagenoeg overeen met de beginselen uit de EU-privacyrichtlijn. Nieuw is wel dat de verwerkingsverantwoordelijke expliciet wordt aangewezen als degene die verantwoordelijk is voor de naleving van deze beginselen en dat de bewijslast daarvoor in beginsel ook bij hem ligt.²⁵ Dat betekent dus dat Amarant Groep de partij is die rekening moet houden met deze *verantwoordingsplicht* en niet haar cliënten.

3.3 Rechtsgrondslagen

Het verwerken van persoonsgegevens is alleen rechtmatig als dit gebeurt op basis van een rechtsgrondslag. De AVG wijst limitatief zes rechtsgrondslagen aan: *toestemming* van de betrokkene, de *uitvoering van een overeenkomst*, het voldoen aan een *wettelijke verplichting*, de *vitale belangen* van de betrokkene of een derde, de *vervulling van een taak van algemeen belang* en de *gerechtvaardigde belangen* van de verwerkingsverantwoordelijke of een derde indien dit belang opweegt tegen de belangen of de fundamentele vrijheden van de betrokkene.²⁶ Ook deze rechtsgrondslagen (en de inhoud daarvan) zijn dezelfde als in de EU-privacyrichtlijn. Er is echter wel wat veranderd. Namelijk, er zijn eisen gesteld aan de manier waarop de nationale wetgever invulling moet geven aan het criterium ‘taak van algemeen belang’.²⁷

Zeer significant voor de dagelijkse praktijk is dat de AVG nu nadrukkelijk erkent dat gegevens ook voor een ander doel mogen worden verwerkt dan het doel waarvoor ze aanvankelijk zijn verzameld, mits de aanvankelijke rechtsgrondslag niet wordt verlaten.

²² Art. 4 AVG.

²³ R.o. 26 AVG.

²⁴ Art. 5 lid 1 AVG.

²⁵ Art. 5 lid 2 AVG.

²⁶ Art. 6 lid 1 AVG.

²⁷ Art. 6 lid 3 AVG.

‘Verdere verwerking’ is toegestaan, mits een afweging plaatsvindt van een aantal expliciet genoemde belangen.²⁸

3.4 Verwerking van persoonsgegevens

Persoonsgegevens zijn *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. Verwerking daarvan is een bewerking of een geheel van bewerkingen met betrekking tot persoonsgegevens of een geheel van persoonsgegevens, al dan niet uitgevoerd via geautomatiseerde procedés, zoals het verzamelen, vastleggen, ordenen, structureren, opslaan, bijwerken of wijzigen, opvragen, raadplegen, gebruiken, verstrekken door middel van doorzending, verspreiden of op andere wijze ter beschikking stellen, aligneren of combineren, afschermen, wissen of vernietigen van gegevens.*²⁹

3.4.1 Bijzondere categorieën van persoonsgegevens

Voor de zorginstelling Amarant Groep is een verwerking van bijzondere categorieën van persoonsgegevens op de juiste wijze zeer van belang. Zeer van belang omdat Amarant Groep over heel veel persoonlijke (vaak ook gevoelige) informatie van haar cliënten beschikt en die dus ook verwerkt. Bijzondere categorieën van persoonsgegevens zijn *persoonsgegevens waaruit ras of etnische afkomst, politieke opvattingen, religieuze of levensbeschouwelijke overtuigingen, of het lidmaatschap van een vakbond blijkt, alsmede 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.*³⁰ Verwerking van deze gegevens zijn toelaatbaar als er wordt voldaan aan de voorwaarden die de AVG stelt. Net als de oude wetgeving kent de AVG grondslagen voor een rechtmatige verwerking, bijvoorbeeld bij uitvoering van een wettelijke plicht of wanneer dit noodzakelijk is ter bescherming van de vitale belangen van de betrokkene. Er is ook een grond dat verwerking van persoonsgegevens toestaat wanneer de betrokkene hiervoor toestemming heeft gegeven. Deze grond is in de AVG gewijzigd. De AVG heeft het over een ‘uitdrukkelijke toestemming’ van de betrokkene.³¹ Dit is een zwaardere vorm van toestemming.

Hieronder staan de voorwaarden voor toestemming beschreven³²:

- Wanneer de verwerking berust op toestemming, moet de verwerkingsverantwoordelijke kunnen aantonen dat de betrokkene toestemming heeft gegeven voor de verwerking van zijn persoonsgegevens.
- Indien de betrokkene toestemming geeft in het kader van een schriftelijke verklaring die ook op andere aangelegenheden betrekking heeft, wordt het verzoek om toestemming in een begrijpelijke en gemakkelijk toegankelijke vorm en in duidelijke en eenvoudige taal zodanig gepresenteerd dat een duidelijk onderscheid kan worden gemaakt met de andere aangelegenheden. Wanneer een gedeelte van een dergelijke verklaring een inbreuk vormt op deze verordening, is dit gedeelte niet bindend.
- De betrokkene heeft het recht zijn toestemming te allen tijde in te trekken. Het intrekken van de toestemming laat de rechtmatigheid van de verwerking op basis van de toestemming vóór de intrekking daarvan, onverlet. Alvorens de betrokkene zijn toestemming geeft, wordt hij daarvan in kennis gesteld. Het intrekken van de toestemming is even eenvoudig als het geven ervan.
- Bij de beoordeling van de vraag of de toestemming vrijelijk kan worden gegeven, wordt onder meer ten sterkste rekening gehouden met de vraag of voor de uitvoering van een overeenkomst, met inbegrip van een dienstenovereenkomst, toestemming vereist is voor een verwerking van persoonsgegevens die niet noodzakelijk is voor de uitvoering van die overeenkomst.

²⁸ R.o. 50 jo. art. 6 lid 4 AVG.

²⁹ Art. 4 onder 2 AVG.

³⁰ Art. 9 lid 1 AVG.

³¹ Art. 9 lid 2 sub a AVG.

³² Art. 7 AVG.

Amarant Groep dient zorgvuldig om te gaan met de gegeven toestemming tot het verwerken van cliëntgegevens. In de AVG is bepaald dat organisaties/instellingen moeten kunnen bewijzen dat zij conform de voorwaarden toestemming hebben gekregen. Naast dat moet het voor cliënten net zo gemakkelijk worden om hun toestemming in te trekken als die te geven. Amarant Groep moet kunnen aantonen dat zij er zorg voor heeft gedragen de cliënt zo goed mogelijk te informeren over waartoe hij of zij toestemming geeft en hoe cliënt de toestemming kan intrekken. De bewijslijst omtrent de toestemming ligt dus bij de zorginstelling Amarant Groep.

3.5 Rechten van de betrokkene

De betrokkene heeft recht op inzage en rectificatie van zijn persoonsgegevens en die zijn fundamenteel van aard.³³ De vormgeving van deze rechten vormt de kern van het hoofdstuk in de AVG waarin de rechten van de betrokkene geregeld zijn. Het is echter noodzakelijk dat de betrokkene weet van het feit dat zijn gegevens worden verwerkt, door wie dat gebeurt en ten behoeve van welke doeleinden, om aan de uitoefeningen van die rechten te kunnen toekomen. Er zijn daarvoor de benodigde verplichtingen in het leven geroepen voor verwerkingsverantwoordelijken.³⁴ Die verplichtingen verschillen inhoudelijk niets van de verplichtingen uit de EU-privacyrichtlijn. De plaatsing van de verplichtingen in de AVG in het hoofdstuk wat betreft de rechten van de betrokkene maakt duidelijk dat aansluiting van rechten en verplichtingen cruciaal is. De regeling van de rechten op inzage³⁵ en op rectificatie³⁶ zijn nauwelijks veranderd ten opzichte van de EU-privacyrichtlijn (zie hiervoor de volgende twee paragrafen). Dat geldt wat de inhoud betreft in de kern eigenlijk ook voor de rechten die in de EU-privacyrichtlijn nog werden aangeduid als de rechten van afscherming en verzet. Het recht op afscherming heeft nu een zelfstandige positie gekregen in de vorm van een recht op beperking.³⁷ Het recht op verzet heet nu recht op bezwaar.³⁸

3.5.1 Inzagerecht

Hieronder staan de eisen van het inzagerecht van de betrokkene beschreven:

Wanneer een betrokkene een verzoek doet tot inzage (bijvoorbeeld een cliënt bij Amarant Groep) zal in een omschrijving vanuit de organisatie *de verwerkingsdoeleinden en de betrokken categorieën van persoonsgegevens* waarop de verwerking betrekking heeft en *de ontvangers of categorieën van ontvangers aan wie de persoonsgegevens zijn of zullen worden verstrekt*, moeten zijn beschreven.³⁹ Dit was ook al zo geregeld onder de oude wetgeving.⁴⁰ De AVG voegt hier nog verdere criteria aan toe. Namelijk, de verwerkingsverantwoordelijke zal bij en inwilliging van het inzagerecht de betrokkene moeten informeren over⁴¹:

- indien mogelijk, de periode gedurende welke de persoonsgegevens naar verwachting zullen worden opgeslagen, of indien dat niet mogelijk is, de criteria om die termijn te bepalen;
- dat de betrokkene het recht heeft de verwerkingsverantwoordelijke te verzoeken dat persoonsgegevens worden gerectificeerd of gewist of dat de verwerking van hem betreffende persoonsgegevens wordt beperkt, alsmede het recht tegen die verwerking bezwaar te maken;
- dat de betrokkene het recht heeft klacht in te dienen bij een toezichthoudende autoriteit;
- alle beschikbare informatie over de bron van die gegevens, wanneer de persoonsgegevens niet bij de betrokkene worden verzameld;
- het bestaan van geautomatiseerde besluitvorming, met inbegrip van de in artikel 22, leden 1 en 4, bedoelde

³³ Art. 8 lid 2 Handvest.

³⁴ Art. 12 en 13 AVG.

³⁵ Art. 15 AVG.

³⁶ Art. 17 lid 1 AVG.

³⁷ Art. 18 AVG.

³⁸ Art. 21 AVG.

³⁹ Art. 15 lid 1 sub a t/m c AVG.

⁴⁰ Art. 12 EU-privacyrichtlijn jo. art. 35 Wbp.

⁴¹ Art. 15 lid 1 sub d t/m h AVG.

profilering, en ten minste in die gevallen, nuttige informatie over de onderliggende logica, alsmede het belang en de verwachte gevolgen van die verwerking voor de betrokkene.

3.5.2 Rectificatierecht

Hieronder staat het recht op rectificatie beschreven:

De betrokkene heeft het recht om van de verwerkingsverantwoordelijke onverwijld rectificatie van hem betreffende onjuiste persoonsgegevens te verkrijgen. Dit was ook zo geregeld onder de oude wetgeving.⁴² Op dit gebied zijn er geen grote verschillen tussen de oude wetgeving en de AVG. De AVG voegt een verdere criterium aan toe. Namelijk, *met inachtneming van de doeleinden van de verwerking heeft de betrokkene het recht vervollediging van onvolledige persoonsgegevens te verkrijgen, onder meer door een aanvullende verklaring te verstrekken.*⁴³ Een dergelijke situatie kan zich voordoen bij Amarant Groep met haar cliënten.

3.5.3 Gegevenswissingsrecht

Het recht op vergetelheid, oftewel recht op gegevenswissing, is nieuw in de AVG.⁴⁴ Hierdoor heeft de betrokkene de mogelijkheid de verwerkingsverantwoordelijke te verzoeken iedere koppeling naar, of kopie of reproductie van de persoonsgegevens van de betrokkene die door de verwerkingsverantwoordelijke openbaar zijn gemaakt te wissen en derde partijen die deze gegevens verder hebben verwerkt van de inwilliging van een dergelijk verzoek op de hoogte te stellen. Sinds het arrest van het Hof van de Justitie van de Europese Unie inzake *Google Spain SL en Google Inc / AEPD en Mario Costeja González*⁴⁵ was de uitoefening van dit recht jegens de exploitanten van zoekmachinediensten al erkend.⁴⁶ Dit recht is, evenzeer als alle andere rechten in de AVG, niet absoluut. In het bijzonder kan dit recht niet tegen de overheid worden ingeroepen.⁴⁷

Een verwerkingsverantwoordelijke kan worden verzocht (bijvoorbeeld Amarant Groep door een cliënt) persoonsgegevens te wissen.⁴⁸ Het is belangrijk dat dit verzoek zonder onredelijke vertraging wordt behandeld. Hieronder staan andere (verplichte) gevallen voor het recht op vergetelheid van de betrokkene beschreven⁴⁹:

- de persoonsgegevens zijn niet langer nodig voor de doeleinden waarvoor zij zijn verzameld of anderszins verwerkt;
- de betrokkene trekt de toestemming waarop de verwerking overeenkomstig artikel 6, lid 1, punt a), of artikel 9, lid 2, punt a), berust, in, en er is geen andere rechtsgrond voor de verwerking;
- de betrokkene maakt overeenkomstig artikel 21, lid 1, bezwaar tegen de verwerking, en er zijn geen prevalerende dwingende gerechtvaardigde gronden voor de verwerking, of de betrokkene maakt bezwaar tegen de verwerking overeenkomstig artikel 21, lid 2;
- de persoonsgegevens zijn onrechtmatig verwerkt;
- de persoonsgegevens moeten worden gewist om te voldoen aan een in het Unierecht of het lidstatelijke recht neergelegde wettelijke verplichting die op de verwerkingsverantwoordelijke rust;
- de persoonsgegevens zijn verzameld in verband met een aanbod van diensten van de informatiemaatschappij als bedoeld in artikel 8, lid 1. (Het gaat hier om gegevens die zijn verwerkt in het kader van leveren van diensten aan kinderen die jonger zijn dan zestien jaar.)

⁴² Art. 12 onder b EU-privacyrichtlijn jo. art. 36 Wbp.

⁴³ Art. 16 AVG.

⁴⁴ Art. 17 lid 2 AVG.

Ook wel bekend als: *right to be forgotten* of *recht om vergeten te worden*.

⁴⁵ HvJ EU 13 mei 2014, C-131/12, ECLI:EU:C:2014:317 (*Google Spain SL en Google Inc/AEPD en Mario Costeja González*).

⁴⁶ I.P.V. van Schelven & P.C. van Schelven, 'Europese gegevensbescherming: van richtlijn naar verordening', *Nederlands tijdschrift voor Europees recht* 2016/3, p. 99-108.

⁴⁷ Art. 17 lid 3 sub b AVG.

⁴⁸ Art. 17 lid 1 AVG.

⁴⁹ Art. 17 lid 1 sub a t/m f AVG.

3.5.4 Gegevensoverdraagbaarheidsrecht

Ook is het recht op gegevensoverdraagbaarheid nieuw.⁵⁰ Die bepaling geeft de betrokkene het recht om zijn gegevens van de ene naar de andere dienstverlener mee te nemen in een gestructureerde, gangbare en machineleesbare vorm. Dat recht is alleen bij verwerkingen in de private sector uit te oefenen.⁵¹ Uitoefening van dat recht vooronderstelt natuurlijk wel dat in de desbetreffende sector overeenstemming bestaat over het gebruik van een bepaalde gegevenssets en verwerkingsmethoden. Amarant Groep maakt deel uit van de zorgsector en zij dient dit recht van haar cliënten te waarborgen.

3.5.5 Profilerings

Het recht niet te worden onderworpen aan een besluit dat tot stand gekomen is na een volledig geautomatiseerde verwerking, wordt uitgebreid.⁵² De toevoeging 'profilering'⁵³ beoogt betrokkenen ook bescherming te bieden tegen het gebruik van hun gegevens in profileringen. Het gaat om 'big data'-toepassingen, een inmiddels veel voorkomend verschijnsel.

*Profilering is elke vorm van geautomatiseerde verwerking van persoonsgegevens waarbij aan de hand van persoonsgegevens bepaalde persoonlijke aspecten van een natuurlijke persoon worden geëvalueerd, met name met de bedoeling zijn beroepsprestaties, economische situatie, gezondheid, persoonlijke voorkeuren, interesses, betrouwbaarheid, gedrag, locatie of verplaatsingen te analyseren of te voorspellen.*⁵⁴ Van profilering is dus sprake als aan de hand van persoonsgegevens algoritmisch een beeld wordt gemaakt van aspecten van de persoonlijkheid of andere eigenschappen van een persoon.⁵⁵

3.5.6 Beperkingen

Beperkingen op de rechten van de betrokkene blijven mogelijk als zwaarwegende algemene belangen zoals de nationale veiligheid, de opsporing van strafbare feiten daartoe aanleiding geven.⁵⁶ Anders dan in de EU-privacyrichtlijn worden in de AVG strenge eisen gesteld aan de wettelijke maatregelen die de AVG voorschrijft voor de inroeping van een dergelijk belang.⁵⁷ Naleving van die eisen vraagt veel van de kwaliteit van de betrokken wetgeving.

3.6 Verplichtingen van de verwerkingsverantwoordelijke

In de AVG wordt de algemene verantwoordelijkheid van de verwerkingsverantwoordelijke voor de naleving van de verordening nader uitgewerkt.⁵⁸ De verwerkingsverantwoordelijke is verplicht technische en organisatorische maatregelen te treffen om te kunnen waarborgen en aantonen dat hij aan de normen van de AVG voldoet. Die verplichting is verijnd. De verwerkingsverantwoordelijke mag rekening houden met de aard, de omvang, de context en het doel van de verwerking en de ernst en waarschijnlijkheid van de risico's die uit de verwerking voortvloeien voor de rechten en vrijheden van natuurlijke personen. Ernst en waarschijnlijkheid van het risico doelen zonder twijfel op de mogelijke

⁵⁰ Art. 20 AVG.

Ook wel bekend als: *data portability* of *gegevensportabiliteit*.

⁵¹ Art. 20 lid 1 sub a en b AVG.

⁵² Art. 22 AVG.

⁵³ Ook wel bekend als: *profiling*.

⁵⁴ Art. 4 onder 4 AVG.

⁵⁵ I.P.V. van Schelven & P.C. van Schelven, 'Europese gegevensbescherming: van richtlijn naar verordening', Nederlands tijdschrift voor Europees recht 2016/3, p. 99-108.

⁵⁶ Art. 23 lid 1 AVG.

⁵⁷ Art. 23 lid 2 AVG.

⁵⁸ Art. 24 AVG.

consequenties die zich bij verwezenlijking van dat risico voordoen. Dat risico speelt een wezenlijke rol in vrijwel alle verplichtingen van de verwerkingsverantwoordelijke. De bedoeling is dat er meer verplichtingen gelden naarmate het risico groter is. In deze Europese verordening worden omschreven welke factoren een rol spelen bij de bepaling of er sprake is van een risico: materiële of immateriële schade, bestaande in of volgend uit discriminatie, identiteitsdiefstal, financiële gevolgen, reputatieverlies enz.⁵⁹ Het gaat hier eigenlijk om de vraag waarom deze Europese verordening persoonsgegevens beschermt. Niet vanwege die gegevens zelf, maar vanwege een scala aan achterliggende beschermde rechtsgoederen.

Zodoende heeft de verwerkingsverantwoordelijke een meer of minder omvangrijke documentatieplicht⁶⁰, een beveiligingsplicht⁶¹, een meldplicht voor datalekken⁶², een verplichting tot het opstellen van een gegevensbeschermingseffectbeoordeling⁶³, of een verplichting tot overleg met de toezichthoudende autoriteit⁶⁴. In enkele categorieën van gevallen moet ook een functionaris voor de gegevensbescherming worden aangesteld⁶⁵.

3.6.1 Ontwerp en standaardinstellingen

De zogenaamde ‘gegevensbescherming door ontwerp en door standaardinstellingen’ brengt nieuwe verplichtingen met zich mee.⁶⁶ Deze gegevensbescherming houdt in dat bij alle facetten van het verwerken van persoonsgegevens rekening gehouden moet worden met de waarborgen van privacy. Organisaties, zoals de zorginstelling Amarant Groep, moeten volgens de AVG interne beleidsmaatregelen nemen en toepassen. Deze moeten voldoen aan de beginselen van gegevensbescherming door ontwerp en door standaardinstellingen.⁶⁷ De technische en organisatorische maatregelen moeten genomen worden gedurende het gehele proces van het verwerken van persoonsgegevens. Dus zowel bij de bepaling van de verwerkingsmiddelen als bij de verwerking zelf. De maatregelen waar men aan kan denken, zijn bijvoorbeeld pseudonimisering, transparantie met betrekking tot de functies en de verwerking van de persoonsgegevens, het in staat stellen van de betrokkene om controle uit te oefenen op de informatieverwerking en het in staat stellen van de verwerkingsverantwoordelijke om beveiligingskenmerken te creëren en te verbeteren. Er mogen in beginsel alleen persoonsgegevens worden verwerkt die noodzakelijk zijn voor elk specifiek doel van verwerking.⁶⁸ Deze bepaling is een uitgebreidere vorm van de vorm in de oude wetgeving: de verplichting om passende technische en organisatorische maatregelen ten uitvoer te leggen om persoonsgegevens te beveiligen tegen verlies of tegen enige vorm van onrechtmatige verwerking.⁶⁹ Bij gegevensbescherming door ontwerp en door standaardinstellingen kan men denken aan nieuwe systemen met een goed autorisatiesysteem waarbij gebruik wordt gemaakt van voldoende sterke authenticatiemiddelen.⁷⁰

⁵⁹ R.o. 75 AVG.

⁶⁰ Art. 30 AVG.

⁶¹ Art. 32 AVG.

⁶² Art. 33 en 34 AVG.

⁶³ Art. 35 AVG.

⁶⁴ Art. 36 AVG.

⁶⁵ Art. 37 AVG.

⁶⁶ Ook wel bekend als: ‘*privacy by design*’ en ‘*privacy by default*’.

⁶⁷ Art. 25 AVG.

⁶⁸ Art. 25 lid 2 AVG.

⁶⁹ Art. 13 Wbp.

⁷⁰ T. Hooghiemstra e.a., *Onderzoek naar de beveiliging van patiëntgegevens* (PBLQ Rapport van 2016).

3.6.2 Gegevensbeschermingseffectbeoordeling

Een ander belangrijk beginsel van de AVG is het beginsel dat voorschrijft dat bij verwerking van persoonsgegevens ook de juistheid moet worden gecontroleerd en gewaarborgd. Daarom biedt de AVG een instrument genaamd 'gegevensbeschermingseffectbeoordeling'.⁷¹ Deze beoordelingen maken privacyeffecten van werkprocessen en de bijbehorende gegevensverwerkingen bevattelijker. Met dit instrument is in de praktijk al enige ervaring opgedaan. Nieuw is dat op grond van de AVG een dergelijke beoordeling verplicht moet worden uitgevoerd door een verwerkingsverantwoordelijke of een verwerker in een aantal gevallen, waaronder bijvoorbeeld profilering, grootschalige monitoring van openbare ruimten, grootschalige verwerking van bijzondere categorieën van persoonsgegevens.⁷² De benaming 'grootschalig' kan verwarringen veroorzaken. De advocaat of medicus die gegevens van cliënten/patiënten verwerkt, doet dat niet op grote schaal: een gegevensbeschermingseffectbeoordeling is dan niet verplicht.⁷³ De toezichthoudende autoriteit zal een lijst openbaar maken van het soort verwerkingen waarvoor een gegevensbeschermingseffectbeoordeling wel of juist niet vereist is.⁷⁴ Wanneer een dergelijke beoordeling uitwijst dat verwerking een hoog risico zou opleveren wat de verwerkingsverantwoordelijke niet met redelijke maatregelen kan beperken, dient vóór de verwerking een raadpleging van toezichthoudende autoriteit plaats te vinden.⁷⁵ Amarant Groep zal verplicht zijn in de toekomst een gegevensbeschermingseffectbeoordeling uit te voeren omdat er blijkt dat Amarant Groep op grootschalige wijze bijzondere categorieën van persoonsgegevens verwerkt. Met name de gezondheidsgegevens van cliënten zijn hier relevant. Hieronder staat wat de beoordeling dan ten minste moet bevatten⁷⁶:

- een systematische beschrijving van de beoogde verwerkingen en de verwerkingsdoeleinden, waaronder, in voorkomend geval, de gerechtvaardigde belangen die door de verwerkingsverantwoordelijke worden behartigd;
- een beoordeling van de noodzaak en de evenredigheid van de verwerkingen met betrekking tot de doeleinden;
- een beoordeling van de in lid 1 bedoelde risico's voor de rechten en vrijheden van betrokkene; en
- de beoogde maatregelen om de risico's aan te pakken, waaronder waarborgen, veiligheidsmaatregelen en mechanismen om de bescherming van persoonsgegevens te garanderen en om aan te tonen dat aan deze verordening is voldaan, met inachtneming van de rechten en gerechtvaardigde belangen van de betrokkenen en andere personen in kwestie.

3.6.3 Functionaris voor gegevensbescherming

Een functionaris voor gegevensbescherming (hierna: FG) is een interne deskundige op het gebied van bescherming persoonsgegevens.⁷⁷ Hij wordt geacht deskundig te zijn in het recht en de praktijk rondom de bescherming van persoonsgegevens en heeft tot taak de verwerkingsverantwoordelijke of verwerker in de meest ruime zin te ondersteunen bij het realiseren van naleving. De verplichting om een FG aan te stellen, geldt alleen voor overheden en overheidsinstanties (met uitzondering van gerechtelijke instanties) en voor verwerkingsverantwoordelijken en verwerkers van wie de kernactiviteiten bestaan uit het op grote schaal en systematisch monitoren van burgers of bestaan uit het verwerken van

⁷¹ Art. 35 AVG.

Ook wel bekend als: *privacy impact assessment (PIA) / data protection impact assessment (DPIA) / privacyeffectbeoordeling*.

⁷² Art. 35 lid 3 AVG.

⁷³ R.o. 71 AVG.

Zie ook: I.P.V. van Schelven & P.C. van Schelven, 'Europese gegevensbescherming: van richtlijn naar verordening', *Nederlands tijdschrift voor Europees recht* 2016/3, p. 99-108.

⁷⁴ Art. 35 lid 4 en 5 AVG.

⁷⁵ Art. 36 AVG.

⁷⁶ Art. 35 lid 7 AVG.

⁷⁷ Ook wel bekend als: *data protection officer (DPO)*.

bijzondere categorieën van persoonsgegevens of strafrechtelijke gegevens. De FG kan een eigen personeelslid van de verwerkingsverantwoordelijke of verwerker zijn, maar de functie mag ook op grond van een dienstverleningsovereenkomst worden vervuld.⁷⁸

Hieronder staat in welke gevallen een FG moet worden benoemd⁷⁹:

- de verwerking wordt verricht door een overheidsinstantie of overheidsorgaan, behalve in het geval van gerechten bij de uitoefening van hun rechterlijke taken;
- een verwerkingsverantwoordelijke of de verwerker hoofdzakelijk is belast met verwerkingen die vanwege hun aard, hun omvang en/of hun doeleinden regelmatige en stelselmatige observatie op grote schaal van betrokkenen vereisen; of
- de verwerkingsverantwoordelijke of de verwerker hoofdzakelijk is belast met grootschalige verwerking van bijzondere categorieën van gegevens uit hoofde van artikel 9 en van persoonsgegevens met betrekking tot strafrechtelijke veroordelingen en strafbare feiten als bedoeld in artikel 10.

Amarant Groep werkt vaak en veel met bijzondere categorieën van persoonsgegevens en moet er dus in dit geval een FG worden aangewezen (een bestaande medewerker als FG mag dus ook). De benoeming geschiedt door de verwerkingsverantwoordelijke of de verwerker. In nationale wetgeving of wetgeving van de Europese Unie kan worden bepaald dat in andere gevallen ook een FG mag of moet worden benoemd.⁸⁰

Hieronder wordt de positie van de FG beschreven⁸¹:

- De verwerkingsverantwoordelijke 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.
- De verwerkingsverantwoordelijke en de verwerker ondersteunen de functionaris voor gegevensbescherming bij de vervulling van de in artikel 39 bedoelde taken door hem toegang te verschaffen tot persoonsgegevens en verwerkingsactiviteiten en door hem de benodigde middelen ter beschikking te stellen voor het vervullen van deze taken en het in stand houden van zijn deskundigheid.
- De verwerkingsverantwoordelijke en de verwerker zorgen ervoor dat de functionaris voor gegevensbescherming geen instructies ontvangt met betrekking tot de uitvoering van die taken. Hij wordt door de verwerkingsverantwoordelijke of de verwerker niet ontslagen of gestraft voor de uitvoering van zijn taken. De functionaris voor gegevensbescherming brengt rechtstreeks verslag uit aan de hoogste leidinggevende van de verwerkingsverantwoordelijke of de verwerker.
- Betrokkenen kunnen met de functionaris voor gegevensbescherming contact opnemen over alle aangelegenheden die verband houden met de verwerking van hun gegevens en met de uitoefening van hun rechten uit hoofde van deze verordening.
- De functionaris voor gegevensbescherming is met betrekking tot de uitvoering van zijn taken overeenkomstig het Unierecht of het lidstatelijk recht tot geheimhouding of vertrouwelijkheid gehouden.
- De functionaris voor gegevensbescherming kan andere taken en plichten vervullen. De verwerkingsverantwoordelijke of de verwerker zorgt ervoor dat deze taken of plichten niet tot een belangenconflict leiden.

Zoals hierboven omschreven, komt aan de FG een prominente plaats toe in de organisatie/instelling en moet hij zijn werk in onafhankelijkheid kunnen uitvoeren. De zorginstelling Amarant Groep moet volgens de AVG rekening houden met deze essentiële kenmerken van de positie van de FG.

Hieronder worden de taken van de FG beschreven⁸²:

- de verwerkingsverantwoordelijke of de verwerker en de werknemers die verwerken, informeren en adviseren over hun verplichtingen uit hoofde van deze verordening en andere Unierechtelijke of lidstaatrechtelijke gegevensbeschermingsbepalingen;
- toezien op naleving van deze verordening, van andere Unierechtelijke of lidstaatrechtelijke gegevensbeschermingsbepalingen en van het beleid van de verwerkingsverantwoordelijke 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;
- desgevraagd advies verstrekken met betrekking tot de gegevensbeschermingseffect-beoordeling en toezien op de uitvoering daarvan in overeenstemming met artikel 35;

⁷⁸ Art. 37 lid 6 AVG.

⁷⁹ Art. 37 lid 1 AVG.

⁸⁰ Art. 37 lid 4 AVG.

⁸¹ Art. 38 AVG.

⁸² Art. 39 lid 1 AVG.

- met de toezichthoudende autoriteit samenwerken;
- optreden als contactpunt voor de toezichthoudende autoriteit inzake met verwerking verband houdende aangelegenheden, met inbegrip van de artikel 36 bedoelde voorafgaande raadpleging, en, waar passend, overleg plegen over enige andere aangelegenheid.

Dit zijn dan de taken die bijvoorbeeld de FG van Amarant Groep op zijn minst moet vervullen. Daarbij kan de zorginstelling nog andere taken opleggen.

3.6.4 Meldplicht voor datalekken

Zoals eerder vermeld, komt de Wbp te vervallen en daarmee ook de Wet meldplicht datalekken. Volgens de nieuwe AVG is er de verplichting om een 'inbreuk in verband met persoonsgegevens' aan de toezichthoudende autoriteit, respectievelijk de betrokkene te melden. De verwerkingsverantwoordelijke, bijvoorbeeld Amarant Groep, stelt de toezichthoudende autoriteit zonder onredelijke vertraging op de hoogte en, indien mogelijk, uiterlijk 72 uur nadat zij van een datalek kennis heeft genomen. Op grond van de Wbp moeten alleen 'ernstige' lekken worden gemeld.⁸³ Op grond van de AVG moeten alle lekken aan de toezichthoudende autoriteit gemeld worden, tenzij de verwerkingsverantwoordelijke conform het verantwoordingsbeginsel kan aantonen dat het onwaarschijnlijk is dat deze inbreuk risico's voor de rechten en vrijheden van natuurlijke personen met zich brengt.⁸⁴ Van de inbreuken die 'waarschijnlijk een hoog risico inhouden voor de rechten en vrijheden van natuurlijke personen', moet de betrokkene onverwijld op de hoogte gesteld worden.⁸⁵ Dit is ook een ander criterium dan wat geldt op grond van de Wbp. In de Wbp wordt gesproken over een inbreuk die 'waarschijnlijk ongunstige gevolgen zal hebben voor diens persoonlijke levenssfeer'.⁸⁶

Hieronder leest men wat de mededeling aan de betrokkene ten minste moet bevatten⁸⁷:

- een omschrijving, in duidelijke en eenvoudige taal, van de aard van de inbreuk in verband met persoonsgegevens;
- de naam en de contactgegevens van de functionaris voor gegevensbescherming of een ander contactpunt waar informatie kan worden verkregen;
- de waarschijnlijke gevolgen van de inbreuk in verband met persoonsgegevens;
- de maatregelen die de verwerkingsverantwoordelijke 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.

Van een datalek is bijvoorbeeld sprake bij verlies van een laptop met persoonsgegevens of bij het ongeautoriseerd hacken van een ICT-systeem.⁸⁸

3.6.5 Bewerkingsovereenkomst

De verplichting om een bewerkingsovereenkomst te sluiten, vloeit al voort uit de Wbp.⁸⁹ Deze verbintenis wordt aangegaan door de verwerkingsverantwoordelijke (voor de persoonsgegevens) en door de partij (verwerker) die de persoonsgegevens in opdracht verwerkt. De AVG herhaalt deze verplichting en stelt verdere eisen aan de bewerkingsovereenkomst. Om te beginnen moet in de overeenkomst zijn omschreven: *het onderwerp en 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 verwerkingsverantwoordelijke*.⁹⁰ Die bewerkingsovereenkomst bepaalt met name dat de verwerker de persoonsgegevens uitsluitend verwerkt op basis

⁸³ Art. 34a lid 1 Wbp.

⁸⁴ Art. 33 lid 1 AVG.

⁸⁵ Art. 34 lid 1 AVG.

⁸⁶ Art. 34a lid 2 Wbp.

⁸⁷ Art. 34 lid 2 jo. art. 33 lid 3 sub b t/m d AVG.

⁸⁸ I.P.V. van Schelven & P.C. van Schelven, 'Europese gegevensbescherming: van richtlijn naar verordening', *Nederlands tijdschrift voor Europees recht* 2016/3, p. 99-108.

⁸⁹ Art. 14 lid 2 Wbp.

⁹⁰ Art. 28 lid 3 AVG.

van schriftelijke instructies van de verwerkingsverantwoordelijke, de gegevens passend beveiligd, na afloop van de verwerkingsdiensten alle persoonsgegevens wist of deze aan de verwerkingsverantwoordelijke terugbezorgt en aan de verwerkingsverantwoordelijke alle informatie ter beschikking stelt die nodig is om de nakoming van de verplichtingen aan te tonen (bijv. audits). Ook belangrijk is dat de verwerker geen andere verwerker in dienst mag nemen zonder voorafgaande schriftelijke toestemming van de verwerkingsverantwoordelijke, in dit geval Amarant Groep.

3.6.6 Register van de verwerkingsactiviteiten

Als een organisatie/instelling, bijvoorbeeld de zorginstelling Amarant Groep, meer dan 250 werknemers in dienst heeft, geldt de verplichting om een register van verwerkingsactiviteiten te houden.⁹¹ Hieronder staat wat het register moet bevatten⁹²:

- de naam en de contactgegevens van de verwerkingsverantwoordelijke en eventuele gezamenlijke verwerkingsverantwoordelijken, en, in voorkomend geval, van de vertegenwoordiger van de verwerkingsverantwoordelijke en van de functionaris voor gegevensbescherming;
- de verwerkingsdoeleinden;
- een beschrijving van de categorieën van betrokkenen en van de categorieën van persoonsgegevens;
- de categorieën van ontvangers aan wie de persoonsgegevens zijn of zullen worden verstrekt, onder meer ontvangers in derde landen of internationale organisaties;
- 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, bedoelde doorgiften, de documenten inzake de passende waarborgen;
- indien mogelijk, de beoogde termijnen waarbinnen de verschillende categorieën van gegevens moeten worden gewist;
- indien mogelijk, een algemene beschrijving van de technische en organisatorische beveiligingsmaatregelen als bedoeld in artikel 32, lid 1.

Het register hoeft niet proactief te worden verstrekt en hoeft niet in de taal en volgens het formulier van de lokale toezichthouder te worden opgesteld.⁹³ De verwerkingsverantwoordelijke en de verwerker (of de vertegenwoordiger) zijn wel verplicht om dit register desgevraagd beschikbaar te stellen aan de toezichthoudende autoriteit.⁹⁴

3.7 Toezicht en handhaving

Zoals eerder vermeld in paragraaf 2.4 van dit onderzoeksrapport, verplichten het Handvest en de VWEU de Europese wetgever om onafhankelijke autoriteiten in te stellen die belast zijn met het toezicht op de naleving van de AVG.⁹⁵ Onafhankelijkheid is essentieel, mede omdat de publieke sector ook onderworpen is aan de regels van de AVG. Die verplichting is daarom uitgevoerd in de AVG.⁹⁶ Die autoriteiten bestaan al, omdat zij al ter uitvoering van de EU-privacyrichtlijn zijn ingesteld.⁹⁷ In Nederland voert de Autoriteit Persoonsgegevens (hierna: AP) het toezicht uit.⁹⁸

De AVG draagt de toezichthoudende autoriteiten een groot aantal taken en bevoegdheden op.⁹⁹ De AVG kent onderzoeksbevoegdheden toe, zoals een inlichtingenrecht; bevoegdheden tot het nemen van corrigerende maatregelen, zoals het opleggen van sancties; en autorisatie- en adviesbevoegdheden. Bovendien regelt de AVG de samenwerking tussen de toezichthoudende autoriteiten in de Europese Unie zodat bevoegdheden in zaken met een grensoverschrijdend karakter effectief kunnen worden

⁹¹ Art. 30 lid 5 AVG.

⁹² Art. 30 lid 1 AVG.

⁹³ H. de Vries & M. Goudsmit, 'Voorsorteren op de Algemene Verordening Gegevensbescherming. Twee stappen vooruit, één stap terug.', *Nederlands Juristenblad* 2016/1077.

⁹⁴ Art. 30 lid 4 AVG.

⁹⁵ Art. 8 lid 3 Handvest en art. 16 lid 2 VWEU.

⁹⁶ Art. 51 AVG.

⁹⁷ Art. 28 EU-privacyrichtlijn.

⁹⁸ Art. 51 Wbp.

⁹⁹ Art. 57 en 58 AVG.

toegepast. In zulke zaken is de primaire bevoegdheid van de toezichthoudende autoriteit van de lidstaat waar de hoofdvestiging van de verwerkingsverantwoordelijke is gevestigd. Voor organisaties/instellingen heeft dat het voordeel dat zij in beginsel met één toezichthoudende autoriteit te maken hebben.¹⁰⁰ Betrokkenen kunnen zich intussen toch tot hun eigen toezichthoudende autoriteit blijven richten, om te voorkomen dat taal- en communicatieproblemen de uitoefening van grondrechten ongunstig beïnvloeden. Om die uitgangspunten met elkaar te conciliëren, voorziet de AVG in een ingewikkeld samenwerkingsmechanisme. Het Europees Comité voor gegevensbescherming¹⁰¹ kan eventuele competentiegeschillen bindend beslechten.

3.8 Sancties

Overtreding van de normen van de AVG wordt primair gesanctioneerd met een administratieve geldboete. De boetemaxima zijn zeer hoog. Het hoogste maximum is twintig miljoen euro of, indien dit meer is, vier procent van de wereldwijde jaaromzet in het voorafgaande boekjaar. Voor inbreuken die niet aan administratieve geldboeten zijn onderworpen, is er een mogelijkheid voor de lidstaten om zelf regels inzake andere sancties vast te stellen.¹⁰²

Om kort te zijn, zijn er twee boetecategorieën: boetes van ten hoogste tien miljoen euro of twee procent van de wereldwijde omzet van de verwerkingsverantwoordelijke of verwerker¹⁰³ en boetes van ten hoogste twintig miljoen euro of vier procent van de wereldwijde omzet¹⁰⁴.

Onder de eerste boetecategorie (tien miljoen of twee procent van omzet) vallen onder andere overtredingen van de informatieverplichtingen en verplichtingen om te voldoen aan inzage- en verbeteringsrechten, en het recht op vergetelheid, alsmede verplichting om zorg te dragen voor 'gegevensbescherming door ontwerp en door standaardinstellingen'. Onder de tweede boetecategorie (twintig miljoen of vier procent van omzet) vallen verder overtredingen van de verplichting om persoonsgegevens alleen te verwerken conform de zogenaamde gegevensverwerkingsbeginselen, zoals met betrekking tot zorgvuldigheid en behoorlijkheid, transparantie, doelbinding en gegevensminimalisatie, op basis van een toereikende verwerkingsgrondslag, alsook de verplichtingen om inzage- en andere rechten van betrokkenen te respecteren en verplichtingen met betrekking tot internationale gegevensdoorgiften etc.¹⁰⁵

¹⁰⁰ Art. 56 AVG.

¹⁰¹ Art. 68 AVG.

¹⁰² Art. 84 AVG.

¹⁰³ Art. 83 lid 4 AVG.

¹⁰⁴ Art. 83 lid 5 AVG.

¹⁰⁵ G-J Zwenne & L. Mommers, 'De tien belangrijkste veranderingen die de algemene verordening gegevensbescherming gaat brengen (in minder dan vijftienduizend woorden)', *Tijdschrift voor Compliance* 2016/4, p. 182-189.

4 Privacy in de praktijk van Amarant Groep

Dit hoofdstuk bevat een analyse van het privacybeleid van Amarant Groep. De analyse omvat de (beleids)regelingen van Amarant Groep die betrekking hebben op de verwerking van persoonsgegevens van cliënten. Daarnaast wordt in dit hoofdstuk het beleid getoetst aan de Europese verordening, de toekomstige privacywetgeving.

4.1 Sectorspecifieke wetten

Amarant Groep is een zorginstelling en heeft te maken met sectorspecifieke wetten. Het is daarom belangrijk om te weten dat sommige wetten blijven gelden waaronder de Wet op de geneeskundige behandelingsovereenkomst (hierna: WGBO) en de Wet bijzondere opnemingen in psychiatrische ziekenhuizen (hierna: Bopz).¹⁰⁶ De regels van de AVG brengen dus geen veranderingen met zich mee voor bijvoorbeeld het medisch beroepsgeheim.¹⁰⁷ De bestaande regels over privacy worden door de AVG bevestigd en op onderdelen versterkt.

4.2 Verwerkingsstappen in vogelvlucht

Zoals eerder is vermeld, verwerkt Amarant Groep verschillende categorieën van persoonsgegevens. Voorbeelden van in welke stappen in de verwerkingsprocessen deze persoonsgegevens voorkomen, zijn¹⁰⁸:

Stap	Uitleg
1. Inschrijving van nieuwe cliënten bij het Klantenbureau van Amarant Groep;	denk aan persoonsgegevens die worden opgenomen zoals naam, adres, woonplaats (NAW) en telefoonnummer, e-mailadres etc. (contactgegevens)
2. Opvragen van (aanvullende) verslagen;	bijvoorbeeld bij de verwijzer
3. Doorsturen van het dossier naar de potentiële passende behandelaar/plaats binnen Amarant Groep;	behandelaar ziet dossier in en doet intake
4. Opmaken van zorgplannen;	
5. Bewaren en beschikbaar maken van cliëntgegevens in digitale vorm;	in de zogenaamde softwaretoepassing PC2
6. Overdracht naar andere zorgverleners;	denk aan (bijzondere categorieën van) persoonsgegevens die worden doorgegeven aan andere zorgverleners buiten Amarant Groep
7. Het op de hoogte houden van andere zorgverleners buiten Amarant Groep, zoals huisartsen, van de situatie van de cliënt nadat de cliënt wordt opgenomen bij Amarant Groep of in ieder geval een 'cliënt' wordt van Amarant Groep.	

Omdat Amarant Groep onder andere met gevoelige persoonsgegevens omgaat, is het van belang dat dit op zorgvuldige wijze gebeurt. Om de privacy van de cliënten te beschermen, zijn er bij Amarant Groep verschillende regelingen van kracht. Deze regelingen waarborgen de privacy. Binnen Amarant Groep wordt er zeker aandacht besteed aan het onderwerp informatieveiligheid.

¹⁰⁶ www.nvz-ziekenhuizen.nl (zoek op *bopz*, klik op *privacy*).

¹⁰⁷ www.autoriteitpersoonsgegevens.nl (zoek op *zorgaanbieders*).

¹⁰⁸ Interview 1 (bijlage 1).

4.3 Kwaliteitshandboek

Bij Amarant Groep wordt een kwaliteitshandboek gebruikt, met als doel de kwaliteit van juiste zorg te waarborgen, maar ook voor een adequate bedrijfsvoering. Het handboek bevat alle schriftelijke regelingen van Amarant Groep waar zij dagelijks mee te maken heeft. Te denken valt aan overeenkomsten, standaardbedingen, reglementen, handreikingen, richtlijnen, gedragscodes, protocollen, procedures, voorschriften, werkinstructies en handleidingen. Hierna worden in de komende paragrafen de meest relevante regelingen besproken die betrekking hebben op privacy.

4.4 Algemene voorwaarden

Amarant Groep hanteert algemene voorwaarden.¹⁰⁹ Deze algemene voorwaarden vormen de basis voor het totstandkomen van een overeenkomst en geven aan wat de cliënt en zorginstelling bij de uitvoering daarvan mogen verwachten. De algemene voorwaarden van Amarant Groep behoren bij alle zorg- en dienstverleningsovereenkomsten van Amarant Groep.¹¹⁰ Zij vormen een onlosmakelijk geheel met de zorg- en dienstverleningsovereenkomst (afgekort: ZDO) en/of geneeskundige behandelingsovereenkomst die met de cliënt wordt gesloten. Daarom worden zij ook uitgereikt aan nieuwe cliënten zodat zij een beeld krijgen van de zorg en alles daaromheen. De algemene voorwaarden zijn ook publiek toegankelijk: te raadplegen via de website van Amarant Groep. In de algemene voorwaarden staat bovendien dat bij het aangaan van de overeenkomst aan de cliënt (schriftelijke) informatie verstrekt moet worden over privacyregelingen.¹¹¹

4.4.1 Privacy en recht op inzage

Het beleid met betrekking tot de privacy van cliënten heeft ook een eigen plek gekregen in de algemene voorwaarden zelf¹¹²:

7. Privacy en Recht op inzage

7.1. De cliënt/vertegenwoordiger heeft recht op inzage in zijn gegevens, evenals het recht op afschrift, aanvulling, correctie, afscherming, vernietiging en verwijdering van zijn gegevens in overeenstemming met de Wet bescherming persoonsgegevens en, voor zover van toepassing, de WGBO, en voor zover dit niet in strijd is met de bescherming van de persoonlijke levenssfeer van een ander.

7.2. Op verzoek van de cliënt verstrekt de Amarant Groep binnen redelijke tijd inzage in en/of afschrift van het dossier.

7.3. De Amarant Groep kan de cliënt/vertegenwoordiger een vergoeding in rekening brengen ter hoogte van maximaal het tarief zoals bepaald in het Besluit Kostenvergoeding rechten betrokkene Wet bescherming persoonsgegevens.

7.4. Op verzoek van de cliënt voegt de Amarant Groep een door de cliënt/vertegenwoordiger afgegeven verklaring met betrekking tot de in het dossier opgenomen stukken aan het dossier toe.

7.5. Een verzoek van de cliënt/vertegenwoordiger tot vernietiging van het dossier moet schriftelijk worden ingediend bij de Amarant Groep. Vernietiging vindt plaats onder de wettelijke voorwaarden. Het verzoek tot vernietiging binnen de wettelijke termijn van bewaring wordt niet uitgevoerd.

7.6. Van de cliënt zullen geen opnamen worden gemaakt ten behoeve van publicatie via gedrukte of audiovisuele media zonder schriftelijke toestemming van de cliënt/vertegenwoordiger. De cliënt is gerechtigd tot een redelijke tijd vóór de publicatie de toestemming in te trekken. De Amarant Groep maakt hierover afspraken met de instantie die de informatie vraagt of de opnamen maakt en zorgt ervoor dat de cliënt/vertegenwoordiger tijdig verneemt op welk moment publicatie zal plaatsvinden.

Zoals genoemd in de algemene voorwaarden hierboven en zoals vermeld in paragraaf 4.1 van dit onderzoeksrapport, is ook de WGBO van toepassing wat betreft de rechten van de

¹⁰⁹ Algemene voorwaarden Amarant Groep. Behorend bij de zorg- en dienstverleningsovereenkomsten van Amarant, Idris, Pauwer, Expertisecentrum Autisme, allen onderdeel van de Amarant Groep (hierna in de voetnoten: Algemene voorwaarden).

Te raadplegen via: www.amarantgroep.nl (klik onderaan op: *algemene voorwaarden*).

¹¹⁰ Zie bijlage 2 voor een voorbeeld van een overeenkomst die Idris, onderdeel van Amarant Groep, hanteert: Zorg- en dienstverleningsovereenkomst Idris.

¹¹¹ Art. 4.3 Algemene voorwaarden.

¹¹² Art. 7 Algemene voorwaarden.

cliënt. De komst van de AVG verandert hier niets aan. Per 25 mei 2018 vervalt de Wbp en de Wbp in de algemene voorwaarden moet daarom vervangen worden door de AVG. Daarbij krijgen sommige rechten een andere benaming. Recht op afscherming heeft met de komst van de AVG een zelfstandige positie gekregen in de vorm van een recht op beperking en voor aanvulling en correctie wordt rectificatie gebruikt. Het toevoegen van een verklaring van de cliënt als de cliënt daar om vraagt, vloeit naast de AVG ook voort uit de WGBO.¹¹³ Zie paragraaf 3.5 e.v. van dit onderzoeksrapport voor deze rechten van de cliënt.

Bovendien mag Amarant Groep volgens de AVG, de WGBO en het Burgerlijk Wetboek (hierna: BW) nog steeds een redelijke vergoeding in rekening brengen wanneer de cliënt om inzage/afschrift vraagt. De AVG zegt echter nu dat dat mag als er sprake is van 'bijkomende kopieën'¹¹⁴: *de verwerkingsverantwoordelijke verstrekt de betrokkene een kopie van de persoonsgegevens die worden verwerkt. Indien de betrokkene om bijkomende kopieën verzoekt, kan de verwerkingsverantwoordelijke op basis van de administratieve kosten een redelijke vergoeding aanrekenen. Wanneer de betrokkene zijn verzoek elektronisch indient, en niet om een andere regeling verzoekt, wordt de informatie in een gangbare elektronische vorm verstrekt.*

Tot slot wordt er in de algemene voorwaarden gesproken over 'opnamen'. Er worden van de cliënt geen opnamen gemaakt ten behoeve van publicatie. Voor onderzoeksdoeleinden worden echter wel opnamen gemaakt. Beeldopnamen van cliënten voor onderzoeksdoeleinden maken het onderzoeksproces steeds eenvoudiger en goedkoper. Daar registratie echter een aanzienlijke inbreuk is op de persoonlijke levenssfeer van eenieder die in het beeld verschijnt, dient aan een aantal randvoorwaarden te worden voldaan alvorens de registratie van beeld wordt ingezet. Deze zorgvuldigheid moet in acht worden genomen om te voldoen aan wet- en regelgeving en heeft ook het voorkomen van misbruik tot doel. Amarant Groep volgt hiervoor een speciale procedure waarin ook toestemmingsverklaringen van de behandelaar en van de wettelijk vertegenwoordiger van de cliënt nodig zijn.¹¹⁵ Tevens kan er foto- en videomateriaal van de cliënt gebruikt worden voor communicatiedoeleinden van Amarant Groep. Bij communicatiedoeleinden kan gedacht worden aan nieuwsbrieven, intranet, websites, social media, folders en het personeelsblad. Hiervoor maakt Amarant Groep gebruik van een toestemmingsformulier.¹¹⁶

4.4.2 Dossier

Voor een goede hulpverlening is het bijhouden van een dossier onmisbaar. Amarant Groep houdt voor iedere cliënt een dossier bij. Daarom zijn er in de algemene voorwaarden regels opgenomen omtrent het dossier van de cliënt¹¹⁷:

6. Dossier

6.1. De Amarant Groep houdt van de cliënt een dossier bij en neemt hierin de gegevens op die nodig zijn voor het verlenen van de behandeling en/of zorg.

6.2. Voor zover van toepassing: het persoonlijk plan maakt deel uit van dit dossier.

6.3. Het medisch dossier is een apart dossier dat berust bij de AVG-artsen. Het medisch dossier is onderworpen aan de regels van de WGBO.

6.4. De dossiers zijn eigendom van de Amarant Groep.

6.5. De Amarant Groep gaat zorgvuldig om met de gegevens van de cliënt. Dit gebeurt conform de Wet bescherming persoonsgegevens (WBP) en, voor zover van toepassing, de Wet op de Geneeskundige Behandelovereenkomst (WGBO) en/of de Wet Bijzondere Opnemingen in Psychiatrische Ziekenhuizen (Wet BOPZ).

6.6. De bepalingen uit het privacyreglement van de Amarant Groep zijn op het dossier van toepassing.

6.7. De Amarant Groep verschaft, in overeenstemming met de privacywetgeving, derden geen inzage in het dossier zonder toestemming van de cliënt/vertegenwoordiger, dit met inachtneming van artikel 7.

¹¹³ Art. 16 AVG en art. 7:454 lid 2 Burgerlijk Wetboek.

¹¹⁴ Art. 12 lid 5 sub a jo. art. 15 lid 3 AVG jo. art. 7:456 jo. 7:403 BW.

¹¹⁵ Zie bijlage 3: Procedure en randvoorwaarden gerichte videoregistratie cliëntenopnames.

¹¹⁶ Zie bijlage 4: Toestemmingsformulier foto- en videomateriaal cliënten.

¹¹⁷ Art. 6 Algemene voorwaarden.

Deze toestemming is niet vereist voor degenen die rechtstreeks zijn betrokken bij de zorg- en dienstverlening, noch in de situatie waarin de wet dat voorschrijft zoals bij rechtmatigheids- en/of kwaliteitscontroles en controles door het Zorgkantoor respectievelijk de Zorgverzekeraar.

6.8. De Amarant Groep bewaart het dossier in beginsel 15 (vijftien) jaar na beëindiging van de zorg respectievelijk behandeling, tenzij de cliënt eerder om vernietiging vraagt. Gegevens waarvan redelijkerwijs aannemelijk is dat de bewaring van aanmerkelijk belang is voor een ander dan de cliënt kunnen van vernietiging worden uitgesloten.

Nota bene de 'AVG' in het woord AVG-artsen zoals genoemd in de algemene voorwaarden staat voor: arts voor verstandelijk gehandicapten.

De algemene voorwaarden geven aan conform de Wbp te werken als het gaat om dossiers. Met komst van de AVG vervalt de Wbp en moet die dus in de algemene voorwaarden worden vervangen.

Het bijhouden van een dossier zoals vermeld in de algemene voorwaarden is een verplichting op grond van de WGBO en de Bopz.¹¹⁸ Dat heeft te maken met een goede hulpverlening. De AVG verandert hier niets aan.

Volgens de algemene voorwaarden is een toestemming van de cliënt niet vereist voor het verschaffen van inzage in het dossier aan degenen die rechtstreeks betrokken zijn bij de zorg- en dienstverlening. Dat is zo geregeld in de WGBO. Ook op dit gebied verandert de AVG niets.¹¹⁹

Zoals hiervoor omschreven, schrijven de algemene voorwaarden van Amarant Groep voor dat de bepalingen uit het privacyreglement van Amarant Groep op het dossier van toepassing zijn -het bijhouden van een dossier betekent immers verwerking van persoonsgegevens-. Dat de algemene voorwaarden dat privacyreglement van toepassing verklaren, is de eerste reden waarom dat privacyreglement zo belangrijk is. Hierna is er in de algemene voorwaarden iets opgenomen over de bewaartermijn: de bewaartermijn voor dossiers is in beginsel vijftien jaar. De tweede reden waarom het privacyreglement zo belangrijk is, is dat óók die richtsnoeren omtrent de bewaartermijn nader worden toegelicht in het privacyreglement. Het privacyreglement komt daarom aan de orde in paragraaf 4.5 e.v. van dit onderzoeksrapport.

Tevens beschikt Amarant Groep over een reglement cliëntdossier. De bepalingen in de algemene voorwaarden over het dossier worden in dit reglement nader uitgewerkt. Reglement cliëntdossier wordt besproken in paragraaf 4.6 van dit onderzoeksrapport. Ten slotte vermelden de algemene voorwaarden dat het persoonlijk plan deel uitmaakt van het dossier. Wat dat precies is en welke gegevens een dergelijk plan bevat, wordt beschreven in de volgende paragraaf.

4.4.3 Persoonlijk plan en behandelplan

Zoals eerder toegelicht in de vorige paragraaf hebben de cliënten van Amarant Groep ieder een dossier. Bij medische zorgverlening hebben ze echter een medisch dossier. Dat is een apart dossier.¹²⁰ Daarom zijn er ook verschillen tussen de bijbehorende plannen, een persoonlijk plan en een behandelplan. Hieronder leest men wat deze plannen bevatten.

Persoonlijk plan

Een persoonlijk plan is een schriftelijke vaststelling van de ondersteuningsvraag van de cliënt. Dit gebeurt nadat de ZDO is gesloten, maar voorafgaand aan de start van de zorg- en dienstverlening respectievelijk de behandeling. Door in te stemmen met het persoonlijk plan geeft de cliënt/vertegenwoordiger toestemming voor de uitvoering van alle handelingen die deel uitmaken van het persoonlijk plan. Dus daarmee ook voor het

¹¹⁸ Art. 7:454 lid 1 BW en art. 56 Bopz.

¹¹⁹ Art. 7:457 lid 2 BW jo. art. 9 lid 2 sub a jo. sub h jo. lid 3 AVG.

¹²⁰ Art. 6.3 Algemene voorwaarden.

verwerken van de persoonsgegevens die daarvoor nodig zijn.¹²¹ Hieronder staan de gegevens die in een persoonlijk plan worden opgenomen¹²²:

18. Gegevens persoonlijk plan

Het persoonlijk plan omvat in ieder geval de volgende gegevens:

- a. personalia van de cliënt;*
- b. beschrijving van de zorgvraag;*
- c. doelstellingen van de zorg- en dienstverlening en/of behandeling en afspraken over de uitvoering daarvan;*
- d. plaats waar de zorg- en dienstverlening en/of behandeling wordt gegeven;*
- e. eventueel toegestaan gebruik van Middelen en Maatregelen als bedoeld in de Wet Bijzondere Opnemingen Psychiatrische Ziekenhuizen (BOPZ) die de vrijheid van de cliënt (kunnen) beperken;*
- f. namen van contactpersonen binnen en buiten de instelling van de Amarant Groep.*

Behandelplan

Een behandelplan is een plan dat hoort bij de behandelingsovereenkomst en dus bij het medisch dossier. Door in te stemmen met het behandelplan geeft de cliënt/vertegenwoordiger toestemming voor alle verrichtingen die deel uitmaken van het behandelplan ter uitvoering van de behandelingsovereenkomst. Dus daarmee ook voor het verwerken van de persoonsgegevens die daarvoor nodig zijn.¹²³ Het behandelplan is net zoals het persoonlijk plan opgenomen in de algemene voorwaarden van Amarant Groep¹²⁴:

27. Behandelplan

27.1. De arts legt de overeengekomen behandeling vast in een behandelplan. Het behandelplan en eventuele bijstelling daarvan wordt besproken met de cliënt/vertegenwoordiger en opgenomen in het medisch dossier.

27.2. De arts vergewist zich er van dat hij over alle voor de behandeling relevante informatie beschikt.

De cliënt heeft naast het feit dat hij/zij contact heeft met de arts, ook vaak contact met een andere verantwoordelijke zorgverlener (de cliënt wordt behandeld/begeleid door een multidisciplinair team, bestaande uit: arts/psychiater, (GZ-)psycholoog of orthopedagoog, soms paramedici, begeleiders van wonen en dagbesteding)¹²⁵:

28. Behandelspecifieke informatie

28.1 De verantwoordelijke zorgverlener zorgt ervoor dat de cliënt op de geëigende momenten in ieder geval informatie krijgt over:

- a. de diagnose;*
- b. de aard en inhoud van de voorgestelde behandeling;*
- c. de gevolgen, risico's en beoogde resultaten van de voorgestelde behandeling;*
- d. de in aanmerking komende alternatieven;*
- e. de door de cliënt voorafgaand aan dan wel na de behandeling in acht te nemen instructies of leefregels, waaronder begrepen de instructies voor begeleiding, opvang en vervoer;*
- en indien de omstandigheden daartoe aanleiding geven, dan wel op verzoek van de cliënt:*
- f. eventuele tussentijdse momenten van evaluatie;*
- g. de wachttijd voor de behandeling;*
- h. de mogelijkheid van een second opinion.*

28.2 De in het eerste lid bedoelde informatie wordt gegeven op een zodanig moment dat de cliënt in de gelegenheid is een weloverwogen besluit te nemen.

De cliënt krijgt bovenstaande informatie dus van de arts en/of van een andere verantwoordelijke zorgverlener. Zoals eerder in paragraaf 4.4.2 van dit onderzoeksrapport vermeld, heeft deze verantwoordelijke hulpverlener geen toestemming nodig van de cliënt/vertegenwoordiger om op de hoogte te kunnen zijn van de situatie van de cliënt of om inzage te kunnen hebben in het dossier omdat hij/zij rechtstreeks betrokken is bij de overeengekomen zorg- en dienstverlening.

¹²¹ Art. 17.6 Algemene voorwaarden jo. art. 6 lid 1 sub b jo. art. 9 lid 2 sub a jo. art. 7 jo. art. 9 lid 2 sub h AVG.

¹²² Art. 18 Algemene voorwaarden.

¹²³ Art. 7:450 lid 1 jo. 7:451 BW jo. art. 6 lid 1 sub b jo. art. 9 lid 2 sub a jo. art. 7 jo. art. 9 lid 2 sub h AVG.

¹²⁴ Art. 27 Algemene voorwaarden.

¹²⁵ Art. 28 Algemene voorwaarden.

4.4.4 Samenwerking en coördinatie

Amarant Groep werkt vaak samen met derden waardoor er persoonsgegevens gedeeld moeten worden. Het beleid met betrekking tot de samenwerking en coördinatie in de keten van behandeling en/of zorg heeft daarom ook een plaats gekregen in de algemene voorwaarden¹²⁶:

8. Samenwerking en coördinatie in de keten van behandeling en/of zorg

8.1. De Amarant Groep werkt samen met andere zorgaanbieder en instanties onder meer met betrekking tot de hulpverlening aan cliënten ten behoeve van een goede coördinatie van de behandeling en/of de zorg- en dienstverlening.

8.2. Voor zover de Amarant Groep dat noodzakelijk acht voor een goede uitoefening van de zorg- en dienstverlening of (vervolg)behandeling door derden, waaronder begrepen de huisarts, andere externe hulpverleners of verwijzers, kunnen ook die derden door de Amarant Groep op de hoogte worden gesteld van de relevante gegevens uit het dossier mits zij betrokken zijn bij de zorg- en dienstverlening en/of behandeling voor de cliënt. Een en ander geldt slechts voor zover de cliënt/vertegenwoordiger daarentegen geen nadrukkelijk bezwaar heeft, welk bezwaar bij voorkeur schriftelijk door de cliënt/vertegenwoordiger dient te worden gemaakt.

8.3. De Amarant Groep participeert in het Convenant Signaleringsstelsel Zorg voor Jeugd in de onderscheiden regio's in Noord-Brabant.

8.4. De Amarant Groep registreert alle (minderjarige) zorgvragers (tot 23 jaar) in het signaleringssysteem "Zorg voor Jeugd". Door ondertekening van de ZDO verleent de cliënt dan wel de vertegenwoordiger van de cliënt toestemming voor de (standaard)registratie in dit systeem.

Indien en voor zover de Amarant Groep daarna overweegt een signaal af te geven (melding te doen over een zorgwekkende situatie) over een cliënt conform de eisen en voorwaarden van het desbetreffend registratiesysteem, zal de Amarant Groep dit vooraf kenbaar maken aan de cliënt en zijn/haar vertegenwoordiger. Informatie over dit systeem staat in brochure "signaleringsstelsel Zorg voor Jeugd".

8.5. Indien de Amarant Groep deelneemt c.q. gaat deelnemen aan andere signaleringssystemen waarin zij de cliënt wil registreren, zal zij tevoren de cliënt respectievelijk diens vertegenwoordiger op de hoogte stellen.

In de algemene voorwaarden is opgenomen dat Amarant Groep vaak gegevens moet opvragen bij derden als dat de zorg van haar cliënten ten goede kan komen. Ook krijgt Amarant Groep vaak verzoeken van derden om informatie te verstrekken over cliënten. Dat zijn derden zoals de gemeente, de huisarts, de school, het ziekenhuis, de kliniek/praktijk/behandelaar, de verzekeraar, maatschappelijke instellingen, de politie, de niet gezaghebbende ouder, familie of naasten.¹²⁷ Door de cliënt wordt een akkoordverklaring getekend bij aanvang van de zorg- en dienstverlening en/of behandeling bij Amarant Groep om gegevens te kunnen opvragen en verstrekken. Die verklaring is in de vorm van een formulier, afkomstig van het Klantenbureau van Amarant Groep.¹²⁸ Daarnaast is er een apart toestemmingsformulier dat Idris, onderdeel van Amarant Groep, hanteert in crisisgevallen -gegevens zijn dan noodzakelijk voor de uitvoering van het psychologische- dan wel psychodiagnostische onderzoek-.¹²⁹ In deze toestemmingsverklaring geeft de cliënt toestemming aan Amarant Groep om zijn of haar persoonsgegevens te mogen delen met bepaalde derden. Delen betekent verstrekken en/of opvragen van relevante informatie dan wel een gesprek met derden en de cliënt kan in het formulier van de toestemmingsverklaring kiezen welke derden precies. Als de cliënt nadrukkelijk (schriftelijk) bezwaar heeft gemaakt, blijft het delen van persoonsgegevens achterwege. Overigens dient de behandelaar van Amarant Groep continu een afweging te maken tussen het medisch beroepsgeheim/geheimhouding en het nut van het delen van de gegevens. Van Amarant Groep wordt verwacht dat zij zorgvuldig omgaat met het delen van de persoonsgegevens van cliënten. Sommige derden vragen namelijk naar (zeer) privacygevoelige informatie.

¹²⁶ Art. 8 Algemene voorwaarden.

¹²⁷ Interview 1 (bijlage 1).

¹²⁸ Zie bijlage 5 voor een voorbeeld een akkoordverklaring die het Klantenbureau van Amarant Groep hanteert: Akkoordverklaring verstrekken gegevens.

¹²⁹ Zie bijlage 6 voor een voorbeeld een toestemmingsverklaring die Idris, onderdeel van Amarant Groep, hanteert: Toestemmingsverklaring opvragen gegevens dan wel een gesprek met derden.

Tevens heeft het geven van inlichtingen over de cliënt dan wel inzage in of afschrift van het dossier van de cliënt aan derden, op basis van een toestemming van de cliënt, ook een grondslag in de WGBO.¹³⁰

Ten slotte is het belangrijk om te realiseren dat het gebruik van één standaard toestemmingsformulier voor Amarant Groep in haar geheel/voor alle onderdelen van Amarant Groep om persoonsgegevens te mogen delen, niet reëel is, want buiten de AVG wordt in elke (toepasselijke) wet iets vermeld over het onderwerp 'toestemming'. Dat betekent dat er telkens verschillen zijn in waarvoor de toestemming wordt gevraagd en op welk moment. Daardoor moet eerst gekeken worden naar wat die toepasselijke, specifieke wetten voorschrijven over de 'toestemming' voordat er gekeken wordt naar wat de AVG voorschrijft over dit onderwerp. Bovendien heeft Amarant Groep vaak als grondslag voor het verwerken/delen: *uitvoering van een overeenkomst of verstrekken van gezondheidszorg* en dus niet zo gauw de grondslag *toestemming*. Daarom is in meeste gevallen geen (aparte) toestemming nodig voor het verwerken, in het bijzonder voor het delen, van persoonsgegevens.¹³¹

4.5 Reglement verwerking persoonsgegevens

Amarant Groep heeft een privacyreglement opgesteld.¹³² Het reglement verwerking persoonsgegevens is publiek niet toegankelijk. Amarant Groep stelt dit reglement intern beschikbaar via intranet. Met dit type beleidsregeling wil Amarant Groep een praktische en toegankelijke uitwerking geven van de bepalingen voor zorgverlener en cliënt op grond van de nu nog geldende privacyregels zoals die voortvloeien uit de Wbp en sectorspecifieke wetten. Na de komst van de AVG zal zij dat moeten doen zoals die voortvloeien uit de AVG en de sectorspecifieke wetten. Overigens voldoet dit reglement al gedeeltelijk aan de AVG. Het reglement ziet toe op papieren en elektronische verwerking van persoonsgegevens van cliënten die onder behandeling zijn bij Amarant Groep.

Bij dit reglement hoort een handreiking bescherming persoonsgegevens cliënten.¹³³ Deze is ook niet publiek toegankelijk, maar wel intern beschikbaar via intranet. Deze handreiking is gemaakt om een vereenvoudigde en informele weergave van de geldende privacywetgeving en het privacyreglement te geven. Het is slechts een hulpmiddel en geen juridisch document. Aan deze handreiking kunnen daarom -dat staat vermeld in de handreiking- geen rechten worden ontleend. Dit kan natuurlijk wel aan de wet- en regelgeving en de uitwerking hiervan in het reglement verwerking persoonsgegevens.

4.5.1 Bewerkingsovereenkomst

Amarant Groep maakt gebruik van bewerkersovereenkomsten oftewel bewerkingsovereenkomsten (lees laatste lid)¹³⁴:

5.2 Voorwaarden voor rechtmatige verwerking van persoonsgegevens

Deze voorwaarden zijn zowel de waarborg aan degene van wie de (bijzondere) persoonsgegevens worden verwerkt als ook de opdracht aan de eigen organisatie, medewerkers en gebruikers om zorg te dragen voor rechtmatige en zorgvuldige verwerking.

1. Amarant Groep verwerkt de persoonsgegevens op behoorlijke en zorgvuldige wijze en in overeenstemming met dit reglement en de wet en is verantwoordelijk voor het naleven van dit reglement;
2. Amarant Groep verwerkt slechts persoonsgegevens indien aan een van de onder 5.1 genoemde wettelijke grondslagen is voldaan en met als doel het verantwoord uitvoeren van de doelstellingen van Amarant Groep zoals genoemd onder 4. Persoonsgegevens worden niet verder verwerkt op een wijze die onverenigbaar is met de doeleinden waarvoor ze zijn verkregen;
3. Persoonsgegevens worden slechts verwerkt voor zover zij, gelet op de doeleinden waarvoor zij worden verzameld of vervolgens worden verwerkt, toereikend, ter zake dienend en niet bovenmatig zijn en voldoen aan de eisen van proportionaliteit en subsidiariteit;

¹³⁰ Art. 7:457 lid 1 BW jo. art. 6 lid 1 sub a jo. art. 9 lid 2 sub a jo. art. 7 AVG.

¹³¹ Interview 2 (bijlage 7).

¹³² Zie bijlage 8: Reglement verwerking persoonsgegevens.

¹³³ Zie bijlage 9: Handreiking bescherming persoonsgegevens cliënten (hierna in de voetnoten: handreiking).

¹³⁴ Art. 5.2 Reglement verwerking persoonsgegevens (bijlage 8) jo. 28 lid 3 AVG.

4. Amarant Groep is verantwoordelijk voor het procesmatig, organisatorisch en technisch goed functioneren van de verwerkingen van persoonsgegevens.

5. Wanneer (delen van) verwerkingen zijn gedelegeerd naar een bewerker, verplicht de Amarant Groep de bewerker dit reglement na te leven. De taken, rechten en verplichtingen van de bewerker zijn schriftelijk vastgelegd in de bewerkersovereenkomst van Amarant Groep. De bewerkersovereenkomst is bij verantwoordelijke op te vragen/in te zien via de leidinggevende.

Er is gekeken naar de bewerkersovereenkomst die Amarant Groep standaard hanteert.¹³⁵ Deze is getoetst aan de eisen die de AVG stelt.¹³⁶ Zie voor de eisen van de AVG paragraaf 3.6.5 van dit onderzoeksrapport.

In de overeenkomst zijn een aantal punten uit de AVG geregeld, waaronder: *de aard en het doel van de verwerking en het soort persoonsgegevens en de categorieën van betrokkenen*¹³⁷. De duur en beëindiging van de bewerkersovereenkomst zelf is geregeld¹³⁸, maar de bewerkersovereenkomst bevat geen informatie over *het onderwerp en de duur van de verwerkingen*. De overeenkomst beschrijft verplichtingen van de verwerker¹³⁹, maar een opsomming van *de rechten en verplichtingen van de verwerkingsverantwoordelijke* is nagelaten. Met ingang van de AVG is dit een aandachtspunt voor Amarant Groep. Verder zijn de onderwerpen 'teruggave van persoonsgegevens', 'geheimhouding' en 'incidentmanagement, datalekken en informatieplichten' uitgebreid beschreven¹⁴⁰. Tot slot dient de verwerker, volgens de AVG, aan de verwerkingsverantwoordelijke alle informatie ter beschikking te stellen die nodig is om de nakoming van de verplichtingen aan te tonen (bijv. audits). Informatie omtrent 'beveiliging en controle' is ook opgenomen in deze overeenkomst: wat, wanneer en hoe de verwerker iets moet aantonen, is uitvoerig beschreven.¹⁴¹

In de bewerkersovereenkomst wordt verwezen naar de Wbp. Na de komst van de AVG zal dit moeten worden veranderd. Ook de termen afkomstig uit de Wbp die gebruikt worden in deze overeenkomst en dit privacyreglement, waaronder 'bewerker', moeten worden veranderd naar de termen van de AVG.

Overigens wordt deze bewerkersovereenkomst binnenkort vervangen door een nog specifiekere op de zorgsector en de AVG afgestemde versie.¹⁴²

4.5.2 Informatieveiligheid

Binnen Amarant Groep wordt er zeker aandacht besteed aan het onderwerp informatieveiligheid. In de vorige paragraaf is naar voren gekomen dat (lees ener laatste lid van het reglementsartikel): Amarant Groep verantwoordelijk is voor het procesmatig, organisatorisch en technisch goed functioneren van de verwerkingen van persoonsgegevens. Dat is conform de Wbp en de AVG.¹⁴³ Deze verplichting is nader uitgewerkt in het volgende artikel van het privacyreglement¹⁴⁴:

7 Bewaren van gegevens

7.1 Organisatie, beheer en beveiliging

1. Alle door of namens de verantwoordelijke gevoerde verwerkingen en registraties vallen onder dit reglement.
2. De verantwoordelijke is eindverantwoordelijk voor de naleving van de wet en de bepalingen van dit reglement en voor de juistheid en de volledigheid van de opgenomen gegevens.
3. De gegevens worden alleen verwerkt door personen die uit hoofde van ambt, beroep of wettelijk voorschrift, dan wel krachtens een overeenkomst tot geheimhouding zijn verplicht.

¹³⁵ Zie bijlage 10: Concept bewerkersovereenkomst.

¹³⁶ Art. 28 lid 3 en lid 4 AVG.

¹³⁷ Zie onder 3 in het Concept bewerkersovereenkomst (bijlage 10).

¹³⁸ Zie onder 4 in het Concept bewerkersovereenkomst (bijlage 10).

¹³⁹ Zie onder 5 in het Concept bewerkersovereenkomst (bijlage 10).

¹⁴⁰ Zie onder 7, 8 en 10 in het Concept bewerkersovereenkomst (bijlage 10).

¹⁴¹ Zie onder 9 in het Concept bewerkersovereenkomst (bijlage 10).

¹⁴² Interview 2 (bijlage 7).

¹⁴³ Art. 13 Wbp en art. 5 lid 1 sub f jo. lid 2 AVG.

¹⁴⁴ Art. 7.1 Reglement verwerking persoonsgegevens (bijlage 8).

4. De verantwoordelijke draagt zorg voor de nodige voorzieningen van fysieke, technische en organisatorische aard ter beveiliging van de verwerkingen en registraties tegen verlies of aantasting van de gegevens en tegen onbevoegde kennisneming, wijziging of verstrekking daarvan alsook de hierbij behorende procedures voor het signaleren en melden van doorbreken van beveiliging en datalekken. Gelijke plicht rust op de beheerder die voor of namens de verantwoordelijke beheer voert voor het geheel of het gedeelte van de verwerking (of de apparatuur waarmee de verwerking wordt gevoerd) die hij onder zich heeft.

5. Door of namens de verantwoordelijke wordt bepaald wie de gebruiker is. De gebruiker is verantwoordelijk voor de naleving van de bepalingen van dit reglement voor het geheel of het gedeelte van de verwerking (of de apparatuur waarmee de verwerking wordt gevoerd) die hij onder zich heeft.

6. Verantwoordelijke kan aanvullende regels en/of protocollen opstellen wanneer aard en inhoud van een verwerking daar aanleiding toe geven. Deze protocollen zoals bijvoorbeeld de Gedragscode e/mail, internet en sociale media of het Protocol Camerabewaking zijn, via de leidinggevende, in te zien bij verantwoordelijke en zullen op passende wijze via de verschillende beschikbare communicatiekanalen (lijnoverleggen, OR/OC-overleggen, Intranet, Nieuwsbrief, Spotlight etc. etc.) bekend worden gemaakt.

Amarant Groep heeft 'beveiligen' als plicht opgelegd gekregen, het treffen van organisatorische maatregelen en het treffen van technische maatregelen. De Wbp verplicht Amarant Groep om de gegevensbewerking te beveiligen. Amarant Groep moet passende organisatorische en technische maatregelen nemen om het verlies van gegevens of onrechtmatige verwerking tegen te gaan. Passende organisatorische maatregelen zijn onder andere de geheimhoudingsplicht voor medewerkers, afspraken over wie autorisatie voor applicaties verkrijgt en hoe diegene autorisatie voor applicaties verkrijgt, afspraken over op welke wijze medewerker moet omgaan met eventuele datalekken en tot slot het maken van afspraken met derden over hoe zij met persoonsgegevens moeten omgaan. Ook heeft Amarant Groep vastgelegd wie tot welke documenten en systemen toegang heeft en met welke rechten (lezen, toevoegen, vervangen, verwijderen etc.). Het bijhouden van zogenaamde 'schaduwdoossiers' is niet toegestaan. Passende technische maatregelen zijn onder andere de beveiliging van de netwerken, de inlogprocedure en het maken van back-ups. Voor systemen die niet bij Amarant Groep draaien, maar bij externen, zijn aanvullende afspraken gemaakt en vastgelegd in zogenaamde bewerkersovereenkomsten.¹⁴⁵

Deze plicht van Amarant Groep in de Wbp wordt in de AVG bevestigd en op onderdelen verijnd. Namelijk, het nemen van passende technische en organisatorische maatregelen is een algemene verplichting/verantwoordelijkheid van Amarant Groep als verwerkingsverantwoordelijke op grond van de AVG en Amarant Groep mag hierbij rekening houden met de aard, de omvang, de context en het doel van de verwerking en de ernst en waarschijnlijkheid van de risico's die uit de verwerking voortvloeien voor de rechten en vrijheden van cliënten.¹⁴⁶ Zie paragraaf 3.6 en 3.6.1 van dit onderzoeksrapport voor deze algemene verplichting van de verwerkingsverantwoordelijke.

4.5.3 Bewaartermijn

Amarant Groep bewaart persoonsgegevens niet langer dan noodzakelijk voor het doel waarvoor zij zijn/worden verwerkt. Dat is in overeenstemming met de Wbp en de AVG.¹⁴⁷ Amarant Groep stelt per verwerking vast hoe lang persoonsgegevens worden bewaard. Dit gebeurt met inachtneming van wettelijke voorschriften. Er zijn een aantal wettelijke bewaartermijnen voor bepaalde gegevens. Voorbeelden hiervan zijn:

- zeven jaar na beëindiging van de overeenkomst met fiscaal relevante gegevens;
- vijf jaar na voorval/behandeling bij Bopz-dossiers¹⁴⁸; en
- vijftien jaar na einde behandeling -tenzij langer bewaren noodzakelijk is- bij medische dossiers¹⁴⁹.

Voor sommige persoonsgegevens bestaan er geen wettelijke bewaartermijnen. Die

¹⁴⁵ Art. 4.5 Handreiking (bijlage 9).

¹⁴⁶ Art. 24 en 25 AVG.

¹⁴⁷ Art. 10 Wbp en art. 5 lid 1 sub c jo. 17 lid 1 sub a AVG.

¹⁴⁸ Art. 2 lid 2 jo. art. 3 Besluit patiëntendossier Bopz jo. art. 4.5.1 Handreiking (bijlage 9) jo. r.o. 39 jo. art. 17 lid 3 sub b AVG.

¹⁴⁹ Art. 7:454 lid 3 BW jo. art. 4.5.1 Handreiking (bijlage 9) jo. r.o. 39 jo. art. 17 lid 3 sub b AVG.

persoonsgegevens worden twee jaar bewaard na einde dienstverlening tenzij er gegronde redenen zijn om langer te bewaren.

Op het moment dat de bewaartermijn is verstreken, worden de persoonsgegevens zo spoedig mogelijk, maar in ieder geval binnen één jaar, vernietigd. In sommige gevallen mogen/kunnen persoonsgegevens niet worden vernietigd. Dat is bijvoorbeeld het geval als bewaring van aanmerkelijk belang is voor een ander persoon, als bewaring op grond van een wettelijk voorschrift noodzakelijk is of als daarover overeenstemming bestaat tussen de betrokkene en verwerkingsverantwoordelijke. Aanduiding 'aanmerkelijk belang' komt uit de WGBO en de AVG bevestigt de bepalingen uit deze sectorspecifieke wet.¹⁵⁰ Ook mag Amarant Groep persoonsgegevens langer bewaren als er sprake is (geweest) van een conflict/rechtszaak. Daarnaast zijn er persoonsgegevens in geanonimiseerde vorm die bewaard mogen blijven. Tot slot komt het wel eens voor dat verwijderen technisch onmogelijk is. In dat geval treft Amarant Groep maatregelen waardoor toegang tot deze persoonsgegevens niet langer mogelijk is of dat die persoonsgegevens niet meer te herleiden zijn naar een persoon.¹⁵¹

4.5.4 Rechten van de cliënt

Het privacyreglement spreekt ten eerste over inzagerecht en gegevensoverdraagbaarheidsrecht¹⁵²:

9.2 Inzage, afschrift en dataportabiliteit

1. De betrokkene heeft het recht kennis te nemen van de op zijn persoon betrekking hebbende verwerkte gegevens. De gevraagde inzage en of het gevraagde afschrift zal zo spoedig mogelijk, doch uiterlijk binnen vier weken, plaatsvinden respectievelijk worden verstrekt.
2. Een mogelijk beperkingsgrond voor inzage en afschrift kan gelegen zijn in de bescherming van redelijke belangen van anderen dan de verzoeker.
3. Voor de verstrekking van een afschrift mag aan de verzoeker of anderen die gerechtigd zijn deze inzage of afschrift te vragen, een redelijke vergoeding in rekening worden gebracht conform de bepalingen in het 'Besluit kostenvergoeding rechten betrokkene Wbp' ("tientjesbesluit").
4. Voor verwerkingen met als grondslagen 'toestemming' of 'contract/overeenkomst' is de verantwoordelijke verplicht om een kopie te verstrekken in een gestructureerde, algemeen gebruikte, leesbare en interoperabele vorm. Dit recht van de betrokkene doet voor de verantwoordelijke geen verplichting ontstaan om technisch compatibele systemen voor gegevensverwerking op te zetten of te houden.

Via de bestaande contactpersoon kan gevraagd worden om inzage. Daarnaast zijn er ook nog APP, Cura, De Heer, Quli of andere systemen om verwerkte gegevens in te zien. Deze zijn bedoeld voor de cliënten zelf of derden die betrokken zijn of die de belangen van de cliënt waarnemen om de verwerkte persoonsgegevens in te zien.¹⁵³

In het privacyreglement, zoals hierboven geciteerd in het eerste lid, staat dat de inzage of het afschrift zo spoedig mogelijk doch uiterlijk binnen vier weken geschiedt/wordt verstrekt.¹⁵⁴ Een termijn hiervoor is dus geregeld en die voldoet aan de termijn waarover de AVG spreekt. Namelijk, binnen een maand.¹⁵⁵ Voor meer informatie over de eisen van de AVG omtrent het inzagerecht, zie paragraaf 3.5.1 van dit onderzoeksrapport.

In het tweede lid van dit artikel uit het privacyreglement staat dat inzage en afschrift achterwege blijven als dat ter bescherming van redelijke belangen van anderen is. Ook dat is in overeenstemming met de wet: de WGBO, de AVG en de Wbp.¹⁵⁶

Tot slot wordt er in het laatste lid gesproken over het gegevensoverdraagbaarheidsrecht oftewel *dataportabiliteit*.¹⁵⁷ Dat is een nieuw recht op grond van de AVG en zoals eerder vermeld, voldoet dit privacyreglement al gedeeltelijk aan de AVG. Uit het interview blijkt

¹⁵⁰ Art. 7:455 lid 2 BW jo. art. 17 lid 3 sub b AVG.

¹⁵¹ Art. 7.2 en 7.3 Reglement verwerking persoonsgegevens (bijlage 8) jo. art. 4.5.1 Handreiking (bijlage 9).

¹⁵² Art. 9.2 Reglement verwerking persoonsgegevens (bijlage 8) jo. art. 15 en 20 AVG.

¹⁵³ Art. 4.4 Handreiking (bijlage 9).

¹⁵⁴ Art. 35 lid 1 Wbp.

¹⁵⁵ R.o. 59 AVG.

¹⁵⁶ Art. 7:456 BW jo. art. 23 lid 1 sub i AVG jo art. 35 lid 3 Wbp.

¹⁵⁷ Art. 20 AVG.

dat in de praktijk van Amarant Groep overdraagbaarheid van gegevens één van de lastigste onderwerpen is qua verwezenlijking, maar Amarant Groep is zich dus (gezien het laatste lid van het reglementsartikel) bewust van het recht en werkt aan dit onderwerp.¹⁵⁸ Zie paragraaf 3.5.4 van dit onderzoeksrapport voor de inhoud van dit recht.

Ten tweede spreekt het privacyreglement over rectificatierecht en gegevenswissingsrecht¹⁵⁹:

9.3 Aanvulling, correctie of vernietiging (recht op vergetelheid)

1. De betrokkene kan verzoeken om correctie van op hem betrekking hebbende gegevens indien deze feitelijk onjuist, voor het doel van de verwerking onvolledig of niet ter zake dienend zijn, dan wel in strijd met een wettelijk voorschrift, in de verwerking voorkomen. De verantwoordelijke draagt zorg dat een beslissing tot correctie zo spoedig mogelijk wordt uitgevoerd.

2. De betrokkene kan verzoeken om verwijdering van op hem betrekking hebbende gegevens. De verantwoordelijke bericht de verzoeker binnen vier weken na ontvangst van het schriftelijk verzoek tot correctie of verwijdering schriftelijk in hoeverre hij daaraan voldoet. Een weigering is met redenen omkleed.

3. De verantwoordelijke verwijdert de gegevens zonder onredelijke vertraging na een daartoe strekkend verzoek van de betrokkene, tenzij redelijkerwijs aannemelijk is dat bewaring van aanmerkelijk belang is voor een ander dan de betrokkene, alsmede voor zover bewaring op grond van een wettelijk voorschrift vereist is.

Het recht op aanvulling en correctie heet nu het rectificatierecht. Het rectificatierecht en het gegevenswissingsrecht (oftewel recht op vergetelheid) zijn opgenomen in het privacyreglement en de verwerkingsverantwoordelijke, Amarant Groep, dient zo spoedig mogelijk/zonder onredelijke vertraging doch binnen vier weken op een dergelijk verzoek te reageren. Een weigering op hetgeen wat is verzocht, is met redenen onderbouwd.¹⁶⁰ Dat is in overeenstemming met de AVG. De AVG heeft namelijk over 'zonder onredelijke vertraging' en 'binnen een maand'.¹⁶¹ De cliënt doet het verzoek schriftelijk zoals vermeld in het reglement en/of via de contactpersoon.¹⁶² Tot slot zegt het privacyreglement dat vernietiging van persoonsgegevens achterwege blijft wanneer redelijkerwijs aannemelijk is dat bewaring van aanmerkelijk belang is voor een ander dan de cliënt, alsmede voor zover die gegevens bij of krachtens de wet zich tegen vernietiging verzetten.¹⁶³ Ook deze bepaling in het reglement is in overeenstemming met de AVG en de WGBO.¹⁶³ Voor meer informatie over rectificatierecht en gegevenswissingsrecht, zie paragrafen 3.5.2 en 3.5.3 van dit onderzoeksrapport.

4.5.5 Functionaris voor gegevensbescherming

In het privacyreglement staat dat wanneer een verwerking van persoonsgegevens wordt gestart en de verwerking niet van melding is vrijgesteld, de verwerking wordt gemeld bij de FG of, wanneer deze niet in de organisatie aanwezig is, bij de AP.¹⁶⁴ Dus mogelijk is er een FG aangewezen bij Amarant Groep. Daarnaast staat er in het privacyreglement dat indien de cliënt een klacht heeft omdat volgens hem of haar de bepalingen van dit reglement niet worden nageleefd, dat de cliënt zich kan wenden tot de FG of, wanneer deze er niet is, tot de AP.¹⁶⁵ Ook uit dit punt blijkt dat Amarant Groep mogelijk een FG heeft. Tot nu toe bestond volgens de privacywetgeving, de Wbp, geen verplichting tot het aanwijzen van een FG.¹⁶⁶ Uit het interview blijkt dat bij Amarant Groep wel een FG is aangewezen.¹⁶⁷

¹⁵⁸ Interview 2 (bijlage 7).

¹⁵⁹ Art. 9.3 Reglement verwerking persoonsgegevens (bijlage 8) jo. art. 16 en 17 AVG.

¹⁶⁰ Art. 36 lid 1 en 2 Wbp.

¹⁶¹ R.o. 59 jo. art. 17 lid 1 AVG.

¹⁶² Art. 4.4 Handreiking (bijlage 9).

¹⁶³ R.o. 65 jo. art. 17 lid 3 sub b jo. art. 23 lid 1 sub i AVG jo. art. 7:455 lid 2 BW.

¹⁶⁴ Art. 8 Reglement verwerking persoonsgegevens (bijlage 8).

¹⁶⁵ Art. 9.5 lid 3 Reglement verwerking persoonsgegevens (bijlage 8).

¹⁶⁶ Art. 62 Wbp.

¹⁶⁷ Interview 2 (bijlage 7).

Overigens is er onder de AVG geen meldplicht bij het verwerken van persoonsgegevens. Amarant Groep hoeft dan geen melding te doen bij de AP. Op grond van de Wbp is er een meldplicht, maar de AP zal per 6 november 2017 niet handhaven op naleving van deze meldplicht. Alleen als er sprake is van een gegevensverwerking met een bepaald risico blijft de AP handhaven totdat de AVG van toepassing is.¹⁶⁸

Amarant Groep is een zorginstelling en houdt zich in overwegende mate bezig met bijzondere categorieën van persoonsgegevens. Hieronder vallen de gezondheidsgegevens van cliënten. Amarant Groep zal daarom met ingang van de AVG de FG moeten behouden.¹⁶⁹

Overigens is het zeer van belang dat Amarant Groep rekening houdt met de positie en de taken van een FG zoals beschreven in paragraaf 3.6.3 van dit onderzoeksrapport.

4.6 Reglement cliëntdossier

Amarant Groep heeft een reglement voor cliëntdossier opgesteld.¹⁷⁰ Het reglement cliëntdossier is niet publiek toegankelijk, maar wel intern voor medewerkers via intranet. Dit reglement berust enerzijds op de Bopz, de WGBO en de Wbp, anderzijds op de uitgangspunten van Amarant Groep ten aanzien van de kwaliteit van de ondersteuning aan cliënten. In plaats van de Wbp dient Amarant Groep in de toekomst dit reglement te baseren op de AVG. Dit type beleidsregeling regelt de wijze waarop het dossier wordt samengesteld, de wijze waarop het wordt bewaard en de toegankelijkheid. Dit reglement verklaart het privacyreglement van Amarant Groep die in paragraaf 4.5 e.v. van dit onderzoeksrapport is besproken, van toepassing op het cliëntdossier.

Het totale dossier van de cliënt kan uit een aantal deeldossiers bestaan. Bijvoorbeeld een medisch deeldossier en een paramedisch deeldossier of een financieel deeldossier en een psychologisch en/of pedagogisch deeldossier etc. Dat varieert afhankelijk van de aard van de hulpverlening. Daarom regelt het cliëntdossierreglement wie toegang heeft tot welk dossier en welke bevoegdheden heeft.

Er staat in het reglement cliëntdossier dat de documenten waarvan het niet meer nodig is dat de volledige tekst wordt bewaard, zo mogelijk worden vervangen door een korte samenvatting. Dat lijkt heel erg veel op het beginsel van minimale gegevensverwerking. Namelijk, dat de persoonsgegevens toereikend moeten zijn, ter zake dienend moeten zijn en beperkt moeten zijn tot wat noodzakelijk is voor de doeleinden waarvoor zijn worden verwerkt. Dat is zo op grond van de Wbp, maar ook op grond van de AVG.¹⁷¹ Nieuw met de komst van de AVG is echter dat Amarant Groep als verwerkingsverantwoordelijke nadrukkelijk wordt aangewezen als de partij die verantwoordelijk is voor de naleving van dit beginsel en dat de bewijslast daarvoor in beginsel ook bij haar ligt: verantwoordingsplicht.¹⁷²

Ook herhaalt dit reglement de rechten van de cliënt (inzage, rectificatie en gegevenswissing) alsmede de bewaartermijnen zoals opgenomen in de algemene voorwaarden en het privacyreglement, besproken in paragraaf 4.4 (e.v.) respectievelijk 4.5 (e.v.) van dit onderzoeksrapport.

Overigens hebben medewerkers die betrokken zijn bij de begeleiding en/of behandeling van de cliënt, in het belang van een goede dienstverlening, toestemming het dossier en/of elkaars dossier in te zien.¹⁷³ Dat bleek ook uit de algemene voorwaarden, besproken in paragraaf 4.4.2 van dit onderzoeksrapport. Het is niet toegestaan om delen uit het dossier te kopiëren of mee te nemen, tenzij dit voor de begeleiding/behandeling van de cliënt

¹⁶⁸ www.autoriteitpersoonsgegevens.nl (zoek op *melden verwerking persoonsgegevens*).

¹⁶⁹ Art. 37 AVG.

¹⁷⁰ Zie bijlage 11: Reglement cliëntdossier.

¹⁷¹ Art. 11 lid 1 Wbp en art. 5 lid 1 sub c AVG.

¹⁷² Art. 5 lid 2 AVG.

¹⁷³ Reglement cliëntdossier, p. 4 (bijlage 11) jo. art. 7:457 lid 2 BW jo. art. 9 lid 2 sub a AVG.

noodzakelijk is. De beheerder registreert op het origineel aan wie en wanneer een kopie is verstrekt. Leerlingen en stagiaires hebben in het kader van hun opleiding na verleende toestemming van de beheerder het recht op inzage op onderdelen die in het kader van de opleiding nodig zijn. In de bijlage van het reglement cliëntdossier worden per medewerker/functie alle bevoegdheden aangegeven die die medewerkers hebben met betrekking tot (deel)dossiers.¹⁷⁴

Daarbij komt in het reglement cliëntdossier het onderwerp 'informatieveiligheid' met passende organisatorische en technische maatregelen alweer aan bod. Dat onderwerp is namelijk opgenomen in het privacyreglement en besproken in paragraaf 4.5.2 van dit onderzoeksrapport. Deze keer wordt in het reglement cliëntdossier over de beveiliging van digitale registratie van cliëntgegevens vermeld: indien de beheerder van het (deel)dossier gegevens die onderdeel uitmaken van het dossier van de cliënt, digitaal vastlegt, dan worden deze gegevens door de betreffende beheerder middels password beveiligd, zodat onbevoegden geen toegang tot de gegevens hebben. Daarnaast maakt de beheerder zodanig regelmatig een back-up zodat gegevens bij calamiteiten niet verloren gaan. Deze back-up wordt in een afgesloten en solide kast bewaard in een af te sluiten ruimte. Het intern noch extern digitaal versturen van gegevens is niet toegestaan. Concrete instructies voor digitale registratie worden uitgewerkt bij invoering van digitaal cliëntenregistratiesysteem.¹⁷⁵

Tot slot zegt het reglement hoe er dient te worden omgegaan met werkaantekeningen: onder het (deel)dossier vallen niet de persoonlijke werkaantekeningen van de interne medewerkers en het dossier van externe behandelaars. Persoonlijke werkaantekeningen moeten worden gehanteerd volgens de eisen die de Wbp stelt.¹⁷⁶ In de toekomst dus volgens de eisen die de AVG stelt. Persoonlijke werkaantekeningen zijn niet toegankelijk voor derden en dienen door de zorgverlener persoonlijk voortdurend te zijn beveiligd. Werkaantekeningen behoren, als ze al in de voorziening worden bewaard, in een persoonlijke kast achter slot en grendel opgeborgen te zijn. Relevante werkaantekeningen worden per half jaar verwerkt in het dossier of anders vernietigd.¹⁷⁷

4.7 Reglement melding en afhandeling datalekken

Amarant Groep heeft een reglement voor melding en afhandeling van datalekken.¹⁷⁸ Dit reglement is alleen intern toegankelijk via intranet en dus niet publiek toegankelijk. De eisen voor het melden van een datalek zijn in de AVG strenger geworden en het beleid van Amarant Groep speelt hier nu al (gedeeltelijk) op in.¹⁷⁹

Dit type beleidsregeling geeft een uitleg over hoe er dient te worden omgegaan met een eventueel datalek. Er wordt gesproken over een FG, want bij Amarant Groep is al een FG aangewezen.¹⁸⁰ In het datalekkenreglement is duidelijk aangegeven wat een datalek is mede aan de hand van voorbeelden. De taal is duidelijk en makkelijk te begrijpen. In de AVG is voorgeschreven dat wanneer er sprake is van een datalek (dus ongeacht de ernst), dit gemeld moet worden aan de AP. Net zoals in de AVG staat in het reglement van Amarant Groep dat alle datalekken, ongeacht de ernst, uiterlijk binnen 72 uur (en dat is conform de AVG) gemeld moeten worden -sommige gedeelten van het reglement zijn nog niet aangepast en daar staat dan weer dat het moet gaan om ernstige datalekken-. Voorts staat er in het reglement dat wanneer een datalek waarschijnlijk ongunstige gevolgen voor de persoonlijke levenssfeer van de betrokkene heeft, dit gemeld moet worden aan de betrokkene. Die grond moet met inachtneming van de AVG gewijzigd

¹⁷⁴ Reglement cliëntdossier, p. 4 (bijlage 11).

¹⁷⁵ Reglement cliëntdossier, p. 5 (bijlage 11) jo. art. 5 lid 1 sub c jo. lid 2 jo. art. 24 AVG.

¹⁷⁶ Reglement cliëntdossier, p. 6 (bijlage 11).

¹⁷⁷ Reglement cliëntdossier, p. 6 (bijlage 11).

¹⁷⁸ Zie bijlage 12: Reglement melding en afhandeling datalekken.

¹⁷⁹ Art. 34a Wbp jo. art. 33 jo. 34 AVG jo. Reglement melding en afhandeling datalekken (bijlage 12).

¹⁸⁰ Art. 4 lid 2 en lid 3 en art. 5.2 Reglement melding en afhandeling datalekken (bijlage 12).

worden in: wanneer een datalek 'waarschijnlijk een hoog risico inhoudt voor de rechten en vrijheden van natuurlijke personen'.

Tevens moeten de hoogten van de boetes in het datalekkenreglement aangepast worden. Die zijn veranderd na de komst van de AVG.¹⁸¹ Voor meer informatie over boetes zie paragraaf 3.8 van dit onderzoeksrapport.

Als laatste staat er in het datalekkenreglement dat de informatie die aan de betrokkene verstrekt wordt, minimaal een aantal punten moet bevatten: wat er aan de hand is, wat de mogelijke gevolgen voor de betrokkene zijn, waar de betrokkene terecht kan met vragen en wat de betrokkene zelf kan doen.¹⁸² Volgens de AVG moet die informatie (ook) andere punten bevatten. Zie voor deze punten paragraaf 3.6.4 van dit onderzoeksrapport.

4.8 Systemen

Binnen Amarant Groep zijn (meerdere) elektronische systemen in gebruik waarin informatie wordt opgeslagen. In de afgelopen jaren is Amarant Groep gefuseerd en overgegaan naar Plancare2 (afgekort: PC2) en APP. De overgang naar APP en met name PC2 is nog niet klaar. Men kan dus (nog) niet spreken over één uniform systeem.

Informatie over de cliënten is nu op veel verschillende plaatsen te vinden. Cliëntinformatie wordt bewaard in papieren dossiers, op harde schijven, in Plancare, in Plancare2, in APP enz. Papieren dossiers worden in de loop van 2018 vernietigd/raken in onbruik. De 'harde schijven' zijn beveiligde deelschijven die op de eigen servers van Amarant Groep staan. De cliëntgegevens op deze schijven zullen zeer binnenkort verdwijnen en worden opgenomen in PC2 of APP.

Er is momenteel dus geen totaaloverzicht van alle informatie over één cliënt en de vereiste informatie is niet snel en efficiënt bij elkaar te zoeken. Dat is niet prettig voor Amarant Groep en haar cliënten. Daarom is er op dit moment een project dat zich bezighoudt met een systeem dat heet: Elektronisch Cliënten Dossier (hierna: ECD). Het ECD is de digitale verzamelplek voor alle cliëntinformatie. Het ECD omvat onder andere het persoonlijk plan, adresgegevens, onderzoeksresultaten en rapportages, maar ook informatie over de aanmelding, de productie, de financiering en de declaratie. Belangrijk is dat ECD niet verward wordt met PC2 of APP. Het ECD is geen op zich zelf staande applicatie, maar een verzamelnaam voor applicaties met cliëntinformatie. Er wordt gestreefd naar dat over twee jaar alle cliëntinformatie alleen digitaal wordt vastgelegd in de applicaties die samen het ECD vormen. Daarnaast is het in de toekomst de bedoeling dat alle applicaties op elkaar aansluiten zodat het werken met het ECD nog makkelijker en overzichtelijker wordt.

Wanneer er in de toekomst door het ECD een totaaloverzicht komt, komen de wensen en zorgvragen van de cliënt en de voortgang daarvan voldoende naar boven. Er wordt dan professioneler en makkelijker gewerkt omdat de cliëntinformatie 24 uur per dag op een veilige manier te lezen, aan te vullen en te delen is met betrokken medewerkers. Dit project omtrent het ECD heeft dus als doel de kwaliteit van zorg te verhogen.

Overigens krijgen de cliënten en hun vertegenwoordigers in de loop van 2018/2019 inzage in de dagrapportages binnen APP. Dat is een start van inzage in het eigen dossier in de verre toekomst.

4.9 Geen beleid

Over sommige onderwerpen is er binnen Amarant Groep niets geregeld. Met de komst van de AVG zou dat echter wel moeten gebeuren. Hieronder volgt een weergave van onderwerpen die aan bod komen op het moment dat de AVG van toepassing is.

¹⁸¹ Art. 66 Wbp jo. art. 83 AVG.

¹⁸² Art. 5.3 Reglement melding en afhandeling datalekken (bijlage 12).

4.9.1 Gegevensbeschermingseffectbeoordeling

Voor Amarant Groep is van belang kennis te nemen van de toekomstige verplichting tot gegevensbeschermingseffectbeoordeling. Hiermee kan een (zorg)instelling zelf controleren of een product of dienst wel echt aan de privacynormen voldoet. Door zo een beoordeling krijgt Amarant Groep inzicht in de risico's die de gegevensverwerking met zich meebrengt voor de cliënten. Omdat Amarant Groep op grote schaal bijzondere categorieën van persoonsgegevens verwerkt, hoofdzakelijk gezondheidsgegevens, zal zij een gegevensbeschermingseffectbeoordeling moeten uitvoeren.¹⁸³ Hiervoor heeft de rijksoverheid een toetsmodel ontwikkeld.¹⁸⁴ Een toetsmodel om een dergelijke beoordeling te kunnen uitvoeren. Amarant Groep kan voordat zij de beoordeling bij haar diensten laat testen, van dit model gebruikmaken.

Voor de uitvoering van een dergelijke beoordeling bestaat er overigens een handreiking.¹⁸⁵

4.9.2 Register van de verwerkingsactiviteiten

Uit het interview blijkt dat Amarant Groep tot op heden geen register in gebruik heeft.¹⁸⁶ Momenteel maakt zij gebruik van een eenvoudig Excel-bestand, maar dat is nog geen echt register van de verwerkingsactiviteiten. Amarant Groep is op de hoogte van een dergelijke verplichting en werkt aan dit onderwerp. De bedoeling is dat zij in de toekomst een uitgebreider register van de verwerkingsactiviteiten heeft.

Amarant Groep heeft meer dan 250 werknemers, ongeveer 5500.¹⁸⁷ Het is daarom wel noodzakelijk om met ingang van de AVG een register van de verwerkingsactiviteiten bij te houden.¹⁸⁸ Paragraaf 3.6.6 van dit onderzoeksrapport geeft de inhoud weer van een dergelijk register.

¹⁸³ Art. 35 AVG.

¹⁸⁴ www.autoriteitpersoonsgegevens.nl (zoek op *toetsmodel PIA*, klik op *privacy impact assessment*).

¹⁸⁵ www.autoriteitpersoonsgegevens.nl (zoek op *handreiking PIA*, klik op *privacy impact assessment*).

¹⁸⁶ Interview 2 (bijlage 7).

¹⁸⁷ Interview 2 (bijlage 7).

¹⁸⁸ Art. 30 AVG.

5 Conclusies en aanbevelingen

In dit onderzoek(srapport) heeft de volgende vraag centraal gestaan: “Welke aanbevelingen kunnen aan de zorginstelling Amarant Groep worden gedaan bij de verwerking van persoonsgegevens van haar cliënten zodat zij voldoet aan de Algemene Verordening Gegevensbescherming die per 25 mei 2018 van toepassing is?”. Dit hoofdstuk is een weergave van de conclusies en aanbevelingen. Conclusies worden getrokken aan de hand van de bevindingen uit dit onderzoek en aan de hand van die conclusies worden aanbevelingen gedaan.

5.1 Conclusies

‡ Privacybeleid

Uit het onderzoek blijkt dat Amarant Groep zich bewust is van het onderwerp ‘privacy’. Dit onderwerp komt meerdere malen aan bod in het beleid van Amarant Groep. Het privacybeleid is gebaseerd op de Wbp. In de toekomst moet het privacybeleid gebaseerd zijn op de AVG.

‡ Uitdrukkelijke toestemming

Als aan cliënt toestemming wordt gevraagd, is de verwerking van zijn/haar persoonsgegevens rechtmatig, want toestemming is één van de gronden voor verwerking. Als de AVG van toepassing is, worden de voorwaarden voor de toestemming zwaarder. Namelijk, er zal een bewijsplicht zijn voor Amarant Groep als verwerkingsverantwoordelijke. Zij moet dan kunnen bewijzen dat er toestemming is gegeven. Op het moment dat de cliënt toestemming verleent, moet de cliënt duidelijk worden gemaakt dat hij/zij de toestemming op elk moment kan intrekken.

‡ Rechten van de cliënt

Volgens de huidige wetgeving Wbp, maar ook volgens de toekomstige wetgeving AVG, heeft de cliënt bepaalde rechten. Bijvoorbeeld inzage recht, rectificatierecht, gegevenswettingsrecht en gegevensoverdraagbaarheidsrecht. Sommige(n) (punten) zijn nieuw op grond van de AVG. Voor zorginstellingen verandert echter niet veel op het gebied van de rechten van de cliënt omdat bij zorginstellingen ook sector specifieke wetten van toepassing zijn. Het belangrijkste voor Amarant Groep is dat de AVG specificeert welke informatie bij inwilliging van het verzoek tot inzage de zorginstelling aan de cliënt moet geven. Daarnaast is het van belang dat Amarant Groep rekening houdt met de gegevensoverdraagbaarheid bij het gebruik van gegevenssets en verwerkingsmethoden.

‡ Bewerkingsovereenkomst

Op grond van de Wbp is het sluiten van een bewerkingsovereenkomst verplicht. Dezelfde verplichting is ook op grond van de AVG. Er is gekeken naar de bewerkingsovereenkomst die Amarant Groep hanteert. De eisen over wat/hoe een bewerkingsovereenkomst moet regelen, zijn in de AVG uitgebreid. Het huidige conceptovereenkomst van Amarant Groep zal binnenkort worden vervangen door een nieuwe vanuit de Zorgkoepels.

‡ Functionaris voor gegevensbescherming

Het aanstellen van een FG is op grond van de Wbp niet verplicht. Op grond van de AVG is het aanstellen van een FG verplicht voor Amarant Groep. Momenteel heeft Amarant Groep een FG in dienst.

‡ Meldplicht voor datalekken

Door de AVG worden de eisen voor een (zorg)instelling om een datalek te melden, verscherpt. Op grond van de Wbp moeten alleen ernstige datalekken worden gemeld aan de AP. Op grond van de AVG moeten alle datalekken aan de AP worden gemeld, tenzij Amarant Groep kan aantonen dat het onwaarschijnlijk is dat deze inbreuk risico's met zich meebrengt voor de rechten en vrijheden van natuurlijke personen. Hiernaast moet op grond van de Wbp, als een inbreuk waarschijnlijk ongunstige gevolgen zal hebben voor

de persoonlijke levenssfeer van cliënt, de cliënt onverwijld op de hoogte worden gesteld van de inbreuk. Dat criterium is veranderd op grond van de AVG en moet de melding aan de cliënt geschieden als de inbreuk waarschijnlijk een hoog risico inhoudt voor de rechten en vrijheden van natuurlijke personen. Overigens dient een datalek in de toekomst binnen 72 uur te worden gemeld aan de AP. Er is kennisgenomen van het reglement dat van kracht is bij Amarant Groep. Met het oog op de AVG is dit reglement nog niet volledig.

‡ Gegevensbeschermingseffectbeoordeling

Vanaf het moment dat de AVG van toepassing is, zal voor Amarant Groep de plicht gaan gelden om een gegevensbeschermingseffectbeoordeling uit te voeren. Hiermee kan een (zorg)instelling zelf controleren of een product of dienst aan de privacynormen voldoet.

‡ Register van de verwerkingsactiviteiten

Op grond van de Wbp bestond er geen verplichting om een register van de verwerkingsactiviteiten te houden. Een dergelijke verplichting is nieuw op grond van de AVG. Amarant Groep heeft tot op heden geen register van de verwerkingsactiviteiten.

5.2 Aanbevelingen

‡ Privacybeleid

Het huidige beleid is gebaseerd op de Wbp. Dat is onder andere af te leiden van verwijzingen naar de Wbp in verschillende schriftelijke regelingen. In de toekomst moet Amarant Groep in die regelingen verwijzen naar de AVG, want de Wbp is dan vervallen. Daarmee wordt ook aanbevolen de begrippen/benamingen die op grond van de Wbp worden gebruikt, te vervangen door begrippen/benamingen in de AVG.

‡ Uitdrukkelijke toestemming

Aan Amarant Groep wordt aanbevolen de toestemming van haar cliënten voor verwerking van hun persoonsgegevens schriftelijk vast te leggen. Hierdoor kan altijd worden aangetoond dat er daadwerkelijk uitdrukkelijke toestemming is gegeven. In het huidige beleid van Amarant Groep wordt gebruik gemaakt van verschillende toestemmingsformulieren. Sommige hiervan zijn echter te summier en op zijn minst moet volgens de AVG in elk formulier worden opgenomen dat de cliënt de gegeven toestemming op elk moment kan intrekken.

‡ Rechten van de cliënt

Wanneer de cliënt een verzoek doet tot inzage moet in een omschrijving vanuit de zorginstelling de verwerkingsdoeleinden en de betrokken categorieën van persoonsgegevens waarop de verwerking betrekking heeft en de ontvanger of categorieën van ontvangers aan wie persoonsgegevens zijn of zullen worden verstrekt, zijn beschreven. Dat is op deze manier geregeld in de Wbp en de AVG. De AVG voegt hier echter verdere criteria aan toe. De AVG specificeert welke bijkomende informatie bij inwilliging van het verzoek tot inzage de zorginstelling aan de cliënt moet geven:

- indien mogelijk, de periode gedurende welke de persoonsgegevens naar verwachting zullen worden opgeslagen, of indien dat niet mogelijk is, de criteria om die termijn te bepalen;
- dat de cliënt het recht heeft Amarant Groep te verzoeken dat persoonsgegevens worden gerectificeerd of gewist of dat de verwerking van hem betreffende persoonsgegevens wordt beperkt, alsmede het recht tegen die verwerking bezwaar te maken;
- dat de cliënt het recht heeft klacht in te dienen bij de AP;
- alle beschikbare informatie over de bron van die gegevens, wanneer de persoonsgegevens niet bij de cliënt worden verzameld;
- het bestaan van geautomatiseerde besluitvorming, met inbegrip van profilering, en ten minste in die gevallen, nuttige informatie over de onderliggende logica, alsmede het belang en de verwachte gevolgen van die verwerking voor de cliënt.

Aan Amarant Groep wordt aanbevolen deze criteria op te nemen in verschillende regelingen van Amarant Groep zodat zij, telkens wanneer een verzoek tot inzage wordt ingediend door een cliënt, zich bewust is van de informatie die zij aan de cliënt moet geven.

Daarnaast wordt Amarant Groep aangeraden om aan de slag te gaan met het verwezenlijken van gegevensoverdraagbaarheid en de manier waarop dat wordt gedaan op te nemen in regelingen van Amarant Groep of op te nemen als in de vorm van een nieuwe regeling.

⋮ **Bewerkingsovereenkomst**

In het toekomstig model bewerkingsovereenkomst zal het onderwerp en 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 Amarant Groep, omschreven moeten worden.

⋮ **Functionaris voor gegevensbescherming**

Het is raadzaam om rekening te houden met de positie en de taken van de FG zoals omschreven in de wet. Alleen dan voldoet Amarant Groep aan de toekomstige wetgeving.

⋮ **Meldplicht voor datalekken**

Het reglement melding en afhandeling datalekken van Amarant Groep zal goed doorgenomen moeten worden. In sommige gedeelten van het reglement wordt gesproken over ernstige datalekken en in andere gedeelten weer over alle datalekken. Ernstige datalekken moeten vervangen worden door alle datalekken. Tevens moet het criterium 'waarschijnlijk ongunstige gevolgen voor de persoonlijke levenssfeer van de betrokkene' vervangen worden door 'waarschijnlijk een hoog risico voor de rechten en vrijheden van natuurlijke personen'.

⋮ **Gegevensbeschermingseffectbeoordeling**

Voor Amarant Groep wordt aangeraden om producten en diensten te testen in hoeverre zij voldoen aan de privacynormen door een gegevensbeschermingseffectbeoordeling uit te voeren. Zij kan hierbij gebruikmaken van het toetsmodel dat door de rijksoverheid is vastgesteld en van een handreiking.

⋮ **Register van de verwerkingsactiviteiten**

Het wordt Amarant Groep aanbevolen om een register van de verwerkingsactiviteiten te houden en desgevraagd beschikbaar te stellen in de tijd dat de AVG van toepassing is.

Bronnenlijst

www.amarantgroep.nl
www.autoriteitpersoonsgegevens.nl
www.eur-lex.europa.eu
www.idris.nl
www.internetconsultatie.nl
www.nvz-ziekenhuizen.nl
www.overheid.nl
www.recht.nl
www.rijksoverheid.nl

Fennell, Kroes en Koppejan 2015

S. Fennell, R. Kroes en F. Koppejan, *Privacy wetgeving. Inclusief voorgestelde meldplichten, boetes en concept algemene verordening gegevensbescherming*, Oisterwijk: Wolf Legal Publishers 2015.

Fennell e.a. 2016

S. Fennell e.a., *Privacy wetgeving; inclusief de Algemene Verordening Gegevensbescherming*, Oisterwijk: Wolf Legal Publishers 2016.

Engelfriet e.a. 2017

A. Engelfriet, L. Meij, P. Kager, *De Algemene Verordening Gegevensbescherming. Artikelsgewijs commentaar*, Ius Mentis 2017.

Versmissen, Terstegge en Krijgsman 2017

K. Versmissen, J. Terstegge en N. Krijgsman, *Grip op de AVG. De nieuwe privacywet voor niet-juristen*, Deventer: Wolters Kluwer 2017.

Berkvens e.a. 2016

J. Berkvens e.a., *Checklist Privacy. Privacybeleid in 30 checklists. Van Wbp naar AVG*, Amsterdam: Berghauser Pont Publishing 2016.

Berkvens & Jakimowicz 2016

J. Berkvens & C. Jakimowicz, *Tekstuitgave privacyverordening. Met geïntegreerde overwegingen, Wbp- en Richtlijn 95/46/EG-teksten en verwijstabellen*, Den Haag: Boom Juridische Uitgevers 2016.

Baarda e.a. 2013

B. Baarda e.a., *Basisboek Kwalitatief Onderzoek. Handleiding voor het opzetten en uitvoeren van kwalitatief onderzoek*, Groningen: Noordhoff Uitgevers 2013.

Bastiaans e.a. 2016

M.H. Bastiaans e.a., *Leidraad voor juridische auteurs*, Deventer: Kluwer 2016.

Ijzermans & Van Schaaijk 2007

M.G. Ijzermans & G.A.F.M. van Schaaijk, *Oefening baart kunst*, Den Haag: Boom Juridische Uitgevers 2007.

Van Schaaijk 2015

G.A.F.M. van Schaaijk, *Praktijkgericht juridisch onderzoek*, Den Haag: Boom Juridische Uitgevers 2015.

Verhoeven 2014

N. Verhoeven, *Wat is onderzoek? Praktijkboek voor methoden en technieken*, Den Haag: Boom Lemma Uitgevers 2014.

De Jong 2016

J.P. de Jong, 'De Algemene verordening gegevensbescherming', *Ars Aequi* 2016/10, p. 770-773.

Snel 2017

M. Snel, 'De 'goede' onderzoeksopzet als succesfactor voor de juridische scriptie', *Ars Aequi* 2017/9, p. 748-754.

Van Schelven & Van Schelven 2016

I.P.V. van Schelven & P.C. van Schelven, 'Europese gegevensbescherming: van richtlijn naar verordening', *Nederlands tijdschrift voor Europees recht* 2016/3, p. 99-108.

De Vries & Goudsmit 2016

H. de Vries & M. Goudsmit, 'Voorsorteren op de Algemene Verordening Gegevensbescherming. Twee stappen vooruit, één stap terug.', *Nederlands Juristenblad* 2016/1077.

Zwenne & Mommers 2016

G-J Zwenne & L. Mommers, 'De tien belangrijkste veranderingen die de algemene verordening gegevensbescherming gaat brengen (in minder dan vijfduizend woorden)', *Tijdschrift voor Compliance* 2016/4, p. 182-189.

HvJ EU 13 mei 2014, C-131/12, ECLI:EU:C:2014:317 (*Google Spain SL en Google Inc/AEPD en Mario Costeja Gonzáles*)

Verordening (EU) 2016/679 van het Europees Parlement en de Raad van 27 april 2016 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens en tot intrekking van Richtlijn 95/46/EG (algemene verordening gegevensbescherming; *PbEU* L 119).

Richtlijn 95/46/EG van het Europees Parlement en de Raad van 24 oktober 1995 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens (*PbEG* L 281).

Richtlijn (EU) 2016/680 van het Europees Parlement en de Raad van 27 april 2016 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens door bevoegde autoriteiten met het oog op de voorkoming, het onderzoek, de opsporing en de vervolging van strafbare feiten of de tenuitvoerlegging van straffen en betreffende het vrije verkeer van die gegevens en tot intrekking van kaderbesluit 2008/977/JBZ van de Raad (*PbEU* L 119).

T. Hooghiemstra e.a., *Onderzoek naar de beveiliging van patiëntgegevens* (PBLQ Rapport van 2016).