

Algemene Verordening Gegevensbescherming

Toepassing van de AVG bij Zorgkwekerij Bloei



Inhoudsopgave

Inleiding	blz. 4
1. Zes grondslagen	blz. 5
1.1 Toestemming	
1.2 Overeenkomst	
1.3 Wettelijke verplichting	
1.4 Vitale belangen	
1.5 Algemeen belang	
1.6 Gerechvaardigde belangen	
1.7 Verwerking van persoonsgegevens	
2. Bijzondere en strafrechtelijke gegevens	blz. 7
2.1 Bijzondere persoonsgegevens	
2.2 Strafrechtelijke persoonsgegevens	
3. Verwerkingsverantwoordelijke en verwerkers	blz. 9
3.1 Verwerkingsverantwoordelijke	
3.2 Verwerkers	
3.3 Verwerkersovereenkomst	
4. Maatregelen voor naleving AVG	blz. 11
4.1 Registerplicht	
4.2 Functionaris voor gegevensbescherming	
4.3 Gegevensbeschermingseffectbeoordeling	
4.4 Voorafgaande raadpleging	
4.5 Privacy door ontwerp en standaardinstellingen	
4.6 Beveiligingseisen	
4.7 Melden van inbreuk	
4.8 Afspraken met verwerkers	
5. Betrokkenen	blz. 14
6. Recht op informatie	blz. 15
6.1 Informatieplicht	
6.2 Uitzonderingen op de informatieplicht	
6.3 Informatieverstrekking	
6.4 Inzage	
6.5 Verwijdering van gegevens	
6.6 Het recht om vergeten te worden	
6.7 Beperking van gegevensverwerking	
6.8 Het recht op verzet	
7. Toezicht	blz. 18
8. Toepassing voor Zorgwekerij Bloei	blz. 19
8.1 Grondslagen	
8.2 Bijzondere persoonsgegevens	
8.3 Verwerkingsverantwoordelijke en verwerker	
8.4 Register van verwerkingsactiviteiten en gegevensbeschermingseffectbeoordeling	

- 8.5 Beveiligingsmaatregelen
- 8.6 Rechten van betrokkenen

Bijlagen

blz. 22

- Bijlage 1 Toestemmingsformulier Persoonsgegevens
- Bijlage 2 Uitleg Persoonsgegevens
- Bijlage 3 Verwerkersovereenkomst
- Bijlage 4 Instructie voor verwerker
- Bijlage 5 Register van verwerkingsactiviteiten
- Bijlage 6 Gegevensbeschermingseffectbeoordeling
- Bijlage 7 Meldingsformulier datalek

Inleiding

Vanaf 25 mei 2018 is de wet 'Algemene Verordening Gegevensbescherming' (verder genoemd: AVG) van toepassing in Europa. Deze wet geldt ook voor (kleine) zorgaanbieders zoals Zorgkwekerij Bloei. In dit protocol is de inhoud van de wet kort uiteengezet en toegepast op de Zorgkwekerij. Hierbij is vooral ingegaan op de zaken die voor zorgboerderijen/zorgkwekerijen gelden. Voor meer informatie over de wet verwijzen wij u naar de website www.autoriteitpersoonsgegevens.nl.

Hoofdstuk 1 tot en met 7 bevat een samenvatting van de belangrijkste bepalingen uit de wet AVG die voor zorgboerderijen/zorgkwekerijen gelden. In hoofdstuk 8 zijn deze bepalingen toegepast op Zorgkwekerij Bloei. Een belangrijke opmerking hierbij is dat deze manier van omgaan met persoonsgegevens geldt vanaf 25 mei 2018.

De bijlagen bevatten documenten waaruit blijkt dat Zorgkwekerij Bloei de AVG volgt en op welke wijze deze wordt toegepast. Het zijn documenten die bijvoorbeeld uitgedeeld aan of ondertekend worden door de wettelijke verzorgers van de cliënt of documenten die ondertekend worden door de verwerkers van persoonsgegevens.

1. Zes grondslagen

De AVG kent zes grondslagen voor het verwerken van persoonsgegevens, namelijk:

1. Toestemming van de betrokken persoon.
2. De gegevensverwerking is noodzakelijk voor de uitvoering van een overeenkomst.
3. De gegevensverwerking is noodzakelijk voor het nakomen van een wettelijke verplichting.
4. De gegevensverwerking is noodzakelijk ter bescherming van de vitale belangen.
5. De gegevensverwerking is noodzakelijk voor de vervulling van een taak van algemeen belang of uitoefening van openbaar gezag.
6. De gegevensverwerking is noodzakelijk voor de behartiging van de gerechtvaardigde belangen.

Bij de verwerking van persoonsgegevens moet Zorgkwekerij Bloei zich kunnen baseren op één van bovenstaande grondslagen. Deze grondslagen worden hieronder verder uitgelegd en in hoofdstuk 8 toegepast op onze Zorgkwekerij Bloei. Bij het openbaar maken van documenten moet ook duidelijk aandacht worden besteed aan het beschermen van de persoonsgegevens die erin staan en moet rekening gehouden worden met onderstaande grondslagen.

1.1 Toestemming

Een organisatie mag persoonsgegevens verwerken wanneer zij daar toestemming voor heeft gekregen van bijvoorbeeld de cliënt, zijn of haar verzorgers of een personeelslid (verder genoemd: persoon). De manier waarop toestemming wordt gevraagd door Zorgkwekerij Bloei is in hoofdstuk 8 uitgelegd. Hieronder is beschreven aan welke eisen de toestemming moet voldoen:

1. Vrijelijk gegeven: de persoon mag niet onder druk gezet worden om toestemming te geven. Daarbij wordt wel gelet op machtsverhoudingen. Een werknemer kan een vraag van zijn werkgever bijvoorbeeld niet weigeren.
2. Ondubbelzinnig: er moet sprake zijn van en duidelijke actieve handeling, zoals een (digitale) schriftelijke of mondelinge verklaring.
3. Geïnformeerd: de organisatie moet de persoon informeren over:
 - de identiteit van de organisatie
 - het doel van elke verwerking waarvoor toestemming wordt gevraagd
 - welke persoonsgegevens worden verzameld en gebruikt
 - het recht dat de persoon heeft om de toestemming weer in te trekken.
4. Specifiek: de toestemming moet gelden voor een specifieke verwerking en een specifiek doel. Wanneer er meerdere doeleinden zijn, moet per doel toestemming gevraagd worden.
5. Het moet net zo makkelijk zijn om de toestemming weer in te trekken als dat het was om de toestemming te geven.
6. De organisatie moet kunnen aantonen dat zij geldige toestemming heeft gekregen.

Als het gaat om persoonsgegevens van kinderen jonger dan 16 jaar, is toestemming nodig van de persoon die de ouderlijke verantwoordelijkheid draagt. Het kind hoeft zelf geen toestemming te geven.

1.2 Overeenkomst

De organisatie mag zich op de grondslag 'overeenkomst' baseren wanneer zij een overeenkomst heeft met de persoon en het verwerken van persoonsgegevens hiervoor noodzakelijk is. Een voorbeeld hiervan is dat Zorgkwekerij Bloei het telefoonnummer van de ouders van een hulpkweker opslaat, zodat zij hen kunnen bellen wanneer nodig.

1.3 Wettelijke verplichting

Om zich als organisatie te baseren op deze grondslag moet de verwerking van de persoonsgegevens noodzakelijk zijn om aan een wettelijke verplichting te voldoen. Het gaat bijvoorbeeld om het verstrekken van gegevens voor de uitvoering van de belastingwet.

1.4 Vitale belangen

Er is sprake van een vitaal belang wanneer iemands leven of gezondheid in gevaar is en de persoon op dat moment niet om toestemming gevraagd kan worden. Wanneer een cliënt bijvoorbeeld bewusteloos is of er acuut gevaar dreigt, kan een medewerker van Zorgkwekerij Bloei, de cliënt niet om toestemming vragen voor de verwerking van medische gegevens. De gegevens mogen dan zonder toestemming verwerkt worden op basis van de grondslag 'vitale belangen'.

1.5 Algemeen belang

Een organisatie kan zich beroepen op de grondslag 'algemeen belang' wanneer zij een publieke taak uitoefent voor het algemeen belang of openbaar gezag. Het gaat daarbij om taken die in de wet zijn vastgelegd en die relevant zijn voor de organisatie.

1.6 Gerechtvaardigde belangen

De organisatie kan zich op deze grondslag baseren als zij aan drie voorwaarden voldoet, namelijk:

1. *Gerechtvaardigd belang*: het moet gaan om een gerechtvaardigd belang, dat rechtmatig is, voldoende duidelijk verwoord is en ook echt aanwezig is. Dat is zo wanneer een verwerking aantoonbaar noodzakelijk is om bedrijfsactiviteiten te verrichten, bijvoorbeeld bij het voeren van een personeelsadministratie.
2. *Noodzakelijkheid*: de verwerking van persoonsgegevens moet noodzakelijk zijn voor de behartiging van het gerechtvaardigd belang. De verwerking moet daarom getoetst worden aan de eisen van proportionaliteit en subsidiariteit. Dat betekent dat de organisatie moet nagaan of het doel van de verwerking in verhouding staat tot de inbreuk voor personen van wie zij de persoonsgegevens verwerkt en of de organisatie het doel niet op een voor de persoon minder nadelige manier kan bereiken.
3. *Afweging belangen*: de organisatie moet de afweging maken tussen haar belangen en de belangen van de persoon. Hierbij moet zij maatregelen treffen om ervoor te zorgen dat de rechten en vrijheden van de persoon niet zwaarder wegen dan het gerechtvaardigd belang van de organisatie. Dit betekent onder andere dat de gegevens niet langer bewaard mogen worden dan nodig is voor het doel van de verwerking.

1.7 Verwerking van persoonsgegevens

Naast bovenstaande zes grondslagen moet elke verwerking van persoonsgegevens in lijn zijn met de volgende beginselen:

1. De verwerking van persoonsgegevens moet rechtmatig, behoorlijk en transparant zijn.
2. De verwerking moet gebonden zijn aan specifieke verzameldoelen.
3. De gegevens moeten toereikend, ter zake dienend en beperkt tot het noodzakelijke zijn.
4. De gegevens moeten juist zijn.
5. De gegevens mogen niet langer worden bewaard dan nodig.
6. De gegevens moeten goed beveiligd zijn en vertrouwelijk blijven.

2. Bijzondere en strafrechtelijke gegevens

Bijzondere en strafrechtelijke gegevens staan los van persoonsgegevens. De verwerking van deze gegevens is verboden. Toch zijn er uitzonderingen die reden geven om deze gegevens wel te mogen verwerken. Deze zijn hieronder beschreven.

2.1 Bijzondere persoonsgegevens

Bijzondere persoonsgegevens zijn gegevens die gezien hun aard extra gevoelig zijn. Het gaat om gegevens over ras of etnische afkomst, politieke opvattingen, religieuze of levensbeschouwelijke overtuigingen, het lidmaatschap van een vakbond, genetische gegevens, biometrische gegevens met het oog op de unieke identificatie van een persoon, gegevens over gezondheid en gegevens met betrekking tot iemands seksueel gedrag of seksuele gerichtheid. De verwerking van deze bijzondere persoonsgegevens is verboden, tenzij de organisatie zich kan beroepen op één van de zes grondslagen in combinatie met één van onderstaande uitzonderingen.

1. De persoon heeft toestemming gegeven voor de verwerking van deze bijzondere gegevens.
2. De verwerking is noodzakelijk met het oog op de uitvoering van verplichtingen en specifieke rechten van de organisatie of de persoon. Dit op het gebied van het arbeidsrecht en het sociale zekerheids- en sociale beschermingsrecht.
3. De verwerking is noodzakelijk ter bescherming van de vitale belangen van de persoon, wanneer diegene fysiek of juridisch niet in staat is om toestemming te geven.
4. De verwerking mag wel gedaan worden door een stichting, vereniging of andere instantie zonder winstoogmerk die op politiek, levensbeschouwelijk, godsdienstig of vakbondsgebied werkzaam is en gegevens verwerkt in het kader van gerechtvaardigde activiteiten en met passende waarborgen.
5. De verwerking heeft betrekking op persoonsgegevens die kennelijk door de betrokkene openbaar zijn gemaakt.
6. De verwerking van bijzondere gegevens mag plaatsvinden wanneer dit noodzakelijk is voor de instelling, uitoefening of onderbouwing van een rechtsvordering of wanneer gerechten handelen in het kader van hun rechtsbevoegdheid.
7. De verwerking is noodzakelijk vanwege een zwaarwegend algemeen belang.
8. De verwerking is noodzakelijk voor doeleinden van preventieve of (arbeids)geneeskundige aard. Voorbeelden zijn het beoordelen van arbeidsgeschiktheid of het verstrekken van gezondheidszorg.
9. De verwerking is noodzakelijk om redenen van algemeen belang op het gebied van de volksgezondheid.
10. De verwerking is noodzakelijk met het oog op de archivering in het algemeen belang, wetenschappelijk of historisch onderzoek of statische doeleinden.

De organisatie mag zich op de nummers 2, 7, 8, 9 en 10 van bovenstaande uitzonderingen alleen beroepen als daarvoor een rechtsbasis is gecreëerd in de nationale wet.

Verder bestaan er per bijzondere categorie persoonsgegevens uitzonderingen die maken dat deze gegevens wel verwerkt mogen worden.

De uitzonderingen waar zorgboerderijen/zorgkwekerijen mee te maken kunnen hebben, zijn de volgende:

- instellingen zoals een zorgboerderij/zorgkwekerij mogen persoonsgegevens waaruit religieuze of levensbeschouwelijke overtuigingen blijken verwerken.
- genetische gegevens mogen verwerkt worden wanneer deze door de betrokkene zelf zijn gegeven.

- gezondheidsgegevens van cliënten mogen verwerkt worden door instellingen die maatschappelijke zorg leveren of zorg leveren in de wet, zodat zij de cliënten goed kunnen begeleiden.
- gezondheidsgegevens van werknemers mogen verwerkt worden voor een goede uitvoering van wettelijke voorschriften, pensioenregelingen, collectieve arbeidsovereenkomsten of re-integratie of begeleiding van zieke of arbeidsongeschikte werknemers.

2.2 Strafrechtelijke persoonsgegevens

Onder strafrechtelijke persoonsgegevens worden de volgende persoonsgegevens verstaan: strafrechtelijke veroordelingen, strafbare feiten, daarmee verband houdende veiligheidsmaatregelen of persoonsgegevens betreffende een door de rechter opgelegd verbod naar aanleiding van onrechtmatig of hinderlijk gedrag. De verwerking van strafrechtelijke persoonsgegevens is verboden, tenzij de organisatie zich kan beroepen op een specifieke wettelijke uitzondering zoals hieronder beschreven in combinatie met één van de zes grondslagen uit hoofdstuk 1.

1. De verwerking staat onder toezicht van de overheid.
2. De verwerking is toegestaan bij nationaal recht. Het gaat daarbij om Unierechtelijke of lidstaatrechtelijke bepalingen, die passende waarborgen bieden voor de rechten en vrijheden van de betrokken personen.

Verder gelden grotendeels dezelfde uitzonderingen als bij de bijzondere persoonsgegevens, namelijk nummer 1, 3, 5, 6, 9 en 10 (zie paragraaf 2.1). Daarnaast mogen strafrechtelijke persoonsgegevens verwerkt worden wanneer dit nodig is voor de beoordeling van een verzoek van de betrokkene om een beslissing over hem te nemen, bijvoorbeeld bij een sollicitatie. Als laatste mogen strafrechtelijke gegevens ter bescherming van eigen belangen bewaard worden, bijvoorbeeld als deze zichtbaar zijn op camerabeelden die door de organisatie zijn gemaakt. Deze beelden mogen echter niet openbaar gemaakt worden.

2.3 Burgerservicenummer

Het Burgerservicenummer valt volgens de AVG niet onder bijzondere persoonsgegevens. Het is belangrijk dat passende waarborgen zijn getroffen voor de bescherming van de rechten en vrijheden van de betrokkene. Europese lidstaten mogen zelf regels bepalen wat betreft het verwerken van het Burgerservicenummer. Welke regels Nederland stelt, staat nog niet vast. In de 'Wet gebruik Burgerservicenummer in de zorg' (Wbsn-z) staat dat zorgaanbieders verplicht zijn het Burgerservicenummer van haar cliënten op te slaan en te gebruiken bij uitwisseling van gegevens.

Redenen voor het gebruik van het Burgerservicenummer zijn volgens de Wbsn-z:

- fouten te voorkomen bij de uitwisseling van financiële en medische gegevens.
- eenvoudiger te declareren bij de zorgverzekering.
- persoonsverwisseling te voorkomen.
- betere bescherming te bieden tegen identiteitsfraude.

3. Verwerkingsverantwoordelijke en verwerkers

3.1 Verwerkingsverantwoordelijke

De verwerkingsverantwoordelijke is verantwoordelijk voor de rechtmatige en zorgvuldige omgang met persoonsgegevens. Dit betekent dat zij de plichten uit de AVG moet naleven en dat zij de goede naleving van deze plichten kan aantonen.

De verwerkingsverantwoordelijke moet de volgende maatregelen nemen:

1. een register van verwerkingsactiviteiten bijhouden (registerplicht).
2. onder bepaalde omstandigheden een functionaris voor gegevensbescherming aanstellen.
3. voorafgaand aan risicovolle verwerkingsactiviteiten een gegevensbeschermingseffectbeoordeling uitvoeren.
4. onder bepaalde omstandigheden voorafgaand aan een nieuwe risicovolle verwerkingsactiviteit de Autoriteit Persoonsgegevens raadplegen.
5. bij het inrichten van verwerkingen rekening houden met het principe van privacy door ontwerp en standaardinstellingen (privacy by design & default).
6. passende beveiligingsmaatregelen treffen met het oog op de bescherming van persoonsgegevens.
7. in geval van een datalek melding doen bij de Autoriteit Persoonsgegevens en onder bepaalde omstandigheden betrokkenen daarover informeren.
8. afspraken maken met verwerkers.

Om aan te tonen dat de organisatie zich aan bovenstaande maatregelen houdt, moet zij de volgende punten in acht nemen:

- een register van verwerkingsactiviteiten bijhouden.
- indien dit in verhouding staat tot de verwerkingsactiviteiten, op schrift stellen van en passend gegevensbeschermingsbeleid.
- documenteren van gegevensbeschermingseffect beoordelingen.
- informatievoorziening aan de betrokkenen op schrift stellen.
- de wijze waarop toestemming gevraagd wordt vastleggen.
- het bewijs van de gegeven toestemming documenteren.
- het gerechtvaardigde belang documenteren wanneer de grondslag 'gerechtvaardigd belang' gehanteerd wordt.
- processen ter waarborging van de rechten van betrokkenen documenteren.
- verwerkersovereenkomsten conform de eisen uit de AVG opstellen voor elke inzet van verwerkers.
- procedures voor de omgang met datalekken documenteren.
- een registratie van datalekken die zich in de organisatie hebben voorgedaan bijhouden.
- de maatregelen die genomen worden om invulling te geven aan de uitgangspunten van gegevensbescherming door ontwerp en door standaardinstellingen.

Zie hoofdstuk 4 voor verdere uitleg van bovenstaande maatregelen.

3.2 Verwerker

De verwerker handelt op basis van de instructies van de verwerkingsverantwoordelijke en helpt de verwerkingsverantwoordelijke bij het uitvoeren van sommige plichten. Daarnaast zijn er enkele plichten die zelfstandig gericht zijn aan de verwerker, namelijk de beveiliging van gegevens, het

bijhouden van een register van verwerkingsactiviteiten en het aanstellen van een functionaris voor gegevensbescherming.

Een verwerkingsverantwoordelijke mag alleen verwerkers inschakelen die voldoende mogelijkheden hebben om de AVG na te volgen. Het gaat om deskundigheid van de verwerker, betrouwbaarheid van de verwerker en de juiste middelen om ervoor te zorgen dat de technische en organisatorische maatregelen getroffen kunnen worden.

Een verwerker mag zelf een andere verwerker (sub-verwerker) inschakelen voor de verwerking van persoonsgegevens, maar moet daarvoor voorafgaand schriftelijke toestemming van de verwerkingsverantwoordelijke krijgen. Wanneer er wijzigingen plaatsvinden in de inzet of taken van de sub-verwerkers, moet de verwerkingsverantwoordelijke hierover geïnformeerd worden. De sub-verwerker moet minimaal hetzelfde niveau van gegevensbescherming hebben als de verwerker en dit moet in een overeenkomst duidelijk worden. De verwerker blijft aansprakelijk ten opzichte van de verwerkingsverantwoordelijke.

Onder bepaalde omstandigheden moeten verwerkers een functionaris voor gegevensbescherming aanstellen. Zie hiervoor paragraaf 4.2.

3.3 Verwerkersovereenkomst

De verwerker dient afspraken te maken met de verwerkingsverantwoordelijke over de wijze waarop zij persoonsgegevens verwerkt en deze in een verwerkersovereenkomst te zetten die ondertekend moet worden door beide partijen. In deze overeenkomst moeten in ieder geval de volgende zaken geregeld worden:

- het onderwerp en de duur van de verwerking.
- de aard en het doel van de verwerking.
- het soort persoonsgegevens en de categorieën van betrokkenen.
- de rechten en verplichtingen van de verwerkingsverantwoordelijke.

Verder moeten onderstaande zaken in de overeenkomst gezet worden:

- de verwerker mag de persoonsgegevens alleen verwerken onder de schriftelijke instructies van de verwerkingsverantwoordelijke.
- de verwerker waarborgt dat de toegang tot de gegevens beperkt is tot gemachtigde personen. Deze personen moeten gebonden zijn aan geheimhouding op grond van een overeenkomst of een wettelijke verplichting.
- de verwerker hanteert hetzelfde niveau van beveiliging voor persoonsgegevens als de verwerkingsverantwoordelijke.
- de verwerkingsverantwoordelijke biedt alle mogelijke ondersteuning bij het nakomen van de verplichtingen van de verwerker met het oog op beantwoording van verzoeken rondom de rechten van betrokkenen.
- de verwerker staat de verwerkingsverantwoordelijke bij wat betreft het nakomen van de verplichtingen op het gebied van beveiliging van persoonsgegevens en de meldplicht datalekken.
- na beëindiging van deze overeenkomst, wist de verwerker de persoonsgegevens of geeft deze aan de verwerkingsverantwoordelijke terug.
- de verwerker stelt alle informatie ter beschikking die nodig is om aantoonbaar te maken dat de verplichtingen op grond van de AVG rondom het inzetten van een verwerker worden nageleefd om audits mogelijk te maken.
- de verwerker maakt afspraken met eventuele sub-verwerkers.

4. Maatregelen voor naleving AVG

In paragraaf 3.1 is genoemd welke maatregelen de verwerkingsverantwoordelijke moet nemen om aan te tonen dat zij aan de plichten van de AVG voldoet. Deze maatregelen worden hieronder verder uitgelegd.

4.1 Registerplicht

Wanneer de verwerking van persoonsgegevens een risico voor de betrokkenen met zich mee kan brengen, wanneer de verwerking structureel (dus niet-incidenteel) is of wanneer er sprake is van bijzondere categorieën van persoonsgegevens, moet de organisatie een register bijhouden. In het register moeten de volgende zaken opgenomen worden:

- naam en contactgegevens van organisatie.
- contactgegevens van eventuele functionaris voor gegevensbescherming.
- verwerkingsdoeleinden.
- beschrijving van categorieën van betrokkenen en van persoonsgegevens.
- categorieën van ontvangers aan wie de persoonsgegevens worden verstrekt.
- indien mogelijk, de beoogde termijn waarbinnen de gegevens moeten worden gewist.
- indien mogelijk, een algemene beschrijving van de technische en organisatorische beveiligingsmaatregelen.

Het register geeft dus inzicht in de verwerkingsactiviteiten. Het bevat niet de persoonsgegevens zelf. Verder moet het register altijd actueel zijn. Wanneer bijvoorbeeld het doel van de verwerking verandert, moet dit opgenomen worden in het register. De Autoriteit Persoonsgegevens en de eventuele functionaris voor gegevensbescherming moeten toegang kunnen krijgen tot het register.

4.2 Functionaris voor gegevensbescherming

De functionaris voor gegevensbescherming houdt intern toezicht op en adviseert over de toepassing en naleving van de AVG. Een functionaris is slechts in een aantal gevallen verplicht (zie paragraaf 5.4 van de 'Handleiding Algemene Verordening Gegevensbescherming').

Zorgboerderijen/zorgkwekerijen vallen niet onder deze verplichting en hoeven dus geen functionaris aan te stellen.

4.3 Gegevensbeschermingseffectbeoordeling

De verwerking van persoonsgegevens kan een hoog risico met zich meebrengen voor de rechten en vrijheden van de betrokkenen. Wanneer daarvan sprake is, moet voorafgaand aan de verwerking van de persoonsgegevens een gegevensbeschermingseffectbeoordeling uitgevoerd worden. Dit is een instrument waarmee de effecten voor betrokkenen op een gestructureerde manier in kaart gebracht en beoordeeld worden. Er is sprake van hoog risico wanneer de verwerking aan twee of meer van onderstaande criteria voldoet:

- evaluatie van personen of scoretoekenning.
- geautomatiseerde besluitvorming met rechtsgevolg of vergelijkbaar wezenlijk gevolg.
- stelselmatige monitoring.
- gevoelige gegevens of gegevens van zeer persoonlijke aard.
- op grote schaal verwerkte gegevens.
- matching of samenvoeging van datasets.
- gegevens met betrekking tot kwetsbare betrokkenen.
- innovatieve toepassing van nieuwe technologische of organisatorische oplossing.
- blokkering van een recht, dienst of contract.

Bij de beoordeling van de risico's voor de betrokkene moeten de volgende omstandigheden meegenomen worden:

- de aard van de voorgenomen gegevensverwerking.
- de omvang, context en doelen van de verwerking.
- de bronnen van de risico's.

Het doel van de gegevensbeschermingseffectbeoordeling is om te onderzoeken welke maatregelen nog genomen kunnen worden om het risico voor de betrokkenen te verkleinen. Van de gegevensbeschermingseffectbeoordeling dient vervolgens een verslag gemaakt te worden waarin de volgende zaken naar voren komen:

- een beschrijving van de beoogde verwerking en de doelen voor die verwerking.
- een oordeel over de noodzakelijkheid van de verwerking.
- een oordeel over de risico's voor de betrokkenen.
- de beoogde veiligheidsmaatregelen om de risico's voor betrokkenen te beperken.

4.4 Voorafgaande raadpleging

Wanneer niet voldoende maatregelen genomen kunnen worden om de risico's voor de betrokkenen te beperken, moet de verwerkingsactiviteit eerst voorgelegd worden aan de Autoriteit Persoonsgegevens. De verwachting is dat hiervan geen sprake zal zijn bij zorgboerderijen/zorgkwekerijen. Wanneer een zorgboerderij/zorgkwekerij toch een voorafgaande raadpleging wil doen, wordt hiervoor verwezen naar paragraaf 5.6 van de 'Handleiding Algemene Verordening Gegevensbescherming'.

4.5 Privacy door ontwerp en standaardinstellingen

De privacy van de betrokkenen moet zoveel mogelijk gewaarborgd blijven. Om die reden moet bij het bepalen van de verwerkingsmiddelen rekening gehouden worden met de volgende elementen:

- de techniek.
- de uitvoeringskosten.
- de aard, omvang, context en het doel van de verwerking.
- de risico's voor de betrokkene.

4.6 Beveiligingseisen

De persoonsgegevens die verwerkt worden, moeten beveiligd worden. Maatregelen om dat te doen zijn bijvoorbeeld:

- pseudonimisering en versleuteling van de persoonsgegevens.
- het vermogen om op permanente basis de vertrouwelijkheid, integriteit, beschikbaarheid en veerkracht van de verwerkingssystemen en diensten te garanderen.
- het vermogen om bij een incident de beschikbaarheid en toegang tot de persoonsgegevens te herstellen.
- een procedure voor het op gezette tijdstippen testen, beoordelen en evalueren van de doeltreffendheid van de maatregelen ter beveiliging van de persoonsgegevens.

Technische maatregelen zijn bijvoorbeeld het toepassen van encryptie (geheime code), het opzetten van een firewall (een systeem dat de computer kan beschermen tegen misbruik van buitenaf) of het opslaan van gegevens in een beveiligde omgeving. Een voorbeeld van een organisatorische maatregel is het beperken van de toegang tot gegevens voor bepaalde medewerkers.

4.7 Melden van inbreuk

Wanneer zich een inbreuk op de persoonsgegevens, ook wel datalek genoemd, heeft plaatsgevonden, moet dit binnen 72 uur na ontdekking gemeld worden aan de Autoriteit Persoonsgegevens. In principe moet iedere datalek gemeld worden. Echter, wanneer de datalek geen risico inhoudt voor de rechten en vrijheden van de betrokkene, is er geen meldplicht. Wanneer het datalek een hoog risico vormt voor de betrokkenen, moeten zij ook geïnformeerd worden, naast de Autoriteit Persoonsgegevens. Er mag enige tijd genomen worden om te bepalen of de betrokkenen geïnformeerd moeten worden. Dit hoeft dus niet binnen 72 uur te gebeuren. Verder moet het datalek gerapporteerd worden. Onderstaande informatie moet verstrekt worden bij een melding:

Informatie aan de Autoriteit Persoonsgegevens:

- de aard en omvang van de inbreuk.
- waar mogelijk de categorieën en het aantal van betrokkenen en de gegevensregisters waar het om gaat.
- de naam en contactgegevens van de functionaris voor gegevensbescherming of een ander contactpunt waar meer informatie kan worden verkregen.
- de waarschijnlijke gevolgen van de inbreuk in verband met persoonsgegevens.
- de maatregelen die de organisatie heeft voorgesteld of heeft genomen om de inbreuk aan te pakken en de maatregelen die de organisatie wil nemen ter beperking van de eventuele nadelige gevolgen daarvan.

Bovenstaande informatie moet ook aan de betrokkenen gegeven worden wanneer de organisatie heeft besloten het datalek ook te melden bij de betrokkenen. Alleen het tweede punt hoeft niet gemeld te worden aan de betrokkenen.

4.8 Afspraken met verwerkers

Wanneer persoonsgegevens door verwerkers worden verwerkt, moet de verwerkingsverantwoordelijke met hen een verwerkersovereenkomst sluiten. In paragraaf 3.3 is te lezen welke informatie opgenomen moet worden in de overeenkomst.

5. Betrokkenen

De betrokkenen bij persoonsgegevens hebben de volgende rechten:

- het recht op informatie over de verwerkingen.
- het recht op inzage in zijn/haar gegevens.
- het recht op correctie van de gegevens als deze niet kloppen.
- het recht op verwijdering van de gegevens en 'het recht om vergeten te worden'.
- het recht op beperking van de gegevensverwerking.
- het recht op verzet tegen de gegevensverwerking.
- het recht op overdracht van zijn/haar gegevens.
- het recht om niet onderworpen te worden aan een geautomatiseerde besluitvorming.

De verwerkingsverantwoordelijke geeft gehoor aan deze rechten, tenzij de verzoeken van de betrokkene kennelijk ongegrond of buitensporig zijn (bijvoorbeeld wanneer de betrokkene heel vaak achter elkaar exact hetzelfde vraagt). De rechten van de betrokkene moeten altijd gerespecteerd worden. De AVG geeft een aantal uitzonderingen waarbij de rechten van de betrokkenen beperkt mogen worden. Voor zorgboerderijen/zorgkwekerijen zou de volgende uitzondering in bepaalde gevallen kunnen gelden: het beperken van de rechten van de betrokkene is noodzakelijk ter waarborging van de bescherming van de betrokkene of van de rechten of vrijheden van anderen.

De verwerkingsverantwoordelijke moet de uitvoering van bovenstaande rechten faciliteren en mag de uitoefening daarvan niet bemoeilijken. Verder mogen geen kosten in rekening gebracht worden voor het uitoefenen van deze rechten, tenzij het gaat om ongegronde of buitensporige verzoeken zoals hierboven beschreven.

Binnen een maand na ontvangst van het verzoek moet de betrokkene geïnformeerd worden over de uitvoering van het verzoek. Ook wanneer de organisatie geen gehoor geeft aan het verzoek van de betrokkene moet dit binnen een maand kenbaar gemaakt worden. Een weigering moet wel gemotiveerd worden en daarbij met de betrokkene gewezen worden op het klachtrecht. Wanneer het om veel of complexe verzoeken gaat, mag de organisatie twee maanden extra de tijd nemen en de betrokkene hierover binnen een maand na ontvangst van het verzoek informeren.

Informatie die gegeven wordt aan de betrokkene moet begrijpelijk zijn en het liefst schriftelijk (mag ook elektronisch) gegeven worden. Wanneer de betrokkene daarom vraagt, mag de informatie ook mondeling gegeven worden.

Wanneer de betrokkene het niet eens is met het besluit van de organisatie om al dan niet aan het verzoek gehoor te geven, kan de betrokkene naar de rechter stappen. De rechter kan de organisatie alsnog bevelen uitvoering te geven aan het verzoek. Daarnaast kan de betrokkene zich wenden tot de Autoriteit Persoonsgegevens. Zie hoofdstuk 7 voor meer uitleg over de Autoriteit Persoonsgegevens.

6. Recht op informatie

6.1 Informatieplicht

De verwerkingsverantwoordelijke heeft de plicht om de betrokkenen te informeren over de gegevensverwerkingen. Zij hebben het recht te weten wat er met hun persoonsgegevens gebeurt en waarom. Ook moeten zij bewust worden gemaakt van de risico's van de gegevensverwerking, de regels die ervoor gelden, de waarborgen en de manier waarop zij hun rechten kunnen uitoefenen.

Wanneer de organisatie persoonsgegevens verwerkt, heeft zij altijd informatieplicht. De AVG maakt onderscheid tussen twee situaties, namelijk:

- de gegevens worden bij de betrokkene zelf verzameld.
- de gegevens worden buiten de betrokkene om verkregen.

In beide situaties geldt de informatieplicht.

6.2 Uitzonderingen op de informatieplicht

Wanneer de organisatie de gegevens bij de betrokkene zelf verzamelt, hoeft zij de betrokkene niet te informeren wanneer deze al over de benodigde informatie beschikt. De organisatie moet hier dan wel zeker van zijn.

Wanneer de organisatie de gegevens buiten de betrokkene om heeft verkregen, hoeft zij de betrokkene in de volgende situaties niet te informeren:

- de betrokkene is al geïnformeerd door de oorspronkelijke verantwoordelijke dat de gegevens naar de huidige verantwoordelijke doorgestuurd worden.
- de informatieverstrekking aan de betrokkene blijkt onmogelijk of vergt een onevenredige inspanning.
- de verkrijging of verstrekking van de persoonsgegevens is uitdrukkelijk bij wet voorgeschreven en in die wet zijn de gerechtvaardigde belangen van de betrokkene gewaarborgd.
- de persoonsgegevens moeten vertrouwelijk blijven in verband met een beroepsgeheim.

6.3 Informatieverstrekking

Wanneer de organisatie de gegevens bij de betrokkene zelf verzamelt, moet zij op het moment van verkrijging van de gegevens de volgende informatie verstrekken:

- de identiteit en contactgegevens van de organisatie of van haar vertegenwoordiger.
- de contactgegevens van de eventuele functionaris voor gegevensbescherming.
- de doelen waarvoor persoonsgegevens worden verwerkt.
- de grondslag waarop de verwerking is gebaseerd.
- wat het gerechtvaardigd belang is wanneer de verwerking is gebaseerd op deze grondslag.
- de eventuele ontvangers van de gegevens.
- in geval van verstrekking aan derde landen:
 - of er een adequaatheidsbesluit van de Commissie bestaat,
 - of passende waarborgen zijn getroffen, welke dit zijn en of hier een kopie van kan worden verkregen, dan wel waar die waarborgen kunnen worden geraadpleegd.
- de bewaartermijn of als dat niet mogelijk is de criteria voor het bepalen ervan.
- de rechten van de betrokkene.

- in het geval van toestemming, dat de betrokkene die toestemming geeft dit altijd weer kan intrekken.
- dat de betrokkene het recht heeft een klacht in te dienen over de verwerking bij de Autoriteit Persoonsgegevens.
- of het verwerken van persoonsgegevens een wettelijke verplichting is of noodzakelijk is voor de uitvoering of het aangaan van een overeenkomst, of de betrokkene verplicht is die gegevens te verstrekken en wat de gevolgen zijn van het niet verstrekken van de gegevens voor de betrokkene.
- ingeval van geautomatiseerde besluitvorming, nuttige informatie over de onderliggende logica, het belang van de verwerking en de verwachte gevolgen van die verwerking voor de betrokkene.

Wanneer de organisatie de gegevens buiten de betrokkene om verzamelt, moet dezelfde informatie als hierboven beschreven verstrekt worden. Daar wordt aan toegevoegd, uit welke bron de persoonsgegevens zijn verkregen. De informatie moet binnen een redelijke termijn na ontvangst van de gegevens aan de betrokkene gegeven worden, in ieder geval binnen een maand.

Wanneer de organisatie aanvullende informatie wil verstrekken om meer duidelijkheid of transparantie te bieden, is dit mogelijk. Wanneer de persoonsgegevens voor andere doelen verwerkt gaan worden, moeten de betrokkenen opnieuw geïnformeerd worden.

6.4 Inzage

Iedere betrokkene heeft het recht om de persoonsgegevens die van hem/haar verzameld zijn in te zien. Een betrokkene mag daarom met redelijke tussenpozen aan de organisatie vragen of, en zo ja welke, persoonsgegevens zij van hem/haar verwerkt. De organisatie is verplicht om gehoor te geven aan deze verzoeken en de beschikbare informatie te verstrekken. De betrokkene mag ook om een kopie van de persoonsgegevens vragen.

Bij het verstrekken van de gegevens moet de organisatie zich ervan vergewissen dat de betrokkene daadwerkelijk degene is op wie de gegevens betrekking hebben. Ook moet rekening gehouden worden met de privacy van anderen. Verstrek niet per ongeluk ook gegevens van anderen.

6.5 Verwijdering van gegevens

De betrokkene heeft het recht om zijn/haar gegevens zo snel mogelijk door de organisatie te laten wissen in één van de volgende gevallen:

- de persoonsgegevens zijn niet langer nodig voor de doeleinden waarvoor zij zijn verzameld of verwerkt.
- de betrokkene trekt zijn/haar toestemming voor het verwerken in en dit is de enige grondslag waarop de verwerking kan berusten.
- de betrokkene heeft gegrond bezwaar gemaakt tegen de verwerking.
- de persoonsgegevens zijn onrechtmatig verwerkt.
- de persoonsgegevens moeten worden gewist om te voldoen aan een wettelijke verplichting die op de organisatie rust.

6.6 Het recht om vergeten te worden

Naast het recht op verwijdering heeft de betrokkene onder bepaalde omstandigheden ook het recht om 'vergeten te worden'. Het gaat dan om situaties waarbij de persoonsgegevens openbaar zijn gemaakt (bijvoorbeeld door ze online te zetten) en de betrokkene wil dat deze gewist worden. De organisatie moet dan de gegevens wissen en daarmee iedere koppeling naar een kopie of reproductie.

Het recht op verwijdering en het recht om vergeten te worden gelden voor iedereen, maar wegen in het bijzonder zwaar bij de verwerking van gegevens van kinderen. Wanneer de gegevens op verzoek van de betrokkene verwijderd zijn, moet de organisatie de betrokkene meedelen dat de gegevens daadwerkelijk verwijderd zijn, tenzij dit onmogelijk blijkt of onevenredige inspanning vergt.

Uitzonderingen op het recht op verwijdering en het recht om vergeten te worden zijn wanneer de verwerking nodig is voor het uitoefenen van het recht op vrijheid van meningsuiting en informatie en als het nakomen van een wettelijke verwerkingsverplichting op de organisatie rust. De AVG geeft nog een aantal uitzonderingen op het recht op verwijdering en het recht om vergeten te worden. Deze gelden echter niet voor zorgboerderij/zorgwekerijen. Hiervoor wordt verwezen naar paragraaf 7.5.3 van de 'Handleiding Algemene Verordening Gegevensbescherming'.

6.7 Beperking van gegevensverwerking

De betrokkene heeft de mogelijkheid om de verwerking van persoonsgegevens tijdelijk 'stil te laten zetten'. De betrokkene kan dit inzetten in de volgende situaties:

- de juistheid van de persoonsgegevens wordt betwist door de betrokkene, gedurende een periode die de verwerkingsverantwoordelijke in staat stelt om de juistheid te controleren.
- de verwerking is onrechtmatig en de betrokkene verzoekt om een beperking van het gebruik in plaats van het verwijderen van de persoonsgegevens.
- de verwerkingsverantwoordelijke heeft de persoonsgegevens niet meer nodig voor de verwerkingsdoeleinden, maar voor de instelling, uitoefening of onderbouwing van een rechtsvordering.
- de betrokkene heeft bezwaar gemaakt tegen de verwerking, in afwachting van het antwoord op de vraag of de gerechtvaardigde gronden van de verwerkingsverantwoordelijke zwaarder wegen dan die van de betrokkene.

6.8 Het recht op verzet

Een betrokkene kan bezwaar maken tegen de (verdere) verwerking van zijn/haar gegevens en het recht op verzet invoeren. De verwerkingsverantwoordelijke moet de verwerkingen dan staken. De betrokkene kan dit recht in de volgende situaties invoeren:

- de betrokkene kan vanwege persoonlijke omstandigheden bezwaar maken tegen verwerkingen die gebaseerd zijn op de grondslagen algemeen belang, openbaar gezag of gerechtvaardigd belang.
- de betrokkene kan bezwaar maken tegen de verwerking van persoonsgegevens met het oog op direct marketing.
- de betrokkene kan bezwaar maken tegen de verwerking van persoonsgegevens voor wetenschappelijk of historisch onderzoek of voor statistische doeleinden.

7. Toezicht

De Autoriteit Persoonsgegevens (AP) houdt toezicht op de naleving van de privacywetgeving. Zij doet onderzoek, adviseert over nieuwe regelgeving en reageert op tips of klachten die zij krijgt van organisaties of betrokkenen.

Verwerkers en/of de verwerkingsverantwoordelijke moeten volledige medewerking verlenen wanneer de Autoriteit Persoonsgegevens een onderzoek doet bij de organisatie. De organisatie moet, als de AP daarom vraagt, ook toegang verlenen tot de persoonsgegevens en de middelen die gebruikt worden voor de verwerking van persoonsgegevens.

Wanneer een organisatie zich niet houdt aan de AVG, kan zij daarvoor een administratieve boete of een andere sanctie krijgen. Ook kan de organisatie aansprakelijk worden gesteld voor eventuele schade en is zij verplicht een schadevergoeding te geven aan de betrokkene.

In principe is de verwerkingsverantwoordelijke aansprakelijk. Een verwerker is alleen aansprakelijk als zij niet heeft voldaan aan de verplichtingen van de AVG of als zij in strijd heeft gehandeld met de afspraken die zijn gemaakt met de verwerkingsverantwoordelijke.

8. Toepassing voor Zorgkwekerij Bloei

In dit hoofdstuk zijn de bepalingen in de AVG toegepast op Zorgkwekerij Bloei. Hierbij wordt regelmatig verwezen naar de bijlagen bij dit protocol.

8.1 Grondslagen

Zorgkwekerij Bloei verwerkt persoonsgegevens van haar cliënten. Onder cliënten worden de mensen verstaan die dagbesteding afnemen, (verder genoemd hulpkwekers) en hun ouders/wettelijke verzorgers (verder genoemd verzorgers). De gegevens worden over het algemeen verwerkt op basis van de grondslag 'toestemming'. De zorgkwekerij vraagt via een formulier toestemming aan alle verzorgers voor het verwerken van de persoonsgegevens van hun en de hulpkweker. Dit formulier is toegevoegd als bijlage 1. De verzorgers krijgen bij dit toestemmingsformulier ter informatie het document 'Uitleg Persoonsgegevens', zie bijlage 2. Het kan in geval van medische nood voorkomen dat Zorgkwekerij Bloei persoonsgegevens moet verwerken op basis van de grondslag 'vitale belangen'. Verder baseert Zorgkwekerij Bloei zich in bepaalde gevallen op de grondslag 'overeenkomst'.

De persoonsgegevens die verwerkt worden, zijn afkomstig uit de volgende bronnen.

- Intakeformulieren
- Zorgovereenkomst
- Beschikking
- Verslagen van bijvoorbeeld onderzoeken
- Extra gegeven informatie door de ouders/verzorgers/begeleiders.

De persoonsgegevens bestaan uit contactgegevens en bijzondere gegevens die door de verzorgers gegeven worden en observaties die eventueel door de medewerkers van Zorgkwekerij Bloei worden gedaan.

8.2 Bijzondere persoonsgegevens

Zorgkwekerij Bloei verwerkt de volgende gegevens die vallen onder bijzondere persoonsgegevens. Zij verwerkt religieuze gegevens van cliënten op basis van toestemming van de verzorgers. Deze religieuze gegevens zijn nodig om de zorg te leveren die de hulpkwekers nodig hebben en rekening te kunnen houden met speciale wensen omtrent bijvoorbeeld voedsel. Verder verwerkt Zorgkwekerij Bloei genetische gegevens wanneer deze informatie gegeven is door de verzorgers en hiervoor toestemming gegeven is. Het gaat om genetische gegevens waaruit blijkt welke beperking en hulpvraag de hulpkweker heeft, zodat de zorgkwekerij adequate hulp kan bieden. Dit geldt ook over gegevens wat betreft de gezondheid van de hulpkweker. Wanneer een hulpkweker bijvoorbeeld astma heeft, is het noodzakelijk dit te weten, zodat de begeleiding medicatie hiervoor kan toedienen, waarvoor overigens ook toestemming en opdracht is gegeven door verzorgers. Strafrechtelijke gegevens worden in principe niet verwerkt. Wel komt het voor dat in een gezin sprake is van bijvoorbeeld een uithuisplaatsing. Zorgkwekerij Bloei moet dit weten voor het contact met de hulpkwekers, de biologische ouders en de huidige verzorgers. Dit alles wordt slechts verwerkt wanneer verzorgers daarvoor toestemming hebben gegeven via het toestemmingsformulier in bijlage 1.

Van alle hulpkwekers wordt het Burgerservicenummer opgeslagen in het papieren en digitale cliëntdossier en op de facturen. Sommige gemeentes wensen in het mailcontact over cliënten niet de naam te gebruiken, maar alleen het Burgerservicenummer.

8.3 Verwerkingsverantwoordelijke en verwerker

Bij Zorgkwekerij Bloei is Marjolein de verwerkingsverantwoordelijke.

De gediplomeerde en ervaren begeleiders van Zorgkwekerij Bloei houden zich bezig met verslaglegging en dossiervorming. De verwerkingsverantwoordelijke sluit met de verwerker een verwerkerovereenkomst. Zie hiervoor bijlage 3. De verwerkingsverantwoordelijke geeft de verwerker opdracht tot het verwerken van persoonsgegevens. Zie hiervoor bijlage 4.

8.4 Register van verwerkingsactiviteiten en gegevensbeschermingseffectbeoordeling

Zorgkwekerij Bloei slaat niet-incidenteel gegevens op en slaat gegevens op van bijzondere aard. Dit maakt dat de verwerking van persoonsgegevens risicovol is. Verder gaat het om gegevens van hulpkwekers. Daar moet voorzichtig mee omgegaan worden. Om die reden houdt Zorgkwekerij Bloei een register van verwerkingsactiviteiten bij. Deze is bij dit protocol toegevoegd als bijlage 5. Om dezelfde reden heeft Zorgkwekerij Bloei een gegevensbeschermingseffect beoordeling uitgevoerd. Deze is beschreven in bijlage 6.

8.5 Beveiligingsmaatregelen

Onderstaande maatregelen zijn getroffen om ervoor te zorgen dat persoonsgegevens op een veilige manier verwerkt en bewaard worden.

- De papieren cliëntdossiers worden bewaard in een kast met een slot erop. De sleutel is alleen bereikbaar voor medewerkers van Zorgkwekerij Bloei.
- Alleen de verwerkingsverantwoordelijke en de verwerkers van Zorgkwekerij Bloei hebben toegang tot het digitale cliëntdossier door middel van een eigen wachtwoord.
- Op de laptops waar begeleidingsplannen en evaluatieverslagen opgeslagen zijn, staat een wachtwoord die alleen bekend is bij de verwerkingsverantwoordelijke en verwerkers.
- Wanneer de laptops niet gebruikt worden, worden zij bewaard in een kast die op slot kan.
- In mailcontact naar gemeentes worden namen van cliënten enigszins gepseudonimiseerd, namelijk door alleen de voorletter en vervolgens de achternaam te geven.
- In het arbeidscontract met de medewerkers is opgenomen dat zij geheimhoudingsplicht hebben. Wanneer zij zich daar niet aan houden, krijgen zij een boete.

Deze beveiligingsmaatregelen zijn ook opgenomen in het register van verwerkingsactiviteiten, zie bijlage 5.

8.6 Rechten van betrokkenen

Zorgkwekerij Bloei volgt de bepalingen aangaande de rechten van betrokkenen. Zo zal zij bijvoorbeeld inzage geven in de persoonsgegevens wanneer daarom gevraagd wordt door de betrokkene. Daarbij moet gezegd worden dat de cliënten van Zorgkwekerij Bloei uit twee categorieën bestaan, namelijk de hulpkwekers en diens wettelijke verzorgers.

8.7 Omgang met datalek

Wanneer zich een datalek van persoonsgegevens heeft voorgedaan en dit een risico vormt voor de betrokkenen, wordt dit door de verwerkingsverantwoordelijke gemeld bij de Autoriteit Persoonsgegevens via de website www.autoriteitpersoonsgegevens.nl (klik op het tabblad 'Tip ons'). Wanneer een verwerker of een ander personeelslid betrokken was bij het datalek, vult zij samen met de verwerkingsverantwoordelijke de melding in. Daarvoor wordt bijlage 7 gebruikt. De melding wordt gedaan binnen 72 uur na ontdekking van het datalek.

Wanneer geen risico bestaat voor de betrokkene, wordt er geen melding gedaan bij de Autoriteit Persoonsgegevens. Wanneer het datalek een hoog risico vormt voor de betrokkenen, worden naast de Autoriteit Persoonsgegevens ook de betrokkenen geïnformeerd. Zij krijgen dezelfde informatie, uit bijlage 7. De betrokkenen hoeven niet binnen 72 uur na ontdekking van het datalek geïnformeerd worden.

Het al dan niet melden van een datalek wordt bepaald door de verwerkingsverantwoordelijke en de verwerkers. Het datalek wordt ten alle tijden gerapporteerd, ook als deze niet gemeld wordt. De rapportage vindt plaats in het FOBO en in het digitale cliëntdossier.

Bijlage 1 Toestemmingsformulier Persoonsgegevens



Op onze Zorgkwekerij Bloei worden verschillende persoonsgegevens verwerkt voor verschillende doeleinden. De twee belangrijkste doeleinden zijn de volgende: het opslaan van contactgegevens om snel contact op te kunnen nemen wanneer er een vraag is over de hulpkweker en het opslaan van bijzondere gegevens/observaties om de hulpkweker adequate begeleiding te kunnen bieden. Behalve de observaties zijn alle gegevens die door de zorgkwekerij verwerkt worden, door u verstrekt. Via die weg heeft u toestemming gegeven om deze persoonsgegevens te verwerken. Echter, volgens de nieuwe wet 'Algemene Verordening Gegevensbescherming' die op 25 mei 2018 ingaat, moet deze toestemming schriftelijk gegeven worden. Via dit toestemmingsformulier vragen wij u toestemming te geven voor het verwerken van onderstaande persoonsgegevens.

Persoonsgegevens die komen uit onderstaande bronnen:

- Intakeformulieren
- Zorgovereenkomst
- Beschikking
- Verslagen van bijvoorbeeld onderzoeken
- Extra gegeven informatie door de ouders/verzorgers
- Observaties van de hulpkweker door de begeleiding

Deze persoonsgegevens worden verwerkt in de volgende documenten:

- Begeleidingsplan
- Evaluatieverslag
- Bijzonderhedenlijst
- Digitaal en papieren cliëntdossier
- Observaties in digitaal rapportagesysteem
- Mailcontact naar de betrokkenen bij de hulpkweker

Doelen voor het verwerken van persoonsgegevens:

- Identificeren van de persoon
- Snel contact op kunnen nemen bij vragen over hulpkweker
- Adequaet kunnen begeleiden van hulpkweker
- Evalueren van de ontwikkeling/groei van hulpkweker

Ik geef toestemming voor het verwerken van bovenstaande persoonsgegevens door de medewerkers van Zorgkwekerij Bloei.

Datum: _____

Naam: _____

Handtekening ouder/verzorger: _____

Bijlage 2 Uitleg Persoonsgegevens

Zorgkwekerij Bloei
Marjolein de Hoog
Europalaan 18
2641 RX Pijnacker
06-51352696

www.zorgkwekerijbloei.nl



Zoals u in het Toestemmingsformulier Persoonsgegevens kunt lezen, worden verschillende gegevens van de hulpkweker op onze Zorgkwekerij Bloei verwerkt. De meeste gegevens worden door uzelf aan ons verstrekt. Daarnaast worden door de begeleiders van Zorgkwekerij Bloei observaties gedaan die opgeslagen worden in ons rapportagesysteem. Via dit document geven wij u meer informatie over het verwerken van deze persoonsgegevens.

Het verwerken van de persoonsgegevens is nodig voor het aangaan van een overeenkomst met u, zodat wij zorg kunnen leveren aan de hulpkweker. Wanneer bijvoorbeeld de zorgovereenkomst niet is ingevuld, kunnen wij geen zorg leveren. Specifieke doelen voor het verwerken van persoonsgegevens kunt u terugzien op het Toestemmingsformulier Persoonsgegevens.

De Wet 'Algemene Verordening Gegevensbescherming' geeft zes grondslagen waarop een organisatie persoonsgegevens mag verwerken. Eén van die grondslagen is 'toestemming'. Zorgkwekerij Bloei hanteert deze grondslag. Zij verwerkt gegevens dus wanneer zij daar toestemming voor heeft gekregen van de wettelijke verzorgers van de hulpkweker. Dit kunt u doen door het Toestemmingsformulier Persoonsgegevens te ondertekenen.

In contact met de gemeente wat betreft de beschikking worden contactgegevens van de hulpkweker gedeeld. Deze gegevens zijn via u ook al bekend bij de gemeente. Begeleidingsplannen en evaluatieverslagen waarin de ontwikkeling beschreven staat, worden niet aan andere instanties gedeeld. Wanneer een Sociaal Team een dergelijk verslag nodig heeft, stuurt u deze zelf naar hen op. Rapportages naar aanleiding van observaties zijn alleen toegankelijk voor Marjolein en de zogenoemde verwerkers van Zorgkwekerij Bloei. Dit zijn de gediplomeerde, ervaren begeleiders die de rapportages schrijven. Verder worden gegevens van u en de hulpkweker alleen aan andere betrokkenen gegeven wanneer u daarvoor toestemming heeft gegeven in het Contactformulier dat is bijgevoegd bij de zorgovereenkomst.

U heeft het recht een verzoek tot inzage of verwijdering van gegevens in te dienen bij Marjolein. Zorgkwekerij Bloei moet dit verzoek respecteren en inzage in gegevens bieden of gegevens verwijderen wanneer daarom gevraagd wordt. In bepaalde gevallen bestaat daarop een uitzondering, namelijk wanneer de bescherming van de hulpkweker of de rechten of vrijheden van anderen in het geding komen wanneer we de gegevens delen of verwijderen. Als dat zo is, krijgt u daar uitleg van. Verder mag u de toestemming tot het verwerken van persoonsgegevens weer intrekken.

Wanneer u een klacht heeft over de verwerking van de gegevens, kunt u de klachtenprocedure van Zorgkwekerij Bloei volgen. Daarnaast kunt u een klacht ook indienen bij de Autoriteit Persoonsgegevens. Hiervoor verwijzen wij u naar de website www.autoriteitpersoonsgegevens.nl, waar u rechts bovenin het scherm kunt klikken op 'Tip ons'.

Bijlage 3 Verwerkersovereenkomst



Naam verwerkingsverantwoordelijke: Marjolein de Hoog

Naam verwerker: _____

Algemene afspraken tussen verwerkingsverantwoordelijke en verwerker:

- de verwerker verwerkt de persoonsgegevens alleen onder de schriftelijke instructies van de verwerkingsverantwoordelijke.
- de verwerker waarborgt dat de toegang tot de gegevens beperkt is tot gemachtigde personen, namelijk de medewerkers van Zorgkwekerij Bloei die de hulpkwekers begeleiden. Deze medewerkers hebben geheimhouding, die gewaarborgd is in het arbeidscontract.
- de verwerker hanteert hetzelfde niveau van beveiliging voor persoonsgegevens als de verwerkingsverantwoordelijke.
- de verwerkingsverantwoordelijke biedt alle mogelijke ondersteuning bij het nakomen van de verplichtingen van de verwerker met het oog op beantwoording van verzoeken rondom de rechten van betrokkenen.
- de verwerker staat de verwerkingsverantwoordelijke bij wat betreft het nakomen van de verplichtingen op het gebied van beveiliging van persoonsgegevens en de meldplicht datalekken.
- na beëindiging van deze overeenkomst, wist de verwerker de persoonsgegevens of geeft deze aan de verwerkingsverantwoordelijke terug.
- de verwerker stelt alle informatie ter beschikking die nodig is om aantoonbaar te maken dat de verplichtingen op grond van de AVG rondom het inzetten van een verwerker worden nageleefd om audits mogelijk te maken.
- de verwerker maakt afspraken met eventuele sub-verwerkers.

Specifieke afspraken tussen verwerkingsverantwoordelijke en verwerker:

- onderwerp van verwerking: contactgegevens en bijzondere persoonsgegevens van de cliënt en gedane observaties van de cliënt.
- aard en doel van verwerking: het op adequate wijze kunnen begeleiden van de cliënt.
- soort persoonsgegevens en categorieën van betrokkenen: contactgegevens en bijzondere persoonsgegevens uit de intakeformulieren en gedane observaties van de cliënt. Betrokkenen zijn de hulpkwekers die in zorg zijn en hun wettelijke verzorgers.
- rechten en verplichtingen van de verwerkingsverantwoordelijke: de verwerkingsverantwoordelijke geeft opdracht aan de verwerkers om persoonsgegevens te verwerken. Zij heeft het recht om hen op de uitvoering en veiligheid hiervan te controleren. Verder heeft zij de plicht hen de mogelijkheden te bieden hun taken goed en veilig uit te kunnen voeren.

Datum: _____

Handtekening verwerkingsverantwoordelijke

Handtekening verwerker

Bijlage 4 Instructie voor verwerker



Bij deze geeft verwerkingsverantwoordelijke Marjolein de Hoog – van Elst
_____ (naam verwerker) de opdracht om de volgende
persoonsgegevens te verwerken:

- contactgegevens in het digitale en papieren cliëntdossier. Zie hiervoor de intakeformulieren, de beschikking/verwijzing en de extra informatie die de verzorgers van de cliënten geven.
- contactgegevens en bijzondere gegevens in het begeleidingsplan en evaluatieverslag die opgeslagen worden in het digitale cliëntdossier. Het gaat om gegevens die door de verzorger verstrekt zijn. Verder worden observaties van de cliënten beschreven in het begeleidingsplan en het evaluatieverslag.
- observaties van de cliënten in het digitale rapportagesysteem (cliëntdossier).
- contactgegevens en observaties van de cliënten in mailcontact met betrokkenen in het gezin.

Voor het verwerken van bovenstaande gegevens is toestemming gegeven door de verzorgers van de cliënt.

Datum: _____

Handtekening verwerkingsverantwoordelijke:

Handtekening verwerker:

Bijlage 5 Register van verwerkingsactiviteiten



Contactgegevens organisatie

Zorgkwekerij Bloei
Europalaan 18
2641 RX Pijnacker
06-51352696

marjolein@zorgkwekerijbloei.nl
www.zorgkwekerijbloei.nl

Verwerkingsdoeleinden

Zorgkwekerij Bloei hanteert de volgende verwerkingsdoeleinden:

- Identificeren van de persoon
- Snel contact op kunnen nemen bij vragen over de cliënt
- Adequaaf kunnen begeleiden van de cliënt
- Evalueren van de ontwikkeling van de cliënt
- Overleg plegen met de betrokkenen in het gezin ter bevordering van de hulpverlening aan de cliënt, wanneer dit nodig is.

Betrokkenen

De betrokkenen zijn de personen van wie gegevens verwerkt worden, namelijk:

- Hulpkwekers bij Zorgkwekerij Bloei
- De ouders/wettelijke verzorgers van de hulpkwekers bij Zorgkwekerij Bloei

Persoonsgegevens

De persoonsgegevens komen uit onderstaande bronnen.

- Intakeformulieren
- Zorgovereenkomst
- Beschikking
- Verslagen van bijvoorbeeld onderzoeken
- Extra gegeven informatie door de ouders/verzorgers
- Observaties

De persoonsgegevens voortkomend uit bovenstaande bronnen kunnen ook bijzondere persoonsgegevens bevatten, zoals genetische gegevens, gegevens over religie, gegevens over gezondheid, gegevens met betrekking tot iemands seksueel gedrag. Deze gegevens worden door de verzorgers van de cliënt gegeven en zij hebben Zorgkwekerij Bloei toestemming gegeven voor het verwerken van deze gegevens.

Ontvangers

De persoonsgegevens worden verstrekt aan de eigenaar van Zorgkwekerij Bloei, namelijk Marjolein de Hoog – van Elst. Verder worden ze ontvangen door de verwerkers die in hoofdstuk 8 van het Protocol AVG genoemd zijn. Wanneer daar aanleiding voor is, kunnen via mailcontact ook persoonsgegevens verstrekt worden aan betrokkenen in het gezin. De medewerkers die geen verwerker zijn, maar wel op de groep staan, mogen de persoonsgegevens inzien.

Beveiligingsmaatregelen

Onderstaande maatregelen zijn getroffen om ervoor te zorgen dat persoonsgegevens op een veilige manier verwerkt en bewaard worden.

- De papieren cliëntdossiers worden bewaard in een kast met een slot erop. De sleutel is alleen bereikbaar voor medewerkers van Zorgkwekerij Bloei.
- Alleen de verwerkingsverantwoordelijke en de verwerkers van Zorgkwekerij Bloei hebben toegang tot het digitale cliëntdossier door middel van een eigen wachtwoord.
- Op de laptops waar begeleidingsplannen en evaluatieverslagen opgeslagen zijn, staat een wachtwoord die alleen bekend is bij de verwerkingsverantwoordelijke en verwerkers.
- Wanneer de laptops niet gebruikt worden, worden zij bewaard in een kast die op slot kan.
- In mailcontact naar gemeentes worden namen van cliënten enigszins gepseudonimiseerd, namelijk door alleen de voorletter en vervolgens de achternaam te geven.
- In het arbeidscontract met de medewerkers is opgenomen dat zij geheimhoudingsplicht hebben. Wanneer zij zich daar niet aan houden, krijgen zij een boete.

Bijlage 6 Gegevensbeschermingseffectbeoordeling

Zorgkwekerij Bloei slaat niet-incidenteel gegevens op en slaat gegevens op van bijzondere aard. Dit maakt dat de verwerking van persoonsgegevens risicovol is. Verder gaat het om gegevens van hulpkwekers. Daar moet voorzichtig mee omgegaan worden. Om die reden heeft Zorgkwekerij Bloei een gegevensbeschermingseffect beoordeling uitgevoerd. Deze is hieronder beschreven.

Aard van de gegevensverwerking

De volgende gegevens van cliënten worden verwerkt. Persoonsgegevens voortkomend uit onderstaande bronnen:

- Intakeformulieren
- Zorgovereenkomst
- Beschikking
- Verslagen van bijvoorbeeld onderzoeken
- Extra gegeven informatie door de ouders/verzorgers
- Observaties van de cliënt door de begeleiding

De persoonsgegevens voortkomend uit bovenstaande bronnen kunnen ook bijzondere persoonsgegevens bevatten, zoals genetische gegevens, gegevens over religie, gegevens over gezondheid, gegevens met betrekking tot iemands seksueel gedrag. Deze gegevens worden door de verzorgers van de cliënt gegeven en zij hebben Zorgkwekerij Bloei toestemming gegeven voor het verwerken van deze gegevens.

Omvang van de gegevensverwerking

Van iedere cliënt/hulpkweker die Zorgkwekerij Bloei in zorg heeft, worden gegevens opgeslagen op de volgende plaatsen:

- Digitaal cliëntdossier
- Papieren cliëntdossier
- Digitale rapportages
- Bijzonderhedenlijst

De gegevens worden beheerd door de verwerkingsverantwoordelijke, verwerkt door de daarvoor aangestelde verwerkers en ingezien door de medewerkers van Zorgkwekerij Bloei. Wanneer dat noodzakelijk is voor de begeleiding van de cliënt en ouders/verzorgers daarvoor toestemming hebben gegeven, kunnen de persoonsgegevens gedeeld worden met andere betrokkenen in het gezin.

Doelen van de gegevensverwerking

De persoonsgegevens van de cliënten worden verwerkt met het oog op onderstaande doelen:

- Identificeren van de persoon.
- Snel contact op kunnen nemen bij vragen over hulpkweker.
- Adequaat kunnen begeleiden van hulpkweker.
- Evalueren van de ontwikkeling/groei van hulpkweker.
- Overleg plegen met de betrokkenen in het gezin ter bevordering van de hulpverlening.

Risico

Het risico bestaat dat de gegevens openbaar worden gemaakt door medewerkers of cliënten. Zorgkwekerij Bloei heeft de volgende maatregelen genomen om dit risico te verkleinen:

- De papieren cliëntdossiers worden bewaard in een kast met een slot erop. De sleutel is alleen bereikbaar voor medewerkers van Zorgkwekerij Bloei.
- Alleen de verwerkingsverantwoordelijke en de verwerkers van Zorgkwekerij Bloei hebben toegang tot het digitale cliëntdossier door middel van een eigen wachtwoord.
- Op de laptops waar begeleidingsplannen en evaluatieverslagen opgeslagen zijn, staat een wachtwoord die alleen bekend is bij de verwerkingsverantwoordelijke en verwerkers.
- Wanneer de laptops niet gebruikt worden, worden zij bewaard in een kast die op slot kan.
- In mailcontact naar gemeentes worden namen van cliënten enigszins gepseudonimiseerd, namelijk door alleen de voorletter en vervolgens de achternaam te geven.
- In het arbeidscontract met de medewerkers is opgenomen dat zij geheimhoudingsplicht hebben. Wanneer zij zich daar niet aan houden, krijgen zij een boete.

Conclusie

De verwerking van persoonsgegevens is noodzakelijk voor het goed kunnen begeleiden van de hulpkwekers. Daarbij komt dat een juiste dossiervorming vereist wordt door de overheid en inspectie. Door de beveiligingsmaatregelen is de kans op een datalek klein. Zorgkwekerij Bloei heeft daarom besloten de persoonsgegevens te (blijven) verwerken, met toestemming van de ouders/verzorgers van de cliënten. Daarbij houdt zij bovenstaande beveiligingsmaatregelen in stand.

Bijlage 7 Meldingsformulier datalek

Datum: _____

Ingevuld door: _____

Functie: _____



Wat zijn de aard en omvang van de inbreuk?

Wie waren de betrokkenen?

Om wat voor soort gegevens gaat het?

Welk risico kan de inbreuk hebben voor de betrokkenen?

Welke maatregelen neemt de organisatie om de inbreuk aan te pakken en de risico's voor betrokkenen te voorkomen of verminderen?

Welke maatregelen neemt de organisatie om een eventuele volgende inbreuk van deze aard te voorkomen?

Voor meer informatie, neem contact op met:

Marjolein de Hoog - Eigenaar
Zorgkwekerij Bloei
Europalaan 18
2641 RX Pijnacker
06-51352696
marjolein@zorgkwekerijbloei.nl
www.zorgkwekerijbloei.nl