Informatiebeheerbeleid

(inclusief privacyreglement en meldplicht datalekken)

Voorwoord

Waarom een informatiebeheerbeleid?

Stichting Omega is een organisatie die veel werkt met persoonsgegevens van cliënten en valt onder de Algemene Verordening Gegevensbescherming (AVG). De AVG richt zich op bescherming van de persoonlijke leefomgeving. Waarden als gelijkheid, vrijheid, autonomie, zelfontwikkeling, democratie en gelijke kansen zijn hiermee verbonden. Privacy in de gehandicaptenzorg is extra belangrijk omdat Stichting Omega beschikt over veel gevoelige gegevens over hun cliënten. Hierbij is vaak sprake van kwetsbare personen, waardoor privacy extra belangrijk is. De cliënten van Stichting Omega zijn afhankelijk van de medewerkers als het gaat over bescherming van hun persoonlijke leefomgeving. Naleving van de AVG is onderdeel van de zorg. Daarnaast is de naleving van de AVG een wettelijke verplichting.
Het is daarom belangrijk om waarde te hechten aan het beschermen van de privacy van de cliënten waar de organisatie mee te maken krijgt. Dit vraagt om een integraal informatiebeheerbeleid waarin rekening gehouden wordt met de bescherming van de persoonsgegevens en het voldoen aan wet – en regelgeving.

De volgende wet- en regelgeving is verankerd in dit informatiebeheerbeleid:

- Algemene Verordening Gegevensbescherming (AVG)

Het informatiebeheerbeleid medewerkers is omschreven in het privacyreglement medewerkers.

Wat staat er in het informatiebeheerbeleid cliënten?

- Verantwoordelijken informatiebeheerbeleid
- Welke informatie in bezit is van Omega
- Hoe de informatie wordt verwerkt en gebruikt
- Waar en hoe de informatie wordt gearchiveerd
- Of er een veiligheidskopie van de betreffende gegevens wordt gemaakt en waar die zich bevindt
- Bewaartermijn en het vernietigen van informatie
- Hoe om te gaan met een klacht/ bezwaar
- Meldplicht datalekken en hoe te handelen bij een datalek

1. Begripsbepalingen

1. Persoonsgegevens: elk gegeven betreffende een geïdentificeerde of identificeerbare natuurlijke persoon.
2. Gezondheidsgegevens: Alle gegevens die de geestelijke of lichamelijke toestand van een cliënt betreffen;
3. Verwerking van persoonsgegevens: elke handeling of elk geheel van handelingen met betrekking tot persoonsgegevens, waaronder in ieder geval het verzamelen, vastleggen, ordenen, bewaren, bijwerken, wijzigen, opvragen, raadplegen, gebruiken, verstrekken door middel van doorzending, verspreiding of enige andere vorm van terbeschikkingstelling, samenbrengen, met elkaar in verband brengen, evenals het afschermen, uitwissen of vernietigen van gegevens;
4. Bestand: Gestructureerd geheel dat betrekking heeft op de persoonsgegevens van de cliënt en dat volgens bepaalde criteria toegankelijk is voor derden;
5. Verwerkingsverantwoordelijke: de natuurlijke persoon, rechtspersoon of ieder ander die of het bestuursorgaan dat, alleen of tezamen met anderen, het doel van en de middelen voor de verwerking van persoonsgegevens vaststelt;
6. Betrokkene: degene op wie een persoonsgegeven betrekking heeft;
7. Verwerker: degene die ten behoeve van de verwerkingsverantwoordelijke persoonsgegevens verwerkt, zonder aan zijn rechtstreeks gezag te zijn onderworpen;
8. Derde: ieder, niet zijnde de betrokkene, de verwerkingsverantwoordelijke, de verwerker, of enig persoon die onder rechtstreeks gezag van de verwekingsverantwoordelijke of de verwerker gemachtigd is om persoonsgegevens te verwerken;
9. Ontvanger: degene aan wie de persoonsgegevens worden verstrekt;
10. Autoriteit Persoonsgegevens; de Autoriteit Persoonsgegevens heeft tot taak toe te zien op de verwerking van persoonsgegevens. Bedrijven, instellingen en overheden die persoonsgegevens verwerken zijn verplicht ernstige datalekken te melden bij de Autoriteit Persoonsgegevens.

2. Reikwijdte

Dit beleid is van toepassing op de geheel of gedeeltelijk geautomatiseerde verwerking van persoonsgegevens, alsmede de niet geautomatiseerde verwerking van persoonsgegevens die in een bestand zijn opgenomen of die bestemd zijn om daarin te worden opgenomen.

3. Informatie in bezit van Omega

De persoonsregistratie binnen Omega bevat de volgende gegevenscategorieën, personalia/ identificatie gegevens:
- financieel/ administratieve gegevens
- medische, paramedische en psychologische gegevens (gezondheidsgegevens)
- zorginhoudelijke gegevens

Deze zijn geregistreerd in een persoonsgebonden elektronisch dossier ‘ONS’ van Nedap.

4. Verantwoordelijken informatiebeheerbeleid

4.1. Houder informatiebeheerbeleid
De directeur van Omega is eindverantwoordelijk voor het informatiebeheerbeleid. De directeur is verantwoordelijk voor het goed functioneren van de persoonsregistratie en aansprakelijk voor eventuele schade als gevolg van het niet naleven van dit beleid.

4.2. Functionaris Gegevensbescherming (FG)
Een onafhankelijke medewerker die belast is met het toezicht op de naleving van de AVG. De FG fungeert ook als aanspreekpunt voor de AP, bijvoorbeeld bij een (vermoeden van) datalek.

4.3. Managers zorg
De managers zorg zijn verantwoordelijk voor de uitvoering en de naleving van het vastgestelde beleid:

- Monitoren beveiligingsincidenten waardoor de vertrouwelijkheid, beschikbaarheid of integriteit kan worden geschonden.
- Verantwoordelijk voor de wijzigingen van autorisaties met goedkeuring van MT.
- Monitoren per kwartaal het escalatielog (toont waarom, wanneer en hoelang medewerkers toegang hebben verkregen tot cliënten buiten hun autorisatie) of dit met een geldige reden is gedaan

4.4. Evaluatie beleid
Het informatiebeheerbeleid wordt elke twee jaar geëvalueerd door de directeur. Bij wijzigingen wordt het beleid ter informatie en/of goedkeuring voorgelegd aan het MT en opnieuw vastgesteld.

5. Doel van de verwerking van de persoonsgegevens

Stichting Omega neemt alleen de persoonsgegevens op, bewerkt en/of bewaart ze met een bepaald doel. De gegevensverzameling en verwerking moet samenhangen met het vooraf gestelde doel.

Doeleinden voor de verwerking van persoonsgegevens:

- Een goede uitvoering van de zorg-, hulp- en dienstverlening die door Stichting Omega wordt verleend;
- Verantwoording van de zorg-, hulp- en dienstverlening;
- Het vastleggen en beschikbaar stellen van persoonsgegevens voor onderzoek en kwaliteitscontrole;
- Het financieel afhandelen van de geboden zorg aan de cliënt.

Stichting Omega zal geen persoonsgegevens verwerken voor andere dan bovengenoemde doeleinden.

6. Voorwaarden voor de verwerking van de persoonsgegevens

Persoonsgegevens mogen slechts worden verwerkt indien aan een van de voorwaarden is voldaan:
- De verwerking is noodzakelijk voor de uitvoering van een overeenkomst;
- De verwerking is noodzakelijk voor de uitvoering van een wettelijke plicht.

7. Kennisgeving aan (vertegenwoordiger van de) betrokkene

7.1.
Stichting Omega zal door middel van een algemene kennisgeving op de website het bestaan van de registratie en van dit beleid vermelden, alsmede daarin aangeven op welke wijze het beleid kan worden ingezien en verkregen en nadere informatie ter zake kan worden ingewonnen.

7.2
Indien andere doeleinden dan genoemd in paragraaf 5 een doelstelling vormen van de registratie, heeft Stichting Omega de plicht de betrokkene vooraf schriftelijk te informeren omtrent de aard van de gegevens die over zijn persoon in de registratie zijn opgenomen, alsmede omtrent de doeleinden die daarmee worden nagestreefd.

8. Verstrekking van persoonsgegevens

8.1.
Voor verstrekking van persoonsgegevens aan derden is toestemming van de (vertegenwoordiger van de) betrokkene vereist. Deze toestemming is niet vereist indien verstrekking noodzakelijk is ter uitvoering van een wettelijke plicht of een andere voorwaarde voor de verwerking van de persoonsgegevens zoals genoemd in paragraaf 6.

8.2.
Binnen Stichting Omega kunnen zonder toestemming van de betrokkene en indien noodzakelijk voor de taakuitoefening, geregistreerde persoonsgegevens worden verstrekt aan:
- Degenen die rechtstreeks betrokken zijn bij de actuele zorgverlening aan de betrokkene;
- Degenen die betrokken zijn bij kwaliteitsdoelstellingen (interne auditteam).

9. Beveiliging van de persoonsgegevens

De persoonsregistratie binnen Omega vindt plaats en wordt bewaard in een elektronisch persoonsgebonden dossier. In het kader van de zorg kunnen audiovisuele opnamen gemaakt worden van een betrokkene.

9.1 Toegang tot en gebruik van persoonsgegevens
Onverminderd eventuele wettelijke voorschriften terzake hebben slechts toegang tot de persoonsgegevens:
- De verwerker die deze gegevens heeft verzameld of diens waarnemer.
- Andere direct bij de verzorging, begeleiding en/ of behandeling betrokken beroepsbeoefenaren voor zover de taakuitoefening noodzakelijk.

- De directeur/ managers zorg en de verwerker, voor zover dit in het kader van beheer en verwerking noodzakelijk is.

9.2 Beveiliging digitale dossiers
Toegang en bewerken van de digitale persoonsgegevens is geregeld door het autoriseren van de toegang en het verlenen van rechten om de informatie in te zien danwel te bewerken.

9.3 Autorisatie
Er zijn per medewerker gebruikersrechten toegekend voor het gebruik van software van de organisatie door middel van een wachtwoord en toegangscode via sms of app. Het wachtwoord is persoonsgebonden en mag niet worden doorgegeven. Medewerkers mogen alleen die persoonsgegevens inzien die voor hun taakuitoefening noodzakelijk zijn.

9.4 Escalatie
Er is een mogelijkheid om buiten de gebruikersrechten een dossier in te zien, denk aan tijdelijk werken op een andere groep ivm zieke collega's. Middels de escalatie functionaliteit in het cliënten dossier ONS vraagt de gebruiker eenmalig toegang tot een dossier waar de gebruiker normaliter geen toegang toe heeft

9.5 Papieren informatievoorziening kinderen/deelnemer
Op de groepen is een onderdeel van de persoonsregistratie op papier aanwezig welke noodzakelijk is voor:
• Noodsituaties. Belangrijke informatie direct bij de hand. Denk aan allergieën voor medicatie, zoals pijnstilling en antibiotica. Dit moet het ambulancepersoneel direct weten.
• Gelijk inspringen met de protocollen, denk aan epilepsie-, luchtweg- en allergieprotocol. Als begeleider moet je in bepaalde situaties snel handelen, waardoor er geen tijd is om de informatie in ONS op te zoeken.
• Wanneer er een internetstoring is op Omega en het dossier daardoor niet toegankelijk
Deze gegevens zitten in persoonsgebonden mappen, welke worden opgeborgen in een afgesloten kast/ruimte op de groep.

9.6 Bewaren en gebruiken van beeld –en geluidsmateriaal
De afspraken hierover zijn vastgelegd in een beleid beeld- en geluidsmateriaal.

9.7 Back-up regeling
De back-up van alle gegevens op de server van Stichting Omega:
- Een onsite back-up via de NAS.
- Een offsite back-up via Constant – IT.

De back-up van alle gegevens in ONS (Infozorg/Nedap):
- Nedap Healthcare maakt (minimaal) 4 keer per dag een volledige back-up van elke database van elke klant. Dit geldt niet alleen voor productie-omgevingen, maar ook voor opleidingsomgevingen, trainingsomgevingen en zelfs voor testomgevingen. Back-ups van omgevingen worden zowel on-site als off-site opgeslagen. Naast de individuele klant-database-back-ups wordt elke 24 uur een back-up van elke database-server gemaakt om een volledige restore van een server te kunnen doen.

- Stichting Omega heeft een overeenkomst (Escrow-regeling) afgesloten met de Software Borg Stichting. De broncode van door Stichting Omega gebruikte software is opgeslagen bij een IT notaris.

10. Bewaartermijn van de persoonsgegevens

10.1
Alle dossiers worden bewaard met als motivatie ‘de uniekheid van de doelgroep’. Omega bewaart de geanonimiseerde persoonsgegevens voor wetenschappelijke doeleinden.

Voorheen werden er papieren dossiers gebruikt, deze zijn binnen Omega ondergebracht in het archief.

11. Maatregelen bij misbruik persoonsgegevens

11.1
Als persoonsgegevens worden gehackt of gegevens komen ‘op straat te liggen’ dan heeft Stichting Omega de verplichting om deze datalek te melden < zie formulier datalek>

11.2
Schending geheimhouding of privacy door een medewerker kan reden zijn voor ontslag, dit is nml een strafrechtelijk vergrijp. Er wordt eerst een zorgvuldig intern onderzoek gedaan, bewijsmateriaal worden verzameld. Aan de hand van de uitkomsten van het onderzoek kan bepaald worden welke stappen er eventueel ondernomen worden.

12. Aanvulling, correctie of vernietiging van persoonsgegevens

12.1.
Op verzoek van de (vertegenwoordiger van de) betrokkene vult de verwerker de opgenomen gegevens aan met de door de (vertegenwoordiger van de) betrokkene gewenste aanvullende gegevens. De (vertegenwoordiger van de) betrokkene kan aan de verwerker van de persoonsregistratie een verklaring afgeven met betrekking tot de opgenomen gegevens; deze verklaring wordt opgenomen in het persoonsdossier.

12.2.
De (vertegenwoordiger van de) betrokkene kan Stichting Omega schriftelijk, gemotiveerd, verzoeken om correctie van op de betrokkene betrekking hebbende gegevens, indien deze
- feitelijk onjuist zijn;
- voor het doel van de registratie onvolledig of niet ter zake dienend zijn;
- in strijd met een wettelijk voorschrift in de registratie voorkomen.

12.3.
De (vertegenwoordiger van de) betrokkene kan Stichting Omega schriftelijk verzoeken om vernietiging van tot zijn persoon herleidbare gegevens.

12.4.
Stichting Omega beslist niet over een verzoek in 12.2 en 12.3, dan na de verwerker die de gegevens heeft verzameld of diens opvolger, te hebben gehoord. Stichting Omega deelt haar beslissing binnen vier weken na ontvangst van het verzoek tot correctie of vernietiging

schriftelijk aan de (vertegenwoordiger van de) betrokkene mee. Een weigering is met redenen omkleed.

12.5.
Stichting Omega draagt zorg dat een beslissing tot correctie zo spoedig mogelijk wordt uitgevoerd.

12.6.
Stichting Omega draagt zorg voor vernietiging van de gegevens zonder onredelijke vertraging na een daartoe strekkend verzoek van de (vertegenwoordiger van de) betrokkene, tenzij
- redelijkerwijs aannemelijk is dat de bewaring van aanmerkelijk belang is voor een ander dan de geregistreerde, alsmede;
- bewaring op grond van een wettelijk voorschrift vereist is.

12.7.
Stichting Omega doet aan degenen, aan wie zij in het haar voorafgaand aan het verzoek en sinds dat verzoek verstreken perioden, gegevens heeft verstrekt, mededeling van de aanvulling, correctie of vernietiging.

12.8.
Stichting Omega doet aan de (vertegenwoordiger van de) betrokkene opgave van degene aan wie zij mededeling als bedoeld in 10.7. heeft gedaan, tenzij de (vertegenwoordiger van de) betrokkene te kennen heeft gegeven op de mededeling geen prijs te stellen.

13. Inzage van de persoonsgegevens

De (vertegenwoordiger van de) betrokkene heeft het recht kennis te nemen van de op de betrokkene betrekking hebbende geregistreerde gegevens.
Stichting Omega geeft betrokkene/ wettelijk vertegenwoordiger inzage in en controle over diens gezondheid/ gegevens met het digitale cliëntenportaal Caren Zorgt. Op www.carenzorgt.nl kan een eigen account aan worden gemaakt met eigen mailadres en wachtwoord

14. Overdracht van opgenomen persoonsgegevens.

14.1.
De (vertegenwoordiger van de) betrokkene heeft het recht op de betrokkene betrekking hebbende gegevens te doen overdragen aan een andere, door hem aan te wijzen houder. Daartoe dient hij een schriftelijk verzoek in bij Stichting Omega. De inwilliging van dit verzoek kan slechts worden geweigerd op grond van een wettelijk voorschrift dan wel worden opgeschort voor zover Stichting Omega jegens de financier van de verleende diensten tot bewaring gehouden is of indien ter zake van die dienstverlening een geschil aanhangig is gemaakt of dreigt te worden gemaakt.

14.2.
In geval Stichting Omega het voornemen heeft tot overdracht van de door haar gehouden persoonsgegevens in verband met beëindiging of wijziging van de juridische status van de instelling, dient Stichting Omega door middel van een (herhaaldelijke) advertentie in een of meer regionale kranten of een maatregel van gelijke strekking, de (vertegenwoordiger van

de) betrokkene over de voorgenomen overdracht te informeren, opdat deze voldoende kans wordt geboden tegen het voornemen bezwaar te maken.

15. Looptijd van de registratie

Onverminderd eventuele wettelijke bepalingen is dit beleid van kracht gedurende de gehele looptijd van de registraties.

16. Klachten

16.1.
Indien de (vertegenwoordiger van de) betrokkene van mening is dat de bepalingen van dit reglement niet worden nageleefd of andere reden heeft tot klagen met betrekking tot de registratie van zijn gegevens, dient hij zich te wenden tot Stichting Omega**.< document klachten>**

16.2.
Indien dit voor de (vertegenwoordiger van de) betrokkene niet leidt tot een voor hem acceptabel resultaat heeft hij de volgende mogelijkheden:

- Zich richten tot de Functionaris Gegevensbescherming van Stichting Omega, bereikbaar via RvPraag@sigra.nl.
- Gebruik maken van de klachtenregeling van Omega.
- Zich wenden tot de Autoriteit Persoonsgegevens met het verzoek te bemiddelen of te adviseren in zijn geschil met Stichting Omega. Dit dient te geschieden binnen een termijn van acht weken na ontvangst van het antwoord van Stichting Omega of, indien Stichting Omega niet binnen de gestelde termijn heeft geantwoord binnen acht weken na afloop van die termijn.

Eén en ander laat onverlet de mogelijkheden een beroep te doen op de rechter, hiervoor geldt dezelfde termijn als voor het inschakelen van de Autoriteit Persoonsgegevens.

17. Vaststelling en wijzigingen van het informatiebeheerbeleid

Dit informatiebeheerbeleid is vastgesteld door de directeur.
Wijzigingen in dit beleid worden aangebracht door de directeur. De wijzigingen in het beleid zijn van kracht vier weken nadat ze bekend zijn gemaakt aan belanghebbenden.

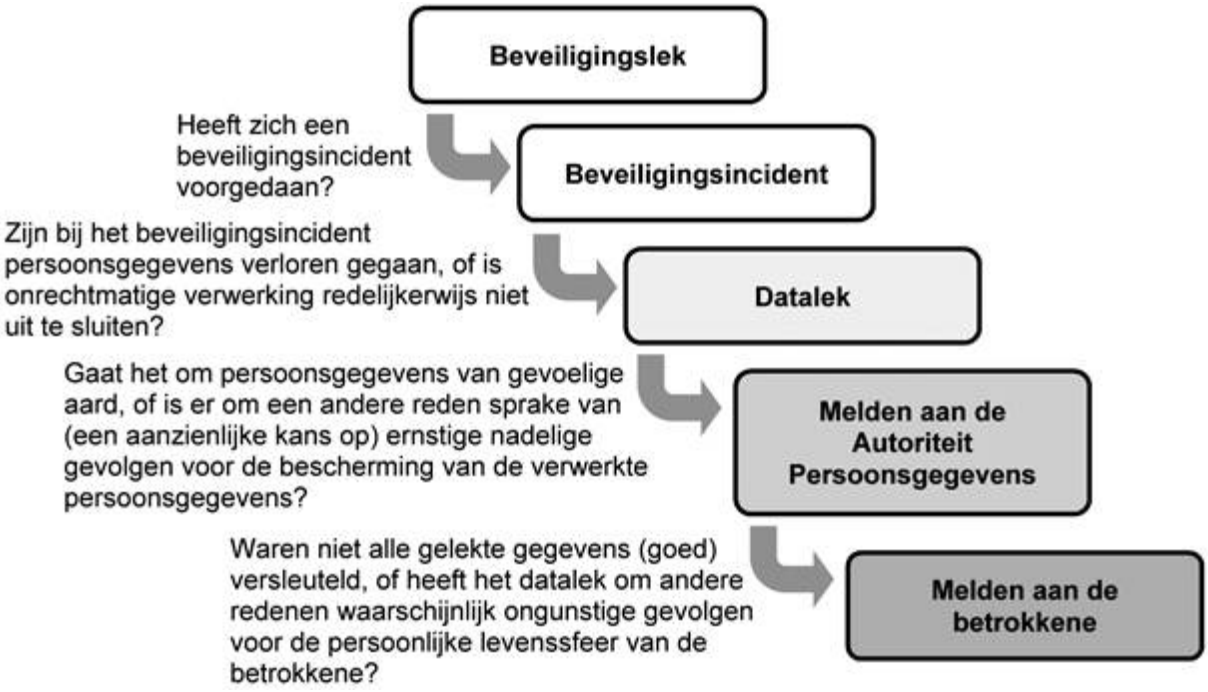
18. Meldplicht datalekken

Sinds mei 2018 maakt de meldplicht van datalekken onderdeel uit van AVG.

18.1 Beveiligingsincident en datalek
Een beveiligingsincident is volgens de wet het verlies of de onrechtmatige verwerking van gegevens, die eventueel nadelige gevolgen kunnen hebben voor de bescherming van die gegevens. Dat kan dus ook dataverlies betreffen waarbij een actuele of complete veiligheidskopie ontbreekt, zonder dat er gerede kans bestaat dat een derde die data in handen heeft gekregen.

Niet ieder beveiligingsincident is ook een datalek. Er is sprake van een datalek als er bij het beveiligingsincident persoonsgegevens verloren zijn gegaan, of als u onrechtmatige verwerking van de persoonsgegevens niet redelijkerwijs kunt uitsluiten.
Alleen als er sprake is van een ernstig datalek moet er melding gedaan worden bij de Autoriteit Persoonsgegevens. Zie figuur 1.

Figuur 1



19.Hoe te handelen bij een beveiligingsincident

19.1
Wanneer een beveiligingsincident wordt ontdekt, is het van belang hier zo snel mogelijk melding van te maken. Dit wordt mondeling gedaan bij een manager (OD of zorg) die aanwezig is. Daarnaast wordt een datalekformulier in de kennisbank ingevuld en deze wordt gemaild naar kwaliteit@stichtingomega.nl. De melding komt via de manager en/of het formulier bij de manager Ondersteunende Diensten en/of de kwaliteitsfunctionaris terecht. Deze neemt direct telefonisch contact op met de FG. De FG beoordeelt of er sprake is van een datalek en of de Autoriteit Persoonsgegevens geïnformeerd moet worden. De directeur, Constant IT en, indien noodzakelijk, andere betrokkenen worden over de melding geïnformeerd. Afhankelijk van de aard van het beveiligingsincident vindt er overleg plaatst met de directeur van Constant IT en de security officer.
De melding wordt geregistreerd door de kwaliteitsfunctionaris in het datalekregister.

19.2
Het datalek wordt uiterlijk binnen 72 uur gemeld via het online ‘meldloket datalekken’ van de Autoriteit Persoonsgegevens. De Autoriteit Persoonsgegevens stuurt een ontvangstbevestiging dat het datalek gemeld is.
Via het meldloket kan de melding tevens aangevuld of ingetrokken worden.

19.3
De Autoriteit Persoonsgegevens neemt contact op met de FG wanneer de melding aanleiding is voor nader te ondernemen activiteiten.

19.4
Indien de FG oordeelt dat er geen sprake is van een datalek, wordt de informatie uit het datalekformulier meegenomen in de jaarrapportage van de FG.

20. Overig

Over zaken waarin dit informatiebeheerbeleid geen uitsluitsel verschaft, beslist de directeur.