Data Protection Impact Assessment Clientgegevens

Resultaten van uitgevoerde DPIA over verwerking cliëntengegevens op datum 12/03/2018

1 Inhoudstafel

2 Management Samenvatting

Dit document bevat de vastlegging van een Data Protection Impact Assessment (DPIA) zoals benoemd in de GDPR. Deze DPIA is een analyse van de beoogde verwerkingen van persoonsgegevens voor clientgegevens en bevat de algemene context, informatie over de verwerkingen, beoordeling van de samenhangende risico's en concrete maatregelen die genomen worden om deze risico's te beheersen en ten slotte een uitspraak over de noodzaak van een voorafgaande raadpleging bij een DPA.

3 Kader

3.1 Context organisatie

Breederzorg is een thuiszorgorganisatie die opereert in de regio's: Oss, Uden, Veghel, Eindhoven en omliggende gebieden. De diensten die Breederzorg biedt zijn: V&V (verzorging en verpleging) en WMO (huishoudelijke verzorging en persoonlijke begeleiding).

In maart 2018 heeft Breederzorg 146 mensen in dienst en levert ze thuiszorg aan 830 cliënten. Deze is op te splitsen in +- 315 cliënten in de V&V en +- 515 cliënten in de WMO.

Het aantal medewerkers en het aantal cliënten fluctueert.
Daarnaast geeft Breederzorg Thuiszorg de mogelijkheid om opleidingen te volgen waardoor medewerkers door kunnen stromen naar andere functies binnen Breederzorg.

3.2 Context verwerking

Breederzorg verwerkt gegevens van cliënten en slaat deze (tijdelijk) op. Te denken valt aan algemene contactgegevens die nodig zijn voor het verlenen van zorg en medische cliëntendossiers.

We onderscheiden drie typen persoonsgegevens: gewone, bijzondere en strafrechtelijke gegevens. Breederzorg verwerkt:

- **Gewone persoonsgegevens**: contactgegevens, personeelsgegevens

- **Bijzondere persoonsgegevens**: gegevens over de gezondheid van cliënten (Electronisch cliënten dossier) en medewerkers (ziekteverzuim).

- Strafrechtelijke persoonsgegevens zijn voor Breederzorg niet van toepassing.

4 Data Protection Impact Assessment Cliëntgegevens

4.1 Algemene Informatie

4.1.1 Scope

Breederzorg Thuiszorg heeft op peildatum maart 2018 +- 830 cliënten. Van deze personen worden gegevens opgeslagen die nodig zijn voor het verlenen van zorg. Deze DPIA beschrijft alle gegevens die worden opgeslagen van huidige cliënten en oud cliënten.

4.1.2 Betrokken actoren

Breederzorg Thuiszorg B.V.
FG – functionaris gegevensbescherming Breederzorg Thuiszorg: Philip van Hout
Cliënten V&V/WMO Breederzorg Thuiszorg
Cliëntenadministratie Breederzorg Thuiszorg

4.1.3 Project planning

DPIA cliëntgegevens moet voldoen voor de invoering van de nieuwe AVG wet op 25 mei 2018. Daarnaast ziet Breederzorg de DPIA als een proces wat minimaal jaarlijks herzien en bijgesteld dient te worden.

4.1.4 Betrokken verwerkers en contractuele afspraken

De betrokken verwerkers omtrent cliëntgegevens zijn:

Intern:
Medewerkers Breederzorg Thuiszorg
Cliëntenadministratie: Erna Krol, Marieke Verbruggen, Linda Essens

Extern:
Nedap ONS

Met externe partijen zijn SLA overeenkomsten gemaakt m.b.t. gegevensbescherming conform de GDPR art. 28. Deze zijn terug te vinden in de map SLA overeenkomsten.

4.2 Beschrijving van de gegevensstroom in detail

Zorgaanvragen

De zorgaanvragen worden, afhankelijk van de financieringsvorm, op verschillende manieren aan Breederzorg gepresenteerd:

WLZ (Wet Langdurige zorg)
Indicaties komen binnen via beveiligd berichtenverkeer (Vecozo) en worden ingelezen in Nedap.

WMO (Wet Maatschappelijke ondersteuning)
Cliënten die behoefte hebben aan ondersteuning in het huishouden of begeleiding kunnen dit aangeven bij hun gemeente. De gemeente gaat vervolgens samen met de aanvragen een 'keukentafelgesprek' aan waarin de behoefte van de zorg wordt besproken en getoetst. Op grond hiervan wordt door de gemeente een indicatie afgegeven. De cliënt mag zelf kiezen door welke zorgaanbieder deze indicatie wordt vervuld.
Indicaties komen bij Breederzorg binnen via beveiligd berichtenverkeer (Vecozo) en worden ingelezen in het Elektronisch Cliënten Dossier- Nedap.

ZVW (ZorgVerzekeringsWet)

Aanvragen komen op diverse manieren binnen:

- Via ziekenhuis Bernhoven (zorgwissel; beveiligd portaal)
- Telefonisch (b.v. via huisarts, cliënt zelf of familie van cliënt). Gegevens worden dan meestal via mail doorgegeven
- Via andere zorgaanbieders: meestal via mail
- Cliënt die al hulp bij huishouden (WMO) heeft en ook zorg van ons wil (gegevens zijn dan bekend)

PGB
Gegevens komen meestal binnen via telefoon of mail (niet altijd beveiligd)

Onbepaald
Via de website kunnen formulieren worden verzonden voor het aanvragen van zorg. In deze formulieren zijn de volgende gegevens verplicht in te vullen:

- Naam
- Geboortedatum
- Adres
- Telefoonnummer
- E-mailadres (niet verplicht)
- Vanaf welke datum wilt u zorg ontvangen?
- Waar kunnen we u bij helpen? Verzorging & verpleging Begeleiding Hulp bij huishouden Weet ik niet / anders
- Opmerkingen

Cliënten in zorg

Vanaf het moment dat een cliënt kiest om zijn of haar zorg door Breederzorg te laten uitvoeren wordt de zorgvraag besproken met de zorg coördinator van het betreffende team. Er wordt gekeken of er voldoende capaciteit is om de zorg te kunnen leveren. Als de cliënt definitief bij ons in zorg komt zal een account in het Elektronisch Cliënten Dossier worden aangemaakt.

Afhankelijk van de zorgvraag kunnen de volgende gegevens worden ingevuld en bijgehouden in het ECD:

Administratieve gegevens

De volgende gegevens worden standaard geregistreerd:

- Naam
- Adres
- Woonplaats
- Contactgegevens
- Geboortedatum
- BSN nummer
- Datum in zorg / Datum uit zorg
- Zorgarrangement (of u gebruik maakt van verzorging/verpleging/hulp bij huishouden/begeleiding)
- Welk team er gekoppeld is aan de cliënt

De volgende gegevens worden niet standaard geregistreerd:

- Verwijzers
- Declaraties en aanvullende diensten

Medische gegevens

Alleen van cliënten die persoonlijke verzorging, verpleging, begeleiding (of een combinatie hiervan) ontvangen worden medische gegevens geregistreerd. Deze gegevens worden bijvoorbeeld ingevuld bij het intakegesprek. Alleen de cliënt kan ons voorzien van deze gegevens, het is door Breederzorg niet extern op te vragen zonder uitdrukkelijke toestemming van de cliënt.

De volgende medische gegevens kunnen bij Breederzorg worden geregistreerd:

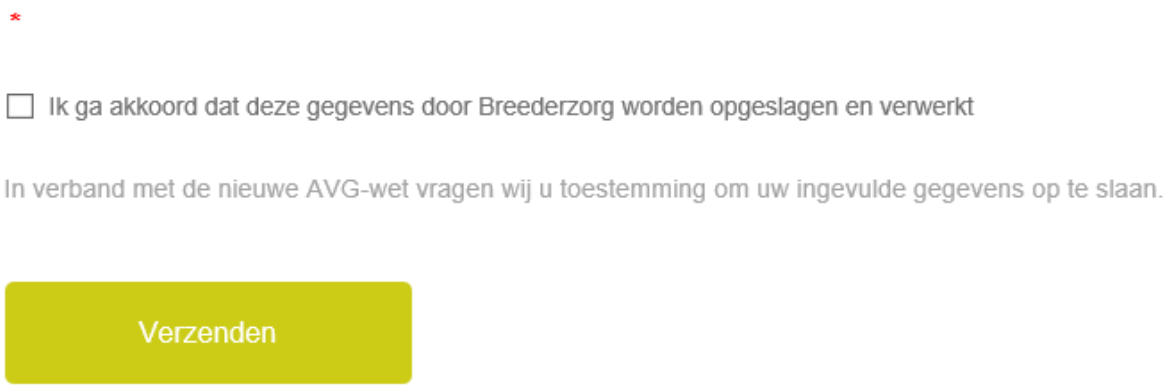
- Zorgopname (hetzelfde als datum in zorg)
- Episodes
- Medische voorgeschiedenis
- Allergieën en overgevoeligheden
- Verpleegkundige notities
- Medisch beleid (reanimatie/chemo/infectie)
- Juridische statussen
- Wilsonbekwaamheden
- Medewerker relaties (de eerst verantwoordelijke verpleegkundige)
- Medische notities
- Dossier (Dit is wat een medewerker invult tijdens of na uw zorg. De zorg-acties worden beschreven en aantekeningen worden gemaakt)

4.3 Toetsing van basisprincipes verwerking persoonsgegevens

De verwerking van de cliëntengegevens zoals genoemd in 4.2 is vastgelegd in het gegevensbeschermingsbeleid van Breederzorg Thuiszorg. Ieder jaar zal dit document+ de medewerkers DPIA worden herzien.

4.3.1 Transparantie, rechtmatigheid

Cliënten die online het formulier invullen op de website worden direct geïnformeerd over de informatie die Breederzorg bewaard en bewerkt. Pas nadat de gebruiker hiermee akkoord gaat kan de informatie ook daadwerkelijk aan Breederzorg worden verzonden.



4.3.2 Doelbinding

Alle cliëntgegevens die door Breederzorg worden opgeslagen zijn bedoeld voor het verlenen van juiste, goede en veilige thuiszorg.

4.3.3 Minimale gegevensverwerking

De volgende gegevens worden standaard geregistreerd:

- Naam
- Adres
- Woonplaats
- Contactgegevens
- Geboortedatum
- BSN nummer
- Datum in zorg / Datum uit zorg
- Zorgarrangement (of u gebruik maakt van verzorging/verpleging/hulp bij huishouden/begeleiding)
- Welk team er gekoppeld is aan de cliënt

4.3.4 Juistheid

Wanneer gegevens veranderen kan de cliënt dit zelf melden (bijvoorbeeld bij een verhuizing). Ook kunnen medewerkers die nieuwe informatie krijgen dit melden bij cliëntenadministratie waarna het in het systeem wordt aangepast..

4.3.5 Opslagbeperking

Wettelijk worden alle clientengegevens opgeslagen voor een periode van ?????????????? jaar. Deze gegevens blijven inzichtelijk voor cliëntenadministratie in het ECD. Medewerkers kunnen de cliënt en het dossier niet meer zien in hun planning en rooster. Wel blijft de cliënt ???????????? weken staan in een aparte sectie: 'cliënten uit zorg'

4.3.6 Integriteit & vertrouwelijkheid

Alle gegevens zijn nooit vrij toegankelijk. Per functie wordt in het systeem ingesteld welke gegevens er van de cliënt zichtbaar zijn. Zo kan een medewerker HV niet bij het dossier. Door de rollenverdeling binnen het systeem is nauwkeurig te zien wie er toegang heeft tot welke gegevens. Ook kunnen cliënten een overzicht opvragen om in te zien wie er allemaal toegang heeft gehad tot hun gegevens.

4.4 Rechten van de betrokkene

Alle cliënten krijgen een brief thuisgestuurd waarin staat dat Breederzorg gegevens verwerkt.

Voorbeeldbrief:

Geachte ……,

Per 25 mei 2018 is er een nieuwe wet: de Algemene verordening gegevensbescherming (AVG). Vanaf die datum geldt dezelfde privacywetgeving in de hele EU. Graag willen we u via deze brief informeren over ons privacy beleid.

Breederzorg registreert middels het Elektronisch Cliënten Dossier gegevens van u. Het gaat om gegevens die we noodzakelijk achten voor het leveren van zorg, begeleiding en/of huishouden. Deze gegevens zijn onder te verdelen in administratieve gegevens en medische gegevens. Afhankelijk van de zorg die u ontvangt is het mogelijk dat sommige gegevens bij ons bekend zijn. Ook nadat u bij ons uit zorg bent zijn wij verplicht om deze gegevens te bewaren voor een periode van ????? jaar.

Wij garanderen u er alles aan te doen om uw gegevens optimaal te beschermen. Allereerst is er een functionaris gegevensbescherming aangesteld binnen onze organisatie. Daarnaast hebben al onze medewerkers een geheimhoudingsplicht als het gaat om privacygevoelige informatie van cliënten. Ook gebruiken we dubbele inlog verificatie, automatisch uitloggen en en kunnen we de Ipads van de medewerker bij verlies of diefstal direct op afstand blokkeren en wissen. Tot slot hebben niet alle medewerkers inzage in uw dossier, maar slechts diegene die gemoeid zijn met uw zorg en bijbehorende administratie. Zo hebben medewerkers van een ander team geen inzage in uw dossier. Een overzicht van de personen die inzage hebben (gehad) in uw dossier is te allen tijden op te vragen bij de beheerder: Nedap ONS. Mocht er ooit een digitale inbreuk zijn op uw privacy dan zullen wij dit meteen aan u melden.

Meer informatie over het privacybeleid van Breederzorg is te vinden op onze website, of door contact met ons op te nemen via 0413 259400

Met vriendelijke groet,

Breederzorg Thuiszorg

5 Risico's

We kijken hoe de situatie nu is gebaseerd op de gegevens die in de vorige hoofdstukken zijn omschreven. Welke risico's of problemen zien we ten aanzien van de gegevens die wij verwerken (b.v. basis principes persoonsgegevensverwerking, beveiliging van de gegevens), en in een bredere context, welke mogelijke impact op personen wiens gegevens verwerkt worden (b.v. rechten van het individu, redelijke verwachtingen, gevoeligheid van de gegevens, mogelijke gevolgen van een datalek).

5.1 Risicoanalyse methodologie

De risico-inventarisatie is gebaseerd op twee vragen:
Hoe groot is de kans dat een risico zich voordoet? Hoe groter de kans, hoe groter de prioriteit.
Hoe groot is de kans dat daarbij ernstige gevolgen voor de cliënt optreden? Hoe groter de kans, hoe dringender het risico moet worden aangepakt.

RISICO-MATRIX			
	Ernst = 1 (klein)	**Ernst = 2 (matig)**	**Ernst = 3 (groot)**
Kans = 1 (klein)	**1**	**2**	**3**
Kans = 2 (matig)	**2**	**4**	**6**
Kans = 3 (groot)	**3**	**6**	**9**

Het **RISICO** van optreden = de **KANS** van optreden x de **ERNST** bij optreden.
Om de **KANS** te bepalen worden de volgende classificaties gehanteerd:

- Klein (1): praktisch onmogelijk of onwaarschijnlijk/< 1x per jaar
- Matig (2): kan voorkomen – is bekend dat het voorkomt / ≥ 1x per jaar maar < 1x per maand
- Groot (3): komt herhaaldelijk voor ≥ 1x per maand

Om de **ERNST** te bepalen worden de volgende classificaties gehanteerd:

- Klein (1): Geen / nauwelijks invloed op privacy. De gegevens worden alleen aan hen getoond die geautoriseerd zijn om de persoonsgegevens in te zien en te bewerken.
- Matig (2): Datalek binnen de organisatie. Slechts gewone persoonsgegevens (NAW) zijn in te zien voor niet geautoriseerde personen binnen de organisatie.
- Groot (3): Datalek binnen of buiten de organisatie. Niet alleen gewone persoonsgegevens maar ook bijzondere persoonsgegevens (ziekteverzuim) zijn in te zien voor personen buiten de organisatie.

5.2 Vastgestelde risico's

NR	OMSCHRIJVING	SCORE RISICO MATRIX
RISK-001	Datalek gewone cliëntgegevens binnen de organisatie	2
RISK-002	Datalek gewone cliëntgegevens buiten de organisatie	1
RISK-003	Datalek bijzondere cliëntgegevens binnen de organisatie	3
RISK-004	Datalek bijzondere cliëntgegevens buiten de organisatie	3
RISK-005	Datalek gewone cliëntgegevens externe partij	4
RISK-006	Datalek bijzondere cliëntgegevens externe partij	6

Omdat het risico van een datalek bij een externe partij niet bekend is, gaan we ervan uit dat de kans 'matig' is.

6 Genomen maatregelen

Voor alle genoemde risico's zijn de volgende maatregelen getroffen:

Privacy by design

- Bewustwording onder medewerkers en cliënten
- Gegevensbeschermingsbeleid is opgesteld en beschikbaar op de website
- Functionaris Gegevensbescherming is aangesteld binnen Breederzorg
- Verwerkingsovereenkomsten met externe partijen
- Inrichting opslag gegevens: sleutelbeheer en afsluitbare kasten, inbraaksysteem kantoorpand, permanent cameratoezicht, rolverdeling in ECD
- Informeren cliënten over privacyrisico's. Bewustwording onder cliënten.
- Clientgegevens en medewerker gegevens worden nooit over de telefoon gedeeld aan derden.
- Het gebruik van Whatsapp en andere niet-beveiligde communicatie apps zijn verboden.
- Afgedrukte documenten van bijvoorbeeld teamvergaderingen bevatten nooit de volledige naam van een cliënt maar geslacht en voorletter en woonplaats (Dhr T. eindhoven)
- Het veilig archiveren van documenten in afgesloten ruimtes. Sleutelbeheer in kaart.

- Vergrendelde papierbak voor privacygevoelige informatie

- Bewaartermijn van documenten opstellen
- Iedere medewerker heeft een beperkte toegang in het ECD (elektronisch cliënten dossier) waarmee slechts een deel van de informatie zichtbaar is. Deze rol toewijzing is per functie aanpasbaar.
- Iedere medewerkers heeft een beperkte toegang tot de server bestanden van Breederzorg.

Privacy by default

Technische en organisatorische maatregelen die Breederzorg, als standaard, de instellingen en functies van de producten of diensten op de meest privacy-vriendelijke stand zet. Gebruikers hoeven dus niets aan de instellingen en functies te wijzigen om hun privacy te beschermen.

- Automatisch vergrendelen en blokkeren op afstand van Ipad en telefoon bij verlies of diefstal
- Automatisch uitloggen bij geen gebruik van een systeem (server computer en ECD)
- Standaard vergrendeling van telefoonnummers en email adressen van medewerkers in het smoelenboek
- Wachtwoorden opslaan en automatisch inloggen is uitgeschakeld in de kantooromgeving