

BELEID VERWERKING PERSOONSGEGEVENS



onderlinge
UITVAARTZORG
NOORD VELUWE

Inhoud

1. Overwegingen	3
2. Verwerking van persoonsgegevens.....	4
2.1 Gegevens omtrent gezondheid	4
2.2 Controle persoonsgegevens	4
2.3 Bewaartermijn.....	4
2.4 Verwerker	4
2.5 De functionaris voor de gegevensverwerking	4
2.6 Data protection impact assessment.....	5
2.7 Privacy by design	5
2.8 Privacy by default	5
2.9 Verwerkingsregister	5
3. Doeleinden en grondslag voor de gegevensverwerking	6
4. Rechten van betrokkene	7
4.1 Informeren betrokkene	7
4.2 Inzage	7
4.3 Verbetering en aanvulling	7
4.4 Verwijdering en het recht op vergetelheid	7
4.5 Overdraagbaarheid.....	8
4.6 Gebruik gegevens marketingdoeleinden	8
4.7 Rechtsmiddelen betrokkene	8
5. Procedure inzake rechten betrokkene	9
6. Beveiligingsmaatregelen	10
7. Meldplicht datalekken.....	11
8. Actiepunten bestuur en medewerkers	12

1. Overwegingen

Het bestuur van Uitvaartzorg Noord Veluwe u.a. verwerkt in het kader van de bedrijfsvoering persoonsgegevens. In dit beleidsdocument worden de regels omtrent het verwerken van deze persoonsgegevens vastgelegd.

Het bestuur heeft de vertrouwelijke en zorgvuldige behandeling van persoonsgegevens hoog in het vaandel staan. Betrokkenen moeten erop kunnen vertrouwen dat zorgvuldig met hun gegevens wordt omgegaan.

Dit beleidsdocument vloeit voort uit de Algemene Verordening Gegevensbescherming (hierna: AVG). In de AVG worden waarborgen gegeven ter bescherming van persoonsgegevens. Deze waarborgen zullen in dit document nader uitgewerkt worden.

De AVG onderscheidt twee verschillende rollen in het proces van gegevensverwerking: de verwerkingsverantwoordelijke (hierna te noemen: de verantwoordelijke) en de verwerker. In het licht van de AVG moet Uitvaartzorg Noord Veluwe u.a. worden gezien als verantwoordelijke. Hier is namelijk sprake van een organisatie die puur voor haar eigen doeleinden gegevens verwerkt, zonder dat er andere partijen bij betrokken zijn. Ook wordt door Uitvaartzorg Noord Veluwe u.a. het doel en de middelen van de verwerking vastgesteld. In dit beleidsdocument zal dan ook uitgegaan worden van de rol van verantwoordelijke.

Op grond van de AVG heeft de verantwoordelijke de volgende verplichtingen:

- vastleggen van afspraken met eventuele verwerkers;
- voorafgaand informeren van betrokkenen;
- privacy by design toepassen;
- privacy by default toepassen;
- het bijhouden van een verwerkingsregister;
- de informatiebeveiliging op orde hebben;
- meldplicht datalekken;
- geheimhoudingsplicht.

Deze verplichtingen zijn in het beleidsdocument verwerkt.

2. Verwerking van persoonsgegevens

Het begrip persoonsgegevens wordt door ons ruim opgevat. Wij zien persoonsgegevens als alle informatie over een betrokkene waardoor hij/zij naar redelijke verwachting geïdentificeerd kan worden (ook al zou dit uiteindelijk niet lukken).

Wij beschouwen gegevens van overleden personen niet als persoonsgegevens. Ingeval er misbruik wordt gemaakt van gegevens van overleden personen, dan kunnen diens nabestaanden een beroep doen op onrechtmatige daad.

Met verwerking van persoonsgegevens bedoelen wij alles wat gedaan wordt met de persoonsgegevens, ook dit begrip vatten wij ruim op. Verwerking ziet bijvoorbeeld op het opslaan, wijzigen, raadplegen of vernietigen van persoonsgegevens. Tijdens dit hele proces van verwerking zullen wij de regels, zoals weergegeven in dit beleidsdocument, in acht nemen. Persoonsgegevens zullen door ons worden verwerkt op een jegens betrokkene rechtmatig, behoorlijk en transparante wijze.

Door ons worden niet meer persoonsgegevens vastgelegd dan strikt noodzakelijk is. De persoonsgegevens worden door ons strikt gecontroleerd. Op al onze medewerkers rust een geheimhoudingsplicht.

2.1 Gegevens omtrent gezondheid

Wij verwerken geen gegevens omtrent de gezondheid voor de beoordeling van het te verzekeren risico en de uitvoering van de overeenkomst.

2.2 Controle persoonsgegevens

Wij voeren jaarlijks, of zoveel vaker als dit nodig is, een controle uit waarbij wij de verzamelde persoonsgegevens toetsen op rechtmatige verkrijging, zorgvuldige toepassing, verenigbaarheid met de grondslag en verwerkingsdoeleinden. Ook toetsen wij of de persoonsgegevens daadwerkelijk nodig zijn om de activiteiten uit te kunnen voeren.

2.3 Bewaartermijn

Wij zullen de persoonsgegevens niet langer bewaren dan nodig is. Eén jaar na realisatie van het doel waarvoor wij de persoonsgegevens hebben verwerkt, worden ze gearchiveerd. Wij vernietigen op zorgvuldige wijze zeven jaar na het einde van de verzekering de gegevens, tenzij er aanleiding bestaat om niet of eerder tot vernietiging over te gaan.

2.4 Verwerker

Wanneer wij gebruik maken van een verwerker (een partij die ten behoeve van ons persoonsgegevens verwerkt, zonder aan ons rechtstreeks gezag onderworpen te zijn) stellen wij regels op met betrekking tot deze verwerker. Deze regels verwerken wij in een verwerkersovereenkomst of in onze algemene voorwaarden. Wij leggen onder andere vast het doel en de middelen van de verwerking, het vereiste beveiligingsniveau, de mogelijkheden tot audit/rapportage en de geheimhoudingsplicht van de verwerker.

2.5 De functionaris voor de gegevensverwerking

Sommige gegevensverwerkingen brengen zoveel privacy risico's met zich mee dat het verplicht is om een functionaris voor gegevensverwerking (hierna: FG) aan te wijzen. Wij vallen niet onder deze verplichtingen, en hebben dan ook geen FG.

2.6 Data protection impact assessment

In de AVG wordt het uitvoeren van de DPIA in een aantal gevallen verplicht. Er moet een DPIA uitgevoerd worden wanneer er sprake is van hoge risico's voor de rechten en vrijheden van de betrokkenen. In onze situatie is hier geen sprake van. Wij voeren dan ook geen DPIA uit.

2.7 Privacy by design

Wij nemen privacy vanaf het begin van het proces mee door na te denken over de benodigde technische en organisatorische maatregelen, en door deze vervolgens in te bouwen in onze processen en systemen. Hierdoor waarborgen wij de uitgangspunten van rechtmatige gegevensverwerking en bouwen wij de nodige waarborgen in ter naleving van de AVG.

2.8 Privacy by default

Indien er sprake is van standaardinstellingen bij de gegevensverwerking, dan zullen wij kiezen voor de standaardinstelling die het meest voldoet aan de regels van de AVG. Hierbij voorkomen wij dat gegevens onnodig openbaar worden gemaakt.

2.9 Verwerkingsregister

Wij houden een verwerkingsregister bij waarin de gegevens die worden verwerkt zijn opgenomen. In dit register is in ieder geval opgenomen:

- onze contactgegevens;
- de verwerkingsdoeleinden;
- een beschrijving van de categorieën van betrokkenen en van de categorieën van persoonsgegevens;
- de categorieën van ontvangers (waaronder eventuele verwerkers) aan wie gegevens zijn of zullen worden verstrekt;
- informatie over doorgiften aan derde landen;
- de beoogde bewaartermijnen;
- een beschrijving op hoofdlijnen van hoe de gegevens beveiligd zijn.

3. Doeleinden en grondslag voor de gegevensverwerking

Persoonsgegevens zullen door ons niet 'zomaar' worden verwerkt. De verwerkingsdoeleinden waarvoor wij persoonsgegevens verwerken zijn:

- Het beoordelen en accepteren van een cliënt (betrokkene).
- Het aangaan en uitvoeren van een overeenkomst met een cliënt (betrokkene).
- Het afwickelen van het betalingsverkeer.
- Het uitvoeren van gerichte marketingactiviteiten teneinde een relatie met een betrokkene tot stand te brengen en/of met een cliënt (betrokkene) in stand te houden, dan wel uit te breiden.
- Het voldoen aan een wettelijke verplichtingen, bijvoorbeeld Wft.
- Analyse ten behoeve van historische, statistische en wetenschappelijke doeleinden.
- Het beheren van een relatie met cliënt (betrokkene).
- Het voorkomen en bestrijden van fraude.

Om persoonsgegevens te mogen verwerken is een grondslag nodig. Wij verwerken persoonsgegevens op basis van één van de hieronder genoemde grondslagen:

- Betrokkene heeft toestemming gegeven.
- De verwerking vindt plaats in het kader van de uitvoering van de overeenkomst waarbij betrokkene partij is.
- De verwerking is in het gerechtvaardigd belang van de verantwoordelijke of een derde.
- De verwerking vindt plaats ter nakoming van een wettelijke plicht.

4. Rechten van betrokkene

De betrokkene heeft op grond van de AVG een aantal rechten. In dit onderdeel zullen wij hier een toelichting op geven. Allereerst zullen wij ingaan op onze informatieplicht jegens de betrokkene.

4.1 Informeren betrokkene

Wij informeren betrokkene over onderstaande rechten voordat betrokkene gegevens aan ons heeft verstrekt. Daarnaast informeren wij betrokkene voorafgaand over onze identiteit, onze contactgegevens en de doeleinden en grondslagen waarvoor wij gegevens verwerken. Ook verstrekken wij aan betrokkene informatie over de (soorten) ontvangers aan wie wij de gegevens verstrekken, alsook over eventuele doorgifte aan niet-EU-landen en de daarbij geboden waarborgen.

Als wij de gegevens niet zelf van de betrokkene verkrijgen, dan laten wij de betrokkene weten om wat voor (soorten) persoonsgegevens het gaat.

Verder laten wij de betrokkene weten hoe lang wij de gegevens bewaren en of de betrokkene wettelijk of contractueel verplicht is om de gegevens te verstrekken, en wat de mogelijke gevolgen zijn als deze niet worden verstrekt (bijvoorbeeld het niet tot stand kunnen komen van een overeenkomst).

4.2 Inzage

De betrokkene heeft het recht om de gegevens in te zien. Als betrokkene een beroep doet op inzage, verstrekken wij een kopie van alle gegevens die wij over de betrokkene verwerken. Doet de betrokkene het verzoek via e-mail of internet, dan beantwoorden wij het verzoek ook via e-mail of internet.

4.3 Verbetering en aanvulling

De gegevens van betrokkene zullen worden verbeterd als betrokkene terecht aangeeft dat de gegevens onjuist zijn, en (voor zover dat redelijk is gelet op de doelen van de verwerking) dat de gegevens aangevuld worden indien deze onvolledig zijn.

4.4 Verwijdering en het recht op vergetelheid

In een aantal gevallen heeft de betrokkene er recht op dat wij op verzoek van de betrokkene de gegevens verwijderen:

- De betrokkene trekt zijn toestemming in en er zijn geen andere grondslagen voor het bewaren van de gegevens.
- Betrokkene maakt bezwaar tegen de verwerking, en wij hebben geen belangen die zwaarder wegen dan het specifieke belang van betrokkene (en wij hebben geen andere grondslag voor het bewaren van de gegevens).
- Wij verwerken de gegevens alleen voor directe marketing-doeleinden.

Wij zullen de gegevens van betrokkene in ieder geval verwijderen wanneer wij:

- De gegevens onrechtmatig verwerken.
- Wettelijk verplicht zijn om de gegevens te verwijderen.
- Gegevens hebben die niet meer nodig zijn, gelet op de doeleinden waarvoor ze verwerkt worden.

Het recht op vergetelheid is een bijzondere vorm van verwijdering, het gaat hier om het recht om vergeten te worden. Wanneer wij op verzoek van betrokkene persoonsgegevens moeten verwijderen die door ons openbaar zijn gemaakt, dan zullen wij binnen redelijke grenzen ons inzetten om ook aan

anderen te laten weten dat de betrokkene graag wil dat iedere koppeling naar of kopie van de gegevens zal worden verwijderd.

Het recht op verwijdering en het recht op vergetelheid zijn niet van toepassing wanneer het noodzakelijk is dat wij de gegevens verwerken:

- In verband met het recht op vrijheid van meningsuiting en informatie.
- Om een wettelijke verplichting na te komen, een taak van algemeen belang te vervullen of openbaar gezag uit te oefenen.
- In het belang van de volksgezondheid.
- Voor archivering, onderzoek of statistiek (en verwijdering het doel daarvan zou ondergraven).
- In verband met een rechtszaak.

4.5 Overdraagbaarheid

De betrokkene heeft het recht op overdraagbaarheid van gegevens, dit wordt ook wel dataportabiliteit genoemd. Dit betekent dat betrokkene op verzoek de gegevens beschikbaar gesteld krijgt van ons op zo'n manier dat betrokkene de gegevens zelf weer makkelijk over kan dragen aan een andere verantwoordelijke.

De betrokkene kan een beroep doen op het recht van overdraagbaarheid onder drie voorwaarden:

- wij verwerken de gegevens op basis van toestemming van betrokkene of op basis van een overeenkomst;
- betrokkene heeft de gegevens zelf aan ons verstrekt;
- het gaat om digitale gegevens, dus niet om papieren dossiers.

4.6 Gebruik gegevens marketingdoeleinden

Naast het hierboven onder paragraaf 4.4 genoemde recht op verwijdering ingeval de gegevens alleen gebruikt worden voor directe marketingdoeleinden, heeft betrokkene het recht van verzet wanneer de gegevens deels worden gebruikt voor marketingdoeleinden.

Betrokkene kan aangeven geen marketing-informatie te willen ontvangen van ons. Na goedkeuring van dit verzoek zullen wij dit direct in onze administratie verwerken.

4.7 Rechtsmiddelen betrokkene

De betrokkene kan, als het verzoek niet goed is afgehandeld of de rechten zijn geschonden, een klacht (verzoek tot handhaving) indienen bij de Autoriteit Persoonsgegevens of een rechtszaak beginnen. De betrokkene heeft dan recht op vergoeding van de schade die is geleden.

5. Procedure inzake rechten betrokkene

Wij informeren betrokkene over hoe en waar een verzoek om informatie of een beroep op een recht kan worden gedaan. Indien een verzoek mondeling wordt gedaan, stellen wij het verzoek op schrift.

Een verzoek om informatie of een beroep op een recht door betrokkene zal in beginsel binnen één maand door ons worden behandeld. Als dat niet is gebeurd, dan zal binnen die periode van één maand in ieder geval door ons worden vermeld waarom het verzoek of beroep niet tijdig door ons is behandeld. Er worden door ons geen kosten gerekend voor informatieverstrekking.

De gevraagde informatie wordt door ons beknopt, eenvoudig, toegankelijk en begrijpelijk verstrekt aan betrokkene. Bij het verstrekken van informatie moeten wij vaststellen dat wij met de juiste betrokkene te maken hebben. Hiervoor kunnen wij aanvullende informatie verlangen, bijvoorbeeld legitimatie.

Wanneer wij een redelijke verwachting hebben dan een derde partij bezwaar heeft tegen de verstrekking van informatie of de uitoefening van een recht, dan stellen wij deze derde partij voorafgaand in de gelegenheid daarover een zienswijze te geven (indien evenredig).

6. Beveiligingsmaatregelen

Wij zullen technische en organisatorische maatregelen treffen om persoonsgegevens te beveiligen tegen verlies of onrechtmatige verwerking. Deze beveiligingsmaatregelen zullen een passend niveau van beveiliging, met inbegrip van vertrouwelijkheid, waarborgen. Er zal rekening worden gehouden met de stand van de techniek en de uitvoeringskosten, afgezet tegen de risico's en de aard van de te beschermen persoonsgegevens. Uitgangspunten die wij hierbij zullen gebruiken zijn:

- *Het pseudonimiseren van persoonsgegevens.* Dit is het zodanig verwerken van persoonsgegevens dat deze zonder aanvullende gegevens niet herleidbaar zijn, bijvoorbeeld door kantnamen te vervangen door nummers en de koppeling elders op te slaan.
- *Het versleutelen van persoonsgegevens.* Versleutelen is het langs wiskundige (cryptografische) weg omzetten van gegevens tot een onbruikbare brij zodanig dat zonder de sleutel de gegevens niet hersteld kunnen worden. De keuze van een goed cryptografisch algoritme en een vooral een sterke, lastig te raden sleutel zijn hierbij cruciaal. Net als bij pseudonimisering zijn bij het versleutelen de persoonsgegevens veel minder bruikbaar in geval van onrechtmatige toegang.
- *Het vermogen om op permanente basis de vertrouwelijkheid, integriteit, beschikbaarheid en veerkracht van de verwerkingsystemen en diensten te garanderen.* Een andere belangrijke waarborg is een kwalitatief goede inrichting van de diensten en systemen. Deze zal gericht zijn op een goede beschikbaarheid en veerkracht (om kunnen gaan met storingen), en ontwikkeld zijn om persoonsgegevens vertrouwelijk en met integriteit (weerstand tegen ongewenste aanpassingen of wissingen) te kunnen behandelen.
- *Een procedure voor het op gezette tijden testen, beoordelen en evalueren van de doeltreffendheid van de technische en organisatorische maatregelen ter beveiliging van de verwerking.*

Wij zullen in ieder geval elk jaar, of zoveel vaker als dit nodig is, een inventarisatie maken met bijbehorende risicoanalyse maken. Op grond hiervan zullen beveiligingsmaatregelen worden genomen. Hierbij kan worden gedacht aan:

- toegangsbeveiliging, beveiliging verbindingen en beveiliging gegevens (autorisaties, versleuteling, hashing);
- Bijhouden en vastleggen van toegang tot vertrouwelijke gegevens (wie heeft toegang gehad tot gegevens);
- maatregelen om vooraf de gevolgen van een eventueel beveiligingsincident te beperken (versleuteling, hashing, remote wissen);
- maatregelen om beveiligingsincidenten te detecteren (logging, geautomatiseerde controle op hacks, malware e.d.);
- opzetten procedure en aanwijzen verantwoordelijke voor incidentenbeheer en de opvolging van beveiligingsincidenten (waaronder meldplicht datalekken);
- inrichten continuïteitsbeheer bij calamiteiten (brand, faillissement, uitval apparatuur).

7. Meldplicht datalekken

Van een datalek is sprake wanneer persoonsgegevens daadwerkelijk zijn vernietigd of verloren, gewijzigd, verstrekt of toegankelijk gemaakt, alles op een manier die onrechtmatig is oftewel buiten de regels van de AVG plaatsvindt; persoonsgegevens komen waar zij niet behoren te zijn.

De AVG kent een registratieplicht en een meldplicht voor datalekken. Daarom zullen wij een registratie bij houden van alle datalekken die in de organisatie plaatsvinden. Daarin zal in ieder geval bijgehouden worden: de details van het datalek, de gevolgen die het had voor de betrokkenen, en de corrigerende maatregelen die zijn genomen.

Elk datalek zal door ons worden gemeld aan de Autoriteit Persoonsgegevens, tenzij het lek geen risico's inhoudt voor de rechten en vrijheden van betrokkenen. Een datalek zal binnen 72 uur nadat het bekend is geworden door ons worden gemeld aan de Autoriteit Persoonsgegevens, tenzij dat echt niet lukt. In dat geval zullen wij binnen drie dagen een gedeeltelijke of pro forma melding doen. Een datalek zal door ons ook aan de betrokkenen worden gemeld wanneer er een hoog risico bestaat dat de rechten en vrijheden van betrokkenen door het datalekken worden aangetast.

8. Actiepunten bestuur en medewerkers

Wat:	Hoe:	Aktie OUNV:
Het vastleggen van afspraken met eventuele verwerkers	Door een verwerkersovereenkomst.	Deze maken voor: van Deutekom, VWC, Arch-It, Profinis
Voorafgaand informeren betrokkenen	Voordat betrokkene informatie aan ons verstrekt, informeren wij betrokkene over de rechten en andere informatie. Dit doen wij bijvoorbeeld door een privacyverklaring.	Staat op: Leden en Depositofonds aanmeldingsformulieren, machtigingsformulieren en begrotingen
Privacy by design toepassen	Vanaf het begin privacy meenemen in het proces door na te denken over de benodigde technische en organisatorische maatregelen, en door deze vervolgens in te bouwen in processen en systemen.	Voor zover als mogelijk wordt gebruik gemaakt van geanonimiseerde gegevens. Ook is het systeem ingericht op data-minimalisering (zo min mogelijk gegevens vastleggen)
Privacy by default toepassen	Ingeval van standaardinstellingen kiezen voor de standaardinstelling die het meest aansluit bij de regels van de AVG, zodat gegevens niet onnodig openbaar worden gemaakt.	De instellingen van de programmatuur, website en in te vullen documenten zijn zodanig dat maximale privacy wordt betracht.
Het bijhouden van een verwerkingsregister	Het bijhouden van een register waarin een aantal gegevens over verwerkingen worden opgenomen.	Zie concept verwerkingsregister
De informatiebeveiliging op orde hebben	Het treffen van technische en organisatorische maatregelen om persoonsgegevens te beveiligen tegen verlies of onrechtmatige verwerking. Hierbij zal rekening worden gehouden met de stand van de techniek en de uitvoeringskosten, afgezet tegen de risico's en de aard van de te beschermen persoonsgegevens.	Wachtwoordbeveiligingen pc's, afsluiten deuren kantoor en kasten
Meldplicht datalekken	Het bijhouden van een registratie van alle datalekken. Een datalek dat risico's inhoudt voor de rechten en vrijheden van betrokkenen, zal door ons binnen 72 uur worden gemeld bij de Autoriteit Persoonsgegevens. Wanneer er sprake is van een hoog risico, zullen ook de betrokkenen door ons worden geïnformeerd.	Indien er een datalek geconstateerd wordt, register aanmaken en genoemde acties uitvoeren.

Geheimhoudingsplicht	Binnen de organisatie gebruik maken van geheimhoudingsovereenkomsten en hier ook handhavend op toe zien.	Het personeel heeft middels de arbeidsovereenkomst (Art. 9) getekend voor geheimhouding.
Jaarlijks, of zoveel vaker, controles uitvoeren	Het uitvoeren van de controles zoals deze in dit document zijn opgenomen.	Jaarlijks, of zoveel vaker als dit nodig is, een controle uitvoeren waarbij de verzamelde persoonsgegevens toetsen op rechtmatige verkrijging, zorgvuldige toepassing, verenigbaarheid met de grondslag en verwerkingsdoeleinden. Ook toetsen of de persoonsgegevens daadwerkelijk nodig zijn om de activiteiten uit te kunnen voeren.