**Privacy Policy – Beleidstekst over Gegevensbescherming**

# Inleiding: Het beleid voor gegevensbescherming van Capenberg Oxaco Center vzw

Voor Capenberg Oxaco Center vzw is het beschermen van de persoonlijke levenssfeer een belangrijk gegeven en een wettelijke verplichting die Capenberg Oxaco Center vzw hoog in het vaandel draagt.

Met deze beleidstekst willen we toelichten op welke manier we de rechten en vrijheden van de residenten, medewerkers en andere betrokkenen vrijwaren wanneer we persoonsgegevens verwerken, zowel op papier als in de digitale informatieomgeving.

We besteden hierbij bijzondere aandacht aan meer risicovolle verwerkingen van persoonsgegevens, zoals het uitwisselen van deze gegevens met andere actoren en het verwerken van de gegevens buiten het strikte kader van toedienen van zorg. We hebben ook oog voor het verwerken van persoonsgegevens van onze personeelsleden en andere actoren binnen het woonzorgcentrum. Zeker wanneer we hierbij technologieën gebruiken die, zonder bescherming, een inbreuk kunnen zijn op hun persoonlijke levenssfeer.

We willen duidelijke doelstellingen formuleren, waarbij we ons in de eerste plaats laten inspireren door het wetgevend kader, meer in het bijzonder verordening (EU) 2016/679 van het Europees Parlement en de Raad van 27 april 2016 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens. Hoewel deze verordening het algemene kader schept voor de verwerking van persoonsgegevens, hebben we hierbij ook oog voor andere relevante wetgeving zoals de wet op de patiëntenrechten.

# De uitvoering van het beleid voor gegevensbescherming

Het beleid voor gegevensbescherming zal in een eerste fase geïmplementeerd worden aan de hand van een implementatieplan. Na de implementatiefase zal dit beleid verder worden opgevolgd via permanente controles en verbeterplannen. We beogen bijgevolg evolutieve herziening van dit beleid.

Na 25 mei 2018 zal deze beleidstekst periodiek of bij belangrijke wijzigingen opnieuw ter goedkeuring voorgelegd worden aan de directie en de Raad van Bestuur van het Capenberg Oxaco Center vzw. Daarbij toetsen we de nieuwe regelgevende kaders af met deze beleidstekst. Op korte termijn hebben we oog voor de (EU) ePrivacy verordening en de (EU) richtlijn voor de beveiliging van informatienetwerken en -systemen.

# De scope van het beleid gegevensbescherming

## Materieel toepassingsgebied

Het beleid is van toepassing op alle persoonsgegevens die Capenberg Oxaco Center vzw verwerkt. We verstaan hieronder niet alleen de gegevens van onze patiënten, maar ook bijvoorbeeld van medewerkers, al dan niet in dienstverband.

## Functioneel toepassingsgebied

Het beleid is van toepassing op alle verwerkingsdoelen. Zowel gegevens die worden verwerkt voor de zorg van de resident, rapporteringsdoeleinden, gemachtigde extramurale gegevensstromen, administratie van medewerkers, financiële gegevens, persoonsgegevens die verwerkt worden in het kader van kwaliteitscontroles of risicobeoordelingen behoren tot de scope van het beleid voor gegevensbescherming.

## Organisatorisch toepassingsgebied

Deze beleidstekst is geschreven voor iedereen die in opdracht van Capenberg Oxaco Center vzw persoonsgegevens verwerkt. Zowel de directie, het management, de personeelsleden en artsen, maar ook elke medewerker of leverancier. We zorgen ervoor dat deze tekst via verschillende kanalen wordt uitgedragen en wordt gepubliceerd.

Het beleid gegevensbescherming is voor Capenberg Oxaco Center vzw het uitgangspunt in haar samenwerking met andere zorginstellingen en -verstrekkers,. De veiligheidsconsulent waakt erover dat de principes van dit veiligheidsbeleid wordt toegepast in alle samenwerkingsverbanden die Capenberg Oxaco Center vzw opzet in de zorg.

# Beleidsdoelstellingen voor gegevensbescherming

Kwaliteitsvolle zorg is een topprioriteit voor Capenberg Oxaco Center vzw . Een belangrijk aspect hierbij is een kwaliteitsvolle verwerking van persoonsgegevens. De directie en het beheer van Capenberg Oxaco Center vzw streeft aan de hand van dit beleid na dat de rechten en vrijheden van eenieder gevrijwaard zijn bij de verwerking van persoonsgegevens. Het uitschrijven van dit beleid heeft als doel om het correct omgaan met persoonsgegevens aan te tonen. Het bespreekt hierbij de beleidsdoelstellingen en formaliseert deze. Het verduidelijkt de cultuur van gegevensverwerking met respect voor eenieders rechten en vrijheden.

Concreet streeft Capenberg Oxaco Center vzw volgende doelstellingen na:

1. Is **transparant** over de persoonsgegevens die het verwerkt en het verwerkingsdoel, zowel naar de betrokkene als naar de toezichthouders. De gevoerde communicatie is eerlijk, eenvoudig toegankelijk en begrijpelijk. Het transparantieprincipe is ook van toepassing wanneer de persoonsgegevens worden uitgewisseld.
2. Verwerkt enkel de gegevens die **relevant** zijn voor het uitvoeren van haar taken. Elke taak waarbij persoonsgegevens worden verwerkt, is **rechtmatig**. Dit betekent onder meer dat de verwerking in overeenstemming is met de wettelijke en statutaire doelen van Capenberg Oxaco Center vzw . Dit wordt telkens geëvalueerd bij een nieuw verwerkingsdoel.
3. Verwerkt enkel de persoonsgegevens die **strikt noodzakelijk** voor de uitvoering van de activiteiten. Zo worden identificatoren die horen bij de persoonsgegevens tot een minimum herleid.
4. Kijkt toe op de **integriteit** van de persoonsgegevens gedurende de ganse verwerkingscyclus.
5. **Bewaart** gegevens niet langer dan noodzakelijk. De noodzakelijkheid is afgetoetst tegenover wettelijke verplichtingen, de doelmatigheid en de rechten en vrijheden van de betrokkene.
6. Doet alle mogelijke inspanningen tot het voorkomen van **inbreuken die voortvloeien uit het** **verwerken** van persoonsgegevens. Informatieveiligheid, gegevensbescherming bij ontwerp en privacy-vriendelijke standaardinstellingen zijn hiervoor hulpmiddelen. Wanneer een inbreuk plaatsvindt, wordt hierover **gerapporteer**d in lijn met de regelgeving ter zake.
7. Doet alle nodige inspanningen om alle geldende **rechten van een betrokkene**, zoals het recht op inzage, afschrift en eventueel ook schrapping uit te voeren. Capenberg Oxaco Center vzw bewaakt hierbij over de eventuele beperkingen die op deze rechten van toepassing zijn.
8. Waakt er actief over dat bij het verwerken van de persoonsgegevens voor een welbepaald doel, de **rechten en vrijheden** (bijvoorbeeld recht op verzekerbaarheid, recht op zorg) van de betrokkene gevrijwaard blijven.
9. Waakt erover dat de verwerking van gegevens in lijn ligt met de rechten en vrijheden die gelden in de Europese Economische Ruimte en controleert de toepassing hiervan wanneer de gegevens worden uitgewisseld daarbuiten. Capenberg Oxaco Center vzw doet bijgevolg alle nodige inspanningen teneinde **alle wettelijke en normerende kaders na te leven** (i.e. zowel Vlaamse, Federale als Europese regels) bij het verwerken van persoonsgegevens en heeft daartoe haar verantwoordelijkheid over de persoonsgegevens en die van andere duidelijk in kaart gebracht. Capenberg Oxaco Center vzw monitort daarenboven ook de in de sector geldende gedragscodes teneinde deze toe passen.
10. Bewaakt haar **verantwoordingsplicht** door intern toezicht en controle en dit op basis van de wettelijk geldende principes.

# De beleidstaken en bijhorende processen

Om de beleidsdoelstellingen te bereiken zijn een aantal taken vastgelegd. Deze taken zijn in lijn met alle wettelijke verplichtingen die Capenberg Oxaco Center vzw dient na te streven. Daarnaast is de lijst van taken, zoals hieronder beschreven, geïnspireerd op praktijken van de Goede Huisvader.

Elke taak die wordt beschreven, wordt ondersteund door een proces. De algemene verantwoordelijkheid voor het uitvoeren van deze taken berust bij de directie van Capenberg Oxaco Center vzw. De specifieke taken en de delegatie van de taken zijn opgenomen in hoofdstuk 7.

De beleidstaken zijn hieronder opgelijst en worden kort besproken.

Capenberg Oxaco Center vzw :

1. Houdt permanent een **register bij van de verwerkingsactiviteiten** waarbij persoonsgegevens van de categorieën van betrokkenen (i.e. medewerkers, residenten, …) worden verwerkt. Dit omvat een overzicht van verwerkingsdoelen en de hierbij horende categorieën van persoonsgegevens. Voor elk verwerkingsdoel wordt in dit register onder meer ook opgenomen welke categorieën van, het al dan niet uitwisselen van deze gegevens en de categorieën van ontvangers.

Het verwerkingsregister wordt bijgewerkt voorafgaand aan het inrichten van nieuwe verwerkingsdoelen en bijhorende processen. Op dat moment wordt het afgetoetst aan de wettelijke en statutaire taken van Capenberg Oxaco Center vzw. Elke verdere verwerking van de persoonsgegevens, bijvoorbeeld voor onderzoek en kwaliteit, ondergaat eveneens een toets van het doel, de doelbinding en gegevensminimalisatie. We waken hierbij over de verenigbaarheid van het nieuwe doel met het oorspronkelijke doel.
Capenberg Oxaco Center vzw houdt het verwerkingsregister bij in digitale vorm en is opvraagbaar volgens de wettelijke bepalingen (i.e. door de Gegevensbeschermingsautoriteit).

1. Stelt een lijst op van criteria die kunnen worden gebruikt om te identificeren of een verwerking een verhoogd risico inhoudt voor de betrokkene. Wanneer dit noodzakelijk is, wordt een **gegevensbeschermingseffectenbeoordeling** uitgevoerd voorafgaand aan de verwerking. Op basis van deze analyse worden maatregelen genomen zodat tijdens de verwerking het risico op een inbreuk beperkt wordt. Indien de risico’s die horen bij de verwerking een te hoog risico blijven betekenen, ook nadat de maatregelen zijn toegepast, worden deze voorgelegd aan de Gegevensbeschermingsautoriteit. Capenberg Oxaco Center vzw beheert naast de lijst van criteria voor het uitvoeren van deze analyse, ook het bedrijfsproces voor het initiëren, bewaken, bijwerken en uitvoeren ervan.
2. Beheert de contractuele bepalingen met **verwerkers,** waarin onder meer de instructies die horen bij de verwerking worden opgelijst, alsook alle verplichtingen waaraan de verwerker moet voldoen in het kader van het naleven van wet- en regelgeving, waaronder de bepalingen rond informatieveiligheid. Capenberg Oxaco Center vzw voert actief toezicht uit op deze contractuele bepalingen. Daar waar de verwerking plaatsvindt onder een **gemeenschappelijke verantwoordelijkheid**, worden duidelijke afspraken gemaakt met het oog op de toepassing van de rechten van de betrokkene en de informatieplicht, tenzij deze verantwoordelijkheid in de wet- en regelgeving is opgenomen. Daarnaast worden ieders verantwoordelijkheden duidelijk gedocumenteerd en gecommuniceerd naar de betrokkene.
3. Voorziet de nodige processen die ervoor zorgen dat de betrokkene wordt **geïnformeerd** over de verwerking. De verstrekte informatie omvat de wettelijk opgelegde elementen, waaronder volgende: de functionaris voor de gegevensverwerking of de data protection officer (DPO), het verwerkingsdoel en de ontvangers van de gegevens. Daarnaast zijn processen gedocumenteerd die de rechten van de betrokkene omvatten (het recht op inzage, afschrift, gegevenswissing, overdraagbaarheid, rectificatie, beperking van de verwerking, kennisgeving). Deze processen houden rekening met de beperkingen die van toepassing zijn uit hoofde van de wet (patiëntenrechten en de verordening 2016/679).
4. Zorgt voor maatregelen ter identificatie van **inbreuken** (preventief), het melden ervan door de personen die deelnemen aan het verwerkingsproces en de afhandeling ervan. Onder de maatregelen die te maken hebben met de afhandeling worden begrepen: het incident afhandelingsproces, de interne communicatie, de registratie van inbreuken in een intern register, de communicatie naar de Gegevensbeschermingsautoriteit en de betrokkene, inclusief de criteria die bepalen wanneer deze communicatie moet plaatsvinden.
5. Zorgt voor **duidelijke instructies en richtlijnen**, in overeenstemming met de verantwoordelijkheden die medewerkers van Capenberg Oxaco Center vzw ten aanzien van persoonsgegevens hebben, alsook verantwoordelijkheden van verwerkers. Deze instructies worden via procedures, bewustwordingssessies, functiebeschrijvingen en opleidingen gecommuniceerd. De naleving van de verplichtingen worden afgedwongen aan de hand van het arbeidsreglement.

# De organisatie van gegevensbescherming

|  |  |
| --- | --- |
| **Verantwoordelijkheid over persoonsgegevens** | De verantwoordelijkheid voor het uitvoeren van de beleidstaken in het kader van gegevensbescherming ligt bij de directie. De directie is verantwoordelijk voor het bekrachtigen van de beleidsdoelen en de hierbij horende taken. In de uitvoering van deze verantwoordelijkheden kan de directie beroep doen op de adviezen van de functionaris voor de gegevensbescherming of data protection officer (DPO). Elke beoordeling van risico’s vindt plaats onder verantwoordelijkheid van de directie, alsook de uitvoering van de bijhorende maatregelen. De directie is daarnaast ook eindverantwoordelijk voor alle verplichtingen uit hoofde van de wet- en regelgeving, waaronder de bepalingen in de verordening 2016/679. Hiervoor delegeert de directie een aantal taken, zoals hieronder opgesomd. |
| **Toezicht gezondheidsgegevens patiënten** | De Dagelijkse Verantwoordelijke (en voor verpleegkundige gegevens in nauwe samenspraak met de hoofdverpleegkundige) heeft vanuit deze opdracht de verantwoordelijkheid inzake de gegevensbescherming van gezondheidsgegevens in het zorgdossier. In de uitvoering van het beleid voor gegevensbescherming krijgt de Dagelijkse Verantwoordelijke de taak toegewezen om te oordelen over de gegevensclassificatie, in relatie met de bijhorende zorgprocessen en andere processen, zoals processen ter evaluatie van de goede werking inzake risicobeheer en veiligheid van de residenten en de verwerking van persoonsgegevens die hiermee verband houden, registratie van activiteiten enz. Op basis van de vooropgestelde classificatie wordt door de DPO criteria vastgelegd en vertaald voor het uitvoeren van een gegevensbeschermingseffectenbeoordeling, het melden van inbreuken, specifieke technische en/of organisatorische maatregelen inclusief gegevensbescherming door ontwerp en door standaardinstellingen en de mogelijkheden daartoe. De Dagelijkse Verantwoordelijke stimuleert de correcte omgang met residentengegevens bij het verzorgend en verplegend personeel van Capenberg Oxaco Center vzw. De Dagelijkse Verantwoordelijke kijkt toe op het onderhoud van het register van verwerkingsactiviteiten met het oog op de verwerking van gezondheidsgegevens. |
| **Toezicht administratieve en financiële gegevens patiënten** | Het secretariaat onder verantwoordelijkheid van de directeur van Capenberg Oxaco Center stelt het register van verwerkingsactiviteiten op binnen de dienst residentenadministratie. De dienst duidt hierbij duidelijk aan welke persoonsgegevens worden ingezameld op basis van een toestemming. De dienst residentenadministratie richt op vraag van de DPO de nodige processen in met het oog op het verstrekken van informatie aan de resident en vragen met betrekking tot de rechten van de resident. De beoordeling van de risico’s met betrekking tot de identificatie van de resident en het beheer van dubbele residentendossiers behoort tot de aandachtsgebieden. Specifieke aandacht gaat uit naar het registreren van toestemmingen in het kader van eHealth, de registratie van verwijzers en de huisarts en de identificatie van de resident, waaronder de gegevensstromen met het rijksregister. |
| **Toezicht persoonsgegevens medewerkers** | Het secretariaat onder verantwoordelijkheid van de directeur krijgt in het beleid voor gegevensbescherming de taak om de gegevensbescherming te bewaken van persoonsgegevens van alle medewerkers. Het is de taak van het secretariaat om bij de implementatie van verwerkingsprocessen waarbij de persoonsgegevens van medewerkers worden verwerkt, het beschreven beleid te vertalen en toe te passen. Het secretariaat levert daarenboven een actieve bijdrage bij het onderhouden van het register van verwerkingsactiviteiten voor personeelsgegevens. |
| **Toezicht toepassing gegevensbescherming door medewerkers** | De directeur heeft de verantwoordelijkheid om de verplichtingen inzake het toepassen van dit beleid te vertalen naar het arbeidsreglement, de toepasselijke handvesten en functieprofielen, het sanctiebeleid en de controles en evaluaties.  |
| **Algemeen toezicht gegevensbescherming bij verwerkers** | Het algemeen toezicht op verwerkers van persoonsgegevens die in opdracht van Capenberg Oxaco Center vzw persoonsgegevens verwerken, wordt uitgevoerd door de DPO voor wat betreft de informatieveiligheid en van het diensthoofd van de dienst waarvoor de verwerking wordt uitgevoerd. |
| **Uitoefenen van de rechten van de betrokkene** | De ombudsfunctie wordt ingevuld volgens de bepalingen in de wet patiënten rechten. In de uitvoering van de taak adviseert de DPO over antwoorden op vragen van de resident betreffende de verwerking van diens persoonsgegevens.  |

# DPO

De directie wordt uit hoofde van verantwoordelijke voor de verwerking geadviseerd door de functionaris voor de gegevensbescherming of DPO.

De DPO adviseert de directie en de Raad van Bestuur inzake alle verantwoordelijkheden die de organisatie rond gegevensbescherming draagt:

* + Het bijsturen van het beleid inzake gegevensbescherming
	+ Het aanstellen van een functionaris voor de gegevensbescherming
	+ Het bewaken van de onafhankelijkheid van de functionaris voor de gegevensbescherming
	+ Het monitoren van de bedrijfsprocessen die in deze beleidstekst zijn beschreven met het oog op gegevensbescherming
	+ Het formuleren van adviesvragen
	+ Het bijsturen van het beleid en de uitvoering ervan op advies van de functionaris
	+ De beslissingen inzake risicobeheer bij het verwerken van persoonsgegevens. De tijdsbesteding van de functionaris is een onderdeel van dit risicobeheer.
	+ De goedkeuring van de classificatieschema’s die bijvoorbeeld bepalen wanneer een gegevensbeschermingseffectenbeoordeling dient plaats te vinden, evenals de classificatieschema’s voor het melden van inbreuken.
	+ De inrichting en het in stand houden van de bedrijfsprocessen die in deze beleidstekst zijn omschreven
	+ Het toekennen van de verantwoordelijkheden voor het uitvoeren van de bedrijfsprocessen
	+ Beslissingen over alle overwegingen uit hoofde van de verordening 2016/679, waaronder verwerkingen gebaseerd op gerechtvaardigd belang, waaronder deze die betrekking hebben op kinderen, alsook beslissingen inzake de verenigbaarheid van de doelen bij een latere verwerking van persoonsgegevens
	+ Het aanleggen van de nodige documentatie bij alle (voorstellen tot) beslissingen
	+ Het formaliseren van de beslissingen door de directie
	+ De toepassing van de sancties bij overtredingen
	+ De rapportering van het beleid gegevensbescherming naar onder meer accreditatiecommissies.
	+ Toekijken op de toepassing van het beleid in horizontale en verticale zorgnetwerken.