# Beleid voor gegevensbescherming Az Damiaan

# 1. Inleiding: Het beleid voor gegevensbescherming van Az Damiaan

Het beschermen van de persoonlijke levenssfeer is een belangrijk strategisch doel en bovenal een wettelijke verplichting die Az Damiaan hoog in het vaandel draagt.

Met deze beleidstekst willen we toelichten op welke manier we de rechten en vrijheden van de patiënten, medewerkers, contractanten en andere personen ('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, het verwerken van de gegevens buiten het strikte kader van toedienen van zorg (zoals het gebruik van persoonsgegevens voor onderzoek en kwaliteit) of het gebruik van de persoonsgegevens in zorginnovatie. We hebben ook oog voor het verwerken van persoonsgegevens van onze personeelsleden, artsen en andere actoren binnen het ziekenhuis. Zeker wanneer we hierbij technologieën gebruiken die, zonder bescherming, een inbreuk kunnen zijn op hun persoonlijke levenssfeer.

Het doel van deze beleidstekst is in de eerste plaats strategisch. 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.

Daarnaast is deze beleidstekst tactisch. We lichten toe op welke manier we de organisatie van gegevensbescherming voorzien voor Az Damiaan. We bespreken de beleidsorganen en de uitvoeringsmodaliteiten van dit beleid voor gegevensbescherming. We gaan bovendien verder in op alle verantwoordelijkheden die gepaard gaan met de uitvoering van het beleid gegevensbescherming.

## 2. De uitvoering van het beleid voor gegevensbescherming

Het beleid voor gegevensbescherming wordt in deze eerste fase (we schrijven deze tekst met het oog op 25 mei 2018, de datum waarop de verordening 2016/679 van kracht zal zijn) geïmplementeerd aan de hand van een implementatieplan. Na de implementatiefase zal dit beleid verder worden opgevolgd via permanente controles en verbeterplannen.

Na 25 mei 2018 zal deze beleidstekst periodiek of bij belangrijke wijzigingen opnieuw ter goedkeuring voorgelegd worden aan de directie, de Raad van Bestuur en de medische raad van Az Damiaan.
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.

## 3. De scope van het beleid gegevensbescherming

### 3.1 Materieel toepassingsgebied

Het beleid is van toepassing op alle persoonsgegevens[1] die Az Damiaan verwerkt. We verstaan hieronder niet alleen de gegevens van onze patiënten en bezoekers, maar ook bijvoorbeeld van medewerkers en contractanten.

### 3.2 Functioneel toepassingsgebied

Het beleid is van toepassing op alle verwerkingsdoelen. Zowel gegevens die worden verwerkt voor (niet limitatief) de zorg van de patiënt, wetenschappelijk onderzoek, rapporteringsdoeleinden, gemachtigde extramurale gegevensstromen, administratie van medewerkers en contractanten, financiële gegevens, persoonsgegevens die verwerkt worden in het kader van kwaliteitscontroles of risicobeoordelingen, alsook persoonsgegevens die in een gerechtelijke of forensische analyse worden verwerkt, behoren tot de scope van het beleid voor gegevensbescherming.

### 3.3 Organisatorisch toepassingsgebied

Deze beleidstekst is geschreven voor iedereen die in opdracht van Az Damiaan 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 op het intranet van Az Damiaan.

Het beleid gegevensbescherming is voor Az Damiaan het uitgangspunt in haar samenwerking met andere zorginstellingen en -verstrekkers, zoals haar participatie in de locoregionale zorgnetwerken. De DPO (Data Protection Officer) of in Az Damiaan de functionaris voor gegevensbescherming / informatieveiligheidsconsulent waakt erover dat de principes van dit veiligheidsbeleid worden toegepast in alle samenwerkingsverbanden die Az Damiaan opzet in de zorg.

[1] Dit geldt niet voor persoonsgegevens van overledenen, gezien zij niet onder de toepassing van de AVG vallen.

## 4. Beleidsdoelstellingen voor gegevensbescherming

Kwaliteitsvolle zorg is een topprioriteit voor Az Damiaan. Een belangrijk aspect hierbij is een kwaliteitsvolle verwerking van persoonsgegevens. De directie en het beheer van Az Damiaan 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 streven we volgende doelstellingen na: Az Damiaan:

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 Az Damiaan. 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, binnen de technische mogelijkheden. De noodzakelijkheid is afgetoetst tegenover wettelijke verplichtingen, de doelmatigheid, de proportionaliteit 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. Az Damiaan 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. Az Damiaan 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. Az Damiaan monitort daarenboven ook de in de sector geldende gedragscodes teneinde deze toe te passen.
10. Bewaakt haar **verantwoordingsplicht** door intern toezicht en controle en dit op basis van de wettelijk geldende principes.

## 5. De beleidstaken en bijhorende bedrijfsprocessen

Om de beleidsdoelstellingen te bereiken zijn een aantal taken vastgelegd. Deze taken zijn in lijn met alle wettelijke verplichtingen die Az Damiaan dient na te streven (het aantoonbaarheidsprincipe). 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 bedrijfsproces. De algemene verantwoordelijkheid voor het uitvoeren van deze taken berust bij het directiecomité van Az Damiaan. De specifieke taken en de delegatie van de taken zijn opgenomen in hoofdstuk 7.

Voor elk bedrijfsproces dienen **implementatienormen en -richtlijnen** te worden uitgeschreven. Deze vullen het beleid voor gegevensbescherming aan en maken er integraal deel van uit.

De beleidstaken zijn hieronder opgelijst en worden kort besproken.

Az Damiaan:

1. Houdt permanent een **register bij van de verwerkingsactiviteiten** waarbij persoonsgegevens van de categorieën van betrokkenen (i.e. medewerkers, contractanten, patiënten, …) 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, met een specifieke vermelding wanneer deze worden uitgewisseld buiten de Europese Economische Ruimte en de passende waarborgen die hierbij vereist zijn. Ook de bewaartermijn en de technische en organisatorische maatregelen zijn hierin opgenomen. Deze wettelijke elementen worden aangevuld met een aanduiding van de verwerkingsgrond.
   Het verwerkingsregister wordt bijgewerkt voorafgaand aan het inrichten van nieuwe verwerkingsdoelen en bijhorende bedrijfsprocessen. Op dat moment wordt het afgetoetst aan de wettelijke en statutaire taken van Az Damiaan. 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.
   Az Damiaan houdt het verwerkingsregister bij in digitale vorm en is opvraagbaar volgens de wettelijke bepalingen (i.e. door de Gegevensbeschermingsautoriteit).
2. 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. Az Damiaan beheert naast de lijst van criteria voor het uitvoeren van deze analyse, ook het bedrijfsproces voor het initiëren, bewaken, bijwerken en uitvoeren ervan.
3. 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. Az Damiaan kan actief toezicht uitoefenen 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.

4. Voorziet de nodige bedrijfsprocessen 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 gegevensbescherming of de data protection officer (DPO), het verwerkingsdoel en de ontvangers van de gegevens. Daarnaast zijn bedrijfsprocessen gedocumenteerd die de rechten van de betrokkene omvatten (het recht op inzage, afschrift, gegevenswissing, overdraagbaarheid, rectificatie, beperking van de verwerking, kennisgeving, overdraagbaarheid). Deze bedrijfsprocessen houden rekening met de beperkingen die van toepassing zijn uit hoofde van de wet (patiëntenrechten en de verordening 2016/679).
5. 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.
6. Zorgt voor **duidelijke instructies en richtlijnen**, in overeenstemming met de verantwoordelijkheden die medewerkers en contractanten van Az Damiaan ten aanzien van persoonsgegevens hebben, alsook (in beperkte mate) 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 of ander handvest en valt onder het toezicht op de medewerker. Overtredingen worden behandeld in lijn met de bepalingen inzake sancties die van toepassing zijn.

## 6. Toepassing van het beleid gegevensbescherming op de locoregionale netwerken

Az Damiaan beoogt de toepassing van de beleidsdoelstellingen niet alleen in de eigen zorgorganisatie, maar tracht de geldende principes ook te extrapoleren naar zorgnetwerken.

Bij de inrichting van een horizontaal zorgnetwerk ziet de beleidscel gegevensbescherming en informatieveiligheid toe op de impact van de samenwerking en de verantwoordelijkheid over de gegevensverwerking.

Bij de inrichting van een verticaal zorgnetwerk zal Az Damiaan haar Goede Huisvaderprincipes ook toepassen op de leden van het netwerk.

Overleg over de toe te passen beleidsprincipes worden op de overlegmomenten van het locoregionale netwerk besproken.

## 7. De organisatie van gegevensbescherming

In dit veiligheidsbeleid concretiseren we bovenstaande beleidstaken in een organisatiestructuur. Hiertoe wordt een matrix opgesteld waarin de beleidstaken worden uitgezet tegenover de verschillende verantwoordelijkheden. De matrix wordt opgesteld en onderhouden onder verantwoordelijkheid van de directie, op advies van de beleidscel gegevensbescherming en informatieveiligheid. De directie ziet toe op de uitvoering van de verantwoordelijkheden. Hieronder worden de belangrijkste taken beschreven.

**Verantwoordelijkheid over persoonsgegevens**

De verantwoordelijkheid voor het uitvoeren van de beleidstaken in het kader van gegevensbescherming ligt bij het directiecomité. Het directiecomité is verantwoordelijk voor het bekrachtigen van de beleidsdoelen en de hierbij horende taken. In de uitvoering van deze verantwoordelijkheden kan het directiecomité 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 het directiecomité, alsook de uitvoering van de bijhorende maatregelen. Het directiecomité is daarnaast ook eindverantwoordelijk voor alle verplichtingen uit hoofde van de wet- en regelgeving, waaronder de bepalingen in de verordening 2016/679. Hiervoor delegeert het directiecomité een aantal taken, zoals hieronder opgesomd.

**Toezicht gezondheidsgegevens patiënten**

Het beleid voor gegevensbescherming doet op geen enkele wijze afbreuk aan de wettelijke verplichtingen die de hoofdarts/Directeur patiëntenzorg hebben met het oog op de toepassing van de wetgeving over gegevensbescherming.
De hoofdarts wordt beschouwd als lasthebber van het ziekenhuis dat optreedt als de verwerkingsverantwoordelijke. De hoofdarts (en voor verpleegkundige gegevens in nauwe samenspraak met de directeur patiëntenzorg) heeft vanuit deze opdracht de verantwoordelijkheid inzake de gegevensbescherming van gezondheidsgegevens in het patiëntendossier. Bij belangrijke wijzigingen, zowel op technologisch vlak als op niveau van de verwerking zelf (zoals het invoeren van geautomatiseerde beslissingen of de inschalingen van zorgzwaartemetingen), assisteert de hoofdarts en de directeur patiëntenzorg in het uitvoeren van de gegevensbeschermingseffectenbeoordeling.
In de uitvoering van het beleid voor gegevensbescherming krijgt de hoofdarts de taak toegewezen om te oordelen over het ontwerp van een model van gegevensclassificatie, in relatie met de bijhorende bedrijfsprocessen (dit zijn zorgprocessen maar ook andere bedrijfsprocessen, zoals processen ter evaluatie van de goede werking inzake risicobeheer en veiligheid van de patiënten en de verwerking van persoonsgegevens die hiermee verband houden, registratie van ziekenhuisactiviteiten enz.). Op basis van de vooropgestelde classificatie worden door de beleidscel gegevensbescherming en informatieveiligheid 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 taak van de hoofdarts inzake het toepassen van de rechten van patiënten is opgenomen in de reglementen dienaangaande.
Voor de toepassing van de rechten van de betrokkene (in het bijzonder deze van de patiënt) voor gezondheidsgegevens die buiten het patiëntendossier worden verwerkt, assisteert de hoofdarts bij het uitwerken van de beleidslijnen.
De hoofdarts stimuleert de correcte omgang met patiëntengegevens bij de medische diensten van Az Damiaan. De hoofdarts neemt bovendien alle relevante aspecten van gegevensbescherming mee in de evaluatie van (kandidaat) artsen en hun opleidingstraject tijdens dienstverband.
De hoofdarts kijkt toe op het onderhoud van het register van verwerkingsactiviteiten met het oog op de verwerking van gezondheidsgegevens.

**Toezicht sociale gegevens patiënten**

De sociale dienst, onder verantwoordelijkheid van de directeur patiëntenzorg van Az Damiaan stelt het register van verwerkingsactiviteiten op en oordeelt hierbij ook over de toepassing van de rechten van de betrokkene op deze gegevens. In de uitvoering van het beleid voor gegevensbescherming krijgt de sociale dienst, onder verantwoordelijkheid van haar directeur, de taak toegewezen om te oordelen over het ontwerp van een model van gegevensclassificatie, in relatie met de bijhorende bedrijfsprocessen. Op basis van de vooropgestelde classificatie worden door de beleidscel gegevensbescherming en informatieveiligheid 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 sociale dienst heeft ook bijzondere aandacht voor de verwerking van persoonsgegevens op basis van toestemming, gerechtvaardigd belang en de verwerking van gegevens van kinderen. Ook de uitwisseling van persoonsgegevens met actoren in de sociale dienstverlening krijgen hierbij extra aandacht.

**Toezicht financiële gegevens patiënten**

De financiële dienst, onder verantwoordelijkheid van de financieel administratief directeur van Az Damiaan stelt het register van verwerkingsactiviteiten op binnen de financiële dienst. De financieel administratief directeur is verantwoordelijk voor het beoordelen van de rechten en vrijheden van de patiënt bij de verwerking van gegevens op de dienst (toegang tot zorg, het recht op zorg, verzekerbaarheid). De financiële dienst, onder verantwoordelijkheid van haar directeur, kijkt toe op de uitwisseling van persoonsgegevens met de overheid, de mutualiteiten, financiële instellingen, private zorgverzekeraars…

**Toezicht administratieve gegevens patiënten**

De dienst patiëntenadministratie, onder verantwoordelijkheid van de financieel administratief directeur van Az Damiaan stelt het register van verwerkingsactiviteiten op binnen de dienst patiëntenadministratie. De dienst duidt hierbij duidelijk aan welke persoonsgegevens worden ingezameld op basis van een toestemming. De dienst patiëntenadministratie richt op vraag van de beleidscel gegevensbescherming en informatieveiligheid de nodige processen in

met het oog op het verstrekken van informatie aan de patiënt en vragen met betrekking tot de rechten van de patiënt (in samenspraak met andere diensten, waaronder de dienst communicatie). De beoordeling van de risico's met betrekking tot de identificatie van de patiënt en het beheer van dubbele patiëntendossiers 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 patiënt, waaronder de gegevensstromen met het rijksregister.

**Toezicht latere verwerking gegevens patiënten**

De hoofdarts, de geneesheer-coördinatoren, de geneesheers-diensthoofden en de geneesheren die aan onderzoek doen houden toezicht op de verantwoordelijkheid bij de latere verwerking van de gezondheidsgegevens en voeren op basis van het oordeel over verantwoordelijkheden de verplichtingen uit met het oog op gegevensbescherming, waaronder het toezicht op de volledigheid van het verwerkingsregister, de overeenkomsten met verwerkers en de analyse van de risico's. Ook de rechten van de betrokkene, evenals eventuele toestemmingen, vallen onder hun beheer. Ze oordelen over de verantwoordelijkheid inzake de gegevensbescherming en stellen hiervoor een reglement op. Ze kijken toe op de toepassing daarvan. De hoofdarts houdt daarenboven het toezicht op de latere verwerking van gezondheidsgegevens die gestoeld is op de wettelijke basis. Informatieveiligheid is hierbij een expliciet onderdeel van het toezicht. In geval van een latere verwerking van gezondheidsgegevens waarvoor het advies van een ethisch comité wordt gevraagd, worden de modaliteiten voor gegevensbescherming afgetoetst.

Voor de latere verwerking van niet-medische persoonsgegevens is het diensthoofd van de dienst die de verwerking uitvoert, verantwoordelijk voor het toezicht. Wanneer deze latere verwerking plaatsvindt uit hoofde van een overheidsverplichting, dan gebeurt het toezicht eveneens door de dienst die hiermee belast is, in coördinatie met de beleidscel gegevensbescherming en informatieveiligheid en op advies van de functionaris voor gegevensbescherming.

De latere verwerking voor kwaliteitsdoeleinden en beleidsrapporteringen, vallen onder verantwoordelijkheid van de dienst aan wie de rapportering plaatsvindt in samenspraak met de datamanager. Het toezicht op de verwerker wordt georganiseerd door de datamanager en de functionaris voor gegevensbescherming / informatieveiligheidsconsulent.

De latere verwerking van gezondheidsgegevens uit het patiëntendossiers voor kwaliteitsdoeleinden ten behoeve van inspectiediensten of accrediteringscommissies, valt onder de verantwoordelijkheid van de hoofdarts.

**Toezicht persoonsgegevens medewerkers en contractanten**

De personeelsdienst, onder verantwoordelijkheid van de directeur HRM krijgt in het beleid voor gegevensbescherming de taak om de gegevensbescherming te bewaken van persoonsgegevens van alle medewerkers en contractanten (al dan niet in dienst), met uitzondering van de artsen. Het is de taak van de personeelsdienst om bij de implementatie van (nieuwe) verwerkingsprocessen waarbij de persoonsgegevens van medewerkers en contractanten worden verwerkt, het beschreven beleid te vertalen en toe te passen. Daar waar nieuwe bedrijfsprocessen worden ingevoerd of bestaande bedrijfsprocessen worden gedigitaliseerd, zorgt de directeur HRM voor de analyse van de verwerkingsgrond, de eventuele bijhorende besprekingen met de personeelsvertegenwoordiging (bijvoorbeeld in het kader van transparantie en de evaluatie van gerechtvaardigde belangen) en de bijhorende gegevensbeschermingseffectenbeoordeling. De directeur HRM levert daarenboven een actieve bijdrage bij het onderhouden van het register van verwerkingsactiviteiten voor personeelsgegevens.
Voor de verwerking van persoonsgegevens van artsen wordt de corresponderende taak toebedeeld aan de verantwoordelijke van de artsenadministratie onder verantwoordelijkheid van de hoofdarts.

**Toezicht toepassing gegevensbescherming door medewerkers en contractanten**

De directeur HRM heeft de verantwoordelijkheid om de verplichtingen inzake het toepassen van dit beleid te vertalen naar het arbeidsreglement, de toepasselijke handvesten en functieprofielen (met uitzondering van de verplichtingen van de artsen), het sanctiebeleid en de controles en evaluaties. Voor de corresponderende verplichtingen voor artsen wordt deze verantwoordelijkheid bij de hoofdarts gelegd.

**Algemeen toezicht gegevensbescherming bij verwerkers**

Het algemeen toezicht op verwerkers van persoonsgegevens die in opdracht van Az Damiaan persoonsgegevens verwerken, wordt uitgevoerd door de functionaris voor gegevensbescherming voor wat betreft de informatieveiligheid en van het diensthoofd van de dienst waarvoor de verwerking wordt uitgevoerd, in samenspraak met de juridische dienst en de functionaris voor de gegevensbescherming. De aankoopdienst voert de instructies hierover uit onder toezicht van het diensthoofd en de bedrijfskundig directeur.

**Gegevensbescherming bij zorginnovatie**

Elk bedrijfsproces dat gedigitaliseerd wordt of voor elk (al dan niet nieuw) bedrijfsproces waarbij innoverende technologieën worden gebruikt wordt de functionaris voor de gegevensbescherming geconsulteerd. De verantwoordelijkheid hiervoor ligt bij de initiatiefnemer. Voor wat betreft de artsen kijkt de hoofdarts, samen met de functionaris voor gegevensbescherming, toe op de correcte toepassing.

**Uitoefenen van de rechten van de betrokkene**

De ombudsfunctie wordt ingevuld volgens de bepalingen in de wet patiëntenrechten. In de uitvoering van de taak adviseert de functionaris voor gegevensbescherming, op vraag van de Ombudsdienst, over antwoorden op vragen van de patiënt betreffende de verwerking van diens persoonsgegevens. Dit antwoord is niet bindend voor de Ombudsdienst, zodat de onafhankelijkheid van deze functie

gevrijwaard blijft. Vragen die rechtstreeks aan de functionaris voor gegevensbescherming worden gesteld worden volgens dezelfde methodologie behandeld. Wanneer het wettelijk kader hierover wordt bijgestuurd met het oog op de verordening 2016/679 of latere wetgeving terzake, zal de verantwoordelijkheid dienaangaande worden bijgestuurd.

## 8. De relatie tussen gegevensbescherming en informatieveiligheid

Het toezicht op informatieveiligheid is de taak van de informatieveiligheidsconsulent.

Voor Az Damiaan wordt de rol van de informatieveiligheidsconsulent ingevuld door de functionaris voor gegevensbescherming. De informatieveiligheidsconsulent en de functionaris voor gegevensbescherming zijn één en dezelfde persoon.

De taken van de informatieveiligheidsconsulent zijn in lijn met het Besluit van de Vlaamse regering van 15 mei 2009 betreffende de veiligheidsconsulenten. Deze taken worden in de functiebeschrijving van de functionaris voor gegevensbescherming in een aparte rubriek opgenomen.

In overeenstemming met de (EU) verordening 2016/679 zorgt de informatieveiligheidsconsulent voor de verplichtingen krachtens Afdeling 2 (Persoonsgegevensbeveiliging) en meer in het bijzonder de beveiliging van de verwerking zoals bepaald in Artikel 32 en het toezicht op de organisatorische en technische maatregelen om te kunnen voldoen aan de verplichtingen zoals bepaald in artikels 33 en 34 (de melding van een inbreuk in verband met persoonsgegevens aan de toezichthoudende autoriteit en aan de betrokkene).

De identiteit van de informatieveiligheidsconsulent moet voorgesteld worden aan het sectoraal comité van de sociale zekerheid en de gezondheid, afdeling gezondheid.

De functionaris voor de gegevensbescherming is lid van de beleidscel gegevensbescherming en informatieveiligheid van Az Damiaan. Deze beleidscel bestaat verder uit de algemeen directeur, de directeur ICT, het diensthoofd operationeel beheer ICT, een stafmedewerker HRM en een stafmedewerker juridische zaken en beleid.

## 9. De beleidscel voor gegevensbescherming en informatieveiligheid

Het directiecomité wordt uit hoofde van verantwoordelijke voor de verwerking geadviseerd door de de Beleidscel voor gegevensbescherming en informatieveiligheid. Deze beleidscel wordt voorgezeten door de functionaris voor gegevensbescherming.

Deze beleidscel adviseert het directiecomité 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 gegevensbescherming
- Het bewaken van de onafhankelijkheid van de functionaris voor 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 het directiecomité
- Het toezicht op 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.

De samenstelling van de beleidscel wordt voorgelegd aan de Raad van Bestuur en het Directiecomité ter beslissing.