



**AZ JAN PORTAELS**  
Algemeen Ziekenhuis Vilvoorde

## **Gegevensbeschermingsbeleid Algemeen Ziekenhuis Jan Portaels VZW (AZJP)**

### **Inhoudsopgave**

1.	Inleiding: Het beleid voor gegevensbescherming	2
2.	De uitvoering van het beleid voor gegevensbescherming	2
3.	Begrippenkader	2
4.	De scope van het beleid gegevensbescherming	4
4.1	Materieel toepassingsgebied	4
4.2	Personeel toepassingsgebied	4
5.	Algemene doelstelling en principes bij gegevensverwerking	4
6.	Verplichtingen van AZJP als verwerkingsverantwoordelijke, gezamenlijke verwerkingsverantwoordelijke en/of verwerker	5
6.1	AZJP als verwerkingsverantwoordelijke	6
6.2	AZJP als gezamenlijke verwerkingsverantwoordelijke	7
6.3	AZJP als verwerker	7
7.	Toepassing van het beleid gegevensbescherming in zorgnetwerken	8
8.	De implementatie van het gegevensbeschermingsbeleid in de organisatiestructuur van het ziekenhuis	8
8.1.	Centraal: de verantwoordelijkheid voor de gegevensbescherming	8
	Raad van bestuur	8
	Delegatie aan het directiecomité	8
8.2.	Decentraal: operationele verantwoordelijkheid voor gegevensbescherming o.b.v. categorie van persoonsgegevens	9
8.3.	Stuurgroep Gegevensbescherming & Informatieveiligheid (SGI): voorbereiding en uitvoering van de beslissingen van het directiecomité	9
8.4.	Adviserend: de functionaris voor de gegevensbescherming (DPO)	9

## 1. Inleiding: het beleid voor gegevensbescherming

Voor AZJP is het beschermen van de persoonlijke levenssfeer en de daaraan verbonden grondrechten niet alleen een wettelijke verplichting, maar ook een belangrijke prioriteit die we hoog in het vaandel dragen.

Met deze beleidstekst willen we toelichten op welke manier we de rechten en vrijheden van de patiënten, medewerkers 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 (gevoelige) persoonsgegevens, zoals het uitwisselen ervan met andere actoren, het verwerken buiten het strikte kader van het toedienen van zorg (zoals het gebruik van persoonsgegevens voor onderzoek en kwaliteit) of het gebruik van deze 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 duidelijke doelstellingen te formuleren met betrekking tot gegevensbescherming in AZJP, 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, zonder andere relevante wetgeving zoals deze m.b.t. de patiëntenrechten, het beroepsgeheim, camerabewaking,... uit het oog te verliezen.

Daarnaast is het ook de bedoeling toe te lichten op welke manier we de gegevensbescherming binnen het AZJP concreet organiseren.

We bespreken de beleidsorganen en de uitvoeringsmodaliteiten van ons beleid voor gegevensbescherming en gaan verder in op alle verantwoordelijkheden die gepaard gaan met de uitvoering ervan.

## 2. De uitvoering van het beleid voor gegevensbescherming

Het beleid voor gegevensbescherming wordt opgevolgd via permanente controles en verbeterplannen.

Deze beleidstekst zal periodiek of bij belangrijke wijzigingen opnieuw ter goedkeuring voorgelegd worden aan de directie en de Raad van Bestuur van het AZJP.

Daarbij zullen telkens eventuele nieuwe regelgevende kaders afgetoetst worden met deze beleidstekst.

## 3. Begrippenkader

Doorheen deze beleidstekst worden verschillende begrippen gebruikt uit het wetgevend kader voor gegevensbescherming. Zij worden hierna kort toegelicht.

**Verordening Gegevensbescherming:** de 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 en tot intrekking van Richtlijn 95/46/EG. Deze Verordening treedt op 25 mei 2018 in werking. Deze Verordening wordt vaak ook GDPR genoemd (General Data Protection Regulation).

**Wet Patiëntenrechten:** de wet van 22 augustus 2002 betreffende de rechten van de patiënt. Hierin worden de rechten van de patiënt en de correlerende plichten voor de zorgverlener bepaald.

**Persoonsgegevens:** alle informatie over een geïdentificeerde of identificeerbare natuurlijke persoon (en dus geen rechtspersoon). Als identificeerbaar wordt beschouwd een natuurlijke persoon die direct of indirect kan worden geïdentificeerd, met name aan de hand van een identifier zoals een naam, een identificatienummer, locatiegegevens, een online identifier of van een of meer elementen die kenmerkend zijn voor de fysieke, fysiologische, genetische, psychische, economische, culturele of sociale identiteit van die natuurlijke persoon. Ook gepseudonimiseerde gegevens die door het gebruik van aanvullende gegevens aan een natuurlijke persoon kunnen worden gekoppeld, zijn dus persoonsgegevens. Anonieme gegevens, die op geen enkele wijze nog kunnen worden gelinkt aan een persoon, vallen niet onder de Verordening Gegevensbescherming.

**Verwerking:** een bewerking of een geheel van bewerkingen met betrekking tot persoonsgegevens of een geheel van persoonsgegevens, al dan niet uitgevoerd via geautomatiseerde procedés, zoals het verzamelen, vastleggen, ordenen, structureren, opslaan, bijwerken of wijzigen, opvragen, raadplegen, gebruiken, verstrekken door middel van doorzending, verspreiden of op andere wijze ter beschikking stellen, aligneren of combineren, afschermen, wissen of vernietigen van gegevens.

**Betrokkene:** de geïdentificeerde of identificeerbare natuurlijke persoon van wie gegevens worden verwerkt.

**Verwerkingsverantwoordelijke:** een natuurlijke persoon of rechtspersoon, een overheidsinstantie, een dienst of een ander orgaan die/dat, alleen of samen met anderen, het doel van en de middelen voor de verwerking van persoonsgegevens vaststelt.

Als vuistregel geldt dat de zorgvoorziening kan worden beschouwd als verwerkingsverantwoordelijke voor alle verwerkingsactiviteiten die binnen haar schoot worden georganiseerd en waarvoor zij instructies kan geven. Wanneer de zorgvoorziening evenwel niet het doel en de middelen bepaalt, kan zij niet gekwalificeerd worden als verwerkingsverantwoordelijke (maar eventueel wel als verwerker, cf. infra).

**Gezamenlijke verwerkingsverantwoordelijken:** wanneer een natuurlijke of rechtspersoon samen met een andere natuurlijke of rechtspersoon optreedt als verwerkingsverantwoordelijke. Het is daarbij niet vereist dat de invloed van beide verantwoordelijken evenwaardig is of dat elk van hen in staat is om op zichzelf te voldoen aan de verplichtingen van de Verordening Gegevensbescherming. Determinerend is dat ze beiden een beslissingsbevoegdheid hebben, ook al is dit niet in dezelfde mate en hebben ze niet dezelfde toegang tot de persoonsgegevens op zich.

**Verwerker:** een natuurlijke persoon of rechtspersoon, een overheidsinstantie, een dienst of een ander orgaan die/dat ten behoeve van de verwerkingsverantwoordelijke persoonsgegevens verwerkt.

Een zorgvoorziening kan ook als verwerker kwalificeren, wanneer het verwerkingsdiensten levert ten behoeve van een verwerkingsverantwoordelijke (bv. een externe arts die gebruik maakt van de ICT-dienst van de zorgvoorziening) zonder dat de zorgvoorziening het doel en de middelen van de verwerking bepaalt.

**Informatieveiligheid:** Informatieveiligheid omvat het geheel van technische en organisatorische maatregelen die ervoor zorgen dat een door het veiligheidsbeleid vooropgesteld veiligheidsniveau wordt nagestreefd. Hierbij staat de integriteit, de beschikbaarheid en de vertrouwelijkheid van de gegevens centraal.

**Gegevensbescherming:** Gegevensbescherming bepaalt en streeft de naleving na van de regels vastgesteld betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van persoonsgegevens, zoals deze worden bepaald in de Verordening (EU) 2016/679 van het Europees Parlement en de Raad van 27 april 2016 en de andere regelgevingen die criteria vastleggen die betrekking hebben op de verwerking van deze persoonsgegevens.

**Data Protection Officer:** een expert die toeziet op de naleving van de Verordening Gegevensbescherming binnen de instelling en die de verwerkingsverantwoordelijke hierin adviseert en bijstaat.

**Gegevensbeschermingsautoriteit:** de 'opvolger' van de Privacycommissie onder de Wet Verwerking Persoonsgegevens. De Gegevensbeschermingsautoriteit is verantwoordelijk voor het toezicht op de naleving van de grondbeginselen van de bescherming van de persoonsgegevens.

## 4. De scope van het beleid voor gegevensbescherming

### 4.1 Materieel toepassingsgebied

Het beleid is van toepassing op alle persoonsgegevens die AZJP als verwerkingsverantwoordelijke (al dan niet samen met anderen) of als verwerker, verwerkt. We verstaan hieronder niet alleen de gegevens van onze patiënten, maar ook bijvoorbeeld van artsen en medewerkers, al dan niet in dienstverband.

Het beleid is niet van toepassing op geanonimiseerde gegevens, dit zijn gegevens die zodanig anoniem zijn gemaakt dat de betrokkene niet of niet meer identificeerbaar is.

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, 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.

Het beleid strekt zich uit tot alle (semi-)geautomatiseerde verwerkingen en tot handmatige verwerkingen indien de persoonsgegevens zijn opgeslagen of bedoeld zijn om te worden opgeslagen in een bestand. Verwerkingen van patiëntgegevens zijn tevens onderworpen aan de Wet Patiëntenrechten (recht op inzage en afschrift van het patiëntendossier) en het beroepsgeheim.

### 4.2 Personeel toepassingsgebied

Deze beleidstekst is geschreven voor iedereen die in opdracht van AZJP persoonsgegevens verwerkt. Zowel de directie, het management, de personeelsleden en artsen, maar ook elke medewerker of leverancier. We zorgen ervoor dat dit beleid via verschillende kanalen wordt uitgedragen.

Het beleid voor gegevensbescherming is voor AZJP ook een belangrijk uitgangspunt in haar samenwerking met andere zorginstellingen en -verstrekkers, zoals haar participatie in zorgnetwerken.

AZJP waakt er dan ook over dat de principes van dit beleid voor gegevensbescherming worden toegepast in alle samenwerkingsverbanden die het opzet in de zorg.

## 5. Algemene doelstelling en principes bij gegevensverwerking

Kwaliteitsvolle zorg is een topprioriteit voor AZJP. Een belangrijk aspect hierbij is een kwaliteitsvolle verwerking van persoonsgegevens. De directie en het bestuur van AZJP 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 correcte 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 leven we volgende verwerkingsprincipes na:

1. We zijn **transparant** over de persoonsgegevens die we verwerken 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. We verwerken enkel de gegevens die **relevant** zijn voor het uitvoeren van onze taken. D.w.z. dat we persoonsgegevens altijd verwerken voor welbepaalde en uitdrukkelijk omschreven doeleinden, die we opnemen in een register van verwerkingsactiviteiten.  
We waken erover dat deze doelen steeds gerechtvaardigd zijn, in lijn met onze juridische eigenheid en onze visie en missie.

Wanneer deze persoonsgegevens verder worden verwerkt voor andere doeleinden waken we erover dat deze doelen verenigbaar zijn.

3. Elke taak waarbij persoonsgegevens worden verwerkt, is **rechtmatig**.

We gebruiken hierbij de voorwaarden en principes die in de Verordening Gegevensbescherming zijn opgenomen. Voor de verwerking van gevoelige gegevens gaan we daarenboven na of de door de wetgever specifieke opgesomde voorwaarden van toepassing zijn, zoals het verstrekken van gezondheidszorg, de instelling en uitoefening van een rechtsvordering, verplichtingen in het kader van het arbeidsrecht of socialezekerheidsrecht, ... In voorkomend geval zal de verwerking enkel plaatsvinden onder verantwoordelijkheid van de hoofddarts van AZJP en onder de naleving van het beroepsgeheim.

Naast de in de Verordening Gegevensbescherming opgesomde rechtmatigheidsregels, waken we erover dat de verwerking van gegevens in lijn ligt met de rechten en vrijheden die gelden in de Europese Economische Ruimte en controleren de toepassing hiervan wanneer de gegevens worden uitgewisseld daarbuiten. AZJP 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.

AZJP monitort daarenboven ook de in de sector geldende gedragscodes teneinde deze toe passen.

4. We verwerken enkel de persoonsgegevens die **strikt noodzakelijk** zijn voor de uitvoering van onze activiteiten. Zo worden identificatoren die horen bij de persoonsgegevens tot een minimum herleid.
5. We kijken toe op de **integriteit en vertrouwelijkheid** van de persoonsgegevens gedurende de ganse verwerkingscyclus. AZJP neemt de passende technische en organisatorische maatregelen met het oog op een passende beveiliging van de persoonsgegevens. Op die manier beschermen we de persoonsgegevens onder meer tegen ongeoorloofde of onrechtmatige verwerking en tegen onopzettelijk verlies, vernietiging of beschadiging.
6. **Juistheid**. AZJP waakt erover dat de persoonsgegevens volledig en juist zijn rekening houdende met het beoogde verwerkingsdoel. Wanneer de kans bestaat dat de persoonsgegevens niet actueel of fout zijn zullen we extra inspanningen leveren om de gegevens te corrigeren of zo nodig te wissen. We gebruiken hierbij alle mogelijke verificatiebronnen (zoals overheidsregisters) die ons ter beschikking worden gesteld. Wanneer de correctheid van gegevens door de betrokkene worden betwist, nemen we weloverwogen beslissingen, in overeenstemming met het toepasselijk recht, met het oog op de juistheid van de gegevens en de vrijwaring van het recht op goede zorg en een kwalitatief dossier.
7. We **bewaren** persoonsgegevens niet langer dan noodzakelijk. Deze noodzakelijkheid is afgetoetst tegenover wettelijke verplichtingen, de doelmatigheid en de rechten en vrijheden van de betrokkene. Wanneer persoonsgegevens worden gearchiveerd respecteren we de wettelijke en administratieve voorschriften die hierop van toepassing zijn en bewaken we het gebruik van deze persoonsgegevens in onze verwerkingsprocessen.
8. We doen 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 **gerapporteerd** in lijn met de regelgeving ter zake.
9. We doen alle nodige inspanningen om alle geldende **rechten van een betrokkene**, zoals het recht op inzage, afschrift en eventueel ook schrapping uit te voeren. We bewaken hierbij de eventuele beperkingen die op deze rechten van toepassing zijn.
10. We waken er actief over dat bij het verwerken van de persoonsgegevens voor een welbepaald doel, de **rechten en vrijheden** (bijvoorbeeld recht op verzekeraarbaarheid, recht op zorg) van de betrokkene gevrijwaard blijven.
11. Bij de toepassing van alle bovenstaande basisprincipes voor gegevensverwerking, bewaken we onze **verantwoordingsplicht** door intern toezicht en controle en dit op basis van de wettelijk geldende principes.

## 6. Verplichtingen van AZJP als verwerkingsverantwoordelijke, gezamenlijke verwerkingsverantwoordelijke en/of verwerker

## 6.1 AZJP als verwerkingsverantwoordelijke

1. AZJP houdt permanent een **register** bij **van alle activiteiten** waarbij persoonsgegevens worden verwerkt. Het beheer hiervan omvat het opstellen, permanent bijwerken en de controlemaatregelen die hierop van toepassing zijn. Dit register geldt als instrument in het kader van de verantwoordingsplicht ten aanzien van de Gegevensbeschermingsautoriteit, maar is niet bestemd voor de betrokkenen noch voor het publiek. Het register wordt bijgehouden in elektronische vorm. Telkens voorafgaand aan het inrichten van een nieuwe of gewijzigde verwerkingsactiviteit wordt het verwerkingsregister bijgewerkt.

De inhoud van het register wordt vastgelegd door de wettelijke bepalingen die hierop van toepassing zijn, aangevuld met elementen die andere verplichtingen ondersteunen, zoals de controle van doelbinding, het nagaan van een geldige toelaatbaarheidsgrond bij de verwerking, het nazicht van de maatregelen met het oog op minimale gegevensverwerking, gegevensbescherming bij ontwerp of de noodzaak om een gegevensbeschermingseffectenbeoordeling uit te voeren.

De volledigheid van het verwerkingsregister moet worden bewaakt.
2. AZJP 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.

AZJP beheert naast de lijst van criteria voor het uitvoeren van deze analyse, ook het bedrijfsproces voor het initiëren, bewaken, bijwerken en uitvoeren ervan.
3. AZJP doet enkel beroep op verwerkers die afdoende garanties bieden met betrekking tot het toepassen van passende technische en organisatorische maatregelen ter bescherming van persoonsgegevens. AZJP sluit hiervoor met elke verwerker een **verwerkersovereenkomst** af en voert actief toezicht uit op de naleving van de 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.

In geval van verwerkingen waarbij **AZJP verwerker** is zal het al haar wettelijke verplichtingen ter zake naleven en hiertoe een verwerkersovereenkomst afsluiten met de verwerkingsverantwoordelijke. Het toezicht van de DPO zal ook van kracht zijn op de verwerkingsactiviteiten waarvoor AZJP als verwerker optreedt.
4. AZJP voorziet de nodige bedrijfsprocessen die ervoor zorgen dat **de betrokkene wordt geïnformeerd** over de verwerking. De verstrekte informatie omvat de wettelijk opgelegde elementen, waaronder (niet limitatief: de data protection officer (DPO), het verwerkingsdoel en de ontvangers van de gegevens.

Daarnaast moeten de bedrijfsprocessen worden gedocumenteerd die uitvoering geven aan de rechten van de betrokkene (het recht op inzage, afschrift, gegevenswissing, overdraagbaarheid, rectificatie, beperking van de verwerking, kennisgeving, overdraagbaarheid). Deze bedrijfsprocessen houden rekening met de wettelijke beperkingen ter zake (Wet patiëntenrechten en verordening gegevensbescherming,...).
5. AZJP neemt maatregelen ter **beveiliging van de verwerking**. Persoonsgegevens mogen slechts verwerkt worden indien er passende technische en organisatorische maatregelen zijn genomen voor het waarborgen van de beschikbaarheid, de integriteit en de vertrouwelijkheid van de verwerkte persoonsgegevens.



AZJP voorziet een informatieveiligheidsbeleid, gebaseerd op, of minstens evenwaardig aan de ISO 27001 standaard, waarin de verschillende verantwoordelijkheden en maatregelen worden vastgesteld. Het toezicht op informatieveiligheid en de relatie met gegevensbescherming wordt verder in deze beleidstekst opgenomen (infra).

6. AZJP zorgt voor **duidelijke instructies en richtlijnen**, in overeenstemming met de verantwoordelijkheden die medewerkers van AZJP hebben ten aanzien van persoonsgegevens. Deze instructies worden via procedures, bewustwordings sessies, functiebeschrijvingen en opleidingen gecommuniceerd. De naleving van de verplichtingen worden afgedwongen aan de hand van het arbeidsreglement (medewerkers), Algemene regeling (artsen) en/of contractueel. Overtredingen worden behandeld in lijn met de bepalingen inzake sancties die van toepassing zijn.
7. AZJP zorgt voor maatregelen ter identificatie, registratie en afhandelen van **inbreuken** die betrekking hebben op het verwerken van persoonsgegevens. Hierbij streeft AZJP naar een maximale integratie van het meldingssysteem in bestaande meldingssystemen. 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.
8. AZJP stelt een **Data Protection Officer (DPO)** aan aangezien haar kerntaak een grootschalige verwerking van gezondheidsgegevens veronderstelt. De DPO geeft advies over en houdt toezicht op de verwerkingsprocessen van alle persoonsgegevens. De DPO moet zijn/haar functie onafhankelijk kunnen uitoefenen. Hij/zij mag dus niet gebonden zijn door inhoudelijke instructies van ziekenhuis. Met dat doel sluit AZJP met de DPO een overeenkomst af, waarin minstens bepalingen worden opgenomen m.b.t. instructies, sanctionering en rapportering. AZJP betreft de DPO vanaf het begin bij alle gelegenheden die raken aan de bescherming van persoonsgegevens (o.a. tijdig inlichten, uitnodigen op vergaderingen, ...). en verleent aan de DPO toegang tot de nodige persoonsgegevens, de verwerkingsactiviteiten en de expertise van de diensten voor zover deze relevant is voor zijn/haar opdracht.

## 6.2 AZJP als gezamenlijke verwerkingsverantwoordelijke

Wanneer er sprake is van een gezamenlijke verantwoordelijkheid, dan zullen de respectievelijke verantwoordelijkheden van AZJP en eventuele gezamenlijke verwerkingsverantwoordelijken op een transparante wijze worden beschreven. Hieronder verstaan we ook de uitoefening van de rechten van de betrokkene en de respectieve verplichtingen inzake het verstrekken van informatie. Dit zal worden opgenomen in de onderlinge regeling tussen AZJP en de medeverantwoordelijke(n). In deze regeling zal duidelijk blijken welke rol de gezamenlijke verwerkingsverantwoordelijken respectievelijk vervullen, en wat hun respectieve verhouding is met de betrokkenen. De wezenlijke inhoud van de regeling wordt aan de betrokkene beschikbaar gesteld. We zullen hierbij rekening houden dat, ongeacht deze regeling, de betrokkene zijn rechten kan uitoefenen bij iedere verwerkingsverantwoordelijke.

AZJP zal aan alle verplichtingen voldoen voor de verwerkingsprocessen waarvoor zij in deze situatie de verantwoordelijkheid draagt.

## 6.3 AZJP als verwerker

In geval van verwerkingen waarbij AZJP verwerker is zal het de verplichte bijstand verlenen aan de verwerkingsverantwoordelijke.

Zo zal AZJP de verwerkingsverantwoordelijke zonder onredelijke vertraging informeren zodra het kennis heeft genomen van een inbreuk in verband met de persoonsgegevens. Tevens zal AZJP zich er, als verwerker, in een verwerkersovereenkomst toe verbinden om de verwerkingsverantwoordelijke waar nodig bij te staan bij de

verdere afhandeling van de meldingsprocedure (door bv. informatie te verstrekken over de feiten omtrent het incident) en zal het de nodige maatregelen nemen op niveau van gegevensbeveiliging om het incident te verhelpen.

Daarnaast staat AZJP de verantwoordelijke voor de verwerking bij in het naleven van de rechten van de betrokkene en bij vragen van de verwerkingsverantwoordelijke met het oog op het uitvoeren van een gegevensbeschermingseffectenbeoordeling.

In geval AZJP optreedt als verwerker, zal het de noodzakelijke bijdrage leveren aan de beveiliging van de verwerking en zal het een register van verwerkingsactiviteiten aanleggen vanuit de rol van verwerker. Het toezicht van de DPO zal ook van kracht zijn op de verwerkingsactiviteiten waarvoor AZJP als verwerker optreedt.

## 7. Toepassing van het beleid gegevensbescherming in zorgnetwerken

AZJP 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 stuurgroep gegevensbescherming toe op de impact van de samenwerking en de verantwoordelijkheid over de gegevensverwerking. Hierbij wordt het beslissingscentrum over het verwerken van persoonsgegevens als leidraad gebruikt.

Bij de inrichting van een verticaal zorgnetwerk zal AZJP haar eigen handelen in lijn met het criterium van de goede huisvaderprincipes ook toepassen op de leden van het netwerk.

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

## 8. De implementatie van het gegevensbeschermingsbeleid in de organisatiestructuur van het ziekenhuis

Om bovenstaande beleidstaken te concretiseren in een organisatiestructuur wordt een matrix opgesteld waarin de beleidstaken worden uitgezet tegenover de verschillende verantwoordelijkheden. De matrix wordt opgesteld en onderhouden door de stuurgroep gegevensbescherming en informatieveiligheid.

Hierna worden de belangrijkste taken beschreven:

### 8.1. Centraal: de verantwoordelijkheid voor de gegevensbescherming

#### Raad van bestuur

De eindverantwoordelijkheid voor het naleven van de wettelijke verplichtingen in het ziekenhuis m.b.t. gegevensbescherming als verwerkingsverantwoordelijke rust bij AZJP, vertegenwoordigd door de Raad van Bestuur. In de uitvoering van het gegevensbeschermingsbeleid bekrachtigt de Raad van Bestuur de beleidsdoelen en kijkt het toe op de naleving van de wettelijke verplichtingen.

#### Delegatie aan het directiecomité

De Raad van Bestuur delegeert de uitvoering van de beleidstaken in het kader van gegevensbescherming aan het directiecomité. In de uitvoering van deze taken wordt het directiecomité bijgestaan door de Stuurgroep Gegevensbescherming & Informatieveiligheid (zie infra).



## 8.2. Decentraal: operationele verantwoordelijkheid voor gegevensbescherming o.b.v. categorie van persoonsgegevens

Gelet op de veelheid aan persoonsgegevens die worden verwerkt in ziekenhuiscontext, wordt de operationele verantwoordelijkheid om de verplichtingen zoals bepaald in de Verordening Gegevensbescherming na te komen, decentraal georganiseerd en gelegd bij de diensten/organen die daadwerkelijk instaan voor de verwerking van de betreffende gegevens. Een (voorstel tot) uitwerking hiervan wordt gedaan in de takenmatrix (bijlage A).

## 8.3. Stuurgroep Gegevensbescherming & Informatieveiligheid (SGI): voorbereiding en uitvoering van de beslissingen van het directiecomité

De SGI komt samen telkens wanneer één van de leden hierom verzoekt en minstens driemaandelijks. De agenda wordt opgesteld door de DPO.

De SGI bereidt beslissingen van het directiecomité voor en voert de door het directiecomité genomen beslissingen uit die betrekking hebben op gegevensbescherming, waaronder:

- Het monitoren van de bedrijfsprocessen die in deze beleidstekst zijn beschreven met het oog op gegevensbescherming
- Het formuleren van adviesvragen aan de DPO
- Het bijsturen van het beleid en de uitvoering ervan op advies van de DPO
- Het bewaken van de onafhankelijkheid van de DPO
- De beslissingen inzake risicobeheer bij het verwerken van persoonsgegevens. De tijdsbesteding van de DPO is een onderdeel van dit risicobeheer.
- De goedkeuring van de classificatieschema's die bijvoorbeeld bepalen wanneer een gegevensbeschermingseffectbeoordeling 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 Gegevensbescherming, waaronder verwerkingen gebaseerd op gerechtvaardigd belang, zoals 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, genomen door de Raad van Bestuur
- De te nemen maatregelen bij overtredingen op grond van het arbeidsreglement, de algemene regeling dan wel op grond van het contract;
- De rapportering van het beleid gegevensbescherming naar onder meer accreditatiecommissies.
- Toekijken op de toepassing van het beleid in horizontale en verticale zorgnetwerken.

## 8.4. Adviserend: de functionaris voor de gegevensbescherming (DPO)

De Data Protection Officer (DPO) geeft advies over en houdt toezicht op de verwerkingsprocessen van alle persoonsgegevens. De precieze opdracht en taakomschrijving van de DPO worden in een afzonderlijk document uiteengezet.