Beleidsverklaring Gegevensbescherming

Inhoudsopgave

1. Inleiding: het beleid voor gegevensbescherming vzw Huize Sint-Jozef

Voor vzw Huize Sint-Jozef is het beschermen van de persoonlijke levenssfeer een belangrijk strategisch doel en bovenal een wettelijke verplichting die we hoog in het vaandel dragen.
De vzw wil voor al haar bewoners een comfortabele omgeving bieden in combinatie met professionele zorg. Met deze beleidstekst willen we toelichten op welke manier we de rechten en vrijheden van de bewoners, 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 persoonsgegevens, zoals het uitwisselen van deze gegevens met andere actoren, het verwerken van de gegevens buiten het strikte kader van het 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 medewerkers, vrijwilligers, studenten, en andere actoren binnen het woonzorgcentrum. 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 Patiëntenrechten.

Daarnaast is deze beleidstekst tactisch. We lichten toe op welke manier we de organisatie van gegevensbescherming voorzien. 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 voor 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 werd) geïmplementeerd aan de hand van een implementatieplan (nulmeting dd 17 mei 2018) . Na de implementatiefase zal dit beleid verder worden opgevolgd via permanente controles en verbeterplannen. We beogen bijgevolg een belangrijke herziening van dit beleid (vooral op tactisch vlak) tegen de voorgenoemde datum. In de periode ervoor zal dit beleid verder worden uitgediept voor de verschillende deeldomeinen.

Na 25 mei 2018 zal deze beleidstekst periodiek of bij belangrijke wijzigingen opnieuw ter goedkeuring worden voorgelegd aan de directie en de raad van bestuur van de vzw. Daarbij toetsen we de nieuwe regelgevende kaders af met deze beleidstekst. Op korte termijn hebben we oog voor de (EU) e-Privacy verordening en de (EU) e-Privacyrichtlijn voor de beveiliging van informatienetwerken en -systemen.

3. De scope van het beleid voor gegevensbescherming

3.1 Materieel toepassingsgebied

Het beleid is van toepassing op alle persoonsgegevens die de vzw verwerkt. We verstaan hieronder niet alleen de gegevens van de bewoners, maar ook bijvoorbeeld van artsen en medewerkers, al dan niet in dienstverband. Ook gegevens van vrijwilligers, studenten, zelfstandige zorgverleners, leveranciers en andere actoren behoren tot het toepassingsgebied voor gegevensbescherming.

3.2 Functioneel toepassingsgebied

Het beleid is van toepassing op alle verwerkingsdoelen. Zowel gegevens die worden verwerkt voor (niet limitatief) de zorg van de bewoner, 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.

3.3 Organisatorisch toepassingsgebied

Deze beleidstekst is geschreven voor iedereen die in opdracht van de vzw persoonsgegevens verwerkt. Zowel de algemeen directeur, het management, de medewerkers en artsen, maar ook elke leverancier. We zorgen ervoor dat deze tekst via verschillende kanalen wordt uitgedragen en wordt gepubliceerd op de website van de vzw Huize Sint-Jozef.

Het beleid voor gegevensbescherming is voor de vzw het uitgangspunt in haar samenwerking met andere zorginstellingen en -verstrekkers, zoals haar participatie in de locoregionale zorgnetwerken. De veiligheidsconsulent/DPO waakt erover dat de principes van dit veiligheidsbeleid worden toegepast in alle samenwerkingsverbanden die de vzw opzet.

4. Beleidsdoelstellingen voor gegevensbescherming

Kwaliteitsvolle zorg is een topprioriteit. Een belangrijk aspect hierbij is een kwaliteitsvolle verwerking van persoonsgegevens. De algemeen directeur en het beheer van de 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 streven we volgende doelstellingen na:

De vzw:

1. is **transparant** over de persoonsgegevens die ze 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 met betrokken actoren, zoals de huisarts, het ziekenhuis, een mutualiteit en andere actoren.
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 de vzw. Dit wordt telkens geëvalueerd bij een nieuw verwerkingsdoel;
3. verwerkt enkel de persoonsgegevens die **strikt noodzakelijk** zijn voor de uitvoering van de activiteiten. Zo worden identificatiegegevens 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 **gerapporteerd** in lijn met de regelgeving ter zake. Inbreuken die kunnen voortvloeien uit de verwerking van persoonsgegevens, zijn het verlies van gegevens, datalekken of fouten in de verwerkte gegevens. Daarnaast wordt het niet toegankelijk zijn van gegevens op het moment van de zorg of wanneer gegevens worden ingekeken door iemand die daartoe niet gemachtigd is, ook als een inbreuk beschouwd. Ook wanneer niet kan worden nagegaan wie welke gegevens inkeek, wijzigde of verwijderde, moet dit als inbreuk worden gerapporteerd. Een laatste omschreven vorm van inbreuk is wanneer verwerkingen niet in lijn liggen met de regelgeving, richtlijnen en normen.
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. De vzw waakt 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** (bv. 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. De 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. De 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. Als verantwoordelijke voor de verwerking, ligt de bevoegdheid van dit veiligheidsbeleid bij het vzw, vertegenwoordigd door de directeur.

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 de vzw dient na te streven (het aantoonbaarheidsprincipe). Daarnaast is de lijst van taken, zoals hieronder beschreven, geïnspireerd op praktijken van 'Goede Huisvader'.

Elke taak die wordt beschreven, wordt ondersteund door een bedrijfsproces. De algemene verantwoordelijkheid voor het uitvoeren van deze taken berust bij de algemeen directeur van de vzw. 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 bedrijfsprocessen worden planmatig geïmplementeerd tegen 25 mei 2018.

De beleidstaken zijn hieronder opgelijst en worden kort besproken.

De vzw:

1. houdt permanent een **register bij van de verwerkingsactiviteiten** waarbij persoonsgegevens van de categorieën van betrokkenen (*i.e.* medewerkers, bewoners…) 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 persoonsgegevens, 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 voorafgaandelijk aan het inrichten van nieuwe verwerkingsdoelen en bijhorende bedrijfsprocessen. Op dat moment wordt het afgetoetst aan de wettelijke en statutaire taken van de 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. De vzw houdt het verwerkingsregister bij in digitale vorm en is opvraagbaar volgens de wettelijke bepalingen (*i.e.* door de Gegevensbeschermingsautoriteit);
2. te verwijderen: "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 **gegevensbeschermingseffectbeoordeling** uitgevoerd voorafgaandelijk 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. De vzw 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. De vzw voert actief toezicht uit op deze contractuele bepalingen (jaarlijkse gdpr-conformiteit bevragen) . 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 *Data Protection Officer* (DPO) en hoe deze te bereiken is, 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 (Wet Patiënten rechten en 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 van De vzw 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 wordt afgedwongen aan de hand van het arbeidsreglement of een 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 voor gegevensbescherming op de locoregionale netwerken

De vzw 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 informatieveiligheid/GDPR van de vzw 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 verticale zorgnetwerken zal de vzw haar 'Goede Huisvader'-principes 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 algemeen directeur en de informatieveiligheidsconsulent/DPO. De algemeen directeur 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 de algemeen directeur. De algemeen directeur is verantwoordelijk voor het bekrachtigen van de beleidsdoelen en de hierbij horende taken. In de uitvoering van deze verantwoordelijkheden kan de algemeen directeur een beroep doen op de adviezen van de functionaris voor gegevensbescherming of *Data Protection Officer* (DPO). Elke beoordeling van risico's vindt plaats onder de verantwoordelijkheid van de algemeen directeur, alsook de uitvoering van de bijhorende maatregelen. De algemeen directeur is daarnaast ook eindverantwoordelijk voor alle verplichtingen uit hoofde van de wet- en regelgeving, waaronder de bepalingen in Verordening 2016/679. Hiervoor delegeert de algemeen directeur een aantal taken, zoals hieronder opgesomd.

Toezicht gezondheidsgegevens bewoners

Het beleid voor gegevensbescherming doet op geen enkele wijze afbreuk aan de wettelijke verplichtingen die de algemeen directeur heeft met het oog op de toepassing van de wetgeving over gegevensbescherming.
De algemeen directeur wordt beschouwd als lasthebber van de vzw dat optreedt als de verwerkingsverantwoordelijke (*cf*. gedragscode). De algemeen directeur (en voor verpleegkundige gegevens in nauwe samenspraak met de diensthoofden zorg) heeft vanuit deze opdracht de verantwoordelijkheid inzake de gegevensbescherming van gezondheidsgegevens in het bewonersdossier. 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 algemeen directeur en de diensthoofden zorg in het uitvoeren van de gegevensbeschermingseffectbeoordeling. In de uitvoering van het beleid voor gegevensbescherming krijgt de algemeen directeur 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 bewoners en de verwerking van persoonsgegevens die hiermee verband houden, registratie van activiteiten enz.).
Op basis van de vooropgestelde classificatie worden door de DPO criteria vastgelegd en vertaald voor het uitvoeren van een gegevensbeschermingseffectbeoordeling, 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 directeur inzake het toepassen van de rechten van bewoners is opgenomen in de reglementen dienaangaande.
Voor de toepassing van de rechten van de betrokkene (in het bijzonder deze van de bewoner) voor gezondheidsgegevens die buiten het bewonersdossier worden verwerkt, assisteert de algemeen directeur bij het uitwerken van de beleidslijnen.
De algemeen directeur stimuleert de correcte omgang met bewonersgegevens bij

de medewerkers van de vzw. De algemeen directeur neemt bovendien alle relevante aspecten van gegevensbescherming mee in de evaluatie van medewerkers en hun opleidingstraject tijdens dienstverband.
De directeur kijkt toe op het onderhoud van het register van verwerkingsactiviteiten met het oog op de verwerking van gezondheidsgegevens.

Toezicht sociale gegevens bewoners

De sociale dienst, onder verantwoordelijkheid van de algemeen directeur van de vzw, 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 de algemeen 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 DPO criteria vastgelegd en vertaald voor het uitvoeren van een gegevensbeschermingseffectbeoordeling, 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 familieleden en andere betrokkenen bij de werking. Ook de uitwisseling van persoonsgegevens met actoren in de sociale dienstverlening krijgen hierbij extra aandacht, zoals overheden, mutualiteiten, OCMW...

Toezicht financiële gegevens bewoners

Het diensthoofd administratie, onder verantwoordelijkheid van de algemeen directeur van de vzw stelt het register van verwerkingsactiviteiten op binnen de dienst boekhouding/administratie. De algemeen directeur is verantwoordelijk voor het beoordelen van de rechten en vrijheden van de bewoner bij de verwerking van gegevens op de dienst (toegang tot zorg, het recht op zorg, verzekerbaarheid). De financiële dienst, onder verantwoordelijkheid van de algemeen directeur, kijkt toe op de uitwisseling van persoonsgegevens met de overheid, de mutualiteiten …

Toezicht administratieve gegevens bewoners

Binnen de vzw behoort de bewonersadministratie gedeeltelijk tot het takenpakket van zowel de sociale dienst als het onthaal beide diensten stellen, onder verantwoordelijkheid van de algemeen directeur van de vzw, een register van verwerkingsactiviteiten op binnen de dienst. De dienst administratie duidt hierbij duidelijk aan welke persoonsgegevens worden ingezameld op basis van een toestemming. De dienst richt op vraag van de DPO de nodige processen in met het oog op het verstrekken van informatie aan de bewoner en vragen met betrekking tot de rechten van de bewoner (in samenspraak met andere diensten, waaronder de dienst communicatie). De beoordeling van de risico's met betrekking tot de identificatie van de bewoner en het beheer van dubbele bewonersdossiers 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 bewoner, waaronder de gegevensstromen met het rijksregister.

Toezicht latere verwerking gegevens bewoners

De algemeen directeur, de diensthoofden zorg en de adjunct-diensthoofden zorg 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 diensthoofden zorg volgen de veiligheidsrichtlijnen op en informeren de medewerkers hierover. De diensthoofden zorg zorgen voor een veiligheidscultuur in hun team en onderhouden deze. De algemeen directeur 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 de teamcoördinator 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 diensthoofden zorg die hiermee belast zijn, in coördinatie met de DPO. De latere verwerking voor kwaliteitsdoeleinden en beleidsrapporteringen vallen onder verantwoordelijkheid van de dienst aan wie de rapportering plaatsvindt in samenspraak met de algemeen directeur. Het toezicht op de verwerker wordt georganiseerd door de informatieveiligheidsconsulent/DPO.
De latere verwerking van gezondheidsgegevens uit het bewonersdossiers voor kwaliteitsdoeleinden ten behoeve van inspectiediensten of accrediteringscommissies, valt onder de verantwoordelijkheid van de algemeen directeur.

Toezicht persoonsgegevens medewerkers en artsen

De diensthoofden zorg, onder verantwoordelijkheid van de algemeen directeur, krijgt in het beleid voor gegevensbescherming de taak om de gegevensbescherming te bewaken van persoonsgegevens van alle medewerkers (al dan niet in dienst), met uitzondering van de artsen. Het is de taak van het diensthoofd zorg om bij de implementatie van (nieuwe) verwerkingsprocessen waarbij de persoonsgegevens van medewerkers worden verwerkt, het beschreven beleid te vertalen en toe te passen. Daar waar nieuwe bedrijfsprocessen worden ingevoerd of bestaande bedrijfsprocessen worden gedigitaliseerd, zorgt de algemeen directeur voor de analyse van de verwerkingsgrond, de eventuele bijhorende besprekingen met de diensthoofden zorg (bv. in het kader van transparantie en de evaluatie van gerechtvaardigde belangen) en de bijhorende gegevensbeschermingseffectbeoordeling (cfr. Input Valerie). Het diensthoofd zorg ziet toe op de wijze waarop men hun opdracht t.a.v.de uitvoering van de veiligheidsbepalingen uitvoeren en stuurt waar dit nodig is bij als directe leidinggevende. De algemeen directeur levert daarenboven een actieve bijdrage bij het onderhouden van het register van verwerkingsactiviteiten voor medewerkers gegevens. Voor de verwerking van persoonsgegevens van artsen wordt de corresponderende taak toebedeeld aan de informatieveiligheidsconsulent/DPO, onder toezicht van de algemeen directeur.

Toezicht toepassing gegevensbescherming door medewerkers en artsen

De algemeen directeur 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.

Algemeen toezicht gegevensbescherming bij verwerkers	Het algemeen toezicht op verwerkers van persoonsgegevens die in opdracht van De vzw persoonsgegevens verwerken, wordt uitgevoerd door de veiligheidsconsulent/DPO voor wat betreft de informatieveiligheid en van het diensthoofd zorg van de verdieping waarvoor de verwerking wordt uitgevoerd, in samenspraak met de directeur en de DPO.
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 gegevensbescherming of DPO geconsulteerd. De verantwoordelijkheid hiervoor ligt bij de initiatiefnemer. Voor wat betreft de artsen, kijken de CRA, samen met de functionaris voor gegevensbescherming of DPO, 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 of DPO, op vraag van de kwaliteitscoördinator, over antwoorden op vragen van de patiënt betreffende de verwerking van diens persoonsgegevens. Dit antwoord is niet bindend voor de kwaliteitscoördinator, zodat de onafhankelijkheid van deze functie gevrijwaard blijft. Vragen die rechtstreeks aan de functionaris voor gegevensbescherming of DPO worden gesteld, worden volgens dezelfde methodologie behandeld. Wanneer het wettelijk kader hierover wordt bijgestuurd met het oog op Verordening 2016/679 of latere wetgeving ter zake, zal de verantwoordelijkheid dienaangaande worden bijgestuurd.
Toezicht gegevens-Bescherming ICT-leverancier	De ICT-leverancier is verantwoordelijk voor het implementeren van de technische maatregelen en het implementeren van de veiligheidsinstellingen in lijn met dit veiligheidshandboek. Daarnaast moet de ICT-leverancier zijn verantwoordelijkheid opnemen door veiligheidsproblemen die ontstaan voor, tijdens of na de implementatie van ICT-middelen te melden aan de informatieveiligheidsconsulent/DPO. Tegelijkertijd fungeert de ICT-leverancier als expert. Vanuit de vzw wordt verwacht dat hij vanuit deze rol deelneemt aan de identificatie zowel als aan de remediëring van de informatieveiligheidsrisico's. De ICT-leverancier gaat er ook mee akkoord om de gedragscode na te leven. Bijkomstig wijst hij ook op veiligheidsrisico's van geleverde toepassingen en op de op te nemen veiligheidstaken. De ICT-leverancier streeft een transparant veiligheidsbeleid na door met de algemeen directeur en de informatieveiligheidsconsulent/DPO te communiceren over het eigen actuele veiligheidsniveau en bij de afhandeling van veiligheidsincidenten.

8. De relatie tussen gegevensbescherming en informatieveiligheid

De vzw Huize Sint-Jozef vertrouwt het toezicht op informatieveiligheid toe aan de informatieveiligheidsconsulent/DPO. De taken van de informatieveiligheidsconsulent/DPO zijn opgenomen in het veiligheidsbeleid, dat onder verantwoordelijkheid van de algemeen directeur valt.

Voor de vzw Huize Sint-Jozef worden de taken van de informatieveiligheidsconsulent/DPO opgenomen door één persoon.
De taken van de informatieveiligheidsconsulent/DPO zijn in lijn met het Besluit van de Vlaamse Regering van 15 mei 2009 betreffende de veiligheidsconsulenten. In overeenstemming met de (EU) Verordening 2016/679 zorgt de veiligheidsconsulent 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 artikelen 33 en 34 (de melding van een inbreuk in verband met persoonsgegevens aan de toezichthoudende autoriteit en aan de betrokkene).
De taken van de functionaris voor gegevensbescherming of DPO zijn hieronder besproken.

9. De functionaris voor gegevensbescherming/DPO

Het algemeen directeur wordt uit hoofde van verantwoordelijke voor de verwerking geadviseerd door de informatieveiligheidsconsulent/ DPO.

De DPO adviseert de algemeen directeur en de raad van bestuur inzake alle verantwoordelijkheden die de organisatie rond gegevensbescherming draagt met:

- het bijsturen van het beleid inzake gegevensbescherming;
- het aanstellen van een functionaris voor gegevensbescherming;
- het bewaken van de onafhankelijkheid van de functionaris voor gegevensbescherming/DPO;
- 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 voor gegevensbescherming;
- de beslissingen inzake risicobeheer bij het verwerken van persoonsgegevens. De tijdsbesteding van de functionaris voor gegevensbescherming/DPO is een onderdeel van dit risicobeheer;
- de goedkeuring van de classificatieschema's die bijvoorbeeld bepalen wanneer een gegevensbescherming effectbeoordeling 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 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;
- 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.