BELEIDSTEKST GEGEVENSBESCHERMING

Ziekenhuis Oost-Limburg

1. Inleiding: Het beleid voor gegevensbescherming Ziekenhuis Oost-Limburg

Voor het Ziekenhuis Oost-Limburg is het beschermen van de persoonlijke levenssfeer van de patiënten een belangrijk strategisch doel en bovenal een wettelijke verplichting die Ziekenhuis Oost-Limburg hoog in het vaandel draagt.

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 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 Ziekenhuis Oost-Limburg. 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. 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 en bij belangrijke wijzigingen opnieuw ter goedkeuring voorgelegd worden aan de directie en de Raad van Bestuur van het Ziekenhuis Oost-Limburg. 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 die Ziekenhuis Oost-Limburg verwerkt. We verstaan hieronder niet alleen de gegevens van onze patiënten, maar ook bijvoorbeeld van artsen en medewerkers, al dan niet in dienstverband.

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, 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 Ziekenhuis Oost-Limburg 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 de website en het intranet van het Ziekenhuis Oost-Limburg.

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

4. Beleidsdoelstellingen voor gegevensbescherming

Kwaliteitsvolle zorg is een topprioriteit voor Ziekenhuis Oost-Limburg. Een belangrijk aspect hierbij is een kwaliteitsvolle verwerking van persoonsgegevens. De directie en het beheer van Ziekenhuis Oost-Limburg streven 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: Ziekenhuis Oost-Limburg:

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 Ziekenhuis Oost-Limburg. Dit wordt telkens geëvalueerd bij een nieuw verwerkingsdoel.
3. Verwerkt enkel de persoonsgegevens die **strikt noodzakelijk** voor de uitvoering van de activiteiten. Zo worden identificatoren die horen bij de persoonsgegevens tot een minimum herleid.
4. Kijkt toe op de **integriteit** van de persoonsgegevens gedurende de ganse verwerkingscyclus.
5. **Bewaart** gegevens niet langer dan noodzakelijk. De noodzakelijkheid is afgetoetst tegenover wettelijke verplichtingen, de doelmatigheid en de rechten en vrijheden van de betrokkene.
6. Doet alle mogelijke inspanningen tot het voorkomen van **inbreuken die voortvloeien uit het verwerken** van persoonsgegevens. Informatieveiligheid, gegevensbescherming bij ontwerp en privacy-vriendelijke standaardinstellingen zijn hiervoor hulpmiddelen. Wanneer een inbreuk plaatsvindt, wordt hierover **gerapporteer**d in lijn met de regelgeving ter zake.
7. Doet alle nodige inspanningen om alle geldende **rechten van een betrokkene**, zoals het recht op inzage, afschrift en eventueel ook schrapping uit te voeren. Ziekenhuis Oost-Limburg 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** (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. Ziekenhuis Oost-Limburg 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. Ziekenhuis Oost-Limburg 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.

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 Ziekenhuis Oost-Limburg 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 en dit op basis van een beleidsbeslissing van de Raad van Bestuur. De algemene verantwoordelijkheid voor het uitvoeren van deze taken berust bij het directiecomité van Ziekenhuis Oost-Limburg. 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.

Ziekenhuis Oost-Limburg:

1. Houdt permanent een **register bij van de verwerkingsactiviteiten** waarbij persoonsgegevens van de categorieën van betrokkenen (i.e. medewerkers, 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 gegevens worden verwerkt, het al dan niet uitwisselen van deze gegevens en de categorieën van ontvangers. Hierbij dient er een specifieke vermelding te gebeuren 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 Ziekenhuis Oost-Limburg. 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. Ziekenhuis Oost-Limburg 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. Ziekenhuis Oost-Limburg 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. Ziekenhuis Oost-Limburg voert actief toezicht uit op deze contractuele bepalingen. Daar waar de verwerking plaatsvindt onder een **gemeenschappelijke verantwoordelijkheid**, worden duidelijke afspraken gemaakt met het oog op de toepassing van de rechten van de betrokkene en de informatieplicht, tenzij deze verantwoordelijkheid in de wet- en regelgeving is opgenomen. Daarnaast worden ieders verantwoordelijkheden duidelijk gedocumenteerd en gecommuniceerd naar de betrokkene.

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 gegevensverwerking 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 van Ziekenhuis Oost-Limburg 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

Ziekenhuis Oost-Limburg beoogt de toepassing van de beleidsdoelstellingen niet alleen in de eigen zorgorganisatie, maar beoogt de geldende principes ook te extrapoleren naar netwerken.

Bij de inrichting van een netwerk 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 netwerk zal Ziekenhuis Oost-Limburg haar Goede Huisvaderprincipes ook toepassen op de leden van het netwerk.

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

7. De organisatie van gegevensbescherming

In dit veiligheidsbeleid concretiseren we bovenstaande taken in een organisatiestructuur. Hiertoe wordt een matrix opgesteld waarin de taken worden uitgezet tegenover de verschillende verantwoordelijkheden. De matrix wordt opgesteld en onderhouden onder verantwoordelijkheid van de Raad van Bestuur en de directie. De directie ziet toe op de uitvoering van de verantwoordelijkheden. De matrix is opgenomen in bijlage A. 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. De Raad van Bestuur is hierbij verantwoordelijk voor het bekrachtigen van de beleidsdoelen en de hierbij horende taken. In de uitvoering van deze verantwoordelijkheden kan de Raad van Bestuur en 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 de Raad van Bestuur en het directiecomité, alsook de uitvoering van de bijhorende maatregelen. De Raad van Bestuur en het directiecomité zijn daarnaast ook eindverantwoordelijk voor alle verplichtingen uit hoofde van de wet- en regelgeving, waaronder de bepalingen in de verordening 2016/679. Hiervoor kunnen een aantal taken gedelegeerd worden zoals hieronder opgesomd.

Toezicht gezondheidsgegevens patiënten

Het beleid voor gegevensbescherming doet op geen enkele wijze afbreuk aan de wettelijke verplichtingen die de hoofdgeneesheer/verpleegkundig paramedich directeur hebben met het oog op de toepassing van de wetgeving over gegevensbescherming.

De hoofdgeneesheer (en voor verpleegkundige gegevens in nauwe samenspraak met de verpleegkundig paramedisch directeur) heeft 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), assisteren de hoofdgeneesheer en de verpleegkundig paramedisch directeur in het uitvoeren van de gegevens-beschermingseffectenbeoordeling.

In de uitvoering van het beleid voor gegevensbescherming krijgt de hoofdgeneesheer 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 stuurgroep gegevensbescherming 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 hoofdgeneesheer 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 hoofdgeneesheer bij het uitwerken van de beleidslijnen.

De hoofdgeneesheer stimuleert de correcte omgang met patiëntengegevens bij de medische diensten van Ziekenhuis Oost-Limburg. De hoofdgeneesheer neemt bovendien alle relevante aspecten van gegevensbescherming mee in de evaluatie van (kandidaat) artsen en hun opleidingstraject tijdens de voorlopige aanstelling.

De hoofdgeneesheer kijkt toe op het onderhoud van het register van

verwerkingsactiviteiten met het oog op de verwerking van gezondheidsgegevens.

Toezicht sociale gegevens patiënten

De dienst patiëntenbegeleiding, onder verantwoordelijkheid van de verpleegkundig paramedisch directeur van Ziekenhuis Oost-Limburg 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 dienst patiëntenbegeleiding, 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 stuurgroep gegevens-bescherming 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 dienst patiëntenbegeleiding 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 dienst patiëntenbegeleidingverlening krijgen hierbij extra aandacht.

Toezicht financiële gegevens patiënten

De financiële dienst, onder verantwoordelijkheid van de financieel directeur van Ziekenhuis Oost-Limburg stelt het register van verwerkingsactiviteiten op binnen de financiële dienst. De financieel 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, …

Toezicht administratieve gegevens patiënten

De dienst patiëntenadministratie, onder verantwoordelijkheid van de hoofdgeneesheer van Ziekenhuis Oost-Limburg 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 stuurgroep gegevensbescherming 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 hoofdgeneesheer, de geneesheer-coördinatoren, de geneesheer-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 hoofdgeneesheer 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 stuurgroep gegevensbescherming en op advies van de functionaris of DPO.
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, veiligheidsconsulent en de functionaris voor de gegevensbescherming.
De latere verwerking van gezondheidsgegevens uit het patiëntendossiers voor kwaliteitsdoeleinden ten behoeve van inspectiediensten of accrediteringscommissies, valt onder de verantwoordelijkheid van de hoofdgeneesheer.

Toezicht persoonsgegevens medewerkers en artsen

De personeelsdienst, onder verantwoordelijkheid van de personeelsdirecteur 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 de personeelsdienst 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 personeelsdirecteur 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 personeelsdirecteur 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 hoofdgeneesheer.

Toezicht toepassing gegevensbescherming door medewerkers en artsen

De personeelsdirecteur 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 hoofdgeneesheer gelegd.

Algemeen toezicht gegevensbescherming bij verwerkers

Het algemeen toezicht op verwerkers van persoonsgegevens die in opdracht van Ziekenhuis Oost-Limburg persoonsgegevens verwerken, wordt uitgevoerd door de veiligheidsconsulent 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 of DPO. 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 of DPO geconsulteerd. De verantwoordelijkheid hiervoor ligt bij de initiatiefnemer (de arts, de coördinator zorginnovatie of het programmanagement office). Voor wat betreft de artsen kijken de hoofdgeneesheer en de medische raad, samen met de functionaris 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 de gegevensbescherming of DPO, 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 of DPO 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

Ziekenhuis Oost-Limburg vertrouwt het toezicht op informatieveiligheid toe aan de veiligheidsconsulent. De taken van de veiligheidsconsulent zijn opgenomen in het veiligheidsbeleid, dat onder verantwoordelijkheid van het directiecomité valt.

Voor Ziekenhuis Oost-Limburg worden de taken van de veiligheidsconsulent en van de functionaris voor de gegevensbescherming of DPO opgenomen door verschillende personen.

De taken van de veiligheidsconsulent 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 artikels 33 en 34 (de melding van een inbreuk in verband met persoonsgegevens aan de toezichthoudende autoriteit en aan de betrokkene).

De veiligheidsconsulent is lid van de stuurgroep gegevensbescherming van Ziekenhuis Oost-Limburg.
De taken van de functionaris voor de gegevensbescherming of DPO zijn hieronder besproken.

9. De stuurgroep gegevensbescherming

De Raad van Bestuur wordt uit hoofde van verantwoordelijke voor de verwerking geadviseerd door de stuurgroep gegevensbescherming. Deze stuurgroep is het Directiecomité, hetwelk geadviseerd wordt door de functionaris voor de gegevensbescherming of DPO. De veiligheidsconsulent en/of de adjunct veiligheidsconsulent maakt tevens deel van de stuurgroep.

De stuurgroep legt de beleidsbeslissingen voor aan de Raad van Bestuur inzake alle verantwoordelijkheden die de organisatie rond gegevensbescherming draagt:

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

De samenstelling van de stuurgroep wordt voorgelegd aan de Raad van Bestuur ter beslissing.

10. Het stakeholdersoverleg voor gegevensbescherming

Aangezien het beleid voor gegevensbescherming bedrijfsprocessen beoogt doorheen de gehele organisatie van het Ziekenhuis Oost-Limburg, wordt er een stakeholdersoverleg georganiseerd.

Op dit stakeholdersoverleg worden alle personen uitgenodigd die een taak hebben in het kader van de gegevensbescherming. Dit stakeholdersoverleg wordt georganiseerd door en voorgezeten door de functionaris voor gegevensbescherming. De bedoeling van dit stakeholdersoverleg is het informeren van de stakeholders omtrent het beleid voor gegevensbescherming, het rapporteren van de voortgang van de bedrijfsprocessen zoals uiteengezet in deze tekst en het vastleggen van de taken die verschillende stakeholders hebben in het kader van het beleid voor gegevensbescherming.

Het verslag van dit stakeholdersoverleg wordt voorgelegd aan de stuurgroep voor gegevensbescherming.

11. Het takenpakket van de functionaris voor de gegevensbescherming of data protection officer (DPO)

Gezien de gevoeligheid van de gegevens die Ziekenhuis Oost-Limburg verwerkt, met name de grootschalige verwerking van gezondheidsgegevens in een steeds meer gedigitaliseerde informatieomgeving, is de aanstelling van een functionaris voor de gegevensbescherming of DPO raadzaam en verplicht.

Het wettelijk takenpakket van de functionaris voor gegevensbescherming of DPO is opgenomen in wetsartikel 39 van de verordening 2016/679. Daarnaast vertrouwt Ziekenhuis Oost-Limburg nog enkele impliciet in de verordening vermelde taken aan de functionaris/DPO toe en delegeert ze enkele taken in het kader van de verordening toe aan de functionaris.

De functionaris geeft advies over en kijkt toe op de verwerkingsprocessen van alle persoonsgegevens. De criteria die de functionaris gebruikt om zijn taken te prioritiseren, zijn niet opgenomen in deze beleidstekst met het oog op het onafhankelijk handelen van de functionaris. De Raad van Bestuur en het directiecomité zullen evenwel zeker advies vragen bij nieuwe verwerkingsprocessen die worden ingericht, verwerkingsprocessen die worden gedigitaliseerd of waarbij nieuwe technologieën worden gebruikt of waarvan de impact op de bescherming van de persoonlijke levenssfeer hoog is.

11.1 Bijstand en advies verlenen (wettelijke taak)

De functionaris of DPO verleent bijstand en verstrekt informatie over de verplichtingen van Ziekenhuis Oost-Limburg ten aanzien van de verordening. Minimaal handelt het advies over de verplichtingen aangaande:

- De principes van het verwerken van persoonsgegevens en in het bijzonder gevoelige persoonsgegevens
- De rechten van de betrokkene en in het bijzonder de rechten van de patiënt
- Gegevensbescherming bij ontwerp en standaardinstellingen, het register voor de verwerkingsactiviteiten
- De informatieveiligheid
- De elementen die horen bij het afhandelen en melden van inbreuken.

Meer in het bijzonder verleent de functionaris zijn adviezen en informatie aan het Directiecomité, al dan niet via de stuurgroep gegevensbescherming van Ziekenhuis Oost-Limburg. De functionaris geeft daarnaast ook, indien nodig, rechtstreeks advies aan het directiecomité en de Raad van Bestuur. Op die manier installeert

hij/zij een cultuur voor gegevensbescherming op het hoogste operationeel en beleidsmatig niveau. Tot slot doet hij/zij de nodige inspanningen voor het creëren van een cultuur voor gegevensbescherming onder de personeelsleden.

11.2 Toekijken op de naleving van de verordening (wettelijke taak)

De functionaris kijkt toe op de naleving van de verordening in het algemeen en de interne bedrijfsprocessen die hiervoor zijn in gericht in het bijzonder. De in deze beleidstekst beschreven bedrijfsprocessen dekken deze verantwoordelijkheidsdomeinen af en het toezicht wordt mogelijk gemaakt door de toegang tot het overleg en alle elementen die horen bij de bedrijfsprocessen, inclusief de persoonsgegevens die hierin worden verwerkt. De bedrijfsprocessen zelf vallen onder verantwoordelijkheid van het directiecomité van Ziekenhuis Oost-Limburg. In dit kader kan de functionaris in het bijzonder informatie verzamelen om de verwerkingsactiviteiten te identificeren, te analyseren en de conformiteit ervan te controleren en informatie, adviezen te verstrekken en aanbevelingen te formuleren. Het toezicht heeft betrekking op:

- De correcte toepassing van onderhavig beleid voor gegevensbescherming
- De correcte toepassing van alle Europese, Federale en Vlaamse regelgeving over het verwerken van persoonsgegevens
- Toekijken of eenieder de in dit beleidsdocument omschreven verantwoordelijkheid opneemt
- Toekijken op het bewustzijn inzake gegevensbescherming bij de stakeholders
- Toekijken en kennisnemen van de inhoud van andere audits en controles die handelen (of elementen bevatten) van audits.

11.3 Advies verstrekken over gegevensbeschermingseffectenbeoordelingen (wettelijk optionele taak)

Ziekenhuis Oost-Limburg vraagt de functionaris om advies te geven over de gegevensbeschermingseffectbeoordeling. Ziekenhuis Oost-Limburg verwacht advies over:

- Het al dan niet uitvoeren van een effectbeoordeling
- De te gebruiken methode voor het uitvoeren van een effectbeoordeling
- De keuze om de effectbeoordeling intern houden of extern laten uitvoeren
- Het soort toe te passen waarborgen om de risico's voor de rechten en vrijheden van de betrokkenen te verminderen
- De evaluatiecriteria om te bepalen of de beoordeling correct werd uitgevoerd en of de conclusies conform de verordening zijn.

11.4 Contactpunt zijn voor de Gegevensbeschermingsautoriteit en hiermee samen werken (wettelijke taak)

De functionaris of DPO is voor Ziekenhuis Oost-Limburg contactpunt voor de (nog op te richten) Gegevensbeschermingsautoriteit en werkt hiermee samen in het algemeen en in de naleving van voorafgaande raadpleging.

Over dat laatste is de wijze waarop dit gebeurt nog niet gekend. De rol van de functionaris voor de gegevensverwerking ten aanzien van het Sectoraal comité sociale zekerheid en gezondheid afdeling gezondheid is immers nog niet verder verduidelijkt, alsook het voortbestaan van het comité. Deze zal opgenomen worden in een volgende versie van deze beleidstekst.

11.5 Optionele taken

Ziekenhuis Oost-Limburg kan de functionaris of DPO tevens belasten met het uitvoeren van optionele taken. In dit geval zal, conform de statuten van het Ziekenhuis Oost-Limburg een delegatie van bevoegdheden worden gegeven aan de functionaris of DPO.

12. De positie van de functionaris voor de gegevensbescherming

In lijn met de bepalingen in verordening 2016/679 voorziet de directie van Ziekenhuis Oost-Limburg volgende bepalingen inzake de positie van de functionaris:

- Ziekenhuis Oost-Limburg zorgt ervoor dat de functionaris tijdig wordt betrokken bij alle gelegenheden die verband houden met de bescherming van persoonsgegevens. We zorgen ervoor dat alle vragen inzake gegevensbescherming worden verzameld.
- Voor dringende vragen is de functionaris telefonisch of per mail bereikbaar.
- De functionaris wordt toegang verleend tot de verwerkingsprocessen en persoonsgegevens.
- De functionaris krijgt voldoende ruimte om zijn competenties bij te werken
- De functionaris brengt rechtstreeks verslag uit aan het directiecomité en de Raad van Bestuur indien noodzakelijk.
- De functionaris krijgt geen instructies met betrekking tot de uitvoering van de taken en is op die manier onafhankelijk.
- In het handvest met de functionaris zijn garanties opgenomen die ervoor zorgen dat dit handvest niet kan worden doorbroken of er geen straffen kunnen volgen voor de uitvoering van de taken.
- De functionaris is aanspreekbaar voor eenieder wiens persoonsgegevens door Ziekenhuis Oost-Limburg worden verwerkt, in het bijzonder de medewerkers en patiënten.
- De in het vorig hoofdstuk opgesomde bijkomende taken worden opgenomen in het functieprofiel.

13. Het kennisniveau van de functionaris voor de gegevensbescherming

Het vereiste kennisniveau van de functionaris voor de gegevensbescherming is opgenomen in het functieprofiel en dwingt professionele kwaliteiten af betreffende de deskundigheid op het gebied van alle wetgeving en de praktijk inzake gegevensbescherming en het vermogen om het takenpakket dat in dit beleid is omschreven uit te voeren. In het functieprofiel is opgenomen dat deze kennis wordt bewezen via een certificaat of attest van het volgen van opleiding. Jaarlijks dient deze kennis te worden bijgewerkt en de bewijzen daarvan moeten op vraag kunnen worden opgeleverd door de functionaris.

14. De benodigde tijd voor het uitvoeren van de taken van de functionaris voor de gegevensbescherming

De functionaris wordt aangesteld op basis van een initiële tijdsinschatting van 0,3 VTE. Deze inschatting ligt in lijn met de inschatting van de functie van veiligheidsconsulent, hoewel het takenpakket verschillend is.
Op basis van voorkomende risico's wordt de tijdsbesteding van de functionaris periodiek geëvalueerd op de stuurgroep gegevensbescherming en gerapporteerd aan het directiecomité. Op basis hiervan zal, zonder afbreuk te doen aan het takenpakket van de functionaris, de tijdsbesteding worden bijgestuurd.

Ziekenhuis Oost-Limburg zal voor het verder inschatten van de benodigde tijd ook rekening houden met eventuele afspraken in de sector (bijvoorbeeld aan de hand van een sectorale gedragscode).

15. Communicatie van de identiteit van de functionaris

De identiteit van de functionaris voor de gegevensbescherming van Ziekenhuis Oost-Limburg wordt meegedeeld aan de Gegevensbeschermingsautoriteit van zodra deze is opgericht en de procedure ter zake gekend is. De identiteit wordt met naam en contactgegevens, inclusief telefoonnummer, voor personeelsleden en medewerkers van Ziekenhuis Oost-Limburg op een intern toegankelijk portaal gepubliceerd. De contactgegevens worden eveneens opgenomen in de privacy policy van Ziekenhuis Oost-Limburg zoals wettelijk bepaald, maar zonder vrijgave van persoonsgegevens (via een generiek e-mailadres).

De stuurgroep gegevensbescherming houdt de betreffende contactgegevens actueel.