PCM
Psychiatrisch Centrum Menen

Handtekening alg. dir.	INSTRUCTIEVADEMECUM	In voege vanaf: 06/07/2018 Laatste revisie: 25/05/2018			
Nr. procedure: Proc.eigenaar: Stafmed. gegs.bescherm	*VISIETEKST* Veiligheidsbeleid gegevensbescherming	pagina	1	van	21

Inhoudsopgave

1. Doel van de visietekst

Voor het Psychiatrisch Centrum Onze Lieve Vrouw van Vrede te Menen - in de tekst verder opgenomen als PCM - is het beschermen van de persoonlijke levenssfeer een belangrijk strategisch doel en bovenal een wettelijke verplichting die het PCM 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 medewerkers, geneesheren 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 het PCM. 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.

Deze visietekst wordt geïntegreerd in het kwaliteitsmanagement van het PCM, onder het toeziend oog van de verantwoordelijke kwaliteitscoördinatoren.

2. Verwante documenten Instructie Vademecum

- Melding van datalek (voorbeelden datalek, wanneer melden, hoe melden, data breach incident register);
- Rechten van betrokkenen (hoe te antwoorden op vragen van de betrokkene, definitie van de rechten + contactgegevens DPO);
- Veiligheidsbeleid informatieveiligheid (omschrijven beveiligingsmaatregelen en richtlijnen m.b.t. gegevensverwerking).

3. De uitvoering van het beleid voor gegevensbescherming

Het beleid voor gegevensbescherming wordt in deze eerste fase geïmplementeerd aan de hand van een implementatieplan die voortvloeit uit de nulmeting van 23 en 24 april 2018. Na de implementatiefase zal dit beleid dynamisch worden opgevolgd via permanente controles en verbeterplannen. We beogen bijgevolg reeds een belangrijke herziening van dit beleid (vooral op tactisch vlak) tegen eind 2018. In de periode ervoor zal dit beleid verder worden uitgediept voor de verschillende deeldomeinen.

Deze beleidstekst zal jaarlijks of bij belangrijke wijzigingen opnieuw ter goedkeuring voorgelegd worden aan de directie en de Raad van Bestuur van het PCM. 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) richtlijn voor de beveiliging van informatienetwerken en -systemen.

Voor een vlot integratie van de verordening 2016/679 werd in januari 2018 een stuurgroep voor de verwerking gegevensbescherming, onder de verantwoordelijkheid van het directiecomité, opgericht. Om aan de wettelijke verplichting, aanstellen van een functionaris voor de gegevensbescherming, te voldoen, koos het PCM ervoor in zee te gaan met het consulting bureau BDO Risk & Assurance Services (BDO RAS) als externe functionaris voor gegevensbescherming en intern een stafmedewerker functionaris gegevensbescherming aan te stellen die de coördinatie binnen het PCM en de contacten met BDO RAS op zich neemt.

4. De scope van het beleid gegevensbescherming

4.1. Materieel toepassingsgebied

Het beleid is van toepassing op alle persoonsgegevens die het PCM verwerkt. We verstaan hieronder niet alleen de gegevens van onze patiënten, maar ook bijvoorbeeld persoonsgegevens van medewerkers, geneesheren, studenten, vrijwilligers, leveranciers, ... en data afkomstig van andere verwerkingsverantwoordelijken waarvoor het PCM als verwerker optreedt.

4.2. 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.

4.3. Organisatorisch toepassingsgebied

Deze beleidstekst is geschreven voor iedereen die in opdracht van het PCM persoonsgegevens verwerkt. Zowel de directie, het management, de medewerkers in dienstverband en geneesheren, maar ook elke medewerker of leverancier die via andere overeenkomsten deelnemen aan de gegevensverwerking (zelfstandige zorgverleners, stagiairs en vrijwilligers). De

bepalingen van dit veiligheidsbeleid worden opgenomen in de contracten en kenbaar gemaakt via bewustwordingssessies. We zorgen ervoor dat deze tekst via verschillende kanalen wordt uitgedragen en wordt gepubliceerd op de websites en het instructievademecum van het PCM.

Het beleid gegevensbescherming is voor het PCM het uitgangspunt in haar samenwerking met andere zorginstellingen en -verstrekkers, zoals haar participatie in de locoregionale zorgnetwerken. De veiligheidsconsulent BDO RAS en de ZIS-dienst waken erover dat de principes van dit veiligheidsbeleid worden toegepast in alle samenwerkingsverbanden die het PCM opzet in de zorg.

5. Beleidsdoelstellingen voor gegevensbescherming

Voor alle verwerkingen van persoonsgegevens waarvoor het PCM verantwoordelijk is, wordt de rechtmatigheid beheerd en afgetoetst. We gebruiken hierbij de algemene voorwaarden die in de Algemene 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, voor de instelling en uitoefening van een rechtsvordering, voor verplichtingen in het kader van het arbeidsrecht of socialezekerheidsrecht, ... In vooropgesteld geval zal de verwerking enkel plaatsvinden onder verantwoordelijkheid van het bestuur en de directie van het PCM en onder de naleving van het beroepsgeheim.

Naast de in de Algemene Verordening Gegevensbescherming opgesomde rechtmatigheidsregels, leven we ook de geldende Vlaamse, Federale en Europese regels na over het verwerken van persoonsgegevens. Met betrekking tot patiëntengegevens omvat dit onder meer, maar niet limitatief, de regelgeving over patiëntenrechten, de omgang met persoonsgegevens bij de uitwisseling ervan, regels over wetenschappelijk onderzoek en specifieke regels over de omgang met gevoelige gegevens. Ook regels inzake de verwerking van persoonsgegevens in financiële stromen en sociale zekerheid worden opgevolgd, alsook de regels met betrekking tot personeels-en loonadministratie.

Het PCM monitort het bestaan en de evoluties van de in de sector geldende gedragscodes en past deze toe volgens de regels die deze voorschrijven. Dit betekent dat het PCM de intentie uitspreekt om zich aan te sluiten bij alle toepasselijke gedragscodes, in het bijzonder de gedragsregels opgesteld door Zorgnet-Icuro.

Concreet streven we volgende doelstellingen na:

Het PCM:

1. Verwerkt persoonsgegevens voor **welbepaalde en uitdrukkelijk omschreven doeleinden**, die we duidelijk communiceren naar de betrokkene en opnemen in een register van verwerkingsactiviteiten. We waken erover dat deze doelen steeds gerechtvaardigd zijn, in lijn met onze juridische eigenheid, onze visie en missie.
2. 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.

3. 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 het PCM. Dit wordt telkens geëvalueerd bij een nieuw verwerkingsdoel.
4. Verwerkt enkel de persoonsgegevens die **strikt noodzakelijk** zijn voor de uitvoering van de activiteiten. Zo worden identificatoren die horen bij de persoonsgegevens tot een minimum herleid.
5. Kijkt toe op de **integriteit** van de persoonsgegevens gedurende de ganse verwerkingscyclus.
6. **Bewaart** gegevens niet langer dan noodzakelijk. De noodzakelijkheid is afgetoetst tegenover wettelijke verplichtingen, de doelmatigheid en de rechten en vrijheden van de betrokkene.
7. 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.
8. Doet alle nodige inspanningen om alle geldende **rechten van een betrokkene**, zoals het recht op inzage, afschrift en eventueel ook schrapping uit te voeren. Het PCM bewaakt hierbij over de eventuele beperkingen die op deze rechten van toepassing zijn.
9. 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.
10. Bewaakt haar **verantwoordingsplicht** door intern toezicht en controle en dit op basis van de wettelijk geldende principes.

6. De beleidstaken, bijhorende processen en verplichtingen als verwerkingsverantwoordelijke

Om de beleidsdoelstellingen te bereiken zijn een aantal taken vastgelegd. Deze taken zijn in lijn met alle wettelijke verplichtingen die het PCM dient na te streven (het aantoonbaarheidsprincipe). Daarnaast is de lijst van taken, zoals hieronder beschreven, geïnspireerd op praktijken van de **Goede Huisvader**.

Elke taak wordt beschreven, wordt ondersteund door een proces. De algemene verantwoordelijkheid voor het uitvoeren van deze taken berust bij het directiecomité van het PCM. De specifieke taken en de delegatie van de taken zijn opgenomen in hoofdstuk 8.

Voor elk proces moeten er implementatienormen en -richtlijnen aanwezig zijn. Deze vullen het beleid voor gegevensbescherming aan en maken er integraal deel van uit. De verwerkingsprocessen worden nadien planmatig geïmplementeerd.

De beleidstaken zijn hieronder opgelijst en worden kort besproken.

Het PCM:

1. Houdt permanent een **register bij van de verwerkingsactiviteiten** waarbij persoonsgegevens van de categorieën van betrokkenen (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 of de gegevens al dan niet worden uitgewisseld, wie daarbij de categorieën van ontvangers zijn, 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.
2. Het verwerkingsregister wordt bijgewerkt voorafgaand aan het inrichten van nieuwe verwerkingsdoelen en bijhorende processen. Op dat moment wordt het afgetoetst aan de wettelijke en statutaire taken van het PCM. 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. Het PCM houdt het verwerkingsregister bij in digitale vorm en is opvraagbaar volgens de wettelijke bepalingen (i.e. door de Gegevensbeschermingsautoriteit).
3. 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. Het PCM beheert naast de lijst van criteria voor het uitvoeren van deze analyse, ook het proces voor het initiëren, bewaken, bijwerken en uitvoeren ervan.
4. 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. Het PCM 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.
5. Voorziet de nodige processen die ervoor zorgen dat de betrokkene wordt **geïnformeerd** over de verwerking. De verstrekte informatie omvat de wettelijk opgelegde elementen,

waaronder volgende: de functionaris voor de gegevensverwerking of de data protection officer (DPO), het verwerkingsdoel en de ontvangers van de gegevens. Daarnaast zijn processen gedocumenteerd die de rechten van de betrokkene omvatten (het recht op inzage, afschrift, gegevenswissing, overdraagbaarheid, rectificatie, beperking van de verwerking, kennisgeving, overdraagbaarheid). Deze processen houden rekening met de beperkingen die van toepassing zijn uit hoofde van de wet (patiëntenrechten en de verordening 2016/679).

6. 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.

7. Zorgt voor **duidelijke instructies en richtlijnen**, in overeenstemming met de verantwoordelijkheden die medewerkers van het PCM 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.

7. Toepassing van het beleid gegevensbescherming op de locoregionale netwerken

Het PCM 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 het PCM haar Goede Huisvaderprincipes ook toepassen op de leden van het netwerk.

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

8. De organisatie van gegevensbescherming

In dit veiligheidsbeleid concretiseren we bovenstaande beleidstaken en rollen in een organisatiestructuur. Hiertoe wordt een matrix opgesteld waarin de beleidstaken worden uitgezet tegenover de verschillende verantwoordelijkheden. De matrix wordt opgesteld en onderhouden

onder verantwoordelijkheid van de directie, op advies van de stuurgroep gegevensbescherming. De directie ziet toe op de uitvoering van de verantwoordelijkheden.

8.1. Beschrijving van de belangrijkste taken

Verantwoordelijkheid over persoonsgegevens

De verantwoordelijkheid voor het uitvoeren van de beleidstaken in het kader van gegevensbescherming ligt bij het directiecomité. Het directiecomité is verantwoordelijk voor het bekrachtigen van de beleidsdoelen en de hierbij horende taken. In de uitvoering van deze verantwoordelijkheden kan het directiecomité beroep doen op de adviezen van de stuurgroep gegevensbescherming en de functionaris voor de gegevensbescherming of data protection officer (DPO). Elke beoordeling van risico's vindt plaats onder verantwoordelijkheid van het directiecomité, alsook de uitvoering van de bijhorende maatregelen. Het directiecomité is daarnaast ook eindverantwoordelijk voor alle verplichtingen uit hoofde van de wet- en regelgeving, waaronder de bepalingen in de verordening 2016/679. Hiervoor delegeert het directiecomité een aantal taken, zoals hieronder opgesomd.

Toezicht gezondheids-gegevens patiënten

Het beleid voor gegevensbescherming doet op geen enkele wijze afbreuk aan de wettelijke verplichtingen die de afdelingsgeneesheer, hoofdverpleegkundigen en de directie patiëntenzorg hebben met het oog op de toepassing van de wetgeving over gegevensbescherming.

De hoofdgeneesheer wordt beschouwd als lasthebber van het ziekenhuis dat optreedt als de verwerkingsverantwoordelijke (cfr. gedragscode). De afdelingsgeneesheer (en voor verpleegkundige gegevens in nauwe samenspraak met de directie patiëntenzorg) heeft vanuit deze opdracht de verantwoordelijkheid inzake de gegevensbescherming van gezondheidsgegevens in het zorgdossier van de patiënt. 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 hoofdverpleegkundige en de directie patiëntenzorg in het uitvoeren van de gegevens-beschermingseffectenbeoordeling.

In de uitvoering van het beleid voor gegevensbescherming krijgt de directie patiëntenzorg de taak toegewezen om te oordelen over het ontwerp van een model van gegevensclassificatie, in relatie met de bijhorende processen (dit zijn zorgprocessen maar ook andere processen, 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 afdelingsgeneesheer 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 zorgdossier van de patiënt worden verwerkt, assisteert de afdelingsgeneesheer bij het uitwerken van de beleidslijnen.

De afdelingsgeneesheer en de hoofdverpleegkundigen stimuleren de correcte omgang met patiëntengegevens bij de medische afdelingen van het PCM. De hoofdverpleegkundige neemt bovendien alle relevante aspecten van gegevensbescherming mee in de evaluatie van nieuwe medewerkers en hun opleidingstraject tijdens dienstverband.

De directie patiëntenzorg kijkt toe op het onderhoud van het register van verwerkingsactiviteiten met het oog op de verwerking van gezondheidsgegevens.

Toezicht sociale gegevens patiënten

De sociale dienst, onder verantwoordelijkheid van de directie patiëntenzorg van het PCM stelt het register van verwerkingsactiviteiten op en oordeelt hierbij ook over de toepassing van de rechten van de betrokkene op deze gegevens. In de uitvoering van het beleid voor gegevensbescherming krijgt de sociale dienst, onder verantwoordelijkheid van haar manager, de taak toegewezen om te oordelen over het ontwerp van een model van gegevensclassificatie, in relatie met de bijhorende processen. 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 sociale dienst heeft ook bijzondere aandacht voor de verwerking van persoonsgegevens op basis van toestemming, gerechtvaardigd belang

	en de verwerking van gegevens van kinderen. Ook de uitwisseling van persoonsgegevens met actoren in de sociale dienstverlening krijgen hierbij extra aandacht.
Toezicht financiële gegevens patiënten	De dienst facturatie, onder verantwoordelijkheid van de administratief directeur van het PCM stelt het register van verwerkingsactiviteiten op binnen de dienst facturatie. De administratief directeur is verantwoordelijk voor het beoordelen van de rechten en vrijheden van de patiënt bij de verwerking van gegevens op de dienst (toegang tot zorg, het recht op zorg, verzekerbaarheid). De dienst facturatie, onder verantwoordelijkheid van haar manager, kijkt toe op de uitwisseling van persoonsgegevens met de overheid, de mutualiteiten, …
Toezicht administratieve gegevens patiënten	De dienst patiëntenadministratie (medische secretariaten, afdelingssecretariaten, patiëntengelden), onder verantwoordelijkheid van de administratief directeur van het PCM 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 verantwoordelijke 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 e-Health, 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 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, valt onder verantwoordelijkheid van de dienst aan wie de rapportering plaatsvindt in samenspraak met het hoofd van de ZIS-dienst. Het toezicht op de verwerker wordt georganiseerd door het hoofd van de ZIS-dienst, veiligheidsconsulent en de functionaris voor de gegevensbescherming.

De latere verwerking van gezondheidsgegevens uit de zorgdossiers van de patiënt voor kwaliteitsdoeleinden ten behoeve van inspectiediensten of accrediteringscommissies, valt onder de verantwoordelijkheid van de hoofdgeneesheer.

Toezicht persoonsgegevens medewerkers en geneesheren

De personeelsdienst, onder verantwoordelijkheid van de coördinator personeelsdienst-HRM 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 geneesheren. 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 processen worden ingevoerd of bestaande processen worden gedigitaliseerd, zorgt de coördinator personeelsdienst-HRM voor de analyse van de verwerkingsgrond, de eventuele bijhorende besprekingen met de personeelsvertegenwoordiging (bijvoorbeeld in het kader van transparantie en de evaluatie van gerechtvaardigde belangen) en de bijhorende gegevensbeschermingseffectenbeoordeling. De coördinator personeelsdienst-HRM levert daarenboven een actieve bijdrage bij het onderhouden van het register van verwerkingsactiviteiten voor personeelsgegevens.

	Voor de verwerking van persoonsgegevens van geneesheren wordt de corresponderende taak toebedeeld aan de verantwoordelijke van het medisch secretariaat onder verantwoordelijkheid van de hoofdgeneesheer.
Toezicht toepassing gegevensbescherming door medewerkers en geneesheren	De coördinator personeelsdienst-HRM heeft de verantwoordelijkheid om de verplichtingen inzake het toepassen van dit beleid te vertalen naar het arbeidsreglement, de toepasselijke handvesten en functieprofielen (met uitzondering van de verplichtingen van de geneesheren), het sanctiebeleid en de controles en evaluaties. Voor de corresponderende verplichtingen voor geneesheren wordt deze verantwoordelijkheid bij de hoofdgeneesheer gelegd.
Algemeen toezicht gegevensbescherming bij verwerkers	Het algemeen toezicht op verwerkers van persoonsgegevens die in opdracht van het PCM 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 coördinator en de functionaris voor de gegevensbescherming of DPO. De aankoopdienst voert de instructies hierover uit onder toezicht van het diensthoofd en de administratief & logistiek directeur.
Gegevensbescherming bij zorginnovatie	Elk proces dat gedigitaliseerd wordt of voor elk (al dan niet nieuw) proces waarbij innoverende technologieën worden gebruikt wordt de functionaris voor de gegevensbescherming of DPO geconsulteerd. De verantwoordelijkheid hiervoor ligt bij de initiatiefnemer. Voor wat betreft de geneesheren 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.

8.2. Beschrijving van de belangrijkste Rollen

De medewerker	Iedereen (intern of extern) die gegevens verwerkt (bijvoorbeeld inkijkt,

(al of niet in dienstverband)	registreert, wijzigt, …), doet dit volgens de beleidsprincipes uit deze visietekst. De gebruiker verwerkt gegevens in overeenstemming met de discretieplicht, en conform volgende principes: • is verantwoordelijk voor de gegevens van patiënten die hij/zij verwerkt; • voert de veiligheidsrichtlijnen uit tijdens zijn/haar verwerkingsopdracht; • verwerkt enkel die gegevens die horen bij de taak; • draagt zorg voor de gegevens; • meldt inbreuken; • leeft artikel 458 van het Strafwetboek na: De gebruiker respecteert het beroepsgeheim.
Dienstverantwoordelijke	Bijkomend aan de verantwoordelijkheden van de medewerker, ziet de dienstverantwoordelijke toe op de goede uitvoering van de veiligheidsbepalingen. De dienstverantwoordelijke volgt de veiligheidsrichtlijnen op en informeert de medewerkers hierover. De dienstverantwoordelijke zorgt voor een veiligheidscultuur en onderhoudt deze, bijvoorbeeld door het bespreken van de beleidsrichtlijnen op het teamoverleg. De dienstverantwoordelijke ondersteunt controleactiviteiten, bijvoorbeeld door het controleren van logging in het elektronisch zorgdossier van de patiënt.
Hoofdgeneesheer	Vanuit de ondersteunende rol voor kwaliteitsbeheer geeft de hoofdgeneesheer op vraag of uit eigen beweging adviezen over de beveiligingseisen ten aanzien van medische gegevens. Op vraag van de veiligheidsconsulent bepaalt de hoofdgeneesheer veiligheidsprincipes voor de bescherming van de medische persoonsgegevens van de patiënten.
Behandelend geneesheer	Naast de veiligheidsprincipes, zoals bepaald voor de medewerker, is de behandelend geneesheer verantwoordelijk voor het afleveren van een correct medisch dossier.
ZIS-medewerker	De ZIS-medewerker is, in toevoeging van de verantwoordelijkheden voor de gebruiker, verantwoordelijk voor: • de implementatie van de technische maatregelen; • veiligheidsinstellingen te implementeren in lijn met deze visietekst; • veiligheidsproblemen die ontstaan voor, tijdens of na de implementatie van ICT-middelen te melden aan de veiligheidsconsulen; • fungeert als expert. Vanuit deze rol neemt hij deel aan de

identificatie zowel als aan de remediëring van de informatieveiligheidsrisico's;
- de gedragscode naleven.

ICT-leverancier

De ICT-leverancier heeft dezelfde verantwoordelijkheden als deze van een ICT-medewerker. Bijkomstig:
- wijst hij op veiligheidsrisico's van geleverde toepassingen;
- wijst de leverancier op de op te nemen veiligheidstaken;
- streeft de leverancier een transparant veiligheidsbeleid na door te communiceren over het eigen actuele veiligheidsniveau en bij de afhandeling van veiligheidsincidenten.

De veiligheidsconsulent

De inhoudelijke opvolging van het veiligheidsbeleid ligt bij de veiligheidsconsulent. Het PCM legt de identiteit (en eventuele wijzigingen) van de veiligheidsconsulent voor aan de Vlaamse Toezichtcommissie ter beoordeling. De veiligheidsconsulent rapporteert aan de directeur van het PCM en is meer in het bijzonder belast met:
- adviezen en aanbevelingen voorleggen aan het directiecomité;
- opdrachten uit te voeren op vraag van het directiecomité;
- bevorderen van de bewustwording van alle actoren binnen het PCM;
- ziet toe op de naleving van het veiligheidsbeleid binnen het PCM;
- documenteert het veiligheidsbeleid, in overleg met de kwaliteitsmedewerker en volgens dezelfde methodiek;
- stelt het veiligheidsplan op voor een periode van 3 jaar en waakt over de uitvoering ervan;
- stelt een jaarverslag op met de vorderingen van het veiligheidsplan en legt dit voor aan het directiecomité;
- registreert overtredingen en maakt deze, samen met een advies, over aan het directiecomité.

De functionaris voor gegevensbescherming (DPO)

BDO RAS die optreed als DPO verleent bijstand, verstrekt informatie over en kijkt toe op de verplichtingen van het PCM ten aanzien van de verordening. Minimaal behandelt de DPO de verplichtingen aangaande:
- bijstand en advies verlenen (wettelijke taak):
  - 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.
- toekijken op de naleving van de verordening:
  - 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.
- advies verstrekken over gegevensbeschermingseffecten-beoordelingen (DPIA);
- contactpunt zijn voor de Gegevensbeschermingsautoriteit en hiermee samen werken;
- coördineren van incidentmeldingen in verband met gegevensbescherming.

9. De relatie tussen gegevensbescherming en informatieveiligheid

Het PCM vertrouwt het toezicht op informatieveiligheid toe aan BDO RAS als veiligheidsconsulent. De taken van de veiligheidsconsulent zijn opgenomen in het veiligheidsbeleid (zie instructie vademecum), dat onder verantwoordelijkheid van het directiecomité valt.

Voor het PCM worden de taken van de veiligheidsconsulent en van de functionaris voor de gegevensbescherming of DPO gecombineerd opgenomen door BDO RAS. De identiteit van de veiligheidsconsulent is voorgesteld en besproken op het directiecomité van 26/11/2012 en werd overgemaakt aan het sectoraal comité van de sociale zekerheid en de gezondheid, afdeling gezondheid.

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 adviseert de stuurgroep gegevensbescherming van het PCM.

De taken van de functionaris voor de gegevensbescherming zijn hierboven beschreven.

10. De stuurgroep gegevensbescherming

Het directiecomité delegeert haar taken uit hoofde van verantwoordelijke voor de verwerking aan de stuurgroep gegevensbescherming. Deze stuurgroep wordt voorgezeten door de algemeen directeur van het PCM. De stuurgroep bestaat uit de applicatieverantwoordelijke zorgdossier van de patiënt, de directie patiëntenzorg, het hoofd van de ZIS-dienst, een kwaliteitsmedewerker, de coördinator personeelsdienst-HRM, de stafmedewerker gegevensbescherming en een vertegenwoordiger HTW en PVT.

De stuurgroep adviseert het directiecomité en bereidt beslissingen voor 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 processen 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 processen die in deze beleidstekst zijn omschreven;
- het toekennen van de verantwoordelijkheden voor het uitvoeren van de processen;
- 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.

11. Aanstellen van een functionaris voor de gegevensbescherming (DPO)

Gezien de gevoeligheid van de gegevens die het PCM verwerkt, met name de grootschalige verwerking van persoonsgegevens (met inbegrip van gezondheidsgegevens) in een steeds meer gedigitaliseerde informatieomgeving, is de aanstelling van een functionaris voor de gegevensbescherming verplicht.

Om aan deze verplichting te voldoen, heeft het PCM ervoor gekozen om BDO RAS aan te stellen als functionaris voor gegevensbescherming in de zin van de AVG.

Om de behoorlijke uitoefening van de taken en verplichtingen van de functionaris voor gegevensbescherming mogelijk te maken besliste het PCM tevens om een tijdelijke interne stafmedewerker medewerker gegevensbescherming, als interne contactpersoon en coördinator, aan te wijzen ter ondersteuning in het ganse GDPR proces. Deze interne stafmedewerker gegevensbescherming zal de nodige tijd krijgen om zijn kennis bij te werken om te kunnen voldoen aan het takenpakket dat in dit beleid is omschreven. Na de opstartfase, zijnde 2019, zal het takenpakket van deze stafmedewerker gegevensbescherming opgenomen worden door de stafmedewerker, kwaliteitsbeleid, communicatie en incidentenmelding.

Het wettelijk takenpakket van de functionaris voor gegevensbescherming is opgenomen in wetsartikel 39 van de verordening 2016/679. Daarnaast vertrouwt het PCM nog enkele impliciet in de verordening vermelde taken aan de functionaris 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 prioriteren, zijn niet opgenomen in deze beleidstekst met het oog op het onafhankelijk handelen van de functionaris. Het directiecomité zal 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. De positie van de functionaris voor de gegevensbescherming

In lijn met de bepalingen in verordening 2016/679 voorziet de directie van het PCM volgende bepalingen inzake de positie van de functionaris:

- Het PCM 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 via de stuurgroep gegevensbescherming, waarin de functionaris zetelt, worden verzameld.
- Voor dringende vragen is de functionaris telefonisch of per mail bereikbaar. Aangezien het PCM gebruik maakt van een dienstverlener, zullen de vereisten rond beschikbaarheid contractueel worden opgenomen.
- De functionaris wordt toegang verleend tot de verwerkingsprocessen en persoonsgegevens. Aangezien het PCM gebruik maakt van een dienstverlener zal een verwerkersovereenkomst worden opgesteld.
- De functionaris krijgt voldoende ruimte om zijn competenties bij te werken. Aangezien het PCM gebruik maakt van een dienstverlener, zal dit opgenomen worden in het servicecontract, evenals de bijhorende deontologische codes en geheimhouding.
- De functionaris brengt rechtstreeks verslag uit aan het directiecomité indien noodzakelijk. Functioneel gebeurt deze rapportage aan de stuurgroep gegevensbescherming.
- 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 het PCM worden verwerkt, in het bijzonder de medewerkers en patiënten.
- De in punt 7.2 opgesomde taken worden opgenomen in het dienstverleningscontract.

11.2. Het kennisniveau van de functionaris voor de gegevensbescherming

Het vereiste kennisniveau van de functionaris voor de gegevensbescherming is opgenomen in het servicecontract 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 servicecontract 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 aanbieder.

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

De externe en interne functionaris wordt aangesteld op basis van een initiële tijdsinschatting. Deze inschatting wordt door BDO RAS gecombineerd met de functie van veiligheidsconsulent, hoewel het takenpakket verschillend is.

Op basis van voorkomende risico's wordt de tijdsbesteding van beide functionarissen jaarlijks geëvalueerd in de twee richtingen. Op basis hiervan zal, zonder afbreuk te doen aan het takenpakket van de functionaris, de tijdsbesteding worden bijgestuurd.

Het PCM 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).

11.4. Communicatie van de identiteit van de functionaris

De identiteit van de functionaris voor de gegevensbescherming zal door het PCM worden 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 medewerkers, studenten, geneesheren en patiënten van het PCM op een intern toegankelijk portaal gepubliceerd. De contactgegevens worden eveneens opgenomen in de privacy policy van het PCM zoals wettelijk bepaald.

De stuurgroep gegevensbescherming houdt de betreffende contactgegevens actueel.

12. Het beheer van risico's

Het PCM brengt de risico's inzake gegevensbescherming in kaart aan de hand van een 0-meting, die voor het eerst werd uitgevoerd op 23 en 24 april 2018. De 0-meting werd uitgevoerd op basis van volgende criteria (toetsingskader):

- de richtsnoeren met betrekking tot de informatiebeveiliging van persoonsgegevens, zoals deze werden gepubliceerd door de **Commissie voor de Bescherming van de Persoonlijke Levenssfeer;**
- de **Algemene Verordening Gegevensbescherming**;
- het decreet betreffende de organisatie van het netwerk voor de gegevensdeling tussen de actoren in de zorg.

De 0-meting bracht operationele en tactische risico's in kaart. Deze risico's werden besproken samen met het directiecomité op 15/06/2018. De risico's werden thematisch gerangschikt en de te nemen maatregelen worden opgenomen in het veiligheidsplan, dat gedurende de volgende 3 jaren wordt gerealiseerd.

Jaarlijks wordt de voortgang van het veiligheidsplan besproken met de directie van het PCM in de vorm van een jaarrapport. Hierin worden ook nieuwe risico's besproken en wordt het toetsingskader gevalideerd.

Elke 3 jaar her-evalueert het PCM de risico's aan de hand van een veiligheidsaudit. Deze analyse heeft als doel de effectiviteit van de genomen maatregelen te controleren en nieuwe risico's in kaart te brengen.

13. Opsomming van de maatregelen: inhoud van het veiligheidsplan

Opsomming van de actiedomeinen 2018 die door de directie werden goedgekeurd:

Actieplan 2018_gegevensbescherming PCM – versie 26/06/2018 -		
Inhoud vlak	*prioriteit*	*Operationele richtdatum*
Organisatorisch		
Implementatie policies websitebezoeker, personeel, patiënt, student, … op websites en IV	**1**	jul/18
Implementeren gegevensbeschermingsbeleid (verwijzing IV, plaatsen op de 3 websites)	**1**	jul/18
Aanstellen van proces eigenaars	**2**	najaar/2018
Bewustwordingsprogramma (inscholing, postercampagne, sensibilisering, communicatie richtlijnen bij indiensttreding)	**2**	nov/18
Uitbreiden informaticareglement en beleid mbt beveiligingsmaatregelen naar één centrale IT policy	**1**	jul/18
Ontwikkelen van een preventief en gedocumenteerd GDPR beleid:		
○ Opslagbeperking: Vastleggen uniforme referentietermijnen voor bewaren van persoonsgegevens, hoe data verwijderen na referentieperiode	**1**	okt/18
○ Juistheid van gegevens en data minimalisatie: vermijden gegevens op te slaan op meerdere plaatsen		jul/18
○ Rechtmatig, behoorlijk en transparant: toestemming om gegevens te delen (huisarts, foto), bijwerken informed consent		aug/18
Aandacht fysieke beveiliging van hardcopy gegevens (gesloten kasten)	**2**	nov/18
Juridisch		
Herbekijken overeenkomsten met verwerkers ifv GDPR	**2**	aug/18
Template verwerkingsovereenkomst		jun/18
Voor welke diensten zijn we verwerkingsverantwoordelijke, dan wel verwerker		aug/18
Aandacht voor data protection by design en by default bij selectie verwerkers		
Refereren privacy clausule (AR) en vertrouwelijkheidsclausule in het arbeidscontract	**1**	sep/18
IT-technisch		
Invoeren van controles:		
○ Periodiek loggin's nakijken op onregelmatigheden	**2**	opgestart
○ Periodiek testen back-ups	**2**	opgestart
Wachtwoordpolicy		okt/18
Standaard lock-out		opgestart
Ontwikkelen polices inzake BYOD, gebruik mobiele toestellen, toegang lokalen, enz.		dec/18
Opsporen, analyseren en documenteren van kwetsbaarheden		najaar/2018
Protcol remote access herzien		dec/18
Data-register		
Opnemen in project management methologie:		
○ Vastleggen verantwoordelijkheid update en documenteren nieuwe verwerkingsactiviteiten	**2**	nov/18
○ Procesverantwoordelijke en beoordeling noodzaak DPIA's vastleggen	**2**	nov/18
Rechten van betrokkenen		
Opstellen procedure hoe het PCM met verzoek van betrokkenen omgaat	**1**	sep/18
Effectiviteit ervan nagaan		okt/18
Melden datalek		
Opstellen procedure om datalekken te melden	**1**	sep/18
Opstellen van template meldingsformulier	**1**	sep/18
Vastleggen rollen en verantwoordelijkheden in het meldingsplicht proces	**1**	sep/18
Vastleggen beoordelingscriteria impact datalek	**1**	sep/18
Bijhouden register met alle datalekken	**1**	sep/18
Effectiviteit ervan nagaan		okt/18
Stimuleren melden lekken		okt/18

14. Historiek van het document

Versie 1:	25/05/2018
Bekrachtigd op het directiecomité:	11/06/2018
Voorgelegd aan de raad van beheer:	05/07/2018
In voege vanaf:	06/07/2018
Versie2:	--/--/2018