Beleid gegevensbescherming

VZW LANGERHEIDE WZC

Langerheide 7 - 3150 Haacht

Inhoudsopgave

1. Inleiding: Het VZW Langerheide WZC-beleid voor gegevensbescherming

Voor VZW LANGERHEIDE WZC is het beschermen van de persoonlijke levenssfeer van de bewoners en de medewerkers één van haar beleidsprioriteiten: het is niet enkel een wettelijke verplichting (met zeer hoge boetes in geval van een inbreuk), maar ook een grondrecht van de betrokkene waar VZW LANGERHEIDE WZC groot belang aan hecht.

Met deze beleidstekst willen we in de eerste plaats duidelijke doelstellingen formuleren 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 toedienen van zorg (zoals het gebruik van persoonsgegevens voor onderzoek en kwaliteit) of het gebruik van de persoonsgegevens in zorginnovatie.

Deze beleidstekst wil in de eerste plaats duidelijke doelstellingen formuleren met betrekking tot het beleid gegevensbescherming in VZW LANGERHEIDE WZC en dit vanuit de toepasselijke regelgeving. De Verordening Gegevensbescherming bepaalt het algemene kader voor de verwerking van persoonsgegevens, dat in de context van de werking van een woonzorgcentrum nog verder wordt aangevuld door andere relevante wetgeving, zoals de Wet Patiëntenrechten, het beroepsgeheim (art. 458 Sw.), de regelgeving m.b.t. camerabewaking, e.d.m.

Daarnaast heeft deze beleidtekst als doel de actoren, intern of extern aan VZW LANGERHEIDE WZC verbonden, te informeren over de wijze waarop de gegevensbescherming in VZW LANGERHEIDE WZC wordt georganiseerd. De beleidsorganen en de uitvoeringsmodaliteiten van het VZW LANGERHEIDE WZC-beleid voor gegevensbescherming worden besproken en er wordt ingegaan op de verantwoordelijkheden die gepaard gaan met de uitvoering van het beleid. Dit document heeft oog voor het verwerken van persoonsgegevens binnen WZC, personeelsleden, artsen en andere actoren.

Versie	Auteur	Datum	Omschrijving
1.0	White Wire	11/12/2017	Template
2.0	White Wire	23/01/2018	Verbeterde versie
3.0	VZW LANGERHEIDE WZC	14/05/2018	Basisdocument VZW LANGERHEIDE WZC

Het beleid voor gegevensbescherming wordt in deze eerste fase (voor de inwerkingtreding van de Verordening Gegevensbescherming op 25 mei 2018) uitgewerkt aan de hand van een implementatieplan om ervoor te zorgen dat de verplichtingen voortvloeiend uit de Verordening Gegevensbescherming tegen 25 mei 2018 zijn geïmplementeerd. Na de implementatiefase zal dit beleid verder worden opgevolgd via permanente controles en verbeterplannen.

Verschillende aspecten en implicaties van de Verordening Gegevensbescherming zullen wellicht (pas) concreter worden rond 25 mei 2018 of later. Er wordt bijgevolg een belangrijke herziening van dit beleid beoogd tegen 25 mei 2018. Na 25 mei 2018 bestaat het opzet om dit beleid jaarlijks of bij belangrijke wijzigingen opnieuw ter goedkeuring voor te leggen aan de Raad van Bestuur van VZW LANGERHEIDE WZC. Op korte termijn hebben we oog voor de (EU) ePrivacy verordening en de Europeuse NIS-richtlijn voor de beveiliging van informatienetwerken en -systemen.

2. Begrippenkader

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

Verordening Gegevensbescherming: de Verordening (EU) 2016/679 van het Europees Parlement en de Raad van 27 april 2016 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens en tot intrekking van Richtlijn 95/46/EG. Deze Verordening treedt op 25 mei 2018 in werking. Deze Verordening wordt vaak ook GDPR genoemd (General Data Protection Regulation).

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

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

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

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

Verwerkingsverantwoordelijke: een natuurlijke persoon of rechtspersoon, een overheidsinstantie, een dienst of een ander orgaan die / dat, alleen of samen met anderen, het doel van en de middelen voor de verwerking van persoonsgegevens vaststelt. Als vuistregel geldt dat de zorgvoorziening kan worden beschouwd als verwerkingsverantwoordelijke voor alle verwerkingsactiviteiten die binnen haar schoot worden georganiseerd en waarvoor zij instructies kan geven. Wanneer de zorgvoorziening evenwel niet het doel en de middelen bepaalt, kan zij niet gekwalificeerd worden als verwerkingsverantwoordelijke (maar eventueel wel als verwerker, cf. infra).

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

Verwerker: een natuurlijke persoon of rechtspersoon, een overheidsinstantie, een dienst of een ander orgaan die / dat ten behoeve van de verwerkingsverantwoordelijke persoonsgegevens verwerkt.
Een zorgvoorziening kan ook als verwerker kwalificeren, wanneer het verwerkingsdiensten levert ten behoeve van een verwerkingsverantwoordelijke (bv. Een externe arts die gebruik maakt van de ICT-dienst van de zorgvoorziening) zonder dat de zorgvoorziening het doel en de middelen van de verwerking bepaalt.

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

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

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

Veiligheidsconsulent: staat in voor het toezicht op de informatieveiligheid. De taken van de veiligheidsconsulent zijn opgenomen in het veiligheidsbeleid.

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

3. Het toepassingsgebied van het beleid voor gegevensbescherming bij VZW LANGERHEIDE WZC

Het VZW LANGERHEIDE WZC-beleid Gegevensbescherming is van toepassing op de verwerking van persoonsgegevens waarbij VZW LANGERHEIDE WZC als verwerkingsverantwoordelijke (al dan niet samen met anderen) of verwerker is.

3.1 Materieel toepassingsgebied

Het beleid is van toepassing op de verwerking van persoonsgegevens. We verstaan hieronder niet alleen de persoonsgevens van bewoners, maar ook bijvoorbeeld van medewerkers, al dan niet in dienstverband, familieleden, bezoekers, derden,... De Verordening Gegevensbescherming is neit van toepassing op geanonimiseerde gegevens, dit zijn gegevens die geen betrekking hebben op een geïdentificeerde of identificeerbare natuurlijke persoon of op persoonsgegevens die zodanig anoniem zijn gemaakt dat de betrokkene niet of niet meer identificeerbaar is.

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

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

3.2 Personeel toepassingsgebied

Deze beleidstekst is geschreven voor iedereen die in opdracht van VZW LANGERHEIDE WZC persoonsgegevens verwerkt, zoals de directie, het management, de personeelsleden en artsen, maar ook elke medewerker of leverancier. Deze tekst wordt via verschillende kanalen uitgedragen.

Het beleid gegevensbescherming is voor VZW LANGERHEIDE WZC het uitgangspunt in haar samenwerking met andere zorginstellingen en -verstrekkers, zoals haar participatie in de zorgnetwerken.

4. Algemene doelstelling gegevensbescherming

De Verordening Gegevensbescherming bepaalt het kader waarbinnen de verwerking van persoonsgegevens geoorloofd kan plaatsvinden. Het stelt algemene beginselen voorop waaraan een verwerking van persoonsgegevens moet voldoen en legt verschillende verplichtingen op wanneer tot verwerking van persooonsgegevens wordt overgegaan.

Het voldoen aan de vereisten uit de Verordening Gegevensbescherming vormt ook meteen de doelstelling van het VZW LANGERHEIDE WZC-beleid Gegevensbescherming.

VZW LANGERHEIDE WZC kiest voor een missie die staat voor een kwalitatief hoogstaande huisvesting en zorgverlening aan ouderen aangevuld met ondersteunende en service gerichte diensten.

Daarnaast wil VZW LANGERHEIDE WZC het welzijn van de gebruiker in al zijn aspecten behartigen. Professionalisme, respect, integriteit en samenwerken staan als gedragsnormen hierbij centraal. Deze missie sluit aan bij de zorg voor alle persoonsgegevens die hierbij worden verwerkt.

De Verordening Gegevensbescherming verplicht naleving van een aantal beginselen wanneer persoonsgegevens worden verwerkt:

4.1 Rechtmatig

Voor alle verwerkingen van persoonsgegevens waarvoor VZW LANGERHEIDE WZC verantwoordelijk is, wordt de regelmatigheid 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 sociale zekerheidsrecht,...
In vooropgesteld geval zal de verwerking enkel plaatsvinden onder verantwoordelijkheid van de VZW LANGERHEIDE WZC en onder naleving van het beroepsgeheim.

Naast de in de Algemene Verordening Gegevensbescherming opgesomde rechtmatigheidsregels, leven we ook de geldende Vlaamse, Federale en Europese regels op 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, de omgang met gevoelige gegevens, zoals biometrische en genetische 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.

VZW LANGERHEIDE WZC monitort het bestaan en de evoluties de in de sector geldende gedragscodes en past deze toe volgens de regels die deze gedragscodes voorschrijven. Dit betekent dat VZW LANGERHEIDE WZC de intentie uitspreekt om zich aan te sluiten bij alle toepasselijke gedragscodes.

4.2 Behoorlijk en transparant

We volgen een ‘fair use’ principe in de omgang met persoonsgegevens, waarbij we behoorlijke gegevensverwerking nastreven, eerlijk en transparant naar alle betrokkenen en de toezichthouder.

4.3 Gerechtvaardigd doel

We verwerken 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 en onze visie en missie.

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

Voor de verdere verwerking in het kader van wetenschappelijk of historisch onderzoek of statistische doeleinden, waarborgen we de rechten en vrijheden van de betrokkene, waaronder in het bijzonder de rechten van de betrokkene. De voorziene waarborgen zorgen ervoor dat er technische en organisatorische maatregelen zijn getroffen om de minimale gegevensverwerking te garanderen, zoals opgelegd door de regelgever. We trachten bij deze verwerkingen de identificatiegegevens maximaal te verwijderen (anonimiseren). Indien dit niet mogelijk blijkt om het beoogde doel te verwezenlijken, passen we de regels inzake pseudonimisering toe, tenzij deze het beoogde doel onmogelijk maken.

4.4 Minimale gegevensverwerking

Bij het verwerken van persoonsgegevens waken we erover dat de persoonsgegevens die we verwerken toereikend, ter zake dienend en noodzakelijk zijn binnen het beoogde doel.

4.5 De juistheid

VZW LANGERHEIDE WZC streeft daarenboven naar een zorgvuldig bijgehouden patiëntendossier. Ook voor alle andere verwerkingen bewaken we integriteit van de persoonsgegevens. Dit betekent in essentie dat persoonsgegevens volledig en juist zijn rekening houdende met het beoogde verwerkingsdoel. Wanneer de kans bestaat dat de persoonsgegevens niet actueel of fout zijn, zullen we extra inspanningen leveren om de gegevens te corrigeren of zo nodig te wissen. We gebruiken hierbij alle mogelijke verificatiebronnen (zoals overheidsregisters) die ons ter beschikking worden gesteld. Wanneer de correctheid van gegevens door de betrokkene worden betwist, nemen we weloverwogen beslissingen, in overeenstemming met het toepasselijk recht, met het oog op de juistheid van de gegevens en de vrijwaring van het recht op goede zorg en een kwalitatief dossier.

4.6 De opslagbeperking

VZW LANGERHEIDE WZC bewaart gegevens niet langer dan noodzakelijk. De noodzakelijkheid is afgetoetst tegenover wettelijke verplichtingen en het beoogde verwerkingsdoel. Wanneer persoonsgegevens worden gearchiveerd respecteren we de wettelijke en administratieve voorschriften die hierop van toepassing zijn en bewaken we het gebruik van deze persoonsgegevens in onze verwerkingsprocessen.

4.7 De integriteit en vertrouwelijkheid

VZW LANGERHEIDE WZC neemt de passende technische en organisatorische maatregelen met het oog op een passende beveiliging van persoonsgegevens. Op die manier beschermen we de persoonsgegevens onder meer tegen ongeoorloofde of onrechtmatige verwerking en tegen onopzettelijk verlies, vernietiging of beschadiging. Om deze beleidsdoelstelling te verwezenlijken heeft VZW LANGERHEIDE WZC een veiligheidsbeleid uitgewerkt (supra).

4.8 Verantwoordingsplicht

Onder de Verordening Gegevensbescherming is de plicht ingevoegd voor de verwerkingsverantwoordelijke om te kunnen aantonen ten aanzien van de Gegevensbeschermingsautoriteit dat hij de basisprincipes voor gegevensverwerking en de overige voorwaarden van het regelgevend kader naleeft.

Deze verantwoordingsplicht wordt bewaakt door een intern toezicht en controle door de DPO en is uitvoerbaar volgens de wettelijk geldende principes.

5. Verplichtingen van VZW LANGERHEIDE WZC als verwerkingsverantwoordelijke

Om de beleidsdoelstellingen te bereiken, zijn een aantal taken vastgelegd. Deze vragenlijst is in lijn met alle wettelijke verplichtingen die VZW LANGERHEIDE WZC dient te vervullen (verwerkingsprincipes) en waarvan VZW LANGERHEIDE WZC de naleving moet kunnen aantonen (de verantwoordingsplicht), en is waar nodig aangevuld met beginselen voortvloeiend uit de algemene zorgvuldigheidsnorm (art;1382 BW)

Elke taak zoals hieronder beschreven, wordt ondersteund door een bedrijfsproces. 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 algemene verantwoordelijkheid voor het uitvoeren van de wettelijke verplichtingen als verwerkingsverantwoordelijke ligt bij VZW LANGERHEIDE WZC, vertegenwoordigd door de Raad van Bestuur. De delegatie van de taken en de concrete uitvoering daarvan, worden *infra* uiteengezet door §9.

5.1 Aanstellen van een functionaris voor de gegevensbescherming (DPO)

Iedere verwerkingsverantwoordelijke of verwerker is verplicht om een *Data Protection Officer (DPO)* aan te stellen indien de kerntaak een grootschalige verwerking van de gezondheidsgegevens veronderstelt. VZW LANGERHEIDE WZC is aldus gehouden tot de aanstelling van een DPO.

Deze DPO geeft advies over en houdt toezicht op de verwerkingsprocessen van alle persoonsgegevens. De DPO moet zijn functie onafhankelijk kunnen uitoefenen. Hij mag dus niet gebonden zijn door inhoudelijke instructies van VZW LANGERHEIDE WZC.

VZW LANGERHEIDE WZC moet de DPO vanaf het begin bij alle gelegenheden betrekken die raken aan de bescherming van persoonsgegevens (o.a. tijdig inlichten, uitnodigen op vergaderingen,...). Tevens moet VZW LANGERHEIDE WZC aan de DPO toegang verlenen tot de nodige persoonsgegevens, de verwerkingsactiviteiten en de expertise van de diensten voor zo ver deze relevant is voor de opdracht van de DPO.

5.2 Maatregelen ter beveiliging van de verwerking

Persoonsgegevens mogen slechts verwerkt worden indien er passende technische en organisatorische maatregelen zijn genomen voor het waarborgen van de beschikbaarheid, de integriteit en de vertrouwelijkheid van de verwerkte persoonsgegevens.

VZW LANGERHEIDE WZC voorziet een informatiebeveiligingsbeleid, gebaseerd op de ISO 27001 standaard, waarin de verschillende verantwoordelijkheden en maatregelen (conform ISO 27002 en ISO 27799) worden vastgesteld. Het toezicht op informatieveiligheid en de relatie met gegevensbescherming wordt verder in deze beleidstekst opgenomen (infra).

5.3 Het bijhouden van een register van verwerkingsactiviteiten

VZW LANGERHEIDE WZC beheert een register van alle activiteiten waarbij persoonsgegevens worden verwerkt. Het beheer omvat het opstellen, permanent bijwerken en de controlemaatregelen die hierop van toepassing zijn. Dit register geldt als instrument in het kader van de verantwoordingsplicht ten aanzien van de Gegevensbeschermingsautoriteit, maar is niet bestemd voor de betrokkenen noch voor het publiek. Het register wordt bijgehouden in een elektronische vorm.

Telkens voorafgaand aan het inrichten van een nieuwe of gewijzigde verwerkingsactiviteit wordt het verwerkingsregister bijgewerkt.

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

De volledigheid van het verwerkingsregister moet worden bewaakt.

5.4 Gegevensbeschermingseffectenbeoordeling uitvoeren

Met de inwerktreding van de Verordening Gegevensbescherming dient voor verwerkingen van persoonsgegevens die gelet op de aard, de omvang, de context en de doeleinden daarvan waarschijnlijk een hoog risico inhouden voor de rechten en vrijheden van de betrokkenen een gegevensbescherming-effectenbeoordeling (data protection impact assessment, DPIA) te worden uitgevoerd. De verwerking van patiëntengegevens in een woonzorgcentrum zal in ieder geval steeds een DPIA vereisen.

VZW LANGERHEIDE WZC stelt een lijst op van criteria die kunnen worden gebruikt om te identificeren of een voorgenomen verwerking een “waarschijnlijk hoog risico” inhoudt voor de betrokkene. Wanneer op basis van de criteria blijkt dat de voorgenomen verwerking een hoog risico inhoudt, wordt een gegevensbeschermings- effectenbeoordeling uitgevoerd voorafgaand aan de verwerking. Op basis van de beoordeling worden de nodige maatregelen genomen om het risico op een inbreuk tijdens de verwerking zo veel mogelijk te beperken. Indien de risico’s ondanks maatregelen niet afdoende kunnen worden ingeperkt, moet de verwerkingsverantwoordelijke de Gegevensbeschermingsautoriteit consulteren.

VZW LANGERHEIDE WZC beheert naast de lijst van criteria voor het uitvoeren van de gegevens-beschermingseffectenbeoordeling, ook het bedrijfsproces voor het initiëren, bewaken, bijwerken en uitvoeren ervan.

5.5 Naleving van de rechten van de betrokkene

VZW LANGERHEIDE WZC dient te voorzien in de nodige bedrijfsprocessen die ervoor zorgen dat de betrokkene wordt geïnformeerd over de verwerking. De verstrekte informatie omvat alle wettelijk opgelegde elementen, waaronder volgende (niet-limitatieve) opsomming: de functionaris voor de gegevensverwerking, het verwerkingsdoel en de ontvangers van de gegevens.

Daarnaast moeten de bedrijfsprocessen worden gedocumenteerd die uitvoering geven aan de rechten van de betrokkene (het recht op inzage, afschrift, gegevenswissing, overdraagbaarheid, rectificatie, beperking van de verwerking, kennisgeving, overdraagbaarheid). Deze bedrijfsprocessen houden rekening met wettelijke beperkingen(Wet Patiëntenrechten, de Verordening Gegevensbescherming,...).

5.6 Opzetten van een incidentmeldingssysteem

Uit de Verordening Gegevensbescherming volgt tevens een plicht voor VZW LANGERHEIDE WZC om een incidentmeldingssysteem voor de interne registratie van inbreuken die betrekking hebben op het verwerken van persoonsgegevens. Hierbij streeft het woonzorgcentrum naar een maximale integratie van het meldingssysteem in bestaande meldingssystemen.

VZW LANGERHEIDE WZC dient bijgevolg te zorgen voor maatregelen ter identificatie van inbreuken (preventief), het melden ervan door de personen die deelnemen aan het verwerkingsproces en de afhandeling na de melding.

Onder de maatregelen die te maken hebben met de afhandeling worden begrepen: het melden van het incident, het incidentafhandelingsproces, de interne communicatie over het incident, de registratie van inbreuken in een intern register, de communicatie naar de Gegevensbeschermingsautoriteit en de betrokkene zoals vastgelegd in de Algemene Verordening Gegevensbescherming, inclusief de criteria die bepalen wanneer deze communicatie moet plaatsvinden.

5.7 Werken met verwerkersovereenkomsten

Wanneer een verwerking namens VZW LANGERHEIDE WZC wordt verricht, doet VZW LANGERHEIDE WZC enkel een beroep op verwerkers die afdoende garanties bieden met betrekking tot het toepassen van passende technische en organisatorische maatregelen.

VZW LANGERHEIDE WZC moet voor die verwerking verwerkersovereenkomsten hanteren die voldoen aan de vereisten van de Verordening Gegevensbescherming. VZW LANGERHEIDE WZC voert actief toezicht uit op deze contractuele bepalingen.

Indien 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.

5.8 Toezicht op de uitvoering van taken onder verantwoordelijkheid van VZW LANGERHEIDE WZC

VZW LANGERHEIDE WZC dient tevens te zorgen voor duidelijke instructies en richtlijnen in overeenstemming met de verantwoordelijkheden die medewerkers van VZW LANGERHEIDE WZC in het kader van verwerkingen hebben. Deze instructies worden via procedures, bewustwordingssessies, functiebeschrijvingen en opleidingen gecommuniceerd. De naleving van de verplichtingen wordt afgedwongen aan de hand van het arbeidsreglement (voor werknemers), de algemene regeling (voor artsen), andere documenten (voor andere zelfstandige medewerkers), een privacyreglement,...

Wanneer een verwerking namens VZW LANGERHEIDE WZC wordt verricht door een verwerker, doet VZW LANGERHEIDE WZC enkel beroep op verwerkers die afdoende garanties bieden met betrekking tot het toepassen van passende technische en organisatorische maatregelen.

De gemaakte (schriftelijke) afspraken met een verwerker betreffen onder meer de opsomming van de specifieke taken van de verwerker in het verwerkingsproces, de te nemen veiligheidsmaatregelen en de plicht tot bijstand bij het uitvoeren van de op VZW LANGERHEIDE WZC rustende verplichtingen die in deze beleidstekst zijn opgenomen. VZW LANGERHEIDE WZC voert actief toezicht uit op deze contractuele bepalingen met een verwerker, onder meer door modaliteiten op te nemen in het contract dat de mogelijkheid biedt controle en inspectietaken uit te voeren op informatie en -systemen die persoonsgegevens verwerken waarvoor VZW LANGERHEIDE WZC verantwoordelijk is.

6. Verplichtingen VZW LANGERHEIDE WZC bij gedeelde verantwoordelijkheid voor verwerking

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

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

7. Verplichtingen van VZW LANGERHEIDE WZC als verwerker

In geval van verwerkingen waarbij VZW LANGERHEIDE WZC verwerker is (en geen verwerkingsverantwoordelijke), is het bijstand verlenen aan de verwerkingsverantwoordelijke.

Zo dient de verwerker de verwerkingsverantwoordelijke zonder onredelijke vertraging te informeren zodat hij kennis heeft genomen van een inbreuk in verband met de persoonsgegevens. Tevens dient de verwerker er zich in een verwerkersovereenkomst toe te verbinden om de verwerkingsverantwoordelijke waar nodig bij te staan bij de verdere afhandeling van de meldingsprocedure (door bv. informatie te verstrekken over de feiten omtrent het incident) en moet hij de nodige maatregelen nemen op niveau van gegevensbeveiliging om het incident te verhelpen.

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

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

8. Toepassing van het beleid gegevensbescherming in zorgnetwerken

VZW LANGERHEIDE WZC 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 wordt de impact van de samenwerking en de verantwoordelijkheid over de gegevensverwerking vastgesteld. Hierbij wordt het beslissingscentrum over het verwerken van persoonsgegevens als leidraad gebruikt.

Bij de inrichting van een verticaal zorgnetwerk zal VZW LANGERHEIDE WZC haar Goede Huisvaderprincipes ook toepassen op de leden van het netwerk.

9. Implementatie van de GDPR in de organisatiestructuur van VZW LANGERHEIDE WZC

Bovenstaande vereisten uit de GDPR worden vertaald naar een VZW LANGERHEIDE WZC-beleid Gegevensbescherming en omgezet in de organisatiestructuur van VZW LANGERHEIDE WZC. Hiertoe wordt een matrix opgemaakt waarin de beleidstaken worden uitgezet tegenover de verschillende verantwoordelijkheden. De matrix wordt bijgehouden door de Stuurgroep Gegevensbescherming & Informatieveiligheid.

Hierna worden de belangrijkste taken beschreven:

9.1 Centraal: de verantwoordelijkheid voor de gegevensbescherming

9.1.1 Raad van Bestuur

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

9.1.2 Delegatie aan het directiecomité

De Raad van Bestuur delegeert de uitvoering van de beleidstaken in het kader van gegevensbescherming aan het directiecomité. In de uitvoering van deze taken wordt het directiecomité bijgestaan door de Stuurgroep Gegevensbescherming & Informatieveiligheid (zie *infra)*. Het directiecomité kan tevens beroep doen op de adviezen van de functionaris voor de gegevensbescherming (al dan niet via het Stuurgroep Gegevensbescherming en Informatieveiligheid).

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

De Raad van Bestuur delegeert haar taken als verwerkingsverantwoordelijke aan een Stuurgroep Gegevensbescherming & Informatieveiligheid (hierna afgekort als ‘SGI’). De stuurgroep wordt voorgezeten door de algemeen directeur. De overige leden van de stuurgroep zijn de leden van de directieraad.

De functionaris voor de gegevensbescherming (in aanloop van de inwerkingtreding van de Verordening Gegevensbescherming is dit het DPO-office, zie verder) adviseert de SGI.

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

- Het aanstellen van een functionaris voor de gegevensbecherming
- 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 aan de functionaris
- Het bijsturen van het beleid en de uitvoering ervan op advies van de functionaris
- De beslissingen inzake risicobeheer bij het verwerken van persoonsgegevens. De tijdbesteding van de functionaris is een onderdeel van dit risicobeheer
- De goedkeuring van de classificatieschema’s die bijvoorbeeld bepalen wanneer een gegevens-bescherlingseffectenbeoordeling dient plaats te vinden, evenals de classificatieschema’s voor het melden van inbreuken
- De inrichting en het in stand houden van de bedrijfsprocessen die in deze beleidstekst zijn omschreven
- Het toekennen van de verantwoordelijkheden voor het uitvoeren van de bedrijfsprocessen

- Beslissingen over alle overwegingen uit hoofde van de Verordening Gegevensbescherming, waaronder verwerkingen gebaseerd op gerechtvaardigd belang, zoals deze die betrekking hebben op kinderen, alsook beslissingen inzake de verenigbaarheid van de doelen bij een latere verwerking van persoonsgegevens
- Het aanleggen van de nodige documentatie bij alle voorstellen tot beslissingen
- Het formaliseren van de beslissingen door de Raad van Bestuur
- De maatregelen bij overtredingen op grond van het arbeidsreglement, de algemene regeling dan wel op grond van het contract
- De rapportering van het beleid gegevensbescherming naar onder meer accreditatiecommissies
- Toekijken op de toepassing van het beleid in horizontale en verticale zorgnetwerken

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

Gelet op de veelheid aan persoonsgegevens die worden verwerkt in het woonzorgcentrumcontext, wordt de operationele verantwoordelijkheid om de verplichtingen zoals bepaald in de Verordening Gegevensbescherming na te komen, decentraal georganiseerd en gelegd bij de diensten / organen die daadwerkelijk instaan voor de verwerking van de betreffende gegevens. Tijdens het implementatietraject zal deze takenmatrix worden geherevalueerd.

9.4 Adviserend: de functionaris voor de gegevensbescherming (DPO)

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

In aanloop naar de inwerkingtreding van de Verordening Gegevensbescherming wordt thans een DPO-office geïnstalleerd met volgende leden: Ellen Nestor, Geert Van Rillaer en Julia Uytterhoeven.

Er is een algemeen e-mailadres aangemaakt waarop het DPO-office kan worden bereikt (info@langerheide.be).

De Stuurgroep Gegevensbescherming & Informatieveiligheid houdt de betreffende contactgegevens actueel.

10. De relatie tussen gegevensbescherming en informatieveiligheid

VZW LANGERHEIDE WZC vertrouwt het toezicht op informatieveiligheid toe aan de veiligheidsconsulent. De taken van de veiligheidsconsulent zijn opgenomen in het informatieveiligheidsbeleid, dat onder verantwoordelijkheid van het directiecomité valt.