Huize Ter Walle
vzw C.I.G.B.
Erkenningsnummer **WZC** PE 781 | **CVK** KPE 781 | **CDV** BE 2356

Kortrijkstraat 126
8930 Menen

T. 056 52 17 40
E. info@htw.be

www.htw.be

BELEID: GEGEVENSBESCHERMING EN INFORMATIEVEILIGHEID

VERSIEBEHEER

VERSIE	AUTEUR	DATUM	OMSCHRIJVING
1.0			
2.0	GEERT DE VOOGHT	22/09/2021	ACTUALISATIE TEKST – INVOEGEN STUK ROND INFORMATIEVEILIGHEID
3.0	DEBBIE JANSSENS	24/08/2022	AANPASSING LAY-OUT NAAR NIEUWE HUISSTIJL
4.0	DEBBIE JANSSENS	14/08/2023	UPDATE

Inhoud

1. INLEIDING

Nu meer dan ooit is informatie één van de belangrijkste pijlers van een organisatie. Informatie op zich, het beheer, de opslag en de verwerking ervan zijn echter onderhevig aan veiligheidsrisico's. WZC Huize Ter Walle is zich bewust van deze risico's en neemt de nodige stappen om deze risico's te beheersen. De beheersing van deze risico's begint met het vaststellen van een gegevensbeschermings- en informatieveiligheidsbeleid. Dit document voorziet hierin.
De beleidsregels die in dit document zijn opgenomen moeten vervolgens ook toegepast worden binnen de organisatie. Waar nodig zal dit onder andere leiden tot specifieker beleid rond specifieke thema's.

2. BELANG VAN INFORMATIEVEILIGHEID EN GEGEVENSBESCHERMING

We staan er als woonzorgcentrum voor garant dat het verzamelen en verwerken van de gegevens van onze bewoners, medewerkers en derden gebeurt met de grootst mogelijke zorgvuldigheid, op een professionele manier, en met aandacht voor het beschermen van de persoonlijke levenssfeer van de betrokkenen. We streven continu naar verbetering, met als doel een veilige informatieomgeving te creëren, en alle persoonsgegevens te beschermen conform de Europese Algemene Verordening voor Gegevensbescherming.

In het bijzonder willen we de gegevens beschermen tegen:

- **Verlies:** de gegevens zijn niet meer beschikbaar.
- **Lekken:** gegevens komen in de verkeerde handen terecht.
- **Fouten:** gegevens zijn niet correct (vb. verouderd of onvolledig).
- **Niet toegankelijk:** op het moment van de zorg zijn gegevens niet toegankelijk.
- **Onterecht inkijken:** ingekeken door personen die hiertoe niet gemachtigd zijn.
- **Ontbrekende verantwoording:** Het niet kunnen nagaan wie de gegevens inkeek, wijzigde of verwijderde.
- **Verwerkingen** die niet in lijn liggen met regelgeving, richtlijnen en normen.

De directie wil beroep doen op iedereen die betrokken is bij het verwerken van persoonsgegevens, in het bijzonder het elektronisch bewonersdossier, om samen vanuit een gemeenschappelijke visie én vanuit onze gezamenlijke wil om kwaliteitsvolle zorg aan te bieden de verwerking van de gezondheidsgegevens van onze bewoners correct te laten verlopen.

Dit beleid dient als norm voor het verwerken van persoonsgegevens. Het is een leidraad voor alle verwerkingsprocessen en biedt een referentie voor audit en controle. Het biedt elke bewoner, medewerker en externe een inzage in het veiligheidsbeleid en de manier waarop we omgaan met gevoelige persoonsgegevens. Deze tekst draagt ook bij aan de bewustwording omtrent informatieveiligheid.

Het is opgesteld voor iedereen die een beleidsfunctie heeft binnen WZC Huize Ter Walle en het kan gebruikt worden bij het ontwerpen van procedures en richtlijnen voor medewerkers en externen. De relevante onderdelen worden verwerkt in overeenkomsten met personeel en leveranciers.

3. TOEPASSINGSGEBIED

Het beleid gegevensbescherming en informatieveiligheid is van toepassing op de verwerking van persoonsgegevens waarbij WZC Huize Ter Walle als verwerkingsverantwoordelijke (al dan niet samen met anderen) of verwerker wordt aangeduid.

Het beleid is van toepassing op alle persoonsgegevens die WZC Huize Ter Walle verwerkt. We verstaan hieronder niet alleen de gegevens van onze bewoners, maar ook bijvoorbeeld van medewerkers, bezoekers, … dus elke geïdentificeerde of identificeerbare persoon. Het gegevensbeschermingsbeleid is van toepassing op alle verwerkingsdoelen (zorggerelateerd, administratief, financieel, kwaliteits-en risicocontroles, rapportering, etc..).

Deze beleidstekst is geschreven voor iedereen die in opdracht van WZC Huize Ter Walle persoonsgegevens verwerkt, zoals de directie, het middenkader, de medewerkers, maar ook elke leverancier.
De functionaris voor de gegevensbescherming (DPO) waakt erover dat de principes van dit gegevensbeschermingsbeleid worden toegepast in alle samenwerkingsverbanden die WZC Huize Ter Walle opzet in de zorg.

Het beleid gegevensbescherming en informatieveiligheid is voor WZC Huize Ter Walle het uitgangspunt in haar samenwerking met andere zorginstellingen en -verstrekkers.

4. DE ORGANISATIE VAN GEGEVENSBESCHERMING EN INFORMATIEVEILIGHEID

De stuurgroep gegevensbescherming en informatieveiligheid

De stuurgroep gegevensbescherming en informatieveiligheid fungeert als formeel beslissingsplatform voor informatieveiligheid. Het is bevoegd om beslissingen te nemen die betrekking hebben op volgende aspecten:

- De risicoanalyse en bijhorende methodiek
- De effectieve risicobeoordeling
- Het ontwikkelen van het informatieveiligheidsbeleid en de bijhorende richtlijnen
- De implementatie van beveiligingsmaatregelen (i.e. de inhoud van het veiligheidsplan)
- Het nakomen van alle wettelijke verplichtingen inzake gegevensbescherming

De functionaris voor gegevensbescherming (DPO)

De DPO verleent bijstand, verstrekt informatie over en kijkt toe op de verplichtingen van WZC Huize Ter Walle 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 beleid voor gegevensbescherming
    - De correcte toepassing van alle Europese, Federale en Vlaamse regelgeving over het verwerken van persoonsgegevens
    - Toekijken of iedereen 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 gegevensbeschermingseffectenbeoordelingen (DPIA)
- Contactpunt zijn voor de Gegevensbeschermingsautoriteit en hiermee samen werken
- Coördineren van incidentmeldingen in verband met gegevensbescherming (optioneel)

De medewerker

Iedereen (intern of extern) die persoonsgegevens verwerkt (bijvoorbeeld inkijkt, registreert, wijzigt, …), doet dit volgens de principes uit dit beleid. De medewerker verwerkt gegevens in overeenstemming met de discretieplicht, en conform volgende principes:

- Is verantwoordelijk voor de gegevens van betrokkenen 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
- Respecteert het beroepsgeheim (artikel 458 van het Strafwetboek)

Het diensthoofd

Bijkomend aan de verantwoordelijkheden van de medewerker, ziet het diensthoofd toe op de goede uitvoering van de veiligheidsbepalingen:

- volgt de veiligheidsrichtlijnen op en informeert de medewerkers hierover (bijv. personaliseren van gekregen paswoorden, na gebruik van bewonersdossier afmelden, informatie op papier niet laten liggen,…).
- zorgt voor een veiligheidscultuur en onderhoudt deze, (bijv. door het bespreken van de beleidsrichtlijnen op het teamoverleg).
- ondersteunt controleactiviteiten, (bijv. door het controleren van logging in het elektronisch bewonersdossier.

Coördinerend en raadgevend arts (CRA)

Vanuit de ondersteunende rol voor kwaliteitsbeheer geeft de CRA op vraag of uit eigen beweging adviezen over de beveiligingseisen ten aanzien van medische gegevens. Op vraag van de DPO beslist de CRA over veiligheidsprincipes voor de bescherming van de medische persoonsgegevens van de bewoners. De CRA wordt aangesteld als gezamenlijke verwerkingsverantwoordelijke.

Behandelend arts

Naast het volgen van de veiligheidsprincipes, zoals bepaald voor de medewerkers, is de behandelend arts verantwoordelijk voor het afleveren van een correct medisch dossier. De behandelend arts wordt aangesteld als gezamenlijke verwerkingsverantwoordelijke.

De ICT-medewerker

De ICT-medewerker en de verantwoordelijke voor de gebruikers (key gebruiker) zijn, in toevoeging van de verantwoordelijkheden voor medewerkers, verantwoordelijk voor:

- Implementatie van de technische maatregelen
- Implementatie van de veiligheidsinstellingen in lijn met dit beleid
- Melden van veiligheidsproblemen die ontstaan voor, tijdens of na de implementatie van ICT-middelen aan de DPO
- Fungeren als expert. Vanuit deze rol neemt hij deel aan de identificatie zowel als aan de remediëring van de informatieveiligheidsrisico’s

ICT-leverancier

De ICT-leverancier heeft dezelfde verantwoordelijkheden als deze van een ICT-medewerker.
Bijkomend:

- Wijst op eventuele veiligheidsrisico’s van geleverde toepassingen (ook door derde partijen)
- Wijst op de op te nemen veiligheidstaken

- Streeft een transparant veiligheidsbeleid na door te communiceren over het eigen actuele veiligheidsniveau
- Geeft ondersteuning bij de afhandeling van veiligheidsincidenten

5. BELEIDSDOELSTELLINGEN VOOR GEGEVENSBESCHERMING

Algemene doelstellingen

WZC Huize Ter Walle in haar rol als verwerkingsverantwoordelijke:

1. Is transparant over de persoonsgegevens die het verwerkt en het verwerkingsdoel, zowel naar de betrokkene, de klanten als naar de toezichthouders. De gevoerde communicatie is eerlijk, eenvoudig toegankelijk en begrijpelijk. Het transparantieprincipe is ook van toepassing wanneer 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 WZC Huize Ter Walle. Dit wordt telkens geëvalueerd bij een nieuw verwerkingsdoel, waar nodig aan de hand van een gegevensbeschermingseffectbeoordeling.
3. Verwerkt enkel de persoonsgegevens die strikt noodzakelijk zijn voor de uitvoering van de activiteiten zoals benoemd in de privacyverklaring die overhandigd wordt aan nieuwe bewoners en ook terug te vinden is op de website van de organisatie.
4. Kijkt toe op de integriteit van de persoonsgegevens tijdens de volledige verwerkingscyclus.
5. Bewaart gegevens niet langer dan noodzakelijk. De noodzakelijkheid is afgetoetst tegenover wettelijke verplichtingen en de rechten en vrijheden van de betrokkene.
6. Voorkomt inbreuken die voortvloeien uit het verwerken van persoonsgegevens. Informatieveiligheid, gegevensbescherming door ontwerp en privacy-vriendelijke standaardinstellingen zijn hiervoor hulpmiddelen. Wanneer een inbreuk plaatsvindt, wordt hierover gerapporteerd in lijn met de regelgeving ter zake.
7. Is in staat om alle geldende rechten van een betrokkene, zoals het recht op inzage, afschrift en eventueel ook schrapping, uit te voeren. WZC Huize Ter Walle waakt hierbij over de eventuele beperkingen die op deze rechten van toepassing zijn.
8. Verwerkt gegevens in lijn met de rechten en vrijheden die gelden in de Europese Economische Ruimte en controleert de toepassing hiervan wanneer de gegevens worden uitgewisseld daarbuiten. WZC Huize Ter Walle leeft bijgevolg alle wettelijke en normerende kaders na (i.e. zowel Vlaamse, Federale als Europese regels) bij het verwerken van persoonsgegevens en heeft daartoe haar verantwoordelijkheid over de persoonsgegevens en die van anderen duidelijk in kaart gebracht.
9. Kan aantonen dat het alle beleidsdoelstellingen naleeft, conform de wettelijke bepalingen. Deze verantwoordingsplicht wordt bewaakt door interne toezicht en controle en is uitvoerbaar volgens de wettelijk geldende principes.
10. WZC Huize Ter Walle gaat na of een voorgenomen verwerking een “verhoogd risico” inhoudt voor de betrokkene. Wanneer blijkt dat de voorgenomen verwerking een hoog risico inhoudt, wordt een gegevensbeschermingseffectenbeoordeling (DPIA) uitgevoerd voorafgaand aan de verwerking. Op basis van de beoordeling worden de nodige maatregelen genomen om het risico op een inbreuk zo veel mogelijk te beperken. Indien de risico’s ondanks maatregelen niet voldoende kunnen worden ingeperkt, moet de verwerkingsverantwoordelijke de Gegevensbeschermingsautoriteit om raad vragen.

Verplichtingen van de verwerkingsverantwoordelijke

Los van de algemene verplichtingen zijn er ook een aantal specifieke verplichtingen die de GDPR oplegt:

- Het bijhouden van een register van verwerkingsactiviteiten
  WZC Huize Ter Walle beheert een register van alle activiteiten waarbij persoonsgegevens worden verwerkt.

- 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, integriteit en vertrouwelijkheid van de verwerkte persoonsgegevens.

- Melden van inbreuken in verband met verwerking van persoonsgegevens
  Uit de AVG volgt een plicht voor WZC Huize Ter Walle om een incidentmeldingssysteem voor de interne registratie van inbreuken te hebben die betrekking heeft op het verwerken van persoonsgegevens.

- Het uitvoeren van een gegevensbeschermingseffectenbeoordeling

- Aanstellen van een functionaris voor de gegevensbescherming (DPO)
  Iedere verwerkingsverantwoordelijke is verplicht om een *Data Protection Officer (DPO)* aan te stellen indien de kerntaak een grootschalige verwerking van gezondheidsgegevens is. Wzc Huize Ter Walle is dus verplicht tot de aanstelling van een DPO.

- Naleving van de rechten van de betrokkene
  WZC Huize Ter Walle dient gedocumenteerde bedrijfsprocessen op te stellen die voorzien in het naleven van de rechten van de betrokkene (het recht op inzage, afschrift, gegevenswissing, rectificatie, beperking van de verwerking, kennisgeving, overdraagbaarheid).

Doelstellingen voor informatieveiligheid

Informatieveiligheid is een belangrijk onderdeel binnen gegevensbescherming, beiden zijn echter wel degelijk verschillend.

Gegevensbescherming omvat alle aspecten zoals benoemd in de GDPR/AVG over de wijze waarop persoonsgegevens mogen worden verwerkt. Het betreft in feite de principes zoals deze ook hierboven benoemd werden. Een onderdeel hiervan is de beveiliging van de gegevens.

Informatieveiligheid betreft de beveiliging van alle soorten informatie binnen een organisatie, waaronder persoonsgegevens. Dit is waar informatieveiligheid relevant is voor gegevensbescherming, en waar de twee elkaar ontmoeten: informatieveiligheid omvat het beveiligen, naast alle andere informatie, van persoonsgegevens en gegevensbescherming omvat dan weer alle aspecten rond de omgang met persoonsgegevens, waaronder de beveiliging.

Als onderdeel van dit gegevensbeschermingsbeleid wordt zodoende ook aandacht besteed aan informatieveiligheid, waarbij de belangrijkste beleidsprincipes rond informatieveiligheid in dit hoofdstuk worden benoemd. De structuur is gebaseerd op de internationaal erkende norm met betrekking tot informatieveiligheid, de ISO27000 (specifiek: het controlekader van de ISO27002).

Specifieke voorwaarden waaraan het beleid informatieveiligheid moet voldoen

Voorwaarde	Toelichting	Minimaal na te leven norm
1. Identiteitsbeheer	Stemt de digitale en de burgerlijke identiteit van de medewerker (natuurlijke persoon) van de Dienst overeen (of met andere woorden: is hij/zij de persoon die hij/zij beweert te zijn).	Een procedure voor identiteitsbeheer en de implementatie van de nodige maatregelen om deze af te dwingen, waaronder zowel technische als maatregelen zoals bewustwording bij de gebruikers. De procedure heeft als doel de levensloop van de digitale identiteit te koppelen aan de bewegingen binnen de organisatie (instroom, doorstroom en uitstroom van medewerkers). Deze procedure wordt ondersteund door een risicoanalyse en bevat maatregelen om deze risico's te beperken
2. Toegangsbeheer	Bewaakt dat iedere medewerker de beoogde bewerking met persoonsgegevens mag uitvoeren (consulteren, wijzigen, bijwerken).	Een procedure die het opstellen en onderhouden van een takenmatrix, alsook de naleving hiervan bij het toewijzen van de taken, garandeert. Maatregelen worden genomen om misbruik, gewild of ongewild, te voorkomen, waaronder toezicht.
3. Relatie met de betrokkene	Een aantoonbare 'overeenkomst', zoals een cliëntenrelatie of zorg-/therapeutische relatie, die het verwerken van de gegevens van de betrokkene rechtvaardigt. In deze overeenkomst is het tevens duidelijk op welke manier de betrokkene rechten kan uitoefenen inzake verwerking van persoonsgegevens en de bijhorende procedures.	Een procedure die toelicht welke stappen er nodig zijn om aan de voorwaarden te voldoen van het verkrijgen van een geldige relatie met de betrokkene en garanties biedt dat deze relatie correct wordt opgevolgd (bijvoorbeeld het beëindigen van de relatie moet correct worden opgevolgd). Deze garanties kunnen bestaan uit technische en organisatorische maatregelen, waaronder bewustwording.
4. Logging	Elke handeling van elke medewerker moet kunnen worden opgespoord en verantwoord	Een procedure die instructies geeft over de wijze van logging en de systematische controle van de logging met het oog op kwaliteitsgaranties.

Naast garanties dat maatregelen en procedures zijn geïmplementeerd met betrekking tot identiteits- en toegangsbeheer, onderhoud van de relatie met de betrokkene en logging, zullen ook garanties worden afgedwongen bij iedereen die bij de verwerking betrokken is, waaronder personeelsleden en leveranciers. Voor personeelsleden omvat dit aandacht voor de nodige afspraken en instructies, inclusief sancties bij overtredingen. Gezien de technische implementatie in quasi alle gevallen in handen is van een leverancier van software, dienen deze eveneens garanties te geven die in een contract met de leverancier zijn voorzien.

Voorwaarde	Toelichting	Na te leven norm
5. Omgang met medewerkers en leveranciers	Afdwingen dat personeelsleden en leveranciers de nodige technische en organisatorische maatregelen in acht nemen bij het uitvoeren van verwerkingsactiviteiten.	Voor personeelsleden: bewustwordingssessies en afspraken. Voor leveranciers: een procedure voor het afsluiten en onderhouden van een contract, inclusief een beheer van alle operationele verplichtingen.

Algemene voorwaarden voor informatieveiligheid

Bovenstaande vijf specifieke voorwaarden worden omkaderd met een algemeen beleid informatieveiligheid en een op een risicoanalyse gebaseerd veiligheidsplan. Dit alles onder toezicht van een functionaris voor de gegevensbescherming.

Voorwaarde	Toelichting	Na te leven norm
Algemene voorwaarde: veiligheidsbeleid	Een beleidstekst waarin de uitgangspunten van het veiligheidsbeleid, inclusief de verantwoordelijkheden en taken worden toegelicht.	Een veiligheidsbeleid dat veiligheidsmaatregelen omkadert en verantwoordelijkheden aanduidt
Algemene voorwaarde: veiligheidsplan	Een op een risicoanalyse gebaseerd veiligheidsplan waarin te implementeren maatregelen om de risico's in te perken, in een plan van aanpak worden uitgezet.	Elke organisatie heeft risico's inzake informatieveiligheid in kaart gebracht.
Algemene voorwaarde: toezicht door functionaris voor gegevensbescherming	De functionaris voor de gegevensbescherming bewaakt de toepassing van de onderhavige richtsnoeren.	De verwerkingsactiviteiten staan onder toezicht van de functionaris voor de gegevensbescherming
Algemene voorwaarde: voldoen aan nalevingsvoorwaarden	De organisatie kan zich steeds verantwoorden voor de naleving van de veiligheidsvoorwaarden en neemt maatregelen wanneer er inbreuken of incidenten plaatsvinden	Voorzien in een procedure voor inbreuken bij verwerkingsactiviteiten of in het kader van de naleving van veiligheidsvoorwaarden.

Welke aandachtspunten voor informatieveiligheid zijn er verder?

Onderstaande punten zijn eveneens na te leven, maar dienen niet noodzakelijk worden omkaderd met door de zorgorganisatie uitgewerkte geformaliseerde procedures. De vermelde punten zijn suggesties/mogelijkheden en kunnen aangevuld of geschrapt worden.

Beheer bedrijfsmiddelen

WZC Huize Ter Walle beheert een overzicht van alle in gebruik zijnde bedrijfsmiddelen en wie deze in gebruik heeft. Dit betreft voornamelijk laptops en smartphones.

Cryptografie

WZC Huize Ter Walle heeft haar website beveiligd met een https verbinding, maakt gebruik van een end-to-end encrypted opslag voor alle digitale gegevens, en heeft alle informatieverwerkende systemen (laptops, smartphones) voorzien van full disk encryption.

Fysieke veiligheid & bescherming van de omgeving

- Tijdens de kantooruren is de accommodatie vrij toegankelijk. Buiten de kantooruren is deze enkel toegankelijk mits vooraf registratie van de vingerafdruk.
- Encryptie op harde schijven.
- Medewerkers worden geacht wanneer ze hun toestellen onbeheerd achterlaten hun schermbeveiliging te activeren.
- Medewerkers worden geacht geen onnodige gegevens (op papier dan wel digitaal) op hun werkplek achter te laten.

Operationele veiligheid

- Backups, backupschema
- Logging in applicaties
- Monitoring van servers en apps
- Antivirus, firewall, spamfilter
- Updates & patching

Communicatieveiligheid

Het privaat domein en publiek domein zijn strikt gescheiden. Enkel de directie beschikt over het wachtwoord dat gebruikt wordt binnen het privaat domein.

Ontwikkeling en onderhoud van systemen

Wanneer nodig geacht door de directie en op advies van de ICT-ondersteuning zal WZC Huize Ter Walle voor nieuwe systemen of software testperiode inplannen om vast te stellen of de beoogde software voldoet aan de gestelde eisen.

Beheer van informatieveiligheidsincidenten

WZC Huize Ter Walle beschikt over een procedure voor veiligheidsincidenten.

Naleving

WZC Huize Ter Walle heeft verantwoordelijkheden toebedeeld om er voor te zorgen dat alle wettelijke, contractuele, en regelgevende kaders bekend zijn en dat WZC Huize Ter Walle hieraan voldoet.

WZC Huize Ter Walle draagt er zorg voor dat enkel legale software gebruikt wordt en dat deze enkel wordt aangeschaft bij erkende verkopers. Waar nodig zijn voldoende licenties beschikbaar voor het aantal gebruikers van gegeven software.

6. ANNEX: BEGRIPPENKADER

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

Verordening Gegevensbescherming (GDPR): 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). Recent wordt ook gebruik gemaakt van de term AVG (*Algemene Verordening Gegevensbescherming*).

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. Deze wet is eveneens van toepassing op bewoners in een woonzorgcentrum.

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 een of meer elementen die kenmerkend zijn voor de fysieke, fysiologische, genetische, psychische, economische, culturele of sociale identiteit van die natuurlijke persoon. Ook gepseudonimiseerde gegevens die door het gebruik van aanvullende gegevens aan een natuurlijke persoon kunnen worden gekoppeld, zijn dus persoonsgegevens. Anonieme gegevens, die op geen enkele wijze nog kunnen worden gelinkt aan een persoon, vallen niet onder de Verordening Gegevensbescherming.

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

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

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

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

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

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

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. Onder de term "**beheersmaatregel**" dienen alle maatregelen verstaan te worden met betrekking tot het beleid, procedures, richtlijnen, werkwijzen en organisatiestructuren. Deze maatregelen kunnen zowel administratief, technisch, beheersmatig als juridisch van aard zijn.

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 (DPO)*: een expert die toeziet op de naleving van de Verordening Gegevensbescherming binnen de instelling en die de verwerkingsverantwoordelijke hierin adviseert en bijstaat.

Gegevensbeschermingsautoriteit: De Gegevensbeschermingsautoriteit is verantwoordelijk voor het toezicht op de naleving van de grondbeginselen van de bescherming van de persoonsgegev