# Gegevensbeschermingsbeleid & informatieveiligheid Eigen Woonst vzw

Mei 2018

# 1. Inleiding: Het beleid voor gegevensbescherming

Voor Eigen Woonst is het beschermen van de persoonlijke levenssfeer van de cliënten en de medewerkers een van haar beleidsprioriteiten.

Met deze beleidstekst willen we in de eerste plaats duidelijke doelstellingen formuleren op welke manier we de rechten en vrijheden van de cliënten, 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).

In het bijzonder wilt Eigen Woonst de gegevens van haar bewoners, het eigen personeel en andere betrokkenen beschermen tegen:

- verlies: gegevens zijn niet meer beschikbaar
- lekken: gegevens komen in verkeerde handen terecht
- fouten: gegevens zijn niet correct, bijvoorbeeld 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
- het niet kunnen nagaan wie de gegevens inkeek, wijzigde of verwijderde
- verwerkingen die niet in lijn liggen met regelgeving, richtlijnen en normen

Deze beleidstekst wil in de eerste plaats duidelijke doelstellingen formuleren met betrekking tot het beleid gegevensbescherming in Eigen Woonst 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 voorziening nog verder wordt aangevuld door andere relevante wetgeving, zoals het K.B. van 10 juli 1990, de Wet Patiëntenrechten, de regelgeving m.b.t. camerabewaking, e.d.

Daarnaast heeft deze beleidstekst als doel de actoren, intern of extern aan Eigen Woonst verbonden, te informeren over de wijze waarop de gegevensbescherming in Eigen Woonst wordt georganiseerd. De beleidsorganen en de uitvoeringsmodaliteiten van het Eigen Woonst -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 de voorziening van bewoners, personeelsleden, directie en andere (externe) actoren.

# 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*).

Het **Koninklijk Besluit van 10 juli 1990** houdende vaststelling van de normen voor de erkenning van initiatieven beschut wonen ten behoeve van psychiatrische patiënten

**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 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.

**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 Privacy commissie 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. De organisatie van gegevensbescherming

**Bevoegdheid**

Als verantwoordelijke voor de verwerking, ligt de bevoegdheid van dit beleid bij het Bestuursorgaan, vertegenwoordigd door de Agendacommissie.
Deze is samengesteld uit 3 Leden van het Bestuursorgaan.
De Agendacommissie is verantwoordelijk voor het formuleren en vaststellen van, en het toezien op de naleving van, de beleidsprincipes binnen Eigen Woonst.
Tijdens de agendacommissie wordt beslist in hoeverre bepaalde topics besproken / voorgelegd moet worden aan het Bestuursorgaan.

**Verantwoordelijke uitvoerder**

Het Bestuursorgaan delegeert de uitvoering van de beleidstaken in het kader van gegevensbescherming aan de *coördinator*. In de uitvoering van deze taken dient coördinator verantwoording af te leggen, stand van zaken door te geven, onduidelijkheden bevragen aan de Agendacommissie
De coördinator is bevoegd om beslissingen te nemen die betrekking hebben op o.a. de volgende aspecten:

- De risicoanalyse en bijhorende methodiek;
- Het ontwikkelen van het gegevensbeschermingsbeleid en de bijhorende richtlijnen;
- De implementatie van beveiligingsmaatregelen (i.e. de inhoud van het veiligheidsplan)
- De structurele reactie op gegevensbeschermingsproblemen en –adviezen (binnen de 3 maanden);

**De medewerker**

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

- Is verantwoordelijk voor de gegevens van bewoners en andere 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 en meldt inbreuken
- Leeft artikel 458 van het Strafwetboek na: De gebruiker respecteert het beroepsgeheim

**ICT-leverancier**

Een ICT-leverancier (zoals providers van externe diensten die Eigen Woonst gebruikt) heeft de volgende verantwoordelijkheden:

- De implementatie van de gepaste technische maatregelen
- De veiligheidsinstellingen te implementeren in lijn met dit beleid.
- Inbreuken ten aanzien van persoonsgegevens tijdig te melden bij Eigen Woonst.
- Te fungeren als expert. Vanuit deze rol neemt hij/zij deel aan zowel de identificatie als de remediëring van de gegevensbeschermingsrisico's.

Bijkomstig:

- Wijst hij op veiligheidsrisico's van geleverde toepassingen
- Wijst de leverancier op de op te nemen veiligheidstaken
- Streeft de leverancier een transparant gegevensbeschermingsbeleid na door te communiceren over het eigen actuele veiligheidsniveau en bij de afhandeling van veiligheidsincidenten.

- **De functionaris voor gegevensbescherming** De DPO verleent bijstand, verstrekt informatie over en kijkt toe op de verplichtingen van Eigen Woonst 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. ieder 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 gegevensbeschermings-effectenbeoordelingen (DPIA)
    - Contactpunt zijn voor de GBA en hiermee samen werken
    - Coördineren van incidentmeldingen in verband met gegevensbescherming

# 4. Het toepassingsgebied van het beleid voor gegevensbescherming bij Eigen Woonst vzw

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

Dit beleid is van toepassing voor de gehele levensduur van informatie binnen Eigen Woonst vzw, van het verkrijgen van informatie tot de uiteindelijke verwijdering van informatie binnen de organisatie.

## 4.1 Materieel toepassingsgebied

Het beleid is van toepassing op de verwerking van persoonsgegevens. We verstaan hieronder niet alleen de persoonsgegevens van bewoners, maar ook bijvoorbeeld van medewerkers, al dan niet in dienstverband, familieleden, studenten, leverancier, derden, … .

Het beleid strekt zich uit tot elke (semi-)geautomatiseerde verwerking en tot handmatige verwerkingen indien de persoonsgegevens zijn opgeslagen of bedoeld zijn om te worden opgeslagen in een bestand. Verwerkingen van cliëntgegevens 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 bewoner, rapporteringsdoeleinden, gemachtigde extramurale gegevensstromen, administratie van medewerkers, financiële gegevens, kwaliteitscontroles of risicobeoordelingen, alsook persoonsgegevens die in een gerechtelijke of forensische analyse worden verwerkt, behoren tot de scope van het beleid voor gegevensbescherming.

## 4.2 Personeel toepassingsgebied

Deze beleidstekst is geschreven voor iedereen die in opdracht van Eigen Woonst persoonsgegevens verwerkt, zoals alle personeelsleden, de psychiater, maar ook elke vrijwilliger of leverancier. Deze tekst wordt via verschillende kanalen uitgedragen.

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

# 5. 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 persoonsgegevens wordt overgegaan.

Het voldoen aan de vereisten uit de Verordening Gegevensbescherming, het vastleggen van het noodzakelijke beleid hierrond, en het scheppen van een kader waarbinnen gegevensbescherming binnen Eigen Woonst worden verwerkt vormen meteen ook de doelstellingen van dit gegevensbeschermingsbeleid.

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

## 5.1 Rechtmatig

Voor alle verwerkingen van persoonsgegevens waarvoor Eigen Woonst 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 de beroepsbeoefenaar van Eigen Woonst 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 op over het verwerken van persoonsgegevens. Met betrekking tot gegevens over de cliënt omvat dit onder meer, maar niet limitatief, het K.B. van 10 juli 1990, de regelgeving over patiëntenrechten, de omgang met persoonsgegevens bij de uitwisseling ervan, 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.

Eigen Woonst 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 Eigen Woonst de intentie uitspreekt om zich aan te sluiten bij alle toepasselijke gedragscodes.

## 5.2 Behoorlijk en transparant

We zijn transparant over de persoonsgegevens die verwerkt worden en met welk verwerkingsdoel.

## 5.3 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, en relevant zijn voor het uitvoeren van de taken.

## 5.4 Minimale gegevensverwerking

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

## 5.5 De juistheid

Eigen Woonst streeft daarenboven naar een zorgvuldig bijgehouden bewonersdossier. 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..

## 5.6 De opslagbeperking

Eigen Woonst 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.

## 5.7 De integriteit en vertrouwelijkheid

Eigen Woonst neemt de passende technische en organisatorische maatregelen met het oog op een passende beveiliging van de persoonsgegevens. Op die manier beschermen we de persoonsgegevens onder meer tegen ongeoorloofde of onrechtmatige verwerking en tegen onopzettelijk verlies, vernietiging of beschadiging. Wanneer een inbreuk plaatsvindt, wordt hierover gerapporteerd in de lijn met de regelgeving ter zake.

## 5.8 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.

# 6. Verplichtingen van Eigen Woonst vzw als verwerkingsverantwoordelijke

Om de beleidsdoelstellingen te bereiken zijn een aantal taken vastgelegd. Deze takenlijst is in lijn met alle wettelijke verplichtingen die Eigen Woonst dient te vervullen (verwerkingsprincipes) en waarvan Eigen Woonst de naleving moet kunnen aantonen (de verantwoordingsplicht).

De algemene verantwoordelijkheid voor het uitvoeren van de wettelijke verplichtingen als verwerkingsverantwoordelijke ligt bij Eigen Woonst , vertegenwoordigd door het Bestuursorgaan.

## 6.1 Aanstellen van 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 gezondheidsgegevens veronderstelt. Eigen Woonst is aldus gehouden tot de aanstelling van een DPO.

De 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 Eigen Woonst over de werking van zijn taak als DPO.

Eigen Woonst 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 Eigen Woonst aan de DPO toegang verlenen tot de nodige persoonsgegevens, de verwerkingsactiviteiten en de expertise van de diensten voor zover deze relevant is voor de opdracht van de DPO.

## 6.2 Maatregelen nemen 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.

Eigen Woonst voorziet een informatiebeveiligingsbeleid, waarin de verschillende verantwoordelijkheden en maatregelen worden vastgesteld. Het toezicht op informatieveiligheid en de relatie met gegevensbescherming wordt verder in deze beleidstekst opgenomen.

## 6.3 Het bijhouden van een register van verwerkingsactiviteiten

Eigen Woonst 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 elektronische vorm.

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

De volledigheid van het verwerkingsregister moet worden bewaakt.

## 6.4 Gegevensbeschermingseffectbeoordeling uitvoeren

Met de inwerkingtreding 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 gegevensbeschermingseffectbeoordeling (data protection impact assessment, DPIA) te worden uitgevoerd.

Eigen Woonst 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 een hoog risico inhoudt, wordt een gegevensbeschermingseffectbeoordeling 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.

## 6.5 Naleving van de rechten van de betrokkene

Eigen Woonst 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, …).

## 6.6 Opzetten van een incidentmeldingssysteem

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

Eigen Woonst 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.

## 6.7 Werken met verwerkersovereenkomsten

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

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

## 6.8 Toezicht op de uitvoering van taken onder verantwoordelijkheid van Eigen Woonst vzw.

Eigen Woonst dient tevens te zorgen voor duidelijke instructies en richtlijnen in overeenstemming met de verantwoordelijkheden die medewerkers van Eigen Woonst 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), andere documenten (voor andere zelfstandige medewerkers, vb. psychiater), een privacyreglement, … .

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 Eigen Woonst rustende verplichtingen die in deze beleidstekst zijn opgenomen. Eigen Woonst 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 Eigen Woonst vzw verantwoordelijk is.

# 7. Verplichtingen Eigen Woonst vzw bij gedeelde verantwoordelijkheid voor verwerking

Wanneer er sprake is van een gezamenlijke verantwoordelijkheid, dan zullen de respectievelijke verantwoordelijkheden van Eigen Woonst en eventuele gezamenlijke verwerkingsverantwoordelijken 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 Eigen Woonst 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.

Eigen Woonst zal aan alle verplichtingen voldoen voor de verwerkingsprocessen waarvoor zij in deze situatie de verantwoordelijkheid draagt.

# 8. De relatie tussen gegevensbescherming en informatieveiligheid

## 8.1 Onderscheid gegevensbescherming en 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. Een onderdeel hiervan is de beveiliging van de gegevens, maar gegevensbescherming is dus breder dan enkel het beveiligen van 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.

## 8.2 Doelstellingen informatieveiligheid

### 8.2.1 Beheer bedrijfsmiddelen

Eigen Woonst beheert een overzicht van alle in gebruik zijnde bedrijfsmiddelen en wie deze in gebruik heeft, het betreft voornamelijk laptops en smartphones.

### 8.2.2 Logische toegangscontrole

- Authenticatiegegevens voor informatieverwerkende systemen (b.v. gebruikersnaam en wachtwoord, en dergelijke meer) zijn persoonlijk en dienen niet doorgegeven te worden

- Gebruikers  hebben de verantwoordelijkheid om op een veilige manier om te gaan met authenticatiegegevens  zoals wachtwoorden en zijn hiervan op de hoogte gebracht door Eigen Woonst
- Het toekennen van authenticatiegegevens gebeurt op een veilige manier waarbij, voor systemen die dit ondersteunen, gebruikers zelf hun wachtwoord wijzigen na toekenning

#### 8.2.3 Fysieke veiligheid & bescherming van de omgeving

- Camera bewaking
- 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.

#### 8.2.4 Communicatieveiligheid

Het netwerk wordt afgeschermd. Er is apart wifi netwerk voor bezoekers

#### 8.2.5 Leveranciersrelaties (zelf in te vullen indien van toepassing)

Toegang van leveranciers tot Eigen Woonst informatie of informatieverwerkende systemen zal beperkt zijn tot hetgeen de leverancier nodig heeft voor de invulling van het contract of de gemaakte afspraken. De gemaakte afspraken bevatten gepaste organisatorische en technische maatregelen ter beveiliging.

#### 8.2.6 Compliance

Eigen Woonst heeft verantwoordelijkheden toebedeeld om er voor te zorgen dat alle wettelijke, contractuele, en regelgevende kaders bekend zijn en dat Eigen Woonst hieraan voldoet.

Eigen Woonst 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.

Eigen Woonst beheert een fysieke opslagruimte voor het bewaren van de noodzakelijke registraties, bijvoorbeeld in verband met de boekhouding, contracten of uitzendkrachten.