1. INLEIDING

Zorg-wooncentrum den Bouw hecht veel waarde aan de privacy en veiligheid van haar bewoners en medewerkers. Het is de taak van den Bouw om de (persoons)gegevens van haar bewoners en medewerkers zo goed mogelijk te beschermen. Den Bouw is transparant over de gegevensverwerkingen en is zich bewust van de gevolgen van datalekken.

Dit protocol beschrijft het beleid dat door den Bouw wordt gevoerd in het kader van de Algemene verordening gegevensbescherming (AVG). De verordening regelt de privacy rechten voor burgers en de verantwoordelijkheden van organisaties in het beschermen hiervan. Dit betekent op de eerste plaats bewustwording van betrokkenen over de zorgvuldige wijze waarop met persoonsgegevens wordt omgegaan.

Informatiebeveiliging vormt een belangrijk onderdeel in de AVG, aangezien de consequenties van het onbedoeld uitlekken van privacygevoelige informatie groot kunnen zijn. Daarbij staat dan, behalve uiteraard allereerst de privacy van de bewoners en medewerkers, ook de goede naam, betrouwbaarheid en imago van de zorgorganisatie op het spel.

Naast de AVG is den Bouw vanwege het gebruik van het BSN van betrokkenen ook gehouden aan de NEN7510, een norm voor informatiebeveiliging in de gezondheidszorg. Deze norm schrijft het gebruik van een managementsysteem voor.

Met dit beleid wordt zowel aan de AVG als de NEN7510 invulling gegeven op een wijze die past bij de omvang en beleidsuitgangspunten van den Bouw: adequaat en rationeel. Dit betekent dat telkens wordt gezocht naar een bij de organisatie passende vorm van informatiebeveiliging die hanteerbaar is en ook wordt gebruikt op alle organisatieniveaus waar met persoonsgegevens wordt omgegaan: zowel bestuurlijk, als management als op operationeel niveau.

In paragraaf twee worden de kaders ten behoeve van het gegevensbeschermingsbeleid uiteengezet. Vervolgens worden op basis van deze kaders in paragraaf drie de concrete afspraken geformuleerd over de wijze waarop met gegevensverwerking en gegevensdragers wordt omgegaan. Paragraaf vier gaat tenslotte in op de verplichte registers die moeten worden bijgehouden in het kader van dit protocol.

2. GEGEVENSBESCHERMINGSBELEID

Uitgangspunt van het gegevensbeschermingsbeleid is een algemeen bewustzijn binnen de organisatie van de gegevens die worden verwerkt, wat het doel, de omvang en de context daarvan zijn. Vastleggen moet een doel dienen en er moet bewustzijn bestaan over wat de impact is wanneer gegevens onbedoeld gedeeld worden met niet-belanghebbenden. Dit vraagt om zorgvuldigheid van alle betrokkenen in de organisatie.

In algemene zin vindt verwerking van persoonsgegevens uitsluitend plaats in relatie tot het organisatiedoel van den Bouw, oftewel een adequate zorg- en dienstverlening. Hierbij wordt voldaan aan wettelijke eisen met betrekking tot het vastleggen van gegevens, maar wordt nooit meer gedaan dan wettelijk op dit gebied is voorgeschreven. Teneinde dit te borgen moet, wanneer sprake is van verwerking van persoonsgegevens altijd de wettelijke basis worden beschreven. Wat betreft de verwerking van bewonergegevens is deze onderbouwing beschreven in het beleid gericht op de Administratieve Organisatie en Interne Controle.

2.1 Borgen van rechten van betrokkenen
Betrokkenen hebben het recht op inzage, correctie en dataportabiliteit van persoonsgegevens.

- Recht op inzage in de persoonsgegevens

Indien een betrokkene hierom vraagt, biedt den Bouw inzage in de persoonsgegevens van de betrokkene die zijn vastgelegd.

- Recht op correctie en verwijdering van persoonsgegevens

Een betrokkene kan om correctie of verwijdering van persoonsgegevens vragen als deze feitelijk onjuist zijn, onvolledig zijn of niet ter zake doen voor het doel waarvoor ze zijn verzameld of op een andere manier in strijd met een wet worden gebruikt. Het correctierecht is niet bedoeld voor het corrigeren van professionele indrukken, meningen en conclusies waarmee iemand het niet eens is, voor zover deze ter zake doen

- Recht op dataportabiliteit

De (digitale) persoonsgegevens die den Bouw verwerkt (met toestemming van betrokkene of om overeenkomst met betrokkene uit te voeren), kunnen op diens verzoek verstrekt worden aan een betrokkene. De vorm waarin de organisatie de gegevens verstrekt moet zodanig zijn dat het voor betrokkene gemakkelijk wordt gemaakt om deze gegevens te hergebruiken en door te geven aan een andere organisatie. Den Bouw verstrekt persoonsgegevens van bewoners in een gesloten enveloppe aan de betreffende bewoner zelf.

2.2 Schriftelijke toestemming betrokkenen voor gegevensverwerking
Aan betrokkenen wordt altijd expliciet en schriftelijk toestemming gevraagd voor het verwerken van persoonsgegevens. Het moet daarbij voor betrokkenen net zo eenvoudig zijn om hun toestemming in te trekken als om die te geven.

Als randvoorwaarden voor deze toestemming geldt dat betrokkenen:

- Geïnformeerd zijn waarover hij toestemming geeft en dat aangetoond kan worden op basis van welke informatie toestemming is gegeven.
- Specifiek toestemming hebben gegeven voor de gegevens die worden verwerkt middels het tekenen van een addendum. In dit addendum staat beschreven waarvoor de persoonsgegevens worden gebruikt.

Indien betrokkenen:

- Bewoners zijn, dan is deze toestemming vastgelegd in de zorgovereenkomst.
- Medewerkers zijn, dan is deze toestemming vastgelegd in de arbeidsovereenkomst.
- Overige betrokken, zoals afnemers van een ontspanningsabonnement.

2.3 Bereik gegevensbeschermingsbeleid
In het onderstaande wordt het bereik van het gegevensbeschermingsbeleid nader geconcretiseerd.
Dit protocol heeft tenminste betrekking op de volgende categorieën persoonsgegevens:

- Bewonergegevens (NAW-gegevens, BSN, indicatiebesluit, verzekeringsgegevens)
- Zorgregistratie-gegevens (datum aanvang zorgverlening, appartement, plaats van zorglevering, door bewoner of mantelzorger ondertekend leefplan/ dienstverleningsovereenkomst, omvang en aard geleverde zorgprestaties, mutaties in de zorgverlening)
- Medewerkersgegevens (NAW-gegevens, BSN, arbeidsovereenkomst, dossier, salarisverwerking)

De bovengenoemde gegevens worden uitsluitend in de door den Bouw aangewezen systemen verwerkt. Indien gegevens buiten deze systemen worden vastgelegd, volgt een verwerkersovereenkomst met derden.

Gegevens worden niet langer bewaard dan strikt noodzakelijk. Hiervoor worden de wettelijke bewaartermijn in acht genomen. De persoonsgegevens moeten worden verwijderd uiterlijk vijf jaar nadat de verlening van zorg is geëindigd. Langer bewaren van de gegevens is alleen toegestaan als de persoonsgegevens noodzakelijk zijn ter voldoening aan een wettelijke bewaarplicht.
Den Bouw verstrekt alleen persoonsgegevens:

- aan de client
- aan de eerste contactpersoon van de client/ wettelijke vertegenwoordiger
- aan derden mét schriftelijke toestemming van de client of wettelijke vertegenwoordiger

2.4 Functionaris voor de gegevensverwerking

De functionaris voor de gegevensverwerking (FG) houdt toezicht op de toepassing en naleving van de AVG volgens dit protocol. Dit betekent onder andere het verzamelen van informatie over verwerkingen, analyseren en controleren aan de hand van dit protocol en adviseren aan de Bestuurder.

Bij den Bouw is deze taak belegd bij de kwaliteitsfunctionaris, hetgeen concreet inhoudt:

- Betrokkenheid bij de implementatie en toepassing van dit protocol
- Minimaal jaarlijks een audit van (een of enkele van) de processen om naleving te toetsen
- Gevraagd en ongevraagd adviseren over de toepassing van dit protocol

Naast de FG zijn de leden van het managementteam verantwoordelijk voor het houden van toezicht op de toepassing en naleving van de AVG volgens dit protocol. Dit betekent dat ook zij gevraagd en ongevraagd adviseren over de toepassing hiervan en elkaar en anderen binnen de organisatie actief aanspreken indien buiten de kaders van dit protocol wordt gehandeld.

2.5 Meldplicht datalekken

Er is sprake van een datalek indien als gevolg van een beveiligingsincident persoonsgegevens verloren zijn gegaan of als onrechtmatige verwerking van persoonsgegevens niet uit te sluiten is. Een voorbeeld hiervan is het kwijtraken van een USB-stick of diefstal van een telefoon/laptop.

Den Bouw doet melding van een datalek bij de Autoriteit Persoonsgegevens indien sprake is van de volgende situaties:

- De gelekte persoonsgegevens zijn van gevoelige aard: bijvoorbeeld de gezondheid of financiële situatie van de betrokkene
- Er is een (grote) kans is op ernstige nadelige gevolgen voor de bescherming van de verwerkte persoonsgegevens: bijvoorbeeld identiteitsfraude bij het lekken van een kopie van het identiteitsbewijs
- Er sprake is van een grote hoeveelheid gelekte persoonsgegevens, zowel per persoon of met betrekking tot het aantal betrokkenen

De melding wordt binnen 72 uur na de ontdekking van het datalek door de Functionaris Gegevensbeschermer van den Bouw gedaan via de website van de Autoriteit Persoonsgegevens.

Indien blijkt dat de gelekte gegevens niet (goed) versleuteld waren, of het datalek waarschijnlijk ongunstige gevolgen heeft voor de persoonlijke levenssfeer van de betrokkene, meldt den Bouw het datalek ook aan de betrokkene. Bij ongunstige gevolgen kan gedacht worden aan (identiteits)fraude, discriminatie of aantasting in eer en goede naam. Bij het lekken van persoonsgegevens van gevoelige aard, meldt den Bouw dit altijd aan de betrokkene. De melding stelt de betrokkene in staat om alert te zijn op mogelijke gevolgen van het datalek en daarop te anticiperen.

3. AFSPRAKEN GEGEVENSVERWERKING

De meldplicht voor datalekken, zoals in de voorgaande paragraaf is beschreven, is in beginsel van toepassing op de afspraken voor gegevensverwerking die in deze paragraaf worden benoemd. In onderstaand schema worden de middelen beschreven waarmee gegevensverwerking plaats mag vinden of waarmee gegevens getransporteerd mogen worden. Niet beschreven middelen zijn niet toegestaan te gebruiken. Per middel wordt aangegeven welke minimale eisen aan het gebruik gesteld worden. Voor medewerkers zijn de richtlijnen gebruik internet, e-mail, social media en privé telefoontjes beschreven in het Kwaliteitshandboek.

Middel	Gebruik
ICT-systemen	De toegangsrechten tot de specifieke onderdelen van de systemen die medewerkers voor hun functie nodig hebben zijn vastgelegd in een autorisatiematrix. In het autorisatiebeleid van den Bouw is beschreven hoe de rollen en toegang door middel van functiescheiding en het toepassen van het vier-ogen principe. Toegang tot klantgegevens is uitsluitend mogelijke bij gebruik binnen den Bouw. Softwareleveranciers zijn gecertificeerd volgens de ISO-eisen voor informatie veiligheid.
USB-sticks	Uitsluitend te gebruiken binnen den Bouw. De USB-stick dient met een code beveiligd te zijn en wordt in een afgesloten ruimte bewaard.
Mobiele telefoon	Den Bouw heeft één zakelijke mobiele telefoon waar alleen mee gebeld kan worden.
Tablet/ laptop	Apparatuur dient met een code beveiligd te worden. Apparaten dienen in een afgesloten ruimte bewaard te worden en mogen nooit onbeheerd achtergelaten worden.
PC	Apparatuur dient met een code beveiligd te worden. Bij het verlaten van de werkplek dient uitgelogd te worden en de werkplek afgesloten achtergelaten te worden.
Leefplan (bewoner)	In het digitale leefplan worden persoonlijke gegevens van de bewoner bewaard. De bewoner of mantelzorger is eigenaar van het leefplan en bepaalt welke informatie in het leefplan wordt opgenomen.
Medewerkersdossier (op papier)	Toegang tot deze gegevens is uitsluitend toegestaan aan de Administratie, Bestuurder en Hoofd van Dienst. Betrokkenen kunnen inzage krijgen via de genoemde functionarissen tot hun eigen dossier. Dossiers worden bewaard in een afsluitbare kast die is opgesteld in een afsluitbare ruimte.
Papieren documenten	Alle documenten met persoonsgegevens moeten in een afsluitbare kast/ ruimte bewaard worden. Post voor medewerkers wordt bewaard in de postvakjes in de printerruimte. Post voor bewoners wordt bewaard in een afsluitbare ruimte bij de receptie. Documenten met persoonsgegevens mogen alleen op een persoonlijke printer geprint en gekopieerd worden. De algemene printer mag alleen gebruikt worden voor documenten zonder persoonsgegevens. (Gekopieerde) documenten mogen nooit onbeheerd bij de printer worden achtergelaten Op verzoek van medewerkers worden documenten per post of beveiligde mail verstuurd, zoals een jaaropgave als de betreffende medewerker uit dienst is.

	Alle documenten met persoonsgegevens moeten in de papierversnipperaar vernietigd worden. Deze documenten worden vernietigd via een gecertificeerde afvoerstroom.
Digitale documenten	Verwerking uitsluitend binnen de digitale, beveiligde omgeving. Deze omgeving is alleen toegankelijk voor daartoe geautoriseerde medewerkers of belanghebbenden.
Facturen (indien daarop persoonsgegevens zijn vermeld)	Verwerking bij voorkeur binnen de digitale, beveiligde omgeving. Indien afdrukken op papier noodzakelijk is, dan geldt hetzelfde als voor papierendocumenten geldt.
Uitslagen medische onderzoeken (per post)	Uitslagen van medische onderzoeken vanuit het ziekenhuis worden aan de bewoner/ mantelzorger meegegeven. Deze informatie wordt bewaard van het leefplan van de bewoner. Informatie van huisartsen is vaak mondeling en wordt in het leefplan door de verzorgende opgenomen (zie Leefplan). Indien afdrukken op papier noodzakelijk is, dan geldt hetzelfde als voor papierendocumenten geldt.
Overdrachten	Verwerking uitsluitend binnen de digitale, beveiligde omgeving. Deze omgeving is alleen toegankelijk voor daartoe geautoriseerde medewerkers. Indien afdrukken op papier noodzakelijk is, dan geldt hetzelfde als voor papierendocumenten geldt. Externe overdracht van gegevens van bewoners gebeurt uitsluitend op een overdrachtsformulier. Dit formulier wordt in een gesloten enveloppe overhandigd aan de familie van de bewoner.
Notulen	In de notulen dienen persoonsgegevens anoniem (voornaam en eerste letter achternaam) te worden behandeld en vastgelegd. Er wordt gebruik gemaakt van initialen in plaats van de gehele naam van betrokkene. Notulen worden bewaard in de digitale databank die toegankelijk is voor daartoe geautoriseerde groepen medewerkers of gebruikers. Notulen van werkoverleggen kunnen op papier worden bewaard. In dat geval geldt hetzelfde als voor papierendocumenten geldt.
E-mail	Persoonsgegevens worden alleen met een beveiligde mail (Zorgmail) verstuurd. Indien het ten behoeve van de uitvoering van werkzaamheden noodzakelijk is om wel persoonsgegevens per e-mail te delen, dan vindt dit uitsluitend plaats tussen functionarissen in de organisatie of met functionarissen buiten de organisaties op basis van een verwerkersovereenkomst. Bij het delen van informatie wordt uitgegaan van minimalisatie, bijvoorbeeld indien mogelijk het gebruik van initialen in plaats van de gehele naam van betrokkene. Bij een e-mail aan meerdere partijen worden alle e-mail adressen in de BCC gezet. De organisatie is zich bewust van het risico dat gepaard gaat met het noodzakelijk delen van privacygevoelige informatie, echter dit risico mag er niet toe leiden dat dit de primaire en ondersteunende werkzaamheden onwerkbaar maakt. Dit vereist van alle betrokkenen een

	grote zorgvuldigheid en het zorgdragen voor een voldoende adequaat beveiligde werkomgeving.
WiFi	Het WiFi netwerk is beveiligd met een wachtwoord.

4. REGISTERS

Er worden in het kader van dit protocol twee registers bijgehouden:

1. Een register van verwerkingsactiviteiten en gegevensbeschermingsbeleid;
2. Een register van datalekken die zijn opgetreden.

4.1 Register van verwerkingsactiviteiten

Het register van verwerkingsactiviteiten bevat informatie over de persoonsgegevens die den Bouw verwerkt en wie daarvoor als verwerker verantwoordelijk is. De bestuurder geldt als eindverantwoordelijk vertegenwoordiger van dit register. Het register is in bijlage 1 uitgewerkt.

Met organisaties die in opdracht van den Bouw persoonsgegevens verwerken is een verwerkersovereenkomst gesloten.

4.2 Bijhouden van een register van datalekken die zijn opgetreden

Alle datalekken worden gedocumenteerd in een register dat controleerbaar is door de Autoriteit Persoonsgegevens. De verantwoordelijkheid voor het bijhouden van dit register en het eventueel melden van een datalek bij de Autoriteit Persoonsgegevens, is belegd bij de functionaris voor de gegevensverwerking.

Onder de AVG worden strengere eisen gesteld aan de registratie van datalekken door de organisatie. Dit onderwerp wordt op Europees niveau nog nader uitgewerkt.

BIJLAGE: REGISTER VAN VERWERKINGSACTIVITEITEN

A. Organisaties waarmee de doelen en middelen van de verwerking zijn vastgesteld op basis van een verwerkersovereenkomst

- Hedan – ICT dienstverlening
- Nedap – ECD en zorgadministratie
- Novicare – inhuur SO
- Vitamee – Verzuimvolgsysteem
- SDB – Salarisadministratie en rooster
- Moore MKW Accountants BV - Externe controller
- Exact – Financiële administratie
- Gerrevink – Documenten vernietiging
- Praktijk leren Nederland – subsidies opleiding

B. Categorieën van ontvangers waaraan persoonsgegevens verstrekt kunnen worden

- Opdrachtgevers met wie een contract Zorg in Natura gesloten is:
  - Zorgkantoor
  - Zorgverzekeraar
  - Gemeente
  - Zorgaanbieder waarvoor zorg in onderaanneming wordt verleend
  - Indicatieorgaan
  - UWV
  - Bedrijfsarts
  - CAK
  - Belastingdienst
- Controlerend accountant in verband met controlewerkzaamheden