Notitie

Betreft : Informatieprotocol – privacy & bescherming persoonsgegevens
Datum : 15 december 2017 – bijgestelde versie d.d. 20-3-2018, d.d. 16-4-2018

---

1. Inleiding

Dit protocol beschrijft het beleid dat door ’t Dijkhuis 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 cliënten en medewerkers, ook de goede naam, betrouwbaarheid en imago van de zorgorganisatie op het spel.

Naast de AVG is ’t Dijkhuis 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 protocol wordt zowel aan de AVG als de NEN7510 invulling gegeven op een wijze die past bij de omvang en beleidsuitgangspunten van ’t Dijkhuis: rationeel, adequaat en no-nonsense. 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 't Dijkhuis, 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 cliëntgegevens 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 't Dijkhuis inzage in de persoonsgegevens 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. De afspraken binnen 't Dijkhuis over persoonlijke werkaantekeningen volgen de richtlijn 'Omgaan met medische gegevens'(KNMG).

- Recht op **dataportabiliteit**
  De (digitale) persoonsgegevens die 't Dijkhuis 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.

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 geld 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.

Indien betrokkenen:

- cliënten zijn, dan is deze toestemming vastgelegd in de zorgovereenkomst.
- medewerkers zijn, dan is deze toestemming vastgelegd in de arbeidsovereenkomst

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:

- Cliëntgegevens (NAW-gegevens, bsn, indicatiebesluit, verzekeringsgegevens)
- Zorgregistratie-gegevens (datum aanvang zorgverlening, appartement, plaats van zorglevering, door cliënt of mantelzorger ondertekend zorgplan/ dienstverlengingsovereenkomst, omvang en aard geleverde zorgprestaties, mutaties in de zorgverlening)
- Medewerkersgegevens (NAW-gegevens, bsn, arbeidsovereenkomst, dossier, salarisverwerking)

De bovengenoemde gegevens worden uitsluitend in de door ’t Dijkhuis aangewezen systemen verwerkt. Indien gegevens buiten deze systemen worden vastgelegd, volgt een verwerkersovereenkomst met derden.

Gegevens worden niet langer bewaard dan strikt noodzakelijk. Hierbij vormt de beleidsnotitie ‘Bewaartermijnen Archivering’ het actuele uitgangspunt.

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 verantwoordelijke (de Raad van Bestuur).

In ’t Dijkhuis 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.

’t Dijkhuis 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 ‘t Dijkhuis 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 ’t Dijkhuis 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 ’t Dijkhuis 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 gegevens verwerking 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.

Middel	Gebruik
Nedap (ECD, HRM)	Uitsluitend toegangsrechten tot de specifieke onderdelen van Nedap die medewerkers voor hun functie nodig hebben. Rechten zijn vastgelegd in Nedap overeenkomstig een door het management vastgestelde toewijzing van gebruiksrechten. Cliënten kunnen inzage krijgen tot hun eigen dossier. Aan externe zorgverleners, zoals de specialist ouderengeneeskunde, paramedici en de huisartsen kan gericht door management toestemming verleend worden voor toegang tot Nedap. Deze gebruikers krijgen uitsluitend toegang tot de informatie die zij ten behoeve van een cliëntgebonden werkzaamheden nodig hebben.
USB-sticks	Uitsluitend te gebruiken binnen ’t Dijkhuis. De USB stick dient met een code beveiligd te zijn en wordt in een afgesloten ruimte bewaard.
Mobiele telefoon	Gebruik uitsluitend persoonsgebonden en op basis van een gebruiksovereenkomst. Telefoon dient met een code beveiligd te worden. Beperkt privégebruik is toegestaan.
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 verlaten werkplek dient uitgelogd te worden en de werkplek afgesloten achtergelaten te worden.
Medewerkersdossier (op papier)	Toegang tot deze gegevens is uitsluitend toegestaan aan de P&O adviseur, team coördinatoren en directeur. 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, waar de directeur en P&O adviseur een sleutel van hebben.
Papierendocumenten	Documenten worden bewaard in een afsluitbare kast die is opgesteld in een afsluitbare ruimte. Afdrukken van documenten is uitsluitend toegestaan binnen de beveiligde omgeving van de printapparatuur (‘printen in de box’). Documenten mogen nooit onbeheerd bij de printer worden achtergelaten. Papieren documenten worden nooit per post verstuurd. 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)	Verwerking binnen de digitale, beveiligde omgeving in Nedap. Bij ontvangst op papier worden uitslagen gedigitaliseerd en bewaard in het ECD. Papieren origineel wordt vernietigd via een gecertificeerde afvoerstroom.

	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.
Notulen	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 / WeTransfer	In principe worden geen persoonsgegevens per e-mail verspreid. 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. 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.
Camerabeelden	Real-life camerabeelden zijn zichtbaar op de pc van de receptie. Camerabeelden blijven 24 uur lang bewaard en kunnen door de directeur en Technische Dienst teruggekeken worden als daar aanleiding toe is. Gebruik van camera's wordt toegepast ten behoeve van het vergroten van de veiligheid van cliënten en medewerkers.

4. Registers

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

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

4.1 Register van verwerkingsactiviteiten

Het register van verwerkingsactiviteiten bevat informatie over de persoonsgegevens die ’t Dijkhuis verwerkt en wie daarvoor als verwerker verantwoordelijk is. De Raad van Bestuur geldt als eindverantwoordelijk vertegenwoordiger van dit register.

Met organisaties die in opdracht van ’t Dijkhuis 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 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.