Privacyreglement DZN

Inhoud

Inleiding[1]

Sinds de Algemene Verordening Gegevensbescherming (avg) van kracht is, 25 mei 2018, heeft het onderwerp privacy meer aandacht gekregen. De avg is van toepassing als een organisatie persoonsgegevens gebruikt van natuurlijke personen. Naast de avg kent de gehandicaptenzorg ook haar eigen speciale regels over de bescherming van persoonsgegevens, bijvoorbeeld in de wlz. In dit privacyreglement staat informatie over de regels en hoe die worden gebruikt binnen DZN. Hieronder de verduidelijking van een paar belangrijke begrippen binnen de avg.

Persoonsgegeven	DZN verwerkt persoonsgegevens van medewerkers en cliënten. Een persoonsgegeven is informatie waarmee een persoon identificeerbaar is. Bijvoorbeeld naam, telefoonnummer, adres, e-mailadres, bankrekeningnummer. Indirecte gegevens die in combinatie met andere gegevens iemand kunnen identificeren horen hier ook bij.
Bijzondere persoonsgegeven (cliënten)	Naast de gewone persoonsgegevens[2], zoals naam, adres en geboortedatum, zijn er ook bijzondere persoonsgegevens zoals informatie over de gezondheid. Hiervoor gelden strengere regels dan bij de gewone persoonsgegevens. Deze gegevens zijn nodig [3] voor een goede behandeling, verzorging en ondersteuning. In de gehandicaptenzorg is dat bijvoorbeeld het gespreksverslag van een cliënt met een persoonlijk begeleider, de behandelgegevens van een arts of orthopedagoog en het ondersteuningsplan.
Wat valt niet onder de avg *Geanonimiseerde gegevens[4]*	Anoniem maken is het veranderen van persoonsgegevens zodat ze niet meer terug te brengen zijn tot één persoon.
Verwerkingen	Een verwerking van persoonsgegevens is elke bewerking van persoonsgegevens, zoals het verzamelen, vastleggen, ordenen, structureren, opslaan, bijwerken of wijzigen, opvragen, raadplegen, gebruiken, doorsturen, verspreiden, samenbrengen of combineren, en ook het afschermen, wissen of vernietigen van gegevens.
Verwerkings-verantwoordelijke[5]	De organisatie of persoon die het doel van en de middelen voor de verwerking van persoonsgegevens bepaald.
Verwerker[6]	De organisatie of persoon die in opdracht van de verwerkingsverantwoordelijke persoonsgegevens verwerkt zoals softwareleveranciers, website hosts, clouddiensten, externe salarisadministratie, externe kwaliteitsauditor, leverancier van het elektronisch cliëntdossier.
Subverwerker[7]	Een partij die in naam van de verwerker persoonsgegevens verwerkt voor de verwerkingsverantwoordelijke. Bijvoorbeeld als de softwareleverancier van het elektronisch cliëntdossier een deel van haar werkzaamheden uitbesteedt aan een ander.

[1] De verplichte maatregelen die de avg noemt worden in de onderstaande tekst zoveel mogelijk behandeld op Taalniveau B1.
[2] *N.B. het Burgerservicenummer (BSN) behoort tot de gewone persoonsgegevens.*
[3] *art. 30 lid 3 sub a UAVG*
[4] Let op! Dit is wat anders dan gepseudonimiseerde gegevens.
[5] Artikel 4 sub 7 AVG
[6] Artikel 4 sub 8 AVG
[7] Artikel 28 lid 2 en 4 AVG

Rechten

Alle betrokken waarvan de gegevens worden verwerkt door DZN hebben rechten [8][9] over hun persoonsgegevens. Dat geldt voor cliënten en voor medewerkers. De rechten in het kader van de avg worden hieronder kort uitgelegd.

Recht op transparante informatie over de verwerkingen[10]

De cliënt of medewerker heeft het recht om te weten of en welke persoonsgegevens DZN verwerkt en waarom. Deze informatie probeert DZN via dit document zo duidelijk mogelijk te maken.

Recht op inzage (en afschrift) van de persoonsgegevens[11]

De cliënt of medewerker heeft het recht om de persoonsgegevens, die DZN gebruikt, in te zien. Ook heeft de betrokkene het recht op een kopie van die gegevens. Zowel de cliënten als de medewerkers binnen DZN hebben een persoonlijk portaal waarmee ze te allen tijde hun persoonlijke dossier kunnen zien.

Recht op rectificatie van de gegevens als deze niet kloppen[12]

Een cliënt of medewerker mag onjuiste persoonsgegevens te laten wijzigen of laten aanvullen. DZN is verantwoordelijk voor het juist verwerken en actualiseren van de gegevens.

Recht op vergetelheid[13]

Een cliënt of medewerker mag verzoeken om zijn/haar persoonsgegevens te laten wissen.
Dit recht is vanwege andere wetgevingen niet altijd toepasbaar.
Het mag wel als:

- DZN de gegevens niet meer nodig heeft voor het doel waarvoor het is verzameld;
- de betrokkene zijn/haar eerder gegeven toestemming intrekt;
- de betrokkene bezwaar maakt tegen de verwerking;
- als het gaat om een onrechtmatige verwerking (bijvoorbeeld omdat er geen grondslag is);
- de wettelijk bepaalde bewaartermijnen zijn verstreken.

Recht op overdraagbaarheid van gegevens (dataportabiliteit)[14]

Een cliënt of medewerker heeft het recht op overdraagbaarheid van persoonsgegevens. Dit houdt in dat betrokkenen het recht hebben om de persoonsgegevens die de DZN van hen heeft te ontvangen om door te geven aan een andere organisatie. Dit recht geldt enkel voor persoonsgegevens die door de betrokkene zelf zijn verstrekt. Papierdossiers vallen hier niet onder.

Recht op beperking van de verwerking[15]

De cliënt, medewerker mag de zorgorganisatie vragen tijdelijk zijn persoonsgegevens niet te gebruiken zolang een bepaald probleem of bezwaar dat gaat over de verwerking van deze persoonsgegevens nog niet is opgelost.

Artikel 41 UAVG

In artikel 41 van de Uitvoeringswet AVG staan belangrijke uitzonderingen. Het gaat hierbij om de bescherming van de betrokkene of van de rechten en vrijheden van anderen. Voor deze uitzonderingen kan DZN de AVG-rechten van de bewoners niet altijd accepteren.

---

[8] Artikel 10 Grondwet
[9] Artikel 12-22 AVG
[10] Artikelen 13, 14 AVG
[11] Artikel 15 AVG
[12] Artikel 16 AVG
[13] Artikel 17 AVG
[14] Artikel 20 AVG
[15] Artikel 18 avg

Verzoeken indienen

- *Een verzoek om **inzage** kan per mail worden ingediend bij de contactpersoon (vermeld onder in het beleidsstuk). Verzoeken worden binnen 4 weken behandeld.*
- *Een verzoek om **rectificatie** kan per mail worden ingediend bij de contactpersoon (vermeld onder in het beleidsstuk). Verzoeken worden binnen 4 weken behandeld.*
- *De persoonsgegevens worden wanneer de betrokkene dat verzoekt binnen drie maanden **vernietigd**.*[16]
- *Een verzoek om **overdragen** kan per mail worden ingediend bij de contactpersoon (vermeld onder in het beleidsstuk). Verzoeken worden binnen 4 weken behandeld*[17]*.*

Basisvoorwaarden

Naast de rechten waar DZN aan moet denken zijn er ook regels voor het verwerken van persoonsgegevens[18].

1. Er moet een duidelijk doel[19] zijn waarom de persoonsgegevens worden gebruikt.
2. DZN moet altijd laten weten dat ze gebruik maken van persoonsgegevens en om welke persoonsgegevens het gaat[20].
    a. *Voor een zorgorganisatie is het ook belangrijk om aan de betrokkene te laten weten wanneer de persoonsgegevens niet van de betrokkene zelf zijn gekregen*[21]*.*
3. DZN mag nooit meer gegevens gebruiken dan nodig[22] en moet deze gegevens zo snel mogelijk wissen wanneer ze niet meer nodig zijn.
    a. *Er zijn wetten die DZN verplichten om bepaalde gegevens langer te bewaren*[23]*.*
4. DZN moet altijd proberen om de juiste persoonsgegevens op te slaan. Anders moet de DZN maatregelen nemen[24].
5. DZN mag alleen op een veilige en vertrouwelijke manier persoonsgegevens verwerken[25]. Dus de juiste beveiligingsmaatregelen nemen.

[16] Persoonsgegevens hoeven niet te worden vernietigd wanneer een derde een aanmerkelijk belang heeft bij het bewaren van het dossier of wanneer een wettelijke bepaling zich hiertegen verzet.
[17] Dit geld ook voor het overdragen aan de hoofdaannemer ingeval van een tussentijdsbeëindiging.
[18] Beginselen
[19] Artikel 5 lid 1 sub b AVG
[20] Artikel 13 AVG
[21] Artikel 14 AVG
[22] Artikel 5 lid 1 sub c AVG
[23] Artikel 6 lid 1 sub c AVG
[24] Artikel 5 lid 1 sub d AVG
[25] Artikel 5 lid 1 sub f AVG

Grondslagen

De persoonsgegevens mogen alleen verwerkt worden als daar een goede reden voor is. Bij bijzondere persoonsgegevens (zoals gegevens over de gezondheid) mag het alleen als het echt nodig is voor een goede behandeling van de betrokkene of de betrokkene moet uitdrukkelijke toestemming geven. Hieronder staan de verschillende redenen waar DZN gebruik van kan maken.

Grondslag 1 Toestemming:
Toestemming vragen kan ingezet worden voor het verwerken van persoonsgegevens. De toestemming mag ook weer worden ingetrokken en dat moet net zo gemakkelijk zijn als het geven van de toestemming. Als dat gebeurt is er geen grondslag meer en mogen de persoonsgegevens ook niet meer worden verwerkt.

Gewone persoonsgegevens
Toestemming moet worden gegeven door een duidelijke actieve handeling. Bijvoorbeeld via een schriftelijke verklaring, met elektronische middelen (zoals het online plaatsen van vinkje in een vakje) of een mondelinge verklaring.

Gezondheidsgegevens[26]
Als er toestemming gevraagd wordt voor het verwerken van bijzondere persoonsgegevens, dan moet de toestemming uitdrukkelijk worden gegeven. Een schriftelijke verklaring mag, maar dat hoeft niet.

Grondslag 2 Overeenkomst[27]
Als je een overeenkomst sluit met DZN kan het zijn dat de overeenkomst niet uitgevoerd kan worden zonder die persoonsgegevens. Hierbij kunnen ook bijzondere persoonsgegevens verwerkt worden. Voor de zorg- en dienstverleningsovereenkomst van DZN zal gegevensuitwisseling plaatsvinden die daarvoor noodzakelijk is voor het bieden van goede zorg. Denk aan het delen van informatie uit het ondersteuningsplan tussen collega's in de zorgorganisatie. Gegevensuitwisseling zal voor dat het er een overeenkomst is kan ook nodig zijn. Bijvoorbeeld om te bepalen of DZN kan voldoen aan de zorgvraag van de toekomstige cliënt. Ook in deze situatie is de grondslag van toepassing.

Grondslag 3 Wettelijke verplichting[28]
Soms moet DZN volgens de wet persoonsgegevens gebruiken. Hierbij moet je denken aan de plicht om een cliëntdossier bij te houden. De gegevens die nodig zijn voor de uitvoering van de zorg- en/of dienstverlening zijn zonder toestemming beschikbaar voor de zorgverleners die rechtstreeks bij de uitvoering van de zorg zijn betrokken. Dit geldt ook voor andere collega's die door hun werk met cliëntgegevens in aanraking. Denk in de gehandicaptensector aan behandelgegevens/rapportages van onder andere paramedici, psychologen, orthopedagogen en persoonlijk begeleiders die nodig zijn voor goede zorg en ondersteuning.

Grondslag 6 Gerechtvaardigd belang
De verwerking is nodig voor DZN. Het mag alleen niet als de waarden van de cliënt belangrijker zijn. Er zijn drie criteria waar DZN aan moet voldoen:

1. *Het moet duidelijk zijn waarom DZN de gegevens verwerkt.*
2. *Het moet duidelijk zijn het doel belangrijker is dan de waarden van de cliënt op dat punt.*
3. *Er moet kritisch gekeken worden of het doelmatig is en of er geen alternatieve oplossing is.*

[26] Artikel 9 AVG en artikel 22 UAVG
[27] Artikel 6 lid 1 sub b AVG
[28] Artikel 6 lid 1 sub c AVG

Gegevensverwerkingen

Tussen het doel en de grondslag moet een goede relatie zijn om gegevens te mogen verwerken. De vragen die hierbij worden gesteld zijn:

- Wordt met de gegevens het juiste doel bereikt?
- Moet er voor dit doel noodzakelijk persoonsgegevens worden verwerkt?
- Kan het doel ook op een andere manier worden bereikt die minder/geen inbreuk maakt op de privacy?
- Hoe lang mogen/moeten de gegevens bewaard worden?

Algemeen

Grondslagen

Naast de verschillende specifieke verwerkingsdoelen gericht op cliënten en medewerkers wordt er ook gebruik gemaakt van camera's op de locatie. De grondslagen "overeenkomst en gerechtvaardigd belang" zijn hierop van toepassing.

Hoofdverwerkingsdoelen

Het doel van deze camera's om te zorgen voor een veilige woonomgeving. De inzet van stelselmatig cameratoezicht moet helpen tegen ongewenste bezoekers (denk aan drugsdealers, loverboys, etc.), ongewenst gedrag (bijvoorbeeld agressie of vandalisme) en ongewenste situaties (Inbraak, diefstal, heling, etc..). Als het om een strafbaar feit gaat doet DZN een beroep op Artikel 41 van de Uitvoeringswet AVG. Voor deze uitzonderingen kan DZN de AVG-rechten van de bewoners niet altijd accepteren. Zie het onderstaande kader voor meer toelichting.

> *"De* ***bescherming van de betrokkene*** *of van de rechten en vrijheden van anderen"* en *"de* ***voorkoming****, het onderzoek, de opsporing en de vervolging* ***van strafbare feiten*** *of de tenuitvoerlegging van straffen, met inbegrip van de bescherming tegen en de voorkoming van gevaren voor de openbare veiligheid."*

Bewaartermijn

De gehanteerde bewaartermijn zal maximaal 4 weken weken zijn voor de opgeslagen data.

Medewerker specifiek

Grondslagen

Persoonsgegevens van de **medewerkers** wordt verwerkt op basis van overeenkomst en daar waar nodig wettelijke verplichting.

Hoofdverwerkingsdoelen

De doelen zijn: werving van personeel, identificatie en het bijhouden van de personeelsadministratie. Alleen de noodzakelijke informatie wordt hiervoor opgeslagen. Voor deze doelen worden geen bijzondere persoonsgegevens verwerkt.

Bewaartermijn

De bewaartermijnen die hiervoor worden gehanteerd zijn in lijn met de richtlijnen van de belastingdienst.

Voor de medewerkers die werkzaam zijn binnen DZN is het van belang om te weten dat er gebruik wordt gemaakt van stelselmatig cameratoezicht op de gangen van de verschillende locaties. Zie het hoofdstuk "Camera's" voor een gedetailleerd overzicht van alle informatie met betrekking tot de verwerking van persoonsgegevens.

Cliënt specifiek

Grondslagen

De persoonsgegevens van **cliënten** wordt verwerkt op basis van overeenkomst en wettelijke verplichting. Als het nodig is zal er om toestemming worden gevraagd voor het delen van informatie.

Hoofdverwerkingsdoelen

Het doel is de zorg te kunnen afstemmen op de behoefte en wensen van de cliënt. Hiervoor worden ook bijzondere persoonsgegevens gebruikt.

Bewaartermijn

Als het specifiek over de zorg gaat dan zijn er meer wetten van invloed zijn op het privacy beleid van DZN. Die wetten hebben voorrang op de avg.

Uitzonderingen

Hieronder volgt een overzicht van uitzonderingen die specifiek gelden voor persoonsgegevens van cliënten.

Cliëntdossier

DZN is verplicht om een apart dossier voor elke cliënt bij te houden. Een dossier is het geheel aan gegevens dat een hulpverlener over een cliënt bijhoudt. In het dossier moeten in ieder geval opgenomen worden (niet uitputtend en voor zover van toepassing op de zorgorganisatie):
NAW-gegevens, BSN, levenshistorie, zorg- en dienstverleningsovereenkomst, ondersteuningsplan[29], diagnostische informatie, testscores, medische informatie, perspectief/beleving van cliënt of (wettelijke) vertegenwoordiger, financiële gegevens, methodische vragenlijsten, verklaring wilsbekwaamheid, behandeladviezen, de ondersteuning, de begeleiding, risico-inventarisaties, informatieverstrekkingen en toestemmingsverklaringen[30].

Geheimhoudings-plicht[31]

De wgbo regelt de relatie tussen de zorgprofessional en cliënt en kent verschillende privacyregels waaronder de geheimhoudingsplicht. Deze geheimhouding geldt voor zorgprofessionals en hun waarnemers. De zorgprofessional (zorgorganisatie) draagt er zorg voor: dat zonder toestemming van de cliënt geen inlichtingen over de cliënt, inzage in of afschrift van de bescheiden van de cliënt aan anderen worden verstrekt tenzij er sprake is van overmacht of van vereisten uit andere wet- en regelgeving. Er zijn uitzonderingen op de geheimhoudingsplicht te weten:

1. De rechtstreeks bij de zorgverlening van de cliënt betrokken zorgprofessionals en hun vervangers[32].
2. De (wettelijk) vertegenwoordiger(s) van de cliënt[33].

Het medisch beroepsgeheim is niet van toepassing als:

- De cliënt of (wettelijk) vertegenwoordiger uitdrukkelijke toestemming heeft gegeven voor het verstrekken van de gegevens;
- een wettelijke bepaling welke met zich mee brengt dat de zorgprofessional cliëntinformatie moet verstrekken;

[29] Artikel 8.1.3 wgbo
[30] Persoonlijke werkaantekeningen van de hulpverlener horen niet in het medisch dossier. Persoonlijke werkaantekeningen zijn indrukken, vermoedens en vragen. Ze dienen als geheugensteun voor de gedachtevorming van de hulpverlener en zijn niet bedoeld voor collegiaal gebruik. Klachtafhandeling en aansprakelijkheidstelling blijven ook buiten het dossier. Hiervoor worden aparte dossiers aangelegd door een onafhankelijke klachtencommissie en de directie.
[31] Artikel 7:457 lid 1 BW (Wgbo).
[32] artikel 7:457 lid 2 Wgbo
[33] artikel 7:457 lid 3 Wgbo

- verschillende verplichtingen met elkaar in strijd zijn.

Het delen van gegevens met zorgprofessionals

DZN mag niet zomaar persoonsgegevens delen met een huisarts, ziekenhuis of psycholoog van een cliënt. Hiervoor is de toestemming van de cliënt of zijn (wettelijk) vertegenwoordiger nodig.

Onderaannemers

Aan een onderaannemer mogen cliëntgegevens worden verstrekt, mits de cliënt en/of (wettelijk) vertegenwoordiger daarvoor uitdrukkelijke toestemming heeft gegeven. Behalve als er op basis van de grondslag[34] de gegevens noodzakelijk zijn voor de uitvoering van een overeenkomst.

Veronderstelde toestemming

Soms mogen gegevens zonder toestemming gedeeld worden, dat heet veronderstelde toestemming. Dat doet zich voor bij:

- Een doorverwijzing naar een andere zorgorganisatie (zoals een doorverwijzing van een arts naar een medisch specialist);
- ketenzorg waar de zorg- en of dienstverlening is gekoppeld aan een bepaalde aandoening en het tot op bepaalde hoogte te voorzien is welke hulpverleners daarbij betrokken zullen zijn.

Het is van belang om betrokkene tijdig in duidelijke en heldere bewoordingen te informeren over deze (en ook andere) gegevensuitwisselingen. Dit vloeit voort uit de informatieplicht van de zorgorganisatie[35]. Dit biedt de cliënt de mogelijkheid zijn (veronderstelde) toestemming in te trekken[36].

Verwerkers

Een verwerker is een organisatie of persoon die in opdracht van DZN persoonsgegevens verwerkt zoals: softwareleveranciers, website hosts, clouddiensten, externe salarisadministratie, externe kwaliteitsauditor, leverancier van het elektronisch cliëntdossier. Met alle verwerkers hebben wij een verwerkersovereenkomst gesloten. Binnen DZN worden verschillende systemen ingezet ter ondersteuning van de dienstverlening. In dit hoofdstuk worden kort de belangrijkste systemen beschreven. Ook wordt kort en bondig het doel, de noodzakelijkheid en de veiligheidsmaatregelen beschreven. In het geval van de camera's wordt ook aanvullen informatie gegeven in navolging op de aanbevelingen vanuit de opgestelde DPIA.

Mextra

DZN werkt met een digitaal cliëntdossier. Hierin wordt alle informatie opgeslagen die belangrijk is voor de zorg. Zoals het zorgplan, evaluaties en de voortgang. Het dossier wordt daarnaast gebruikt voor rapportages. Tijdens een bezoek van een begeleider wordt er samen met de cliënt een verslag gemaakt van de bevindingen en worden er afspraken gemaakt. Dit wordt gerapporteerd in het cliëntdossier. Gegevens die in MEXTRA worden bewaard zijn vaak privacy gevoelig. Mextra voldoet aan de eisen die hieraan gesteld zijn volgens de wet. Ze voldoen daarnaast aan de NEN7510 & ISO27002 eisen. De bewoners van DZN hebben zelf ook toegang tot hun eigen dossier. Zo kunnen ze altijd terug lezen wat er is gerapporteerd en waar ze op dit moment aan werken.

Siilo

Siilo is een systeem dat wordt gebruik voor een veilige manier van app-contact tussen begeleiders en bewoners. De App is in veel gevallen een makkelijke mogelijkheid voor een bewoner om snel contact te leggen met de begeleiding. Het geeft veel mogelijkheden voor bijvoorbeeld het maken van afspraken.

[34] artikel 6 lid 1 sub b AVG
[35] artikel 13 AVG
[36] artikel 7 lid 3 AVG

De app voldoet aan de eisen van AVG, E-Privacy, NHS information governance, NEN, DCB 0129, ICO en ISO-27001. Alleen jij en de persoon met wie je chat kunnen de berichten lezen. Geen enkele derde partij heeft toegang tot de inhoud van je gesprek. Na 30 dagen worden berichten automatisch verwijderd. Bij diefstal of verlies van een telefoon kan dankzij de verwijder-op-afstand-functie van Siilo alle gegevens op de app wissen.

SDB

SDB wordt ingezet voor het beheren van het personeelsdossier, het berekenen van de salarissen en het opstellen van het rooster. SDB is gecertificeerd voor de ISO 27001. Deze is aangevuld met de NEN7510. De cloud beveiliging is conform de ISAE 3402 assurance standaard.

Camera's

Om de veiligheid te borgen kiest DZN voor stelselmatig cameratoezicht binnen de gemeenschappelijke ruimtes van de portiekflats. De camera's worden alléén in het trappenhuis geplaatst. Dit wordt ook duidelijk gemaakt bij de ingang van ieder pand. De camera's worden ingezet voor de algemene veiligheid en bescherming van iedereen die bij DZN op bezoek komt, woont of werkt. Hierbij kan gedacht worden aan cliënten, familieleden, bezoekers, zorgprofessionals en andere (zorg)medewerkers. Het gebruiken van camera's valt onder het verwerken van persoonsgegevens[37]. De beelden zullen alleen beschikbaar zijn voor de teamleider en de begeleiders op de locatie tenzij er sprake is van een strafbaar feit. De beelden worden niet langer dan vier weken bewaard[38]. Daarna worden ze gewist uit onze systemen.

Naast de systemen die hier boven staan maken we ook gebruik van: Nomadesk, Microsoft, Reiswolf, Arboned, Vodaphone, PFZW en De witjes. Met alle partijen zijn verwerkingsovereenkomsten opgesteld. Ook voldoen alle partijen aan de gestelde eisen die nodig zijn in het kader van de AVG.

Gegevensbescherming

Privacy by design[39] staat voor gegevensbescherming door ontwerp. Naast de verplichting tot beveiliging van persoonsgegevens[40] is DZN ook verplichting bij de ontwikkeling van nieuw beleid of nieuwe systemen rekening te houden met privacy. Het doel is de beveiliging van persoonsgegevens zo goed mogelijk te maken. Dat begint bij het nadenken over welke gegevens zijn echt nodig en welke niet?

Besluitvorming

Bij nieuwe beleidstukken of systemen binnen DZN wordt rekening gehouden met het onderwerp privacy. Om dit zo goed mogelijk te doen wordt er zoveel mogelijk volgens een vast proces gewerkt.

Complementaire functies zijn het uitgangspunt voor de besluitvormingsstructuur binnen de organisatie. Het principe is erop gericht dat iedere functionaris noodzakelijk is om elkaar aangaande zaken af te stemmen. Vanuit dat idee bestaat er dus geen hiërarchische manier van samenwerken, maar is elk van de functionarissen autonoom binnen zijn of haar functie-gebied. In onderling overleg worden de functie-gebieden afgebakend en worden de grenzen afgesproken en bijgesteld.

Als er mogelijk hoge risico's zijn gebonden aan het nieuwe systeem zal er een en *Data Protection Impact Assessment* [41] (hierna: DPIA) worden uitgevoerd. Een DPIA is een instrument om bij (voorgenomen) verwerkingen van persoonsgegevens, de effecten voor betrokkenen op een gestructureerde en gestandaardiseerde wijze in kaart te brengen en te beoordelen.

[37] AVG artikel 4 onderdeel 2
[38] Als er een incident is vastgelegd mogen de desbetreffende beelden worden bewaard tot het incident is afgehandeld.
[39] artikel 25 AVG
[40] artikel 24 AVG
[41] artikel 35 AVG

Bewaren

DZN mag de gegevens niet langer bewaren dan nodig is voor het doel. Is de bewaartermijn van persoonsgegevens voorbij of zijn de gegevens niet meer nodig? Dan moeten de gegevens vernietigd worden. Voor sommige gegevens geldt door andere wetten dan de avg een langere bewaarplicht. Eén keer per jaar worden alle dossiers gecontroleerd. De gegevens waarbij de bewaartermijn voorbij is worden uit het dossier verwijderd. De algemene bewaartermijn van een dossier is 15 jaar[42]. Na afloop van de bewaartermijn wordt het dossier vernietigt. Uitzonderingen op deze bewaartermijn kunnen zijn:

- Als het nodig is voor de continuïteit van zorg.
- Wettelijke verplichtingen.
- Verzoek vanuit de cliënt.

Door cliënt zelf verstrekte financiële informatie zoals uitkering of salaris, bankafschriften worden bewaard zolang als nodig is om de zorg te leveren.

Gegevens van cliënten op verpakkingen, zoals naam, adres of geboortedatum, zijn persoonsgegevens. Bij verpakkingen kan bijvoorbeeld gedacht worden etiketten op medicijndoosjes of -flesjes, Baxterverpakkingen of verpakkingen van incontinentiemateriaal. Deze persoonsgegevens moeten vernietigd worden als ze niet meer nodig zijn. Dit betekent dat verpakkingen met persoonsgegevens niet in de 'gewone' prullenmand mogen worden gedeponeerd.

Verwerkingsregister

De avg legt de verantwoordelijkheid bij DZN om te laten zien dat ze aan de privacyregels voldoet. Zo moet DZN verantwoording[43] af kunnen leggen over alle gegevensverwerkingen. Daarvoor moet iedere stap waarbij persoonsgegevens worden verwerkt vermeld worden in het verwerkingsregister. De volgende punten komen terug in het verwerkingsregister:

- Wie kan de gegevens zien;
- met wie de gegevens worden gedeeld;
- een omschrijving van de categorieën persoonsgegevens die worden verwerkt;
- een beschrijving van de doeleinden waarvoor de persoonsgegevens worden verwerkt;
- welke organisatorische en technische maatregelen er zijn genomen om de persoonsgegevens te beveiligen;
- in welk systeem / hoe persoonsgegevens worden verwerkt;
- hoe lang de persoonsgegevens worden bewaard.

Risico's en maatregelen

De grootste risico's kunnen worden ingedeeld in de volgende hoofdcategorieën:

1. Onrechtmatige (verdere) verwerking
2. Verlies van vertrouwelijkheid
3. Verlies van controle op het gebruik van de gegevens
4. Heridentificatie van gepseudonimiseerde gegevens
5. Onmogelijkheid voor betrokkenen om hun rechten uit te oefenen

Deze risico's moeten worden afgewogen tegen de mate van waarschijnlijkheid waarin ze kunnen voorkomen en tegen de ernst van de impact. In de onderstaande tabel staan technische en organisatorische maatregelen die DZN heeft genomen om de grootste risico's te verlagen.

[42] Artikel 454 WGBO
[43] accountability-principe

Risico's	Maatregelen
Onrechtmatige (verdere) verwerking	• Cliëntgegevens worden alleen in Mextra bewaard. • Personeelsgegevens worden alleen in SDB bewaard. • DZN maakt géén kopieën van paspoort, rijbewijs of identiteitskaart van cliënten, wel kan gevraagd worden om deze te tonen. • Met nieuwe Leveranciers zal voorafgaand aan het delen van informatie een verwerkersovereenkomst worden overlegd. • Bewustwordingsproces verloopt via de interne overlegstructuur waarbij het beleid inhoudelijk besproken wordt, daarnaast wordt het privacy beleid behandeld bij de inwerkprocedure. • Middels de interne audit wordt er getoetst in hoeverre de medewerkers op de hoogte zijn van de verschillende privacy maatregelen (borging bewustwordingsproces).
Verlies van vertrouwelijkheid	• Toegang om gegevens in te zien is verdeeld op basis van bevoegdheden. • De gemeenschappelijke toegangscodes worden periodiek (1x per 90 dagen) aangepast door de teamleider en als teamleden weggaan. • Alle digitale systemen zijn beveiligd met unieke wachtwoorden *(N.B. de wachtwoorden mogen onder geen enkele omstandigheid automatisch worden opgeslagen).* • Het is verplichting om na gebruik van je account direct uit te loggen en/of bij het verlaten van de laptop of PC. • De in- en uitdiensttredingsprocedures waarborgen de continuïteit en veiligheid.
Verlies van controle op het gebruik van de gegevens	• Alle computers binnen DZN worden beveiligd door Norton Security. • Er wordt geen gebruik gemaakt van USB-sticks of externe harde schijven om persoonsgegevens op te slaan of te delen. • Het is niet toegestaan om thuis data van DZN te verwerken. • Mobiele telefoons worden in geen enkele hoedanigheid gebruikt om persoonsgegevens te versturen of op te slaan. • DZN zal nooit om bijzondere persoonsgegevens vragen via haar eigen website. • Voor het versturen van persoonsgegevens wordt er gebruik gemaakt van een beveiligde filetransfer volgens het mailprotocol. Hierbij verlaat de data nooit het beveiligde domein en wordt toegang alleen en specifieke andere verleent via een wachtwoord dat afzonderlijk wordt gecommuniceerd. • De mailserver wordt beheerd door Microsoft online services. • Interne ICT wordt georganiseerd en getoetst door een extern gespecialiseerd bedrijf.
Heridentificatie van gepseudonimiseerde gegevens	• Cliëntgegevens worden gepseudonimiseerd. • DZN hanteert de bewaartermijnen zoals aangegeven in het verwerkingsregister en schoont jaarlijks de dossiers op. • Papieren datadragers worden vernietigd door Reiswolf datavernietiging volgens beschermingsgraad 2 en vernietigingsklasse P3. • Dataminimalisatie door zo min mogelijk persoonsgegevens te verwerken. Alleen de gegevens die noodzakelijk zijn voor het doel door te werken met vooraf opgestelde vragenlijsten.
Onmogelijkheid voor betrokkenen om hun rechten uit te oefenen	• Zowel cliënten als medewerkers kunnen via een eigen login hun eigen dossiers inzien. • Er zijn onafhankelijke vertrouwenspersonen en klachten functionarissen beschikbaar voor zowel cliënten, als medewerkers. • Inzage, rectificatie, vernietiging of overdragen van data is mogelijk via de contactpersoon binnen de privacy commissie.

Meldplicht datalekken

Er is sprake van een datalek als er een inbreuk is op de beveiliging van persoonsgegevens[44]. Bij een datalek zijn de persoonsgegevens kwetsbaar voor verlies of onrechtmatig gebruik. Onder een datalek valt dus niet alleen het vrijkomen (lekken) van gegevens, maar ook onrechtmatig gebruik van gegevens.

Voorbeelden van datalekken zijn: een kwijtgeraakte USB-stick met persoonsgegevens, een gestolen laptop of een inbraak in een databestand door een hacker.

Alle datalekken moeten worden gedocumenteerd in het datalekregister. Met deze documentatie moet de autoriteit persoonsgegevens (AP) kunnen controleren of de organisatie aan de meldplicht heeft voldaan. Daarnaast is het doel van het registreren is dat ervan kan worden geleerd, om datalekken in de toekomst zo veel mogelijk te voorkomen.

Een datalek moet bij de Autoriteit Persoonsgegevens gemeld worden als dit leidt tot ernstige nadelige gevolgen voor de bescherming van persoonsgegevens. Of als een grote kans bestaat dat dit gebeurt. De beleidsregels meldplicht datalekken van de Autoriteit Persoonsgegevens kunnen helpen om te bepalen of sprake is van ernstige nadelige gevolgen[45]. Soms moet de datalek ook gemeld worden aan de betrokkenen (de mensen van wie de persoonsgegevens zijn gelekt).

Als er sprake is van een lek of een potentieel lek dan moet het datalekprotocol gevolgd worden.

Privacy commissie

De privacy commissie komt twee keer per jaar samen in de vorm van het managementteam waarbij er inhoudelijk wordt gekeken naar de bevindingen uit de interne audit ten aanzien van het privacy beleid.

Contactinformatie

Naam	DZN B.V.
Adres	Kerkenbos 1001 6546 BB Nijmegen
Website	http://www.dzn-nijmegen.nl
KVK-nummer	71660690
Contactpersoon[46]	Said Echargui
E-mail	Said@dzn-nijmegen.nl
Telefoon	0643819785
Klachtenfunctionaris	klachten indienen DZN info@klachtenportaalzorg.nl

Voor het indienen van een verzoek of het intrekken van een toestemmingsverklaring kan je contact opnemen met de aangewezen contactpersoon. Voor klachten verwijzen we graag naar de klachtenfunctionaris en de klachtenprocedure.

[44] Zoals bedoeld in artikel 13 van de Wet bescherming persoonsgegevens.
[45] Is de meldplicht datalekken ingegaan en meldt u een datalek ten onrechte niet bij de Autoriteit Persoonsgegevens? Dan kan de Autoriteit Persoonsgegevens u een boete geven.
[46] DZN is een kleine zorginstelling waarvan de kernactiviteit niet het volgen van individuen is, of op grote schaal bijzondere persoonsgegevens verwerken. Klein refereert naar de vergelijking met een gemiddelde huisartsenpraktijk van 2095 patiënten gemiddeld (NZA, 2018). Om die redenen is er geen specifieke FG aangesteld.