Privacyreglement DZN

Inhoud

AVG[1]

Vanaf 25 mei 2018 is de Algemene verordening gegevensbescherming (AVG) van toepassing. De AVG verbetert de positie van de mensen van wie gegevens worden opgeslagen en verwerkt (cliënten en personeel). Veranderingen in de wet zorgen er onder andere voor dat:

- Actieve toestemming van de betrokkenen verplicht is;
- de betrokkenen het recht heeft op het wissen van gegevens op verzoek;
- de betrokkenen het recht heeft om geregistreerde gegevens te ontvangen;
- de betrokkenen het recht heeft om bezwaar te maken tegen verwerkingen;
- daarnaast heeft de organisatie de plicht om te kunnen aantonen dat ze aan alle regels voldoet.

Doeleinde en grondslagen

DZN bewaard persoonlijke gegevens van zowel cliënten als personeel. De cliëntinformatie wordt verzameld in een dossier, met als doel de zorg te kunnen afstemmen op de behoefte en wensen van de cliënt. Bij het opvragen van de informatie proberen wij altijd uit te leggen waarom de informatie nodig is. De bijzondere persoonsgegevens worden alleen met toestemming van de cliënt bewaard, tenzij dit bij wet[2] anders is geregeld.

De personeelsinformatie wordt opgeslagen op basis van overeenkomst. Alleen de noodzakelijke informatie wordt hiervoor opgeslagen.

1. ***Toestemming:*** *Toestemming vragen kan ingezet worden voor het verwerken van gewone persoonsgegevens. De manier waarop we toestemming vragen moet voldoen aan een aantal specifieke eisen (zie toestemmingsverklaring).*
    - *Volgens de Algemene verordening gegevensbescherming (AVG) behoort het Burgerservicenummer (BSN) tot de gewone persoonsgegevens.*
2. ***Overeenkomst****: Hierop mag een organisatie zich baseren als het een overeenkomst heeft met iemand en hiervoor het verwerken van persoonsgegevens noodzakelijk is. De overeenkomst zelf mag niet gericht zijn op het verwerken van persoonsgegevens, maar moet een ander doel hebben. Hierbij kunnen bijzondere persoonsgegevens verwerkt worden.*

Persoonsgegevens

DZN verwerkt privacygevoelige gegevens van personeelsleden en van cliënten. Alle gegevens worden zoveel mogelijk gedigitaliseerd. De documenten waar op getekend is worden naast de digitale versie ook bewaard in een afgesloten kast.

Personeel persoonsgegevens

De grondslag voor het verwerken van de personeel persoonsgegevens is een overeenkomst tussen de medewerker en de organisatie. De gegevens die hiervoor verwerkt worden zijn niet bijzondere persoonsgegevens. Ook zal er niet meer informatie worden opgeslagen nodig om de overeenkomst te honoreren. De persoonsgegevens worden verwerkt via SDB Ayton. Daarnaast wordt informatie in geval van een ziekmelding gedeeld met “de Goudse verzekeringen” de tussenpersoon voor ArboNed.

Cliënt persoonsgegevens

De cliënt heeft een overeenkomst met DZN en Pluryn. In deze overeenkomst staan verschillende afspraken over het zorgarrangement en ook persoonsgegevens. Naast de overeenkomst stelt DZN ook samen met de cliënt een zorgplan op. Hierin worden bijzondere persoonsgegevens verwerkt vanuit

[1] De verplichte maatregelen die de AVG noemt worden in de onderstaande tekst zoveel mogelijk behandeld op Taalniveau B1.

[2] Wet op de geneeskundige behandelingsovereenkomst.

het cliëntendossier van voorgaande zorginstellingen. Daarnaast worden nieuwe bijzondere persoonsgegevens toegevoegd om de zorg zo goed mogelijk te laten aansluiten. DZN maakt gebruik van Mextra om de zorgplannen te beheren[3].

Privacy cliënten

Volgens de wet[4] moet DZN de privacy van cliënten beschermen en bewaren. Alles moet zo vertrouwelijk mogelijk worden behandeld. Het dossier mag alleen gezien worden door de begeleiders en degenen die betrokken zijn bij de behandeling. DZN mag geen enkele informatie aan andere geven, tenzij de cliënt daar toestemming voor geeft of dit noodzakelijkerwijs nodig is voor het verlenen van zorg aan de cliënt, of als dat volgens de wet moet.

DZN is ook 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 de basisgegevens opgenomen worden. Dit zijn onder meer de bevindingen bij lichamelijk en psychiatrisch onderzoek, de diagnose, de ingestelde behandeling, de voortgang van de behandeling, verwijs- en ontslagbrieven, aantekeningen van gesprekken en bevindingen van vroegere hulpverleners of geraadpleegde deskundigen. Ook de informatieverstrekking en toestemmingsverklaringen moeten in het dossier worden opgenomen[5].

Bewaartermijnen

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 een langere bewaarplicht. Bijvoorbeeld loonbelastingverklaring en identiteitsbewijs van medewerkers.

Eén keer per jaar worden alle dossiers gecontroleerd (voor 31 januari). De gegevens waarbij de bewaartermijn voorbij is worden uit het dossier verwijderd[6]. Er kan bij uitzondering van deze regel afgeweken worden als het langer bewaren van gegevens voortvloeit uit de hulpverlening. De algemene bewaartermijn van een dossier is 15 jaar[7]. Na afloop van de bewaartermijn wordt het dossier vernietigt. Uitzonderingen op 15 jaar bewaartermijn zijn:

- Goed hulpverlenerschap.
- Uw medische gegevens kunnen langer bewaard worden indien dit redelijkerwijs voortvloeit uit de zorg van een goed hulpverlener of in het kader van continuïteit van zorg.
- Wettelijke plicht.
- Verzoek van de cliënt.
- Als de hulpverlener de gegevens anonimiseert, kunnen ze langer dan 15 jaar worden bewaard.

Vernietiging

Het vernietigen van data papieren datadragers in het bijzonder worden vernietigd in samenwerking met Reisswolf secret service. Reisswolf hanteert hiervoor beschermingsgraad 2 en vernietigingsklasse P3.

[3]Deze gegevens zullen nooit buiten Nederland gebruikt worden of ingezet worden voor geautomatiseerde besluitvorming.

[4] Wet op geneeskundige behandelingsovereenkomst (WGBO)

[5] 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.

[6] De verschillende gehanteerde bewaartermijnen zijn vermeld in bijlage 2 het verwerkingsregister.

[7] Artikel 454 WGBO

Verwerkingsregister

De AVG legt meer verantwoordelijkheid bij DZN om te laten zien dat ze aan de privacy regels voldoet. Zo moet DZN verantwoording af kunnen leggen over alle gegevensverwerkingen. Daarvoor moet iedere stap waarbij persoonsgegevens[8] 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 bewaart.

Het register wordt net als de gegevensstromen en procedures bijgehouden door de kwaliteitsmedewerker. Het register en de hierboven benoemde informatie is terug te vinden in Bijlage 2: Verwerkingsregister

Privacy rechten

Zowel de cliënten als de medewerkers hebben rechten ten aanzien van hun persoonsgegevens, te weten:

- Recht op inzage;
- recht op rectificatie en aanvulling;
- recht op vergetelheid;
- recht op dataportabiliteit;
- recht op informatie.

Recht op inzage

Een betrokkene (cliënt of medewerker) mag **een verzoek om inzage doen.** Hiermee kan de betrokkene zien welke informatie over hem/haar wordt gebruikt. Wanneer DZN dit verzoek binnen krijgt verstrekken we kopieën van de persoonsgegevens die worden gebruikt. Daarbij geven we ook aan wat we met de gegevens doen en met wie ze worden gedeeld. Daarnaast kunnen we laten zien hoe we aan de gegevens zijn gekomen en hoe lang deze worden bewaard. Ook hebben zowel de cliënten als de medewerkers binnen DZN een persoonlijk portaal waarmee ze te allen tijde hun persoonlijke dossier kunnen zien. **Een verzoek om inzage kan per mail worden ingediend bij het contactpersoon (vermeld onder in het beleidsstuk). Verzoeken worden binnen 4 weken behandeld.**

Recht op rectificatie en aanvulling

Een betrokkene (cliënt of medewerker) mag onjuiste persoonsgegevens te laten wijzigen of laten aanvullen. DZN is verantwoordelijk voor het juist verwerken en actualiseren van de gegevens. **Een verzoek om rectificatie kan per mail worden ingediend bij het contactpersoon (vermeld onder in het beleidsstuk). Verzoeken worden binnen 4 weken behandeld.**

Recht op vergetelheid

Een betrokkene (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 de doeleinden waarvoor het is verzameld.

[8] Waarvan de verwerking niet incidenteel is, die een hoog risico inhouden voor de rechten en vrijheden van de personen van wie u persoonsgegevens verwerkt en/of; die vallen onder de categorie bijzondere persoonsgegevens.

- De betrokkene zijn/haar eerder gegeven toestemming intrekt.
- De betrokkene bezwaar maakt tegen de verwerking.
- Er sprake is van een onrechtmatige verwerking (bijvoorbeeld omdat er geen wettelijke grondslag is).
- De wettelijk bepaalde bewaartermijnen zijn verstreken.

De persoonsgegevens moeten wanneer de betrokkene dat verzoekt binnen drie maanden worden vernietigd.[9]

Recht op dataportabiliteit

Een betrokkene (cliënt, medewerker) heeft het recht op overdraagbaarheid van persoonsgegevens. Dit houdt in dat betrokkenen het recht hebben om de persoonsgegevens die de organisatie van hen heeft te ontvangen. Zo kunnen gegevens makkelijk worden doorgeven aan een andere zorgaanbieder. Papierdossiers vallen hier niet onder. **Een verzoek om overdragen kan per mail worden ingediend bij het contactpersoon (vermeld onder in het beleidsstuk). Verzoeken worden binnen 4 weken behandeld**[10]**.**

Recht op informatie

Onder de nieuwe privacywetgeving heeft de organisatie een informatieplicht. Dat betekent dat DZN verplicht is om nieuwe en bestaande betrokkene duidelijk te informeren over wat we met hun persoonsgegevens doen. Zie het stuk over *"persoonsgegevens bewaren"* om te zien welke informatie DZN gebruikt.

WLZ en WMO

Voor zover in de Wlz/WMO wordt afgeweken van de AVG, geldt dat de bepalingen uit die wetgevingen voor gaan.

- Zorgaanbieders mogen persoonsgegevens, waaronder gegevens betreffende de gezondheid delen (via afschrift of inzage) met Wlz-uitvoerders, het CAK en het Centraal Indicatieorgaan Zorg (CIZ) voor zover dit noodzakelijk is voor onder meer de zorgverlening, het nemen van een indicatiebesluit en het onderzoek daarvoor door het CIZ, het sluiten van overeenkomsten met Wlz-uitvoerders, het bijhouden van wachtlijsten, het declareren van de zorg, controles door Wlz-uitvoerders en de vaststelling en inning van eigen bijdragen door het CAK.
- Alleen met uitdrukkelijke toestemming van de cliënt mag u persoonsgegevens van cliënten, waaronder gezondheidsgegevens, delen met het CIZ.[11]
- De Wlz biedt een grondslag voor het verwerken van het BSN van cliënten. Zorgaanbieders moeten op grond van de Wet aanvullende bepalingen verwerking persoonsgegevens de identiteit en het BSN van cliënten vaststellen.[12]
- Wanneer op grond van de Wlz een zorgplan wordt opgesteld, moet dit worden toegevoegd aan het zorgdossier.
- De Wmo 2015 biedt een grondslag voor het verwerken (en verstrekken) van het BSN door een zorgaanbieder en andere instellingen zoals het CAK, de SVB, de toezichthoudende ambtenaren, het AMHK en de zorgverzekeraar. U moet als zorgaanbieder de identiteit van uw cliënt controleren en het BSN in uw administratie opnemen.[13]

[9] 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.
[10] Dit geld ook voor het overdragen aan de hoofdaannemer ingeval van een tussentijdsbeëindiging.
[11] Art. 9.1.3 lid 1 Wlz. Art. 9.1.3 lid 2 Wlz.
[12] Art. 9.1.1 Wlz
[13] Art. 5.2.9 Wmo 2015.

Privacy by design

Met privacy by design streeft DZN na om maatregelen te nemen om de persoonsgegevens maximaal te beschermen. Hierbij kan een verschil gemaakt worden tussen verwerkingsverantwoordelijke en een verwerker.

1. De **verwerkingsverantwoordelijke** is DZN. DZN heeft formeel-juridisch zeggenschap over de verwerking en heeft het doel en de middelen voor de verwerking vast gestelt.
2. De **verwerkers** van DZN zijn Mextra en SDB Ayton. Zij verwerken persoonsgegevens in opdracht van DZN. Deze bedrijven mogen de persoonsgegevens niet voor eigen doeleinden gebruiken.

Hieronder een overzicht van de getroffen maatregelen.

- 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.
- Toegang om gegevens in te zien is verdeeld op basis van bevoegdheden.
- 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 gemeenschappelijke toegangscodes worden periodiek (1x per 90 dagen) aangepast door de teamleider en als teamleden weggaan.
- Zowel cliënten als medewerkers kunnen via een eigen login hun eigen dossiers inzien.
- DZN vraagt voor iedere verwerking expliciet om toestemming zie bijlage 3 toestemmingsverklaring.
- DZN zal nooit om persoonsinformatie vragen via haar eigen website.
- Dataminimalisatie door zo min mogelijk persoonsgegevens te verwerken. Alleen de gegevens die noodzakelijk zijn voor het doel door te werken met vooraf opgestelde vragenlijsten.
- DZN hanteert de bewaartermijnen zoals aangegeven in het verwerkingsregister en schoont jaarlijks de dossiers op.
- Oude documenten worden vernietigd door Reiswolf datavernietiging volgens beschermingsgraad 2 en vernietigingsklasse P3.
- Persoonsgegevens versturen we volgens het mailprotocol waarbij de data wordt versleuteld en de wachtwoorden afzonderlijk gecommuniceerd.
- Cliëntgegevens worden alleen in Mextra bewaard.
- Personeelsgegevens worden alleen in SDB bewaard.
- Mextra beschikt over de NEN 7510 & ISO 270001 in controle statement.
- SDB beschikt over de NEN 7510 & ISO 270001 in controle statement.
- DZN maakt géén kopieën van paspoort, rijbewijs of identiteitskaart van cliënten, wel kan gevraagd worden om deze te tonen.
- De mailserver wordt beheerd door Microsoft online services (Bijlage 7)
- De in- en uitdiensttredingsprocedures waarborgen de continuïteit van veilig.
- Interne ICT wordt georganiseerd en getoetst door een extern gespecialiseerd bedrijf, *de Witjes* (algemene voorwaarden en privacybeleid).
- 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 (format interne audit) (borging bewustwordingsproces).

Meldplicht datalekken

Er is sprake van een datalek als er een inbreuk is op de beveiliging van persoonsgegevens[14]. 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[15]. 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 bestuur waarbij er inhoudelijk wordt gekeken naar de bevindingen uit de interne audit ten aanzien van het privacy beleid.

Contactinformatie

Naam	DZN B.V.
Adres	Fenikshof 194 6541 RW Nijmegen
Website	http://www.dzn-nijmegen.nl
KVK nummer	67275974
Contact persoon[16]	Said Echargui
E-mail	Said@dzn-nijmegen.nl
Telefoon	0643819785
Klachtenfunctionaris	Klachten@pluryn.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.

[14] Zoals bedoeld in artikel 13 van de Wet bescherming persoonsgegevens.
[15] 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.
[16] Organisaties kunnen verplicht zijn een functionaris voor de gegevensbescherming (FG) aan te stellen op grond van artikel 37 van de AVG. 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.