Privacyreglement DZN

Inhoud

Inleiding[1]

Sinds de Algemene Verordening Gegevensbescherming (avg) van kracht is, 25 mei 2018, heeft dit onderwerp nog 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.

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.

Verwerkingsverantwoordelijke[4]

De organisatie of persoon die het doel van en de middelen voor de verwerking van persoonsgegevens bepaald.

Verwerker[5]

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[6]

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] Artikel 4 sub 7 AVG

[5] Artikel 4 sub 8 AVG

[6] Artikel 28 lid 2 en 4 AVG

Basisvoorwaarden

Er zijn een aantal basisvoorwaarden[7] waar alle organisaties die met persoonsgegevens werken aan moeten voldoen.

- Zo moet er een duidelijk doel[8] zijn waarom een organisatie persoonsgegevens gebruikt. Dit doel moet worden uitgelegd in het privacyreglement en moet passen bij de gegevens die worden verzameld.
- Een organisatie moet ook altijd laten weten dat ze gebruik maken van persoonsgegevens en om welke persoonsgegevens het gaat[9]. De betrokkene moet altijd weten waarom zijn/haar persoonsgegevens worden gebruikt. Voor een zorgorganisatie is het dan ook belangrijk om aan de betrokkene te laten weten wanneer de persoonsgegevens niet van de betrokkene zelf zijn gekregen[10].
- Daarnaast moet er altijd 'netjes' worden omgegaan met de persoonsgegevens. Een organisatie mag nooit meer gegevens gebruiken dan nodig[11] en moet deze gegevens zo snel mogelijk wissen wanneer ze niet meer nodig zijn. Daar staat tegenover dat er verschillende wetten zijn die een organisatie verplichten om bepaalde gegevens te bewaren gedurende een bepaalde tijd[12].
- Een organisatie moet altijd proberen om de juiste persoonsgegevens op te slaan. Als het er toch iets niet klopt, dan moet de organisatie maatregelen nemen[13]. De organisatie is verplicht hier een actieve houding in te nemen.
- Organisaties mogen alleen met persoonsgegevens werken als ze dat op een veilige en vertrouwelijke manier doen[14] met daarbij passende beveiliging.

Doeleinde en grondslagen

De persoonsgegevens mogen alleen verwerkt worden als er 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 maakt.

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[15]

[7] Beginselen
[8] Artikel 5 lid 1 sub b AVG
[9] Artikel 13 AVG
[10] Artikel 14 AVG
[11] Artikel 5 lid 1 sub c AVG
[12] Artikel 6 lid 1 sub c AVG
[13] Artikel 5 lid 1 sub d AVG
[14] Artikel 5 lid 1 sub f AVG
[15] Artikel 9 AVG en artikel 22 UAVG

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[16]
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[17]
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.

Tussen het doel en de grondslag moet een goede relatie zijn. 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?

DZN gebruikt persoonlijke gegevens van cliënten en medewerkers.
- 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. Het doel is de zorg te kunnen afstemmen op de behoefte en wensen van de cliënt. Hiervoor worden ook bijzondere persoonsgegevens gebruikt.

- Persoonsgegevens van de **medewerkers** wordt verwerkt op basis van overeenkomst en daar waar nodig wettelijke verplichting. Het doel kan zijn identificatie, werving van personeel of personeelsadministratie. Alleen de noodzakelijke informatie wordt hiervoor opgeslagen. Hiervoor worden geen bijzondere persoonsgegevens gebruikt.

[16] Artikel 6 lid 1 sub b AVG
[17] Artikel 6 lid 1 sub c AVG

Privacy rechten

Zowel de cliënten als de medewerkers hebben rechten[18][19] ten aanzien van hun persoonsgegevens. De rechten in het kader van de avg worden hieronder getoond.

Recht op transparante informatie over de verwerkingen[20]

De betrokkene (cliënt of medewerker) heeft het recht om te weten of, en zo ja welke persoonsgegevens de zorgorganisatie verwerkt en waarom zij dat doen.

Recht op inzage (en afschrift) van de persoonsgegevens[21]

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

N.B. Een verzoek om inzage kan per mail worden ingediend bij de contactpersoon (vermeld onder in het beleidsstuk). Verzoeken worden binnen 4 weken behandeld.

Recht op rectificatie van de gegevens als deze niet kloppen[22]

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.

N.B. Een verzoek om rectificatie kan per mail worden ingediend bij de contactpersoon (vermeld onder in het beleidsstuk). Verzoeken worden binnen 4 weken behandeld.

Recht op vergetelheid[23]

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;
- 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.

N.B. De persoonsgegevens moeten wanneer de betrokkene dat verzoekt binnen drie maanden worden vernietigd.[24]

Recht op overdraagbaarheid van gegevens (dataportabiliteit)[25]

Een betrokkene (cliënt, 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 zorgaanbieder. Dit recht geldt enkel voor persoonsgegevens die door de betrokkene zelf zijn verstrekt. Papierdossiers vallen hier niet onder.

---

[18] Artikel 10 Grondwet
[19] Artikel 12-22 AVG
[20] Artikelen 13, 14 AVG
[21] Artikel 15 AVG
[22] Artikel 16 AVG
[23] Artikel 17 AVG
[24] 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.
[25] Artikel 20 AVG

N.B. Een verzoek om overdragen kan per mail worden ingediend bij de contactpersoon (vermeld onder in het beleidsstuk). Verzoeken worden binnen 4 weken behandeld[26].

Recht op beperking van de verwerking[27]

De betrokkene (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.

Cliënt specifiek

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. 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[28], 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[29].

Geheimhoudingsplicht[30]

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[31].
2. De (wettelijk) vertegenwoordiger(s) van de cliënt[32].

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;
- verschillende verplichtingen met elkaar in strijd zijn.

---

[26] Dit geld ook voor het overdragen aan de hoofdaannemer ingeval van een tussentijdsbeëindiging.
[27] Artikel 18 avg
[28] Artikel 8.1.3 wgbo
[29] 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.
[30] Artikel 7:457 lid 1 BW (Wgbo).
[31] artikel 7:457 lid 2 Wgbo
[32] artikel 7:457 lid 3 Wgbo

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.

Onderaannemer

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[33] de gegevens noodzakelijk zijn voor de uitvoering van een overeenkomst.

Financiën

De verwerking van financieel-administratieve persoonsgegevens is noodzakelijk voor de uitvoering van de zorg- en/of dienstverlening[34].

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].

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

Privacy by design

Privacy by design[37] staat voor gegevensbescherming door ontwerp. Naast de verplichting tot beveiliging van persoonsgegevens[38] 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 te zo goed mogelijk te maken. Dat kan al door na te denken over de noodzakelijkheid van het opslaan, welke gegevens zijn echt nodig en welke niet?

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[39]. 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[40] 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.

Maatregelen

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.

[37] artikel 25 AVG
[38] artikel 24 AVG
[39] Artikel 454 WGBO
[40] accountability-principe

- 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.
- Cliëntgegevens worden gepseudonimiseerd.
- 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 bijzondere persoonsgegevens 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.
- Papieren datadragers worden vernietigd door Reiswolf datavernietiging volgens beschermingsgraad 2 en vernietigingsklasse P3.
- 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.
- Cliëntgegevens worden alleen in Mextra bewaard.
- Personeelsgegevens worden alleen in SDB bewaard.
- Mextra beschikt over de NEN 7510, 7512, 7513 & ISO 270001 in controle statement.
- SDB beschikt over de NEN 7510, 7512, 7513 & 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 privacy beleid).
- 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[41]. 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[42]. 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 1051 6546 BB Nijmegen
Website	http://www.dzn-nijmegen.nl
KVK-nummer	71660690
Contactpersoon[43]	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.

[41] Zoals bedoeld in artikel 13 van de Wet bescherming persoonsgegevens.

[42] 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.

[43] 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.