

Inleiding

Per 25 mei 2018 geldt de Algemene verordening gegevensbescherming (AVG). Dit is een nieuwe Europese privacywet. Daardoor is de privacy in alle landen van de EU gelijk. Nu hebben de lidstaten nog hun eigen nationale wetten. De Algemene verordening gegevensbescherming (AVG) komt dus in plaats van de oude Wet bescherming persoonsgegevens (Wbp). In de AVG staan een aantal verplichte maatregelen genoemd waaraan je, als vaktherapeut, moet voldoen omdat u gegevens vastlegt in cliëntendossiers.

Verplichte maatregelen

De verplichte maatregelen die de AVG concreet noemt zijn:

- het bijhouden van een register van verwerkingsactiviteiten;
- het (laten) uitvoeren van een veiligheidscontrole van het digitale cliëntendossier.

Dit kun je o.a. doen door de leverancier te laten verklaren van het digitale cliëntendossier voldoet aan de NEN 7510. Dit is de standaard beveiligingseis die gesteld wordt aan software die in de zorg gebruikt wordt om persoonsgegevens te verwerken.

- het bijhouden van een register van datalekken die zijn opgetreden;
- het aantonen dat een patiënt, of cliënt daadwerkelijk toestemming heeft gegeven voor het vastleggen van gegevens in het cliëntendossier.

Het register van verwerkingsactiviteiten

Het register van verwerkingsactiviteiten bevat informatie over de persoonsgegevens die je vast legt in het cliëntendossier, of in een digitaal programma. Je mag zelf weten hoe je het register opstelt. Wel schrijft de AVG voor welke informatie je als vaktherapeut in het register moet zetten. Als de Autoriteit Persoonsgegevens (AP) daar om vraagt, moet je het register direct kunnen laten zien.

In het register van verwerkingsactiviteiten moet je opnemen:

1. een omschrijving van de categorieën persoonsgegevens (= cliëntgegevens) die je verwerkt;
2. een beschrijving van de doeleinden waarvoor je persoonsgegevens verwerkt. In de handleiding hebben wij dit alvast als voorbeeld voor je vastgelegd;
3. welke rechten betrokkenen (cliënten) hebben en hoe zij die rechten kunnen uitoefenen. Zoals het recht op inzage, wijzigen, wissen en het ontvangen van alle geregistreerde gegevens;
4. welke organisatorische en technische maatregelen je genomen heeft om de persoonsgegevens te beveiligen;
5. hoe lang je de persoonsgegevens bewaart; en
6. hoe je omgaat met een datalek.

Over dit document

Met behulp van dit document kunt je aan de hand van een aantal stappen vastleggen op welke manier je voldoet aan de Algemene verordening gegevensbescherming (AVG).

Stap 1. Benoemen persoonsgegevens

Bij minderjarige cliënten:

Indien dit in belang is van de begeleiding/behandeling, leg ik de volgende verdere gegevens vast:

Opmerking over het vastleggen van bijzondere persoonsgegevens:

Gegevens over godsdienst of levensovertuiging, gezondheid, zaken m.b.t. de seksualiteit, of strafrechtelijke gegevens worden bijzondere gegevens genoemd. Het verwerken van bijzondere persoonsgegevens is in principe verboden, tenzij u zich op een wettelijke uitzondering kunt beroepen. Indien de gegevens worden verwerkt in het kader van gezondheidszorg, hulpverlening, of sociale dienstverlening is verwerking toegestaan, maar alleen als dat gebeurt door een beroepsbeoefenaar met een beroepsgeheim of andere persoon die aan geheimhouding is gebonden. Deze uitzondering geldt dus op basis van de Wet op de geneeskundige behandelovereenkomst (WGBO) ook voor vrijgevestigde vaktherapeuten.

Indien dit in belang is van de begeleiding/behandeling, leg ik de volgende bijzondere persoonsgegevens vast:

x	Naam, adres, postcode, woonplaats van de cliënt(en)
x	Geboortedatum van de cliënt(en)
	Telefoonnummer en e-mail van de cliënt(en)
x	Ook naam, adres, postcode, woonplaats, telefoonnummer en e-mailadres van beide ouders
x	Huisarts;
x	Huisarts;
	Godsdienst of levensovertuiging;
x	Gezondheid;
x	Zaken m.b.t. de seksualiteit;
x	Mogelijke strafrechtelijke gegevens zoals een melding bij Veilig Thuis, begeleiding door jeugdzorg, geweldconflicten in het gezin.

Het Burger Service Nummer (BSN)

Opmerking over het vastleggen van het Burgerservicenummer (BSN):

Organisaties buiten de overheid mogen een Burgerservicenummer alleen gebruiken als dit in een wet is bepaald. En alleen voor het doel dat in de wet staat omschreven.

Zorgverleners mogen het BSN bijvoorbeeld gebruiken als zij werken in het kader van de Zorgverzekeringswet, de Jeugdwet, de WMO en de Wet langdurige zorg. De declaratie in het kader van de aanvullende zorgverzekering valt niet onder de Zorgverzekeringswet en is GEEN grond voor het gebruik van het BSN. Reden waarom ik het Burgerservicenummer vastleg is (wetgeving op grond waarvan u dat doet noemen): • Ik verricht werkzaamheden die onder de jeugdwet, WLZ of WMO kunnen vallen

Stap 2. De doeleinden vastleggen van de persoonsgegevens die worden verwerkt

Doeleinden van de persoonsgegevens die door mij worden verwerkt.

Behalve de AVG, zijn de WGBO (Wet op de geneeskundige behandelingsovereenkomst) en de beroepscode van mijn beroepsvereniging en de Richtlijnen voor de Vrijgevestigde Vaktherapeut van toepassing op mijn werk. Deze zijn van invloed op de doeleinden waarvoor ik persoonsgegevens vastleg. Om die reden ga ik als volgt om met persoonsgegevens:

1. Dossierplicht
Op grond van de Wet op de geneeskundige behandelingsovereenkomst (WGBO) ben ik als zorgverlener verplicht een medisch dossier bij te houden.

2. Bewaartermijn
De hoofdregel voor het bewaren van medische dossiers staat in de WGBO. Dat is 15 jaar, gerekend vanaf de datum van vastlegging van ieder afzonderlijk gegeven. De termijn kan langer zijn indien dit noodzakelijk is met het oog op de behandeling (bijvoorbeeld indien iemand een chronische ziekte heeft).

Deze wet regelt dat mensen het recht hebben om hun zorgverlener te vragen om de gegevens eerder te vernietigen. Je moet daar gehoor aan geven, tenzij een bepaald voorschrift of specifieke wet bepaalt dat je de gegevens moet bewaren. Bijvoorbeeld vanwege het belang van iemand anders. Of omdat de gegevens nodig zijn voor het leveren van zorg.

Heeft een patiënt je gevraagd om vernietiging van zijn of haar medisch dossier? Dan moet je als zorgverlener binnen 3 maanden aan dit verzoek voldoen. Wanneer je het verzoek afwijst, dan moet je de patiënt laten weten waarom. Het liefst schriftelijk. Verwijder je alleen een onderdeel uit het medisch dossier? Dan kun je in het dossier vermelden dat een deel van de gegevens op verzoek van de patiënt is verwijderd.

x	Ik leg het Burgerservicenummer wel vast
---	---

3. Beroepsgeheim

Voor mij als vaktherapeut geldt op grond van de beroepscode en het wettelijk geregeld medisch beroepsgeheim een geheimhoudingsplicht. Medewerkers van vaktherapie praktijk zijn via een arbeidscontract aan een geheimhoudingsplicht gebonden.

4. Minderjarigen

Volgens de patiëntenrechten uit de WGBO komen de wilsbekwame minderjarige tussen 12-16 jaar zelf en de ouder(s) met gezag toe. Ouder(s) van minderjarigen tot 16 jaar hebben medebeslissingsrecht over de behandeling. Ouders hebben recht op informatie en inzage in het dossier, wanneer dit gekoppeld is aan het medebeslissingsrecht voor de behandeling. Er bestaat een uitzondering op dit inzagerecht, namelijk wanneer de professional van mening is dat de uitoefening van bepaalde

patiëntenrechten indruist tegen het belang van de patiënt. Wilsbekwame patiënten van 12 jaar en ouder zijn zelf bevoegd om toestemming te verlenen voor doorbreking van de geheimhouding.

Stap 3: Leg vast hoe de cliënt/patiënt geïnformeerd wordt

In deze stap leg je vast hoe je de cliënt informeert. Je kunt dit aangeven door een vinkje, of een kruisje in het hokje van je keuze te plaatsen. Je kunt ook nog andere tekst toevoegen

x	Ik informeer de cliënten mondeling over de dossierplicht tijdens de intake.
x	Deze informatie ligt vast in een schriftelijke behandelovereenkomst. Zo ja, sluit deze behandelovereenkomst bij in dit document.
x	Op mijn website staat informatie over mijn werkwijze, de dossierplicht en de verplichtingen als gevolg van de WGB0, de Wkkgz en de beroepscode.
x	Indien kinderen jonger zijn dan 16 jaar, geven beide ouders schriftelijk toestemming tot de behandeling en daarmee tot het vastleggen van gegevens in een dossier. Zo ja, sluit deze behandelovereenkomst bij in dit document.
	Ik vraag bezoekers van mijn site om hun naam, e-mailadres e.d. in te vullen. Ik leg uit waarvoor deze persoonsgegevens zijn en wat ik ermee doe.

Opmerking:

Je kunt de behandelovereenkomsten blijven gebruiken die je nu ook al gebruikt.

Stap 4: Leg vast wie er daadwerkelijk werken met de cliëntdossiers?

In deze stap leg je vast wie daadwerkelijk werkt met de cliëntdossiers. Door een vinkje, of een kruisje in het hokje van je keuze te plaatsen. Leg je vast welke situaties op jou van toepassing zijn. Je kunt ook nog andere tekst toevoegen.

x	Ik ben ZZP-er en ben de enige die toegang heeft tot de dossiers. Vanuit de beroepscode heb ik een beroepsgeheim.
x	Verschillende collega's hebben toegang tot patiëntdossiers. Zij vallen eveneens onder het beroepsgeheim en hanteren dezelfde regels
x	Er zijn ook medewerkers die toegang hebben tot de patiëntdossiers. In de arbeidsovereenkomst is de geheimhouding geregeld.
x	Ik bereek wel eens met collega's, of in intervisiegroepen casuïstiek uit de praktijk. Dat gaat altijd anoniem en onherkenbaar

Opmerking:

Een van de consequenties van de AVG is dat een therapeut **vooraf** en **expliciet** (via de behandelovereenkomst/informed consent) **toestemming** moet vragen aan een cliënt om casuïstiek **geanonimiseerd** te mogen gebruiken voor Supervisie en Intervisie. Je kunt dit afdekken door dit gebruik in je privacy policy op te nemen en naar de policy te verwijzen in de behandelovereenkomst. Niet anoniem inbrengen was al een schending van de privacy en dat wordt het nu nog des te meer.

Stap 5: Vastleggen hoe je de beveiliging van de persoonsgegevens (cliëntendossiers) hebt geregeld

Je bent verplicht om passende technische en organisatorische maatregelen te nemen om het verlies van persoonsgegevens of onrechtmatige verwerking tegen te gaan. Je kunt hier aangeven hoe je de beveiliging hebt geregeld door een vinkje, of een kruisje in het vierkant te plaatsen. Je kunt ook nog andere tekst toevoegen.

	Ik werk met papieren cliëntendossiers. Deze worden in een afgesloten kast bewaard
x	Ik werk met een digitaal cliëntendossier. Dit is beveiligd door een wachtwoord.
	Ik werk met een digitaal cliëntendossier dat is versleuteld en beveiligd met een wachtwoord
x	Ik maak regelmatig een back-up van mijn cliëntbestanden
x	Doordat ik regelmatig de laatste versie update van mijn software installeer, zorg ik er voor dat mijn software optimaal beveiligd is

Een manier om je cliëntendossiers te beveiligen is te werken met een elektronisch patiëntendossier of met behulp van bijv. AxCrypt ID je documenten op je computer te beveiligen.

Toevoeging:

1. Als je ambulantly werkt, geef dan aan hoe je de cliëntgegevens onderweg beveiligd hebt: Gegevens zijn beveiligd via een computerwachtwoord, en een wachtwoord voor opslag van gegevens

Stap 6: Leg vast welke externe personen of bedrijven toegang hebben tot de persoonsgegevens en daarmee tot de groep verwerkers behoren waarmee je een werkersovereenkomst moet afsluiten.

Er zijn geen specifieke personen die toegang hebben tot mijn cliëntgegevens

Stap 7: Leg vast hoe je omgaat met datalekken

Toelichting op deze stap:

Sinds 1 januari 2016 geldt de meldplicht datalekken. Deze meldplicht houdt in dat organisaties (dus ook vaktherapeuten) direct (binnen 72 uur na het datalek) een melding moeten doen bij de Autoriteit Persoonsgegevens zodra zij een ernstig datalek hebben. Soms moeten zij het datalek ook melden aan de betrokkenen (de mensen van wie de persoonsgegevens zijn gelekt).

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

Wanneer moet je een datalek melden?

Je hoeft een datalek alleen te melden aan de Autoriteit Persoonsgegevens, als dit leidt tot ernstige nadelige gevolgen voor de bescherming van persoonsgegevens, of als een aanzienlijke kans bestaat dat dit gebeurt. Dat is het geval als er bij het datalek ofwel persoonsgegevens verloren zijn gegaan (ze zijn voor u niet meer terug te halen en er was geen back-up) ofwel onrechtmatige verwerking van de persoonsgegevens niet is uit te sluiten (iemand heeft mogelijk toegang (gehad) tot de

persoonsgegevens terwijl diegene daartoe niet bevoegd was en je hebt geen controle over wat diegene met de gegevens heeft gedaan of nog zal doen).

Je hoeft de betrokkenen (de cliënten van wie je gegevens verwerkt) alleen te informeren als een datalek waarschijnlijk ongunstige gevolgen heeft voor hun persoonlijke levenssfeer. Dat kan het geval zijn als er gegevens van gevoelige aard zijn gelekt (bijvoorbeeld gezondheidsgegevens) die door derden kunnen worden misbruikt.

Ik heb de uitleg begrepen en zal er naar handelen. Ik geef aan met een kruisje of vinkje in het vierkant wat in mijn situatie van toepassing is.

<input checked="" type="checkbox"/>	Ik begrijp wanneer ik een datalek moet melden en zal daar naar handelen
<input type="checkbox"/>	Ik heb afspraken gemaakt in de verwerkersovereenkomst met leveranciers en ik word daardoor tijdig geïnformeerd als er een datalek is geweest

Boskoop, 1 juni 2018