

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 de plaats van de oude Wet bescherming persoonsgegevens (Wbp). In de AVG staan een aantal verplichte maatregelen genoemd waaraan u, als therapeut, 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 kan gedaan worden door de leverancier, maar u kunt het ook zelf doen (als u de kennis in huis hebt) of een externe partij inschakelen;
- 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 u vastlegt in het cliëntendossier, of in een digitaal programma. U mag zelf weten hoe u het register opstelt. Wel schrijft de AVG voor welke informatie u als therapeut in het register moet zetten. Als de Autoriteit Persoonsgegevens (AP) daarom vraagt, moet u het register direct kunnen laten zien.

In het register van verwerkingsactiviteiten moet u opnemen:

- a) een omschrijving van de categorieën persoonsgegevens (=cliëntgegevens) die u verwerkt;
- b) een beschrijving van de doeleinden waarvoor u persoonsgegevens verwerkt. In de handleiding hebben wij dit alvast als voorbeeld voor u vastgelegd;
- c) 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;
- d) welke organisatorische en technische maatregelen u genomen heeft om de persoonsgegevens te beveiligen;
- e) hoe lang u de persoonsgegevens bewaart; en
- f) hoe u omgaat met een datalek.

Hieronder treft u een handleiding aan waarmee u dit register kunt opstellen.

Over dit document

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

Zo ver als mogelijk is hebben wij alvast een voorstel voor een definitie aangegeven. Uiteraard kunt u dat wijzigen en aanvullen. Als u alle stappen heeft ingevuld en aangepast, heeft u hiermee een register van verwerkingsactiviteiten ingesteld. U kunt dit uitprinten en archiveren. U kunt dit tijdens de visitatie laten zien.

U ziet steeds een toelichting.

Stap 1. Benoemen persoonsgegevens

- ☐ Naam, adres, postcode, woonplaats van de cliënt(en)
- ☐ Geboortedatum van de cliënt(en)
- ☐ Telefoonnummer en e-mail van de cliënt(en)

Bij minderjarige cliënten:

- ☐ Ook naam, adres, postcode, woonplaats, telefoonnummer en e-mailadres van beide ouders of tekenbevoegden

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

- ☐ Huisarts
- ☐ School van de minderjarige cliënt

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 complementaire of alternatieve zorgverleners die zijn geregistreerd bij RBCZ.

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

- ☐ Godsdienst of levensovertuiging;
- ☐ Gezondheid;
- ☐ Zaken m.b.t. de seksualiteit;
- ☐ Mogelijke strafrechtelijke gegevens zoals een melding bij Veilig Thuis, begeleiding door jeugdzorg, geweldconflicten in het gezin.

Het Burger Service Nummer (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 en de Wet langdurige zorg. Dat is niet het geval bij een complementair, of alternatief therapeut. Zij mogen dus het BSN niet vastleggen. De declaratie in het kader van de aanvullende zorgverzekering valt niet onder de Zorgverzekeringswet en is geen grond voor het gebruik van het BSN.

☐

Ik leg het Burgersevicenummer niet vast

Reden waarom ik het Burgerservicenummer vastleg is (wetgeving op grond waarvan u dat doet noemen):

Als u nog meer vastlegt in het cliëntdossier kunt u dat hieronder aanvullen:

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 van het Register Beroepsbeoefenaren Complementaire Zorg (RBCZ) 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 20 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).
3. **Beroepsgeheim**
Voor mij als therapeut geldt op grond van de beroepscode en het wettelijk geregeld medisch beroepsgeheim een geheimhoudingsplicht. Medewerkers van een psychosociale of complementaire praktijk zijn via 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.

Nog meer doelen van het cliëntdossier toevoegen:

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

- ☐ Ik informeer de cliënten mondeling over de dossierplicht tijdens de intake.
- ☐ Deze informatie ligt vast in een schriftelijke behandelovereenkomst. Zo ja, sluit deze behandelovereenkomst bij dit document.
- ☐ Op mijn website staat informatie over mijn werkwijze, de dossierplicht en de verplichtingen als gevolg van de WGBO, de Wkkgz en de beroepscode.
- ☐ 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 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: u kunt de behandelovereenkomsten blijven gebruiken die u nu ook al gebruikt.

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

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

Toevoeging:

Stap 5: vastleggen hoe u de beveiliging van de persoonsgegevens (cliëntdossiers) heeft geregeld

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

Toevoeging:

1. Als u ambulant werkt, geef dan aan hoe u de cliëntgegevens onderweg beveiligd hebt en de privacy van de cliënt tijdens het ambulante werken.

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

Leveranciers waarmee ik een verwerkersovereenkomst hebt afgesloten zijn:

Stap 7: Leg vast hoe u omgaat met datalekken

Toelichting op deze stap:

Sinds 1 januari 2016 geldt de meldplicht datalekken. Deze meldplicht houdt in dat organisaties (dus ook therapeuten) 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 gesloten laptop of een inbraak in een databestand door een hacker.

Wanneer moet u een datalek melden?

U 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 u hebt geen controle over wat diegene met de gegevens heeft gedaan of nog zal doen).

U hoeft de betrokkenen (de cliënten van wie u 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 ernaar handelen. Ik geef aan met een kruisje of vinkje in het vierkan wat in mijn situatie van toepassing is.

☐
☐

Ik begrijp wanneer ik een datalek moet melden en zal daarnaar handelen.

Ik heb afspraken gemaakt in de verwerkersovereenkomst met leveranciers en ik wordt daardoor tijdig geïnformeerd als er een datalek is geweest.

Ondertekening en datum