Stappenplan AVG

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 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) daar om 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 al vast 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.

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 register gemaakt. Uiteraard kunt u dat wijzigen en aanvullen. Als u alle stappen heeft ingevuld en aangepast, heeft u hiermee een register van verwerkingsactiviteiten opgesteld. U kunt dit uitprinten en archiveren. U kunt dit tijdens een eventuele inspectie of visitatie laten zien.

Stap 1. Benoemen persoonsgegevens

In deze stap legt u vast welke persoonsgegevens u vastlegt in het cliëntendossier. U kunt dit aangeven door een vinkje, of een kruisje in eerste hokje te plaatsen

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

Bij minderjarige cliënten:

v	Ook naam, adres, postcode, woonplaats, telefoonnummer en e-mailadres van 1 ouder

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;
v	Gezondheid; voorgeschiedenis, behandelplan
v	Zaken m.b.t. de seksualiteit;
v	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 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.

Als u het BSN wel vastlegt kunt u dit aangeven door een vinkje, of een kruisje in het hokje van uw keuze te plaatsen. Geef ook de reden van gebruik aan

	Ik leg het Burgerservicenummer wel 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

1.

Stap 2. de doeleinden vastleggen van de persoonsgegevens die worden verwerkt
In deze stap legt u vast waarom u de persoonsgegevens van stap 1 vastlegt.

We hebben een aantal algemene omschrijvingen alvast voor u geformuleerd omdat die voor de meeste RBCZ therapeuten gelden. Indien iets niet van toepassing is kunt u de tekst verwijderen en andere tekst toevoegen.

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

Indien de patiënt minderjarig is en de leeftijd van twaalf maar nog niet die van zestien jaren heeft bereikt, is tevens de toestemming van de ouders die het gezag over hem uitoefenen of van zijn voogd vereist. De verrichting kan evenwel zonder de toestemming van de ouders of de voogd worden uitgevoerd, indien zij kennelijk nodig is teneinde ernstig nadeel voor de patiënt te voorkomen, alsmede indien de patiënt ook na de weigering van de toestemming, de verrichting weloverwogen blijft wensen. 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 cliëntendossier toevoegen:

1.

Stap 3: Leg vast hoe de cliënt/patiënt geïnformeerd wordt
In deze stap legt u vast hoe u de cliënt informeert. U kunt dit aangeven door een vinkje of een kruisje in het hokje van uw keuze te plaatsen. U kunt ook nog andere tekst toevoegen

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

Stap 4: Leg vast wie er daadwerkelijk werken met de cliëntdossiers
In deze stap legt u vast wie daadwerkelijk werkt met de cliëntendossiers. Door een vinkje, of een kruisje in het hokje van uw keuze te plaatsen. legt u vast welke situaties op u van toepassing zijn. U kunt ook nog andere tekst toevoegen

v	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.
v	Ik bepreek wel eens met collega's of in intervisiegroepen casuïstiek uit de praktijk. Dat gaat altijd anoniem en onherkenbaar en nadrukkelijk met de toestemming van de patiënt

Toevoeging:

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

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

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

Toevoeging:

1. Als u ambulant werkt, geef dan aan hoe u de cliëntgegevens onderweg beveiligd hebt:

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.

Er zijn situaties waarin er externe leveranciers zijn die de persoonsgegevens uit het cliëntendossier soms kunnen inzien. U kunt hierbij denken aan:

- de websitebouwer;
- de leveranciers van het programma van de digitale cliëntendossiers
- de drukker die adresbestanden krijgt om samen te voegen tot een brief, of etiket;
- de accountant, of het administratiebureau die de nota's verzendt en administreert
- de software-aanbieder van de digitale nieuwsbrief;
- enz.

Met deze leveranciers moet u een z.g. verwerkersovereenkomst afsluiten.

Er is een voorbeeld opgenomen van een dergelijke overeenkomst als bijlage bij dit document.

Leveranciers waarmee ik een verwerkersovereenkomst heb afgesloten zijn:

1. ICT By Thomas (Mail)
2. Spynn (webbouwer)

Stap 7: Leg vast hoe u omgaat met datalekken

In deze stap leest u eerst onderstaande tekst en daarna kunt u aangeven met een vinkje of kruisje in het vierkant te plaatsen dat u conform deze beschrijving zult handelen

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 gestolen 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 vierkant wat in mijn situatie van toepassing is.

v	Ik begrijp wanneer ik een datalek moet melden en zal daarnaar handelen
v	Ik heb afspraken gemaakt in de verwerkersovereenkomst met leveranciers en ik word daardoor tijdig geïnformeerd als er een datalek is geweest

Ondertekening en datum