Body Stress Release
Aurora

VERWERKINGSACTIVITEITEN

Inleiding

Sinds 25 mei 2018 geldt de Algemene Verordening Gegevensbescherming (AVG). Dit is een nieuwe Europese privacywet. Daardoor is de privacy in alle landen van de Europese Unie gelijk. Nu hebben de lidstaten nog hun eigen nationale wetten.
De Algemene Verordening Gegevensbescherming is in de plaats gekomen van de oude Wet bescherming persoonsgegevens (Wbp). In de AVG staan een aantal verplichte maatregelen genoemd waaraan als therapeut moet worden voldaan omdat gegevens in een cliëntendossier wordt vastgelegd.

Verplichte maatregelen

De verplichte maatregelen die de AVG concreet noemt zijn:

1. het bijhouden van een register van verwerkingsactiviteiten;
2. het (laten) uitvoeren van een veiligheidscontrole van het digitale cliëntendossier. Dit kan door de leverancier gedaan worden, maar ook zelf, indien de kennis daarvoor in huis is of door een ingeschakelde externe partij.
3. het bijhouden van een register van datalekken die zijn opgetreden;
4. het aantonen dat een patiënt of cliënt daadwerkelijk toestemming heeft gegeven voor het vastleggen van gegevens in het cliëntendossier.

Register van verwerkingsactiviteiten

Het register van verwerkingsactiviteiten bevat informatie over de persoonsgegevens die worden vastgelegd in het cliëntendossier of een digitaal programma. Zelf mag gekozen worden hoe het register wordt opgesteld. Wel schrijft de AVG voor welke informatie de therapeut in het register moet zetten. Als de Autoriteit Persoonsgegevens (AP) daar om vraagt, moet het register direct getoond kunnen worden.

In het register van verwerkingsactiviteiten moet worden opgenomen:

a. een omschrijving van de categorieën persoonsgegevens (cliëntgegevens) die worden verwerkt;
b. een beschrijving van de doeleinden waarvoor persoonsgegevens worden verwerkt.;
c. welke rechten betrokkenen (cliënten) hebben en hoe zij die rechten kunnen uitoefenen. Zoals bv. het recht op inzage, wijzigen, wissen en het ontvangen van alle geregistreerde gegevens (zie Privacyverklaring Body Stress Release Aurora);
d. welke organisatorische en technische maatregelen genomen zijn om de persoonsgegevens te beveiligen;
e. hoe lang de persoonsgegevens worden bewaard; en
f. hoe wordt omgegaan met een datalek.

Aan de hand van de volgende stappen is vastgelegd op welke wijze Body Stress Release Aurora/practitioner Wouter Olsthoorn voldoet aan de AVG.

Body Stress Release
Aurora

Algemene persoonsgegevens

Naam, adres, postcode, woonplaats van de cliënt	ja
Geboortedatum van de cliënt	ja
Telefoonnummer en e-mailadres van de cliënt	ja

Minderjarige cliënten

Telefoonnummer en e-mailadres van contact ouder	ja

Extra gegevens in belang is van de begeleiding/behandeling

Huisarts; alleen bij directe verwijzing door de huisarts en waar terugkoppeling aan huisarts gevraagd wordt. Alleen met toestemming van de cliënt.	ja
School van de minderjarige cliënt	nee

Vastleggen van bijzondere persoonsgegevens

Gegevens over godsdienst of levensovertuiging, gezondheid, zaken m.b.t. de seksualiteit of strafrechtelijke gegevens worden bijzondere persoonsgegevens genoemd.
Het verwerken van bijzondere persoonsgegevens is in principe verboden, tenzij men zich op een wettelijke uitzondering kan 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 op basis van de Wet op de Geneeskundige Behandelovereenkomst (WGBO) ook voor complementaire of alternatieve zorgverleners die bij Register Beroepsbeoefenaren Complementaire Zorg (RBCZ) zijn geregistreerd.

Bijzondere persoonsgegevens

Godsdienst of levensovertuiging	nee
Gezondheid	ja
Zaken m.b.t. de seksualiteit; alleen met toestemming van de cliënt	ja
Mogelijke strafrechtelijke gegevens zoals een melding bij Veilig Thuis, begeleiding door jeugdzorg, geweldconflicten in het gezin. Alleen indien sprake is van protocol 'Huiselijk geweld / kindermishandeling'.	ja

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 (Wlz). Dat is bij een complementair of alternatief therapeut niet het geval. Zij mogen het BSN dus 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.

Burgerservicenummer	nee
Bij intakegesprek een identiteitsbewijs controleren	nee

Omschrijving van evt. reden waarom het burgerservicenummer wordt vastgelegd en tevens de wetgeving op grond waarvan dat wordt gedaan benoemen.
n.v.t.

Meer informatie die in het cliëntdossier wordt vastgelegd

Zorgverzekering & polisnummer	ja
Beroep	ja
Sociale situatie	
Gezondheidsklachten fysiek en mentaal & gezondheidgeschiedenis	ja
Operaties	ja
Medicatiegebruik	ja

Doeleinden van de persoonsgegevens die worden verwerkt
Behalve de AVG zijn ook de WGBO, de beroepscode van de beroepsvereniging VBAG en het RBCZ op het werk van toepassing. Deze zijn van invloed op de doeleinden waarvoor persoonsgegevens worden vastgelegd.

Dossierplicht
Op grond van de WGBO is de zorgverlener verplicht een cliëntendossier bij te houden.

Bewaartermijn
De hoofdregel voor het bewaren van medische- cliëntendossiers staat in de WGBO. De bewaartermijn is 20 jaar, gerekend vanaf de datum van vastlegging van ieder afzonderlijk gegeven. De termijn kan langer zijn indien dit met het oog op de behandeling (bijvoorbeeld als iemand een chronische aandoening heeft) noodzakelijk is.

Beroepsgeheim
Als BSR-practitioner geldt op grond van de beroepscode en het wettelijk geregeld medisch beroepsgeheim een geheimhoudingsplicht. Medewerkers van psychosociale of complementaire praktijken zijn via arbeidscontract c.q. beroepsvereniging aan een geheimhoudingsplicht gebonden.

Minderjarigen
Volgens de WGBO komen patiëntenrechten de wilsbekwame minderjarigen 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 patiënten rechten 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.

Eventuele andere doelen van het cliëntendossier
n.v.t.

Hoe de cliënt wordt geïnformeerd

Cliënten worden mondeling over de dossierplicht tijdens de intake geïnformeerd.	nee
In de behandelovereenkomst en privacyverklaring staat alle informatie over de werkwijze, dossierplicht en verplichtingen als gevolg van de WGBO, Wkkgz en de beroepscode beschreven.	ja
Indien kinderen jonger zijn dan 16 jaar geven (beide) ouders schriftelijk toestemming tot de behandeling en daarmee tot het vastleggen van	ja

gegevens in een dossier. Zie Behandelovereenkomst en Toestemmingsformulier Body Stress Release Aurora	
Cliënten wordt gevraagd om hun persoonsgegevens en informatie zelf, via een beveiligde digitale link, in het dossier in te vullen. Deze link wordt voorafgaand aan de eerste afspraak per email toegestuurd.	ja

Wie daadwerkelijk met de cliëntdossiers werkt

Als ZZP-er is Wouter Olsthoorn de enige die toegang heeft tot de dossiers. Vanuit de beroepscode is er beroepsgeheim.	ja
Verschillende collega's hebben toegang tot de patiëntendossiers. Zij vallen eveneens onder het beroepsgeheim en hanteren dezelfde regels.	nee
Er zijn medewerkers die toegang hebben tot de patiëntendossiers. In de arbeidsovereenkomst is de geheimhouding geregeld.	nee
Ten behoeve van leerdoeleinden wordt met collega's of in een intervisiegroep casuïstiek uit de praktijk besproken. Dat gaat altijd anoniem en onherkenbaar.	ja

Hoe de vastlegging van de beveiliging van de persoonsgegevens (cliëntendossiers) is geregeld

Bij waarneming van de cliënten van collega wordt met papieren cliëntendossiers gewerkt. Deze dossiers worden in een afgesloten kast bewaard.	ja
Body Stress Release Aurora werkt met een digitaal cliëntendossier. Dit is beveiligd door een wachtwoord.	ja
Het digitaal cliëntendossier is versleuteld en beveiligd met een wachtwoord. Om in het dossier te kunnen wordt er tevens gebruik gemaakt van een tweestapsverificatie.	ja
Om de computer goed te beveiligen tegen inbreuk door derden wordt ieder kwartaal het wachtwoord van de computer gewijzigd. Waarbij de laatste vier tekens/cijfers het laatste half jaar niet zijn gebruikt.	ja
Er wordt automatisch een back-up van het cliëntbestanden gemaakt.	ja
Door regelmatig de laatste versie software-update te update te installeren, is de software optimaal beveiligd is	ja

Toevoeging
Als ambulant wordt gewerkt, geef dan aan hoe de cliëntgegevens onderweg worden beveiligd.

Het cliëntendossier-programma wordt voor transport afgesloten.

Externe personen of bedrijven welke toegang tot de persoonsgegevens hebben en die daarmee tot de groep verwerkers behoren waarmee een verwerkersovereenkomst of geheimhoudingsverklaring is afgesloten:
1. BSR Manager/TIZM, Ron Beskers – leverancier van het digitale cliëntdossier en boekhoudprogramma;
2. Administratiekantoor Winkelaar, Danielle Rekers - boekhouder en diens medewerkers.

Ondersteunende collega waarmee een waarnemingsovereenkomst is ondertekend:
1. Rimke Pepers – BSR Hoorn

Executeurs welke bij langdurige ziekte of overlijden mijn belangen zullen behartigen c.q. zaken zullen afhandelen, waarmee een geheimhoudingsverklaring is ondertekend:
1. Jos Koenis - executeur
2. - executeur

Meldplicht datalek Autoriteit Persoonsgegevens
Sinds 01 januari 2016 geldt de meldplicht datalekken. Deze meldplicht houdt in dat organisaties (dus ook therapeuten) direct (binnen 72 uur) na een datalek een melding van de datalek maken bij de Autoriteit Persoonsgegevens (AP). Soms moet het datalek ook aan de betrokkenen, degenen van wie de persoonsgegevens zijn gelekt, gemeld worden.

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

Wanneer moet een datalek worden gemeld?
Een datalek hoeft alleen aan de Autoriteit Persoonsgegevens te worden gemeld, als de datalek leidt tot ernstige nadelige gevolgen voor de bescherming van persoonsgegevens of als een aanzienlijke kans bestaat dat dit zal gebeuren.
Dat is het geval wanneer er bij het datalek ofwel persoonsgegevens verloren zijn gegaan (ze zijn niet meer terug te halen en er was geen back-up) ofwel onrechtmatige verwerking van de persoonsgegevens niet uit te sluiten is (iemand heeft mogelijk toegang tot de persoonsgegevens (gehad), terwijl diegene daartoe niet bevoegd was en er geen controle is over wat diegene met de gegevens heeft gedaan of zal gaan doen).

Het is alleen nodig de betrokkenen (cliënten van wie gegevens worden verwerkt) te informeren als een datalek waarschijnlijk ongunstige gevolgen heeft voor hun persoonlijke levenssfeer. Dat kan het geval zijn als gegevens van gevoelige aard (bv. gezondheidsgegevens) zijn gelekt, die door derden kunnen worden misbruikt.

De organisatie is in het bezit van een stappenplan Datalek	ja
In de verwerkersovereenkomst met de leverancier beschreven dat de organisatie tijdig wordt geïnformeerd indien bij een leverancier een datalek is geweest.	ja

Bijlagen:
- behandelovereenkomst Body Stress Release Aurora
- privacyverklaring Body Stress Release Aurora
- toestemmingsformulier minderjarige
- verwerkersovereenkomst BSR Manager/TIZM
- waarnemingsovereenkomst
- geheimhoudingsverklaringen