

De AVG voor therapeuten.

Op 25 mei 2018 wordt de Europese wetgeving AVG (*Algemene Verordening Gegevensbescherming*, in het Engels GDPR – *General Data Protection Regulation*) van kracht. Nederland heeft daarbij een aantal aanvullende regels opgesteld in de vorm van de *Uitvoeringswet AVG* (UAVG).

Deze handleiding schetst hoe *zelfstandig werkende therapeuten in de alternatieve geneeskunde* kunnen voldoen aan deze wetgeving. In de bijlagen vindt u een aantal documenten die illustreren hoe een therapie-praktijk de AVG kan invoeren, en formaliseren.

Deze handleiding is met zorg en aandacht samengesteld. Echter, u kunt er geen rechten aan ontleen: de uiteindelijke wettekst(en), die u kunt downloaden via de website van de *Autoriteit Persoonsgegevens*, zijn leidend. Op die website kunt u eveneens een uitgebreide *Handleiding AVG* vinden. Die handleiding is door de overheid opgesteld, en vormt de belangrijkste informatiebron voor belangstellenden.

Inleiding

De wet stelt onder meer: '*De verwerking van persoonsgegevens moet rechtmatig, behoorlijk en transparant zijn*'. Wat betekent dat praktisch? U dient cliënten te informeren *welke* gegevens u verzameld en *waarom* (de *informatieplicht*), en *hoe* u deze gegevens veilig beheerd. U mag (als therapeut) alleen gegevens verzamelen na de *uitdrukkelijke* en formele toestemming van uw cliënt. Cliënten hebben het recht deze toestemming later te *herroepen*, en ook het recht om de door u verzamelde gegevens in te zien, of om te eisen dat u deze vernietigt ('*het recht om vergeten te worden*').

Het verzamelen van persoonsgegevens moet *legitiem* (rechtmatig) zijn. Dat kan onder andere worden bewerkstelligd door het krijgen van *toestemming* van de betrokkene (uw cliënt). Voor therapeuten is dit de aangewezen methode, omdat andere manieren van legitimeren (bijvoorbeeld: '*de gegevens zijn noodzakelijk voor het uitvoeren van een overeenkomst*') niet voldoen aan de aanvullende eisen die gelden voor de speciale categorieën (privacy-gevoelige) informatie die therapeuten vaak van hun cliënt krijgen.

Als u constateert dat persoonsgegevens in onbevoegde handen zijn gekomen (of dat zouden kunnen komen) – het zogenaamde *data-lek* – dan dient u de Autoriteit Persoonsgegevens op de hoogte te stellen. U bent daarnaast verplicht om aan te kunnen tonen dat u voldoet aan de voorschriften (*accountability*), onder meer door het bijhouden van een *Register* waarin u allereerst uw algemene werkwijze ten aanzien van persoonsgegevens beschrijft, en daarna handelingen en veranderingen bijhoudt.

Een deel van de bovenstaande zaken vereist niet veel werk. U kunt vrij eenvoudig een document maken, dat u eenmalig laat ondertekenen door cliënten, waarin zij *geïnformeerd* worden over uw werkwijze bij de omgang met persoonsgegevens, en waarmee zij *toestemming* geven voor het registreren van die gegevens. En de naam *Register* klinkt imponerend, maar u mag zelf bepalen *hoe* u uw werkwijze daarin beschrijft. U kunt volstaan met een eenvoudig tekstdocument. Met andere woorden: de AVG *kán* in het begin overkomen als een veelheid aan voorschriften, maar dat valt erg mee. Na het opstellen van enkele documenten bij aanvang kunt u daarna volstaan met vooral routinematige handelingen, zoals het laten tekenen van een informatie- en toestemmingsdocument door nieuwe cliënten. Die praktische kanten van de AVG behandelen we later in deze handleiding, en in de bijlage vindt u enkele voorbeelden van documenten, die u zelf als uitgangspunt kunt nemen.

Er is echter één taak die de AVG verlangt die *niet* eenvoudig is. Dat is het kiezen van de *manier* waarop u met persoonsgegevens omgaat – de *procedure*, de manier waarop u de gegevens bewaard (bijvoorbeeld in een kast, of digitaal op een PC of laptop).

De wetgever zegt eigenlijk: "U mag uw werkwijze *zélf* bepalen, maar u moet uw keuzes kunnen *verantwoorden* en *beargumenteren*". U kunt dus alleen aan de wet voldoen, als u de *bedoeling* van de wet begrijpt, en deze in de praktijk toepast. Het is uw *voortdurende verantwoordelijkheid* om steeds een juiste afweging te maken – bij het bepalen van de juiste mate van inspanning en investering bij het beveiligen van persoonsgegevens.

Een eenvoudig voorbeeld. Een cliënte geeft u, ten behoeve van een therapie, een verzameling zelfgeschreven gedichten, en een dagboek ter inzage. U kiest ervoor de papieren met gedichten op uw bureau te bewaren, omdat u ziet dat er geen naam op staat vermeld. Het dagboek bevat zeer persoonlijke informatie, en op het schutblad ervan heeft uw cliënte haar naam geschreven. U bewaard het dagboek daarom in een brandkast. En dan gebeurt het onfortuinlijke: er wordt bij u ingebroken, en de dief neemt alle papieren op uw bureau mee, waaronder de

gedichten. Het dagboek is *niet* gestolen: de dief heeft blijkbaar onvoldoende tijd gehad om de brandkast te openen. Desondanks klaagt uw cliënt u aan vanwege het *onzorgvuldig* bewaren van haar gedichten. De Autoriteit Persoonsgegevens doet naar aanleiding van deze klacht een onderzoek. En spreekt u vrij: u heeft gehandeld volgens een *verdedigbare afweging* tussen het belang van de privacy van uw cliënt, en datgene wat praktisch van u verwacht kan worden. Omdat u de *bedoeling* van de wet heeft begrepen.

En diezelfde zorgvuldigheid heeft u als therapeut nodig bij het nadenken over de beste *werkwijze* bij het omgaan met persoonsgegevens van cliënten. De AVG zegt níet: “*Iedereen moet een goede virus-scanner voor de PC aanschaffen*”, maar: “*Iedereen moet nadenken hoe de privacy van personen gewaarborgd kan worden*”. Zo'n veilige werkwijze is niet 1-2-3 bedacht. Maar, als u eenmaal tot een bepaalde werkwijze heeft besloten, hoeft u deze daarna slechts in het Register te beschrijven, en voldoet daarmee al grotendeels aan de AVG.

Privacy by Design, Privacy by Default

De AVG wet benoemd enkele bijzondere *categorieën* persoonsgegevens, waarvoor verschillende voorschriften gelden. Denk aan medische informatie, strafrechtelijke gegevens, en gegevens over ras of etnische afkomst. U mag deze bijzondere gegevens alleen registreren bij *uitdrukkelijke* toestemming van uw cliënt. Daarnaast hecht de wet extra belang aan de bescherming van gegevens van ‘*kwetsbare personen, met name van kinderen*’ en bij het omgaan met ‘*gevoelige gegevens of gegevens van zeer persoonlijke aard*’.

Dat benadrukt nog eens dat therapeuten toegang hebben tot zeer privacy-gevoelige informatie. Als die informatie, door opzet of door nalatigheid, in handen komt van onbevoegden, kan dat zeer ernstige nadelige gevolgen hebben voor een cliënt. Een therapeut gaat dagelijks om met dergelijke informatie. Daardoor kan onbedoeld gewinning en onachtzaamheid optreden. De AVG legt daarom de nadruk op ‘*Privacy by Design, Privacy by Default*’ (*‘privacy door ontwerp en standaardinstellingen*’).

Dat betekent dat u een werkwijze voor het omgaan met persoonsgegevens moet ontwikkelen die veilig is en een *inherente* bescherming biedt tegen privacy-schending. U dient *aantoonbaar* te maken dat u, bij de ontwikkeling van een nieuwe werkwijze, er zorg voor heeft gedragen dat de bescherming van persoonsgegevens voor betrokkenen zo optimaal mogelijk is. Het eenvoudigste voorbeeld daarvan is: terughoudendheid bij wát u registreert. Het is dan ook een onderdeel van uw verantwoordelijkheid om alleen datgene te registreren wat toepasselijk of noodzakelijk is voor uw behandeling. Ook indien u op de grondslag van *toestemming* gegevens registreert, bent u verplicht zich te beperken tot een hoeveelheid gegevens die in *proportionele* verhouding staat met het omschreven *doel* (zie hierna).

Opmerking: U mag alleen gegevens verzamelen die u vooraf heeft omschreven, en u dient het doel te beschrijven waarvoor u deze gegevens verzameld. U dient uw cliënten te informeren over dit doel, en eenmaal verzamelde gegevens mag u op een later moment niet voor een geheel ander doel gebruiken, tenzij u opnieuw toestemming vraagt aan uw cliënten. Een praktisch voorbeeld: u mag geen nieuwsbrief sturen aan uw cliënten, tenzij u dit heeft opgenomen in de toestemmingsovereenkomst. Wilt u dit alsnog doen, dan zult u hiervoor eerst toestemming dienen te vragen. Van belang zijn hierbij ook ‘de redelijke verwachtingen die de betrokkene heeft ten aanzien van het verdere gebruik van zijn persoonsgegevens door u’. U mag dus (bijvoorbeeld) wel een nieuwsbrief aanbieden indien u bij het verkrijgen van toestemming heeft vermeldt dat u (bijvoorbeeld) ‘de gegevens gebruikt voor het per e-mail aanbieden van binnen het aandachtsgebied van de therapie toepasselijke informatie’.

Het komen tot een werkwijze

Er is geen eenduidig recept te geven voor een goede werkwijze voor het veilig omgaan met persoonsgegevens door therapeuten. In de komende alinea's daarom een aantal tips en uitgangspunten die u kunnen helpen bij het ontwerpen van een werkwijze.

Papier en digitaal.

De AVG geldt óók voor gegevens die u bewaard op papier. Elke verzameling papieren waarin een *structuur* is aangebracht is een *bestand*, en daarvoor geldt de AVG. Een aantal losse papieren op een bureau is geen bestand, maar uiteraard is een enkel, nog niet opgeborgen intake-formulier dat op uw bureau ligt wél een onderdeel van de regels van de AVG.

Bewaarlocaties.

U kunt, bij het nadenken over een werkwijze, in gedachten bepaalde *bewaarlocaties* visualiseren, zoals 'een goed beveiligde kast' of 'een goed beveiligde map op mijn PC waarin meerdere documenten kunnen worden bewaard'. Dit voorkomt dat u in een te vroeg stadium gaat nadenken over de praktische of technische invulling van zo'n locatie. Eerst bedenkt u zich (bijvoorbeeld) dat u 2 dossierkasten nodig heeft: één met een zeer goede beveiliging (die bijvoorbeeld kleiner kan zijn), en één grotere met een lagere beveiliging. Een ander voorbeeld: u kunt besluiten alle digitale gegevens slechts op één laptop te bewaren, en deze extra goed te beveiligen.

Scenario's.

Samen met *locaties* vormen *scenario's* het tweede type bouwsteen bij het nadenken over uw werkwijze. Voorbeelden van scenario's waarop u zich kunt voorbereiden zijn: 'Er wordt ingebroken, en mijn laptop wordt gestolen'. Of 'Ik ben mijn mobiele telefoon verloren, vermoedelijk in de trein'. En ook: 'Ik verlies de sleutel van mijn brandkast'.

Pseudonimisering.

Dit is een uitstekend hulpmiddel bij het beschermen van persoonsgegevens. Stel, u maakt vaak uitgebreide sessie-verslagen op papier. Die zijn tezamen in de loop der tijd een groot volume gaan vormen, en u bewaarde deze tot nog toe in archiefmappen, samen met de intake-formulieren, in een afsluitbare, maar niet al te sterke kast. Bij *pseudonimisering* bewaard u de sessie-verslagen echter apart, en voorziet ieder verslag van een *verwijsnummer*, dat de verbinding aangeeft met een bepaald intake-formulier (en dus een cliënt). Voor de intake-formulieren (die de *identificerende* informatie bevatten) schaft u vervolgens een versterkte, beter beveiligde kast aan (bijvoorbeeld een brandkast). Indien nu de sessie-verslagen worden gestolen, dan heeft de dief geen manier om te bepalen bij welke persoon deze verslagen horen. Uw cliënten zijn *niet identificeerbaar*.

Uw bestaande persoonsgegevens

Een van de factoren bij het ontwerpen van een nieuwe werkwijze is ook, **wat dit betekent voor uw bestaande persoonsgegevens**. De beste methode hierbij is wellicht om deze in eerste instantie buiten beschouwing te laten. Denk eerst na over wat de meest optimale werkwijze zou zijn. Pas als u dat helder voor ogen heeft, met alle facetten en overwegingen in gedachten, is het een goed moment om u af te vragen of en hoe uw bestaande gegevens daarin passen, en welke werkzaamheden dit verlangt. Bijvoorbeeld: alle sessie-verslagen die u tot nu toe heeft opgesteld scheiden van de intake-formulieren waarbij u ze (bijvoorbeeld) nu bewaard. U kunt daarna alternatieven in uw werkwijze overwegen, waardoor de conversie mogelijk minder inspanning zou vergen.

Een van de mogelijkheden is natuurlijk om een deel van uw bestaande persoonsgegevens en cliëntinformatie **eenvoudigweg te vernietigen**. Logischerwijze is dat niet mogelijk voor die cliëntgegevens die u dient te bewaren als gevolg van uw verplichting aan de belastingdienst (bijvoorbeeld facturen). Het vernietigen van gegevens komt tegemoet aan de grondgedachte van 'Privacy by Design' – dat wat u niet (langer) heeft geregistreerd, kan immers ook geen bron van privacy-schending worden. En het beheer van een kleiner volume informatie kan uw werkwijze vereenvoudigen, en ook toestaan dat u voor de informatie die u wél bewaard, veiliger kunt bewaren (bijvoorbeeld door de mogelijkheid om een kleinere brandkast aan te schaffen, maar met een hogere beschermings-classificatie).

Tegenover deze voordelen staan een aantal overwegingen. In de *Wet op de geneeskundige behandelovereenkomst (Wgbo)* staat **vermeld dat medische dossiers tenminste 15 jaar bewaard** dienen te worden. Patiënten hebben volgens deze wet wel het recht om te verlangen dat u gegevens vernietigt, als aan bepaalde voorwaarden is voldaan. Vermoedelijk is die wet ook de gedachte achter het advies van veel beroepsverenigingen om uw cliëntinformatie minimaal 15 jaar te bewaren. Zo adviseert (bijvoorbeeld) de beroepsvereniging LNVG deze termijn, maar merkt daarbij op: "**tenzij vaststaat dat een gegeven reeds eerder aan betekenis heeft verloren**". **Overigens geldt de bewaartermijn niet voor cliënten die zijn overleden.**

Uiteraard is een belangrijke overweging, welke therapievorm u toepast, en hoe relevant (oudere) dossiers over uw behandeling in de toekomst van belang zijn voor de continuïteit in de behandeling van uw cliënt, door uzelf of door anderen. Bij een alternatieve therapie lijkt niet de verantwoordelijkheid te rusten om gegevens over bijvoorbeeld medicijngebruik te bewaren – die is immers al elders geregistreerd. Ook is de vraag of persoonlijke, emotionele informatie bewaard moet worden, indien u niet verwacht dat uw cliënt opnieuw therapie bij u zal volgen. De AVG verlangt immers een afweging tussen het belang van de privacy van uw cliënt, en andere belangen. Als u niet verwacht dat een voormalige behandeling onderdeel kan worden van een klachten- of tuchtrechtprocedure, en u niet, redelijkerwijs, verwacht dat het bewaren van de informatie in het belang is van uw cliënt zelf, is het zeker het overwegen waard om een deel van uw dossier te vernietigen, en alleen een selectie van uw dossiers te bewaren. U kunt dit uiteraard ook overleggen met uw beroepsvereniging.

Voor wat betreft uw werkwijze, kunt u ook kiezen voor een gehele of gedeeltelijke *splitsing*, waarbij u de bestaande cliëntgegevens in hun huidige vorm laat, en toekomstig te registreren persoonsgegevens verwerkt volgens de nieuwe werkwijze. Heeft u bijvoorbeeld besloten tot pseudonimisering van de sessie-aantekeningen, dan begint u daarmee vanaf nu, en bewaard de bestaande gegevens zoals voorheen. Het is dan wel van belang dat

u het beschermingsniveau (de wijze van bewaren) van deze bestaande gegevens afstemt op de meest privacy-gevoelige gegevens die daarin voorkomen. U dient dan bijvoorbeeld alle oude (bestaande) sessie-verslagen te bewaren in een brandkast, of (indien deze digitaal worden bewaard) met een grote zorgvuldigheid voor wat betreft de bescherming van uw PC of laptop.

Back-ups.

Ook de procedures voor het maken van *back-ups* (van digitale gegevens, waaronder geluidsopnames) en/of *kopieën* (van papier) hebben invloed op de privacy-veiligheid. Een goed doordachte procedure vermindert de kans op fouten (bijvoorbeeld het laten 'slingeren' van een USB-stick).

Als u papieren kopieën elders bewaard, dienen deze uiteraard hetzelfde beschermingsniveau te hebben als de originelen. Ook hier geldt overigens de eis van de wetgever dat u een 'afgewogen' keuze maakt tussen de mate van inspanning en investering, en het privacy-belang van uw cliënten. Een (willekeurig) voorbeeld is, dat u de originelen thuis in een 'middelmaticaal beschermd' kast bewaard, omdat u een goede alarminstallatie heeft, maar de kopieën juist in een eenvoudige brandkast (met een betere bescherming) die u bijvoorbeeld bij een collega plaatst. Uiteraard kunt u ook digitale kopieën van papieren op een PC bewaren.

Bij de *digitale* gegevens is het maken van een back-up meer urgent, omdat digitale opslag-media niet alleen kunnen worden gestolen (al dan niet als een intern onderdeel van een laptop, een PC of een mobiele telefoon), maar ook defect kunnen raken.

Een mogelijke oplossing is de volgende. U maakt op één laptop of PC een met *encryptie* (zie later) beveiligde map (*folder*) aan, waarin u vele documenten kunt plaatsen. Hier plaatst u alle gevoelige informatie in, waaronder bijvoorbeeld die van uw financiële administratie. Vervolgens koopt u 2 externe (draagbare) hard-disks aan, die u met een USB kabel kunt verbinden aan uw PC. U maakt aan het einde van iedere week een kopie van de speciale, beveiligde map op uw PC, op een van de externe HD's. Deze brengt u ter bewaring naar een andere locatie (bijvoorbeeld een collega). Bij het afleveren haalt u tegelijkertijd de 2e externe HD op, waar u de week daarvoor een kopie op heeft gemaakt. Omdat de externe HD's eveneens met encryptie zijn beveiligd, verkleint u de risico's die optreden als een van de HD's wordt gestolen, of verloren raakt.

Encryptie.

Dit is een ander woord voor *versleuteling* en houdt in dat u alleen toegang tot een digitaal document (of een map met meerdere documenten) kunt krijgen na het ingeven van een wachtwoord. Denkt u eraan dat de standaard beveiliging van Microsoft Office documenten (via een wachtwoord) niet voldoende krachtig is. **Voor het werken met encryptie is diverse software beschikbaar. Voor Windows kunt u eventueel gebruik maken van het gratis ('open-source') programma 7-ZIP.**

Uw e-mailadres.

Vaak vindt een deel van de communicatie met cliënten via *e-mail* plaats. Een deel van die e-mails bevat privacy-gevoelige informatie. Denk bijvoorbeeld aan e-mails waarin belangstellenden informeren naar de geschiktheid van therapie voor hun situatie, bijvoorbeeld via een contactformulier op uw website.

Veel mensen lezen hun e-mail via een *app* op een mobiele telefoon, waarbij e-mails automatisch binnenkomen, zonder dat u het wachtwoord van uw e-mailaccount hoeft in te voeren. Hetzelfde geldt voor PC-programma's zoals *Outlook*, *Windows Mail* of *Thunderbird*. Daarom is het belangrijk dat u zowel uw mobiele telefoon als uw PC of laptop met een sterk wachtwoord, of een andere beproefde toegangsmethode beveiligt.

Het is te adviseren om, voor het contact met uw cliënten, een (zakelijk) e-mailadres te gebruiken, dat u *alleen* gebruikt voor zakelijke doeleinden. **U kunt er daarbij ook voor kiezen om gebruik te maken van Webmail. Daarbij opent u uw e-mail via de internet-browser, en dient daarbij steeds het wachtwoord van uw e-mailadres in te voeren. Dat is omslachtig, maar biedt extra bescherming.**

De bescherming van uw PC, laptop en/of mobiele telefoon.

Wie een brandkast heeft, heeft een zekere rust – want wat méér kun je doen, dan die stevige slot en grendel? Bij een digitaal apparaat zijn meer bedreigingen. Verlies, diefstal, of 'gehacked' worden. USB-sticks die onbedoeld achterblijven in het zijvak van een handtas. En niet iedereen voelt zich vertrouwd met de betreffende terminologie: *virus-scanner*, *encryptie*, *ZIP-bestand*, *.EXE bestand*, etc.

Een sluitend advies, of een omvattende uitleg is niet in enkele alinea's te geven. Het is wel een goed uitgangspunt om uw werkwijze zo eenvoudig (overzichtelijk) mogelijk te houden. Gebruik één laptop voor zakelijke (persoons)gegevens, en plaats daarop één beveiligde map met privacy-gevoelige bestanden. Investeer in de juiste hulpmiddelen voor het maken van back-ups, en wen aan een vaste routine bij het uitvoeren van handelingen die persoonsgegevens betreffen. En vraag als nodig herhaald om uitleg in eenvoudige termen, door iemand die wél vertrouwd is met de terminologie. Wen u aan om de bescherming van persoonsgegevens, en de integriteit van uw digitale apparatuur, te beschouwen als een van de grondvesten van uw praktijkvoering.

De afronding

Als u heeft besloten tot een bepaalde werkwijze, zijn er een aantal documenten waarmee u de invoering van de AVG formaliseert.

Het Register

In het eerder genoemde *Register* beschrijft u onder meer de door u gekozen werkwijze. Omdat u als therapeut omgaat met categorieën van bijzondere persoonsgegevens, geldt de plicht tot het opstellen en bijhouden van een Register ook voor u, en krijgt u geen vrijstelling vanwege de beperkte omvang van uw onderneming (in beginsel geldt de registerplicht voor bedrijven met meer dan 250 werknemers). In het Register beschrijft u verder onder meer op welke *grondslag* u de registratie van persoonsgegevens legitimeert, en, indien dit op basis van de toestemming van cliënten is, hoe u deze toestemming krijgt en registreert. U bent verder verplicht *wijzigingen* in uw werkwijze, en eventuele data-lekken te vermelden in het register.

Opmerking: als u uw werkwijze wijzigt, neem deze wijziging dan op zonder de beschrijving van de oorspronkelijke werkwijze te verwijderen uit het Register. Op deze manier kunt u zich beter verantwoorden bij geschillen die zijn gebaseerd op een eerdere werkwijze.

De Data Protection Impact Assessment (DPIA)

De DPIA (in het Nederlands *gegevensbeschermings-effectbeoordeling*) is een analyse van de privacy-risico's die uw verwerking van persoonsgegevens voor de betrokkenen kan betekenen, met als doel om maatregelen te nemen om die risico's te voorkomen of verkleinen. De AVG stelt dat u verplicht bent om een DPIA uit te voeren *als u voldoet aan tenminste 2 van 9 genoemde omstandigheden*. Voor therapeuten kunnen 2 omstandigheden als relevant worden beschouwd: u gaat om met een categorie gevoelige persoonsgegevens, en u heeft te maken met 'kwetsbare personen {...} waarbij er sprake is van afhankelijkheid tussen de verantwoordelijke en de betrokken personen'. Met deze laatste wordt met name kinderen bedoeld. Een van de argumenten hierbij is, dat kinderen minder goed kunnen inschatten wat het betekent als zij toestemming geven voor het verwerken van hun persoonsgegevens. Indien u veel kinderen behandelt, is het aan te bevelen een DPIA uit te voeren (zie ook 'Links'). *In dient in ieder geval in het Register een verantwoording op te nemen als u ervoor kiest om géén DPIA uit te voeren.*

Opmerking: Een DPIA kan ook nodig zijn als u een nieuw type verwerking van persoonsgegevens start, die mogelijk risico's met zich meebrengt voor de betrokkenen. Denk bijvoorbeeld aan de digitalisering van de (gedurende jaren) opgebouwde, en uitgebreide dossiers, uit te voeren door een externe dienstverlener. Is de conclusie na het uitvoeren van een DPIA dat er ondanks maatregelen risico's blijven bestaan, dan dient u de Autoriteit Persoonsgegevens vooraf te raadplegen.

Informeren en toestemming vragen

Voor het zowel *informeren* van uw (nieuwe en huidige) cliënten, als het vragen van hun *toestemming* voor de registratie van persoonsgegevens, kunt u één *informatie- en toestemmingsdocument* maken (dit is geen officiële term), dat u door deze cliënten laat ondertekenen. Geef een kopie, of een 2^e getekend exemplaar mee aan uw cliënt. Bewaar dit document goed – de *bewijslast* voor toestemming ligt namelijk bij uzelf als therapeut.

Een Privacy-statement op uw website

Op uw website plaatst u een Privacy-statement. Indien u geen website heeft, dient u uw voormalige cliënten te informeren op een andere wijze, via e-mail of schriftelijk. In het *Privacy-statement* beschrijft u (in meer algemene termen) hoe u te werk gaat met betrekking tot persoonsgegevens, welke rechten uw cliënten hebben ten aanzien van die gegevens, en hoe ze die kunnen uitvoeren. Ook kunt in een *Privacy-statement* de registratie van persoonsgegevens via een contactformulier formaliseren.

Overeenkomsten met verwerkers en mede-gegevensverantwoordelijken

U bent als therapeut(e) de *gegevensverantwoordelijke* met betrekking tot de persoonsgegevens die u verwerkt. Er komen echter situaties voor waarbij *anderen* eveneens toegang hebben tot deze persoonsgegevens. Bijvoorbeeld, als u een jubileumfeest organiseert, en de organisator (die u inhuurt) voor u de uitnodigingen aan uw voormalige en bestaande cliënten verzorgt. Of, als een (meestal groter) bedrijf de salarisadministratie van haar personeelsleden uitbesteedt. De AVG wet kent het begrip *verwerker*: een externe partij waaraan u als *gegevensverantwoordelijke* de opdracht geeft om een deel van uw persoonsgegevens te verwerken. Voor *verwerkers* gelden speciale voorschriften. Echter, er is alléén sprake van een *verwerker* als die opdracht *primair* gericht is op de verwerking van persoonsgegevens, zoals in het voorbeeld van de salarisadministratie. De evenementenorganisator die uw jubileumfeest verzorgt, is geen *verwerker*, maar een *mede-gegevensverantwoordelijke*.

Het onderscheid is in de praktijk niet altijd belangrijk. De AVG stelt dat u in het geval van een opdracht aan een *verwerker* een *verwerkingsovereenkomst* dient op te stellen. Echter, als u als gegevensverantwoordelijke persoonsgegevens deelt met een andere partij, blijft u *eindverantwoordelijk*, en daarom is het óók als er sprake is van een *medeverantwoordelijke* aan te bevelen om een en ander schriftelijk te regelen.

Maakt u bijvoorbeeld gebruik van een *webbouwer* voor uw website, en heeft deze toegang tot persoonsgegevens als verlengde van diens werkzaamheden (bijvoorbeeld als uw website een contactformulier bevat waarmee belangstellenden contact met u kunnen opnemen), dan dient de webbouwer als *medeverantwoordelijke* formeel te verklaren de integriteit van deze persoonsgegevens te bewaren (*geheimhoudingsplicht*), en met u samen te werken bij een coherente beveiliging van deze gegevens.

Nog een voorbeeld. U werkt nauw samen met een collega-therapeut, en u vat het plan op om aan uw (beider) cliënten een e-mail te sturen ter promotie van een gezamenlijk te geven workshop. Hiertoe wilt u een Excel bestand met alle namen en e-mailadressen aan uw collega geven, die de organisatie ter hand neemt (uiteraard is dit alleen toegestaan als u dit gebruik heeft omschreven in uw *verwerkingsdoelen*, en uw cliënten hiervoor toestemming hebben gegeven). U stelt een overeenkomst op met uw collega-therapeut, waarin onder meer staat welke gegevens u overdraagt, hoe deze door uw collega worden aangewend en beveiligd, en op welke termijn deze gegevens weer worden vernietigd. Pas daarna mag u de gegevens overdragen. NB.: Het betreft in dit geval dus geen *verwerkersovereenkomst*; maar in feite een overeenkomst waarmee u uw verplichting tot zorgvuldigheid nakomt.

Uw voormalige cliënten informeren.

De AVG is duidelijk als het gaat om persoonsgegevens die u *na* 25 mei 2018 verwerkt: u dient de betrokkenen hierover uitdrukkelijk te informeren, en de bewijslast van die informatieplicht ligt bij uzelf. Maar hoe zit het met de persoonsgegevens van voormalige cliënten? Van hen heeft u immers geen '*uitdrukkelijke toestemming*' voor het verwerken (beheren) van hun gegevens. Op dit moment is daar eigenlijk nog geen helder beeld over, en lijkt de interpretatie van de wet te zijn, dat een Privacy-statement (met een overzicht van de rechten van betrokkenen) op uw website voldoende is om voormalige cliënten te informeren. Dus (onder voorbehoud): u bent niet verplicht om al uw voormalige cliënten te benaderen, via e-mail of schriftelijk, om hen te informeren over de inhoud en het doel van uw verwerking van gegevens, of om hen te informeren over hun rechten. Voor wat betreft uw *huidige* cliënten geldt dat u vanaf 25 mei 2018 *alleen* nadere persoonsgegevens mag verwerken ná het voldoen aan uw informatieplicht, en het krijgen van hun uitdrukkelijke toestemming. U heeft met andere woorden geen toestemming met terugwerkende kracht nodig, maar mag de huidige dossiers alleen uitbreiden of wijzigen na informering en toestemming.

In de bijlagen vindt u enkele voorbeelddocumenten.

In de praktijk.

Als dit alles geregeld is, voldoet u aan de AVG. Tijdens uw praktijkvoering zal de uitvoering ervan vooral bestaan uit het laten tekenen van het informatie- en toestemmingsdocument door nieuwe cliënten, en het alert zijn op de veiligheid van de persoonsgegevens die u beheert. Ook dient u zich af te vragen of nieuwe toepassingen van deze persoonsgegevens *legitiem* zijn: bijvoorbeeld als u uw cliënten per post een kerstgroet wilt sturen.

U dient de *Autoriteit Persoonsgegevens* op de hoogte te stellen als u een '*data-lek*' constateert, bijvoorbeeld bij een diefstal van uw laptop, met daarop persoonsgegevens die niet beveiligd zijn met encryptie. In dat geval dient u ook de betrokkenen (cliënten) onverwijld op de hoogte te stellen, zodat deze maatregelen kunnen nemen om eventuele schade te voorkomen. Als u na het constateren van een data-lek maatregelen heeft kunnen nemen die schadelijke effecten hebben voorkomen, hoeft u de betrokkenen niet te informeren. Op de website van de *Autoriteit Persoonsgegevens* vindt u meer informatie.

De rechten van uw cliënten

Iedere persoon heeft, na de invoering van de AVG en de UAVG, bepaalde rechten ten aanzien van de persoonsgegevens die van hem of haar door een instantie of bedrijf worden verwerkt. Hieronder volgt een kort overzicht van de rechten van cliënten waarmee u als gegevensverantwoordelijke (naar verwachting) mee te maken kunt krijgen. Er zijn daarnaast aanvullende rechten, uitzonderingen en bepalingen die mogelijk van belang kunnen zijn. Deze kunt u, indien een cliënt gebruik wil maken van een recht en u twijfelt over de juiste handelswijze, nalezen in de handleiding AVG op de website van de Autoriteit Persoonsgegevens.

Indien u een verzoek tot uitoefening van een van deze rechten krijgt, dient u de aanvrager binnen één maand na aanvraag te informeren over uw besluit om het verzoek wel of niet in te willigen, en om welke reden(en).

Het recht op inzage

U bent verplicht gehoor te geven aan een verzoek van een cliënt, om *inzage* in de gegevens die u van deze cliënt heeft verwerkt. U kunt dit alleen weigeren als de frequentie van achtereenvolgende verzoeken onredelijk is. U mag geen kosten in rekening brengen, tenzij wordt gevraagd om meerdere kopieën. De overdracht mag schriftelijk of digitaal plaats vinden. Als het verzoek digitaal (per e-mail) is gedaan, dient u de gegevens digitaal aan te bieden. U hoeft geen inzage te bieden in uw '*persoonlijke werkaantekeningen*'. En uiteraard blijven verplichtingen op het gebied van het *beroepsgeheim* van kracht – u mag alleen inzage bieden als u zich heeft overtuigd van de identiteit van de aanvrager.

Het recht op verwijdering

Een cliënt kan u vragen om de persoonsgegevens te *verwijderen*. U bent verplicht hieraan gehoor te geven, omdat dit verzoek altijd gerechtigd is als uw gegevensverwerking gebaseerd is op de grondslag *toestemming*. U hoeft geen gegevens te verwijderen die u verplicht bent om te bewaren vanwege wettelijke verplichtingen zoals bijvoorbeeld die van de belastingdienst (bijvoorbeeld de informatie opgenomen in facturen).

Het recht op wijziging

Dit recht zal maar zelden relevant zijn voor een cliënt, maar desondanks dient u uw cliënten wel over dit recht te informeren. Als gegevensverantwoordelijke bent u verplicht om persoonsgegevens correct bij te houden. Een cliënt kan inzage eisen in zijn of haar persoonsgegevens, en vereisen dat u wijzigingen aanbrengt indien de cliënt de gegevens niet correct, of onvolledig acht. Dit formele recht zal vermoedelijk (!) betwistbaar zijn in het geval van (bijvoorbeeld) aantekeningen over een therapie-sessie, omdat deze kunnen worden beschouwd als 'afgeleide gegevens' (interpretaties, of conclusies die u als therapeut trekt op basis van de informatie van een cliënt).

Het recht op beperking

Ook dit recht zal zelden relevant zijn, maar ook hier dient u cliënten op dit recht te wijzen. Het recht houdt in dat u elke vorm van verwerking van de gegevens van een cliënt stopt, en deze gegevens ook 'isoleert' van uw reguliere werkwijze en systemen.

Het recht op het indienen van een klacht bij de toezichthouder

Iedereen heeft het recht om ten aanzien van de verwerking van persoonsgegevens een klacht in te dienen bij de Autoriteit Persoonsgegevens.

Goed om te weten.

U mag als therapeut (of als gegevensverantwoordelijke) geen gebruik maken van het BSN nummer van cliënten (tenzij u aan een aantal aanvullende voorwaarden voldoet, waaronder het voldoen aan de NEN 7510 beveiligingsstandaard).

De AVG en UAVG zijn niet van toepassing op personen die overleden zijn.

Als een cliënt materiële of immateriële schade heeft geleden als gevolg van een overtreding of nalatigheid in het kader van de AVG voor wat betreft uw verwerking van persoonsgegevens, dan heeft uw cliënt het recht om een *schadevergoeding* te ontvangen voor de geleden schade. Als verwerkingsverantwoordelijke bent u aansprakelijk voor de geleden schade.

Links

Als u zich verder wilt verdiepen in de AVG en de UAVG, dan is de *Handleiding AVG* op de website van de Autoriteit Persoonsgegevens een uitstekende bron. Deze handleiding van het Ministerie van Justitie en Veiligheid wordt ook regelmatig bijgewerkt.

Handleiding AVG:

<https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/handleidingalgemeneverordeninggegevensbescherming.pdf>

Wettekst AVG in het Nederlands:

https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/verordening_2016_-_679_definitief.pdf

Wetsvoorstel UAVG:

<https://www.rijksoverheid.nl/binaries/rijksoverheid/documenten/kamerstukken/2017/12/13/wetsvoorstel-uitvoeringswet-algemene-verordening-gegevensbescherming/Wetsvoorstel+Uitvoeringswet+Algemene+verordening+gegevensbescherming.pdf>

Het uitvoeren van een DPIA (*Data Protection Impact Assessment*):

<https://autoriteitpersoonsgegevens.nl/nl/onderwerpen/avg-nieuwe-europese-privacywetgeving/data-protection-impact-assessment-dpia#op-welke-manier-moet-ik-een-dpia-uitvoeren-5885>

Bijlage

Voorbeeldimplementatie

Documenten AVG en UAVG.

In deze voorbeelddocumenten wordt beschreven hoe een (denkbeeldige) therapeute *Anna* de wetgeving in het kader van de AVG en de UAVG heeft verwerkt in haar praktijkvoering.

De 3 documenten *Register*, *Informatie- en toestemmingsdocument* en *Privacy-statement* (voor publicatie op een website) bevatten een aantal overeenkomstige onderdelen. Om redenen van eenvoud is zoveel mogelijk geprobeerd deze in ieder document gelijk te laten zijn, op enkele details na.

In het (openbare) *Privacy-statement* is ervoor gekozen om slechts in *algemene* termen te beschrijven welke gegevens worden geregistreerd, om redenen van privacy en veiligheid.

Bij deze documenten vindt u geen *verwerkersovereenkomst*. Partijen en dienstverleners die door de wet aangemerkt worden als *verwerker* zullen deze vaak voorhanden hebben, als een dergelijke overeenkomst nodig is. Wel is er een voorbeeld opgenomen van een overeenkomst die u kunt gebruiken als u een deel van uw persoonsgegevens in handen geeft van een andere partij, zonder dat deze partij als verwerker kan worden aangemerkt.

Deze documenten zijn met aandacht samengesteld, maar u kunt er geen rechten aan ontleen in de zin van gegarandeerde rechtsgeldigheid. © 2018 Primagine Online Communicatie. Voor dienstverlening en advies op het gebied van de AVG en online marketing (bijvoorbeeld websites en fotografie) zie www.primagine.nl.

Register

Zoals bedoeld in de Algemene Verordening Gegevensbescherming en de Uitvoeringswet AVG.

Anna Jansen, Praktijk voor Regressietherapie, Stationsweg 1, 1772 AB Gelderdorp,
mobiel: 06 12345678, e-mail info@annajansen.nl, KvK 1288819.

1. Welke persoonsgegevens ik verwerk, en met welk doel.

Als therapeute verwerk ik de volgende persoonsgegevens:

(G1) Basis-persoonsgegevens van cliënten

Ik registreer de volgende gegevens: naam, adres, telefoonnummer, e-mailadres, geboortedatum, geslacht, verzekeringsnummer ziektekostenverzekering, contactgegevens contactpersoon bij nood (naam, telefoonnummer). Ik verzamel deze gegevens ten behoeve van het onderhouden van contact per telefoon en e-mail, het bezoeken van cliënten, het opstellen van facturen, en het bijhouden van een digitale afsprakenagenda.

De contactgegevens gebruik ik tevens voor het per e-mail benaderen van cliënten met informatie en eventueel aanbiedingen die zijn gerelateerd aan het aandachtsgebied van de therapieën die ik geef.

(G2) Behandel- en medische voorgeschiedenis

Ik informeer bij cliënten over hun (globale) medische en therapeutische voorgeschiedenis, en maak daarover notities. Het doel hiervan is het bijdragen aan de veiligheid tijdens de therapie, en een mogelijk inhoudelijke bijdrage aan de therapie zelf.

(G3) Persoonlijke geschiedenis, gevoelens, overtuigingen etc.

Tijdens sessies met cliënten komen veel persoonlijke en emotionele onderwerpen aan bod. Ik kan hierover aantekeningen maken in een 'sessie-verslag'. Deze verslagen zijn gericht op de inhoudelijke continuïteit en ontwikkeling van de therapie.

(G4) Bezoekgegevens, e-maildialoog en telefonische contacthistorie

Ik registreer afspraken met cliënten in een digitale behandelagenda. Ik e-mail met cliënten via het e-mailadres info@annajansen.nl. Deze e-mails worden opgeslagen op de e-mailserver van het domein annajansen.nl. Op mijn mobiele telefoon wordt de contacthistorie (telefonisch) bijgehouden.

2. Wettelijke grondslag voor de registratie.

Ik ben als therapeute gerechtigd in de zin van de wet AVG (*Algemene Verordening Persoonsgegevens*) om persoonsgegevens van cliënten te registreren op de grondslag dat ik cliënten hiervoor middels een document uitdrukkelijk toestemming voor vraag. Cliënten kunnen deze toestemming op elk moment herroepen, waarvan zij mij dan op de hoogte dienen te stellen. De formele toestemming verkrijg ik door het laten ondertekenen van een *informatie- en toestemmingsdocument*, waarin ik cliënten tevens wijs op hun rechten ten aanzien van de registratie van persoonsgegevens. Cliënten ontvangen een kopie van dit document na ondertekening.

3. Werkwijze bij het registreren en bewaren van persoonsgegevens.

Bij mijn registratie van persoonsgegevens hanteer ik de volgende bewaarlocaties:

(L1) Een brandkast (classificatie CEN-2, praktijkadres);

(L2) Een stalen, afsluitbare archiefkast (praktijkadres);

(L3) Een Lenovo laptop met Windows, met een harddisk met een met encryptie beveiligde *data-map*.

(L4) Een Lacie externe harddisk (met encryptie)

(L5) Een HP Windows Phone met Windows Mobile 10 met encryptie.

Ik hanteer de volgende bestanden die persoonsgegevens bevatten, en bewaar (en beveilig) deze op de volgende wijze:

(B1) *'Basisdocumenten cliënten'*. Per cliënt vorm ik één dossier op papier, met de gegevens genoemd bij G1 en G2. De getekende verklaringen voor het geven van toestemming door cliënten voor de registratie van persoonsgegevens bewaar ik bij deze dossiers. De basisdocumenten bewaar ik in een brandkast (L1).

(B2) *'Sessieverslagen'*. Deze verslagen (op papier) zijn via *pseudonimisering* via een verwijfsnummer gekoppeld aan de basisdocumenten (B1). Ik bewaar deze in een stalen kast (L2), of, indien ik oordeel dat informatie uit een verslag identificerend dan wel extra gevoelig is, in de brandkast.

(B3) *Een digitaal 'overzichtsbestand'*. Ik neem een aantal gegevens van alle basisdocumenten over in één Excel bestand. Dit bestand vormt een (minimale) digitale back-up van de papieren basisdocumenten (B1), en gebruik ik daarnaast voor het raadplegen van contactgegevens onderweg. Het bestand werk ik bij op de laptop (L3). Kopieën bevinden zich op L4 en L5.

(B4) *Een digitale agenda met behandelafspraken, e-mails in de mappen bij het e-mailadres info@annajansen.nl, en de contacthistorie telefoon*. Deze gegevens worden deels automatisch geregistreerd, en ten dele gesynchroniseerd tussen mijn laptop en telefoon. De beveiliging bestaat uit *encryptie* (en zorgvuldigheid). Laptop (L3): Regelmatig kies ik een nieuw wachtwoord voor mijn inlog-account. Alle persoonsgegevens bevinden zich in een met encryptie (AES-256) beveiligde data-map. Ik gebruik deze laptop *alleen* voor mijn praktijkvoering. Ik bewaar de laptop 's nachts en bij afwezigheid (als ik de laptop niet mee neem) in de brandkast. Telefoon (L5): De telefoon is beveiligd met een PIN-code en/of vingerafdrukherkenning, *file-encryptie* en met een beveiliging ten behoeve van het wissen van gegevens bij diefstal of vermissing.

(B5) *Facturen*. Deze facturen bevatten de meeste gegevens genoemd bij G1 en ik bewaar deze in een met encryptie beveiligde map op L4 en L5.

4. ***Argumenten voor het achterwege laten van een DPIA (Data Protection Impact Assessment).***

In mijn praktijk behandel ik weliswaar incidenteel kinderen, maar voorafgaande aan de behandeling bespreek ik deze behandeling, en aspecten van privacy, uitgebreid met de ouders of verzorgers. Bij het verkrijgen van toestemming voor het verwerken van persoonsgegevens laat ik de ouders/verzorgers bovendien tekenen voor deze toestemming.

Informatie- en toestemmingsdocument

Anna Jansen, Praktijk voor Regressie-therapie, Stationsweg 1, 1772 AB Gelderdorp
Mobiel 06 12345678, e-mail info@annajansen.nl

Dit document betreft de persoonsgegevens welke (mogelijk) door mij worden verwerkt tijdens het geven van therapie aan u als cliënt

1. **Welke persoonsgegevens ik verwerk, en met welk doel.**

Als therapeute verwerk ik de volgende persoonsgegevens:

Basis-persoonsgegevens van cliënten

Ik registreer de volgende gegevens: *naam, adres, telefoonnummer, e-mailadres, geboortedatum, geslacht, verzekeringsnummer ziektekostenverzekering, contactgegevens contactpersoon bij nood (naam, telefoonnummer)*. Ik verzamel deze gegevens ten behoeve van het onderhouden van contact per telefoon en e-mail, het bezoeken van cliënten, het opstellen van facturen, en het bijhouden van een digitale afsprakenagenda. De contactgegevens gebruik ik tevens voor het per e-mail benaderen van cliënten met informatie en eventueel aanbiedingen die zijn gerelateerd aan het aandachtsgebied van de therapieën die ik geef. Ik verstrek geen persoonsgegevens aan derden, anders dan ter ondersteuning van één van de bovenstaande doelen.

Behandel- en medische voorgeschiedenis

Ik informeer bij cliënten over hun (globale) medische en therapeutische voorgeschiedenis, en kan hierover aantekeningen maken. Het doel hiervan is het bijdragen aan de veiligheid tijdens de therapie, en een mogelijk inhoudelijke bijdrage aan de therapie zelf.

Persoonlijke geschiedenis, gevoelens, overtuigingen etc.

Tijdens sessies met cliënten komen veel persoonlijke en emotionele onderwerpen aan bod. Ik kan hierover aantekeningen maken in een 'sessie-verslag'. Deze verslagen zijn gericht op de inhoudelijke continuïteit en ontwikkeling van de therapie.

Bezoekgegevens, e-maildialoog en telefonische contacthistorie

Ik registreer afspraken met cliënten in een digitale behandelagenda. Ik e-mail met cliënten via het e-mailadres info@annajansen.nl. Deze e-mails worden opgeslagen op de e-mailserver van het domein annajansen.nl. Op mijn mobiele telefoon wordt de contacthistorie (telefonisch) bijgehouden.

2. **Wettelijke grondslag voor de registratie**

Ik ben als therapeute gerechtigd in de zin van de wet AVG (Algemene Verordening Persoonsgegevens) om uw persoonsgegevens te registreren en verwerken op de grondslag dat ik u hiervoor middels dit document uitdrukkelijk toestemming voor vraag. U kunt deze toestemming op elk moment herroepen, waarvan u mij dan op de hoogte dient te stellen.

2b. U bent uiteraard niet verplicht om gegevens aan mij te verstrekken. Voor het uitvoeren van de overeenkomst voor het geven van therapie zijn echter *enkele gegevens* noodzakelijk te noemen. Dit betreft uw naam en adres, ten behoeve van de facturatie, en uw geboortedatum, ten behoeve van dit document. Indien u de facturen voor de therapie (deels) wilt declareren bij uw zorgverzekeraar, is uw geboortedatum, uw sekse en een verzekeringsnummer eveneens noodzakelijk. U kunt voor wat betreft de overige genoemde informatie aangeven dat u niet wilt dat deze in enigerlei wijze, schriftelijk of digitaal door mij wordt geregistreerd. Dit kunt u onderaan dit document aangeven.

3. **Bewaartermijn**

Een deel van de persoonsgegevens *bewaar* ik tenminste 10 jaar, voortvloeiende uit mijn verplichtingen aan de belastingdienst. De overige informatie kan ik minimaal 15 jaar bewaren, vanuit het door mijn beroepsvereniging aangegeven advies ter ondersteuning van eventuele geschillen over de behandeling. Ik kan echter oordelen dat het bewaren van de informatie niet noodzakelijk is.

4. Voorzorgsmaatregelen ten aanzien van de veiligheid (privacy) van gegevens.

Het is niet alleen mijn wettelijke plicht, maar ook mijn uitdrukkelijke intentie om bij de verwerking van uw persoonsgegevens zorgvuldig en veilig te handelen, binnen de grenzen van redelijkheid ten aanzien van de inspanningen en investeringen die ik hiervoor kan doen. Voor wat betreft documenten en aantekeningen op papier tref ik voorzorgsmaatregelen op het gebied van brand, waterschade, verlies en diefstal. Bij digitale, en eventueel geautomatiseerd verwerkte gegevens tref ik aanvullende beschermingsmaatregelen tegen data-verlies door apparatuur-defecten, ongeoorloofde inzage ('hacken') en diefstal of verlies van apparatuur. Indien de veiligheid en integriteit van de informatie voor u redenen tot zorg zijn, dan kan ik u op verzoek nader informeren over de genoemde veiligheidsmaatregelen.

5. Uw rechten ten aanzien van de verwerking van persoonsgegevens

In het overzicht hieronder vermeld ik een aantal rechten die u heeft. Een volledig overzicht, en aanvullende bepalingen kunt u vinden op de website van de *Autoriteit Persoonsgegevens*.

Het recht op inzage

U heeft het recht om inzage te vragen in uw persoonsgegevens, en de informatie over de therapie, die ik heb geregistreerd. De frequentie van verzoeken hiertoe dient redelijk te zijn. Ik breng u hiervoor geen kosten in rekening. U kunt vragen om een schriftelijke, of digitale inzage in uw gegevens.

Het recht op verwijdering

U heeft het recht om uw persoonsgegevens, en de informatie over de therapie, die ik heb geregistreerd, te laten verwijderen, uitgezonderd de gegevens die ik vanuit andere wettelijke verplichtingen dien te bewaren (bijvoorbeeld gegevens op facturen), of gegevens die ik op basis van voorschriften van mijn beroepsvereniging(en) en/of geschillencommissies dien te bewaren.

Het recht op wijziging

Indien u het vermoeden heeft dat uw gegevens die ik verwerk niet correct zijn, dan wel incompleet, kunt u een verzoek indienen tot wijziging of aanvulling van deze gegevens.

Het recht op beperking

U heeft het recht om te eisen dat ik als therapeute elke verwerking (wijziging, aanvulling etc.) van uw gegevens staak, en de gegevens isoleer van de reguliere verwerking van gegevens, handmatig of geautomatiseerd.

Het recht op het indienen van een klacht bij de toezichthouder

U heeft het recht om ten aanzien van mijn verwerking van uw persoonsgegevens een klacht in te dienen bij de Autoriteit Persoonsgegevens.

Het recht op het op elk moment intrekken van deze toestemming.

U heeft het recht deze toestemming te *herroepen*. Vanaf dat moment mag ik als therapeut uw persoonsgegevens niet meer gebruiken, en geen nieuwe persoonsgegevens van u verwerken.

Indien u een verzoek aan mij richt in het kader van een van de bovenstaande rechten, ontvangt u binnen één maand een reactie op uw verzoek.

Verklaring van uw toestemming.

Hierbij verklaar ik,

Naam:

Geboortedatum:

.....

.....

en eventueel mede-ouder of verzorger:

Naam:

Geboortedatum:

.....

.....

Dat ik dit document heb ontvangen en aldus ben geïnformeerd over de verplichtingen van Anna Jansen, Praktijk voor Regressie-therapie ten aanzien van de verwerking van persoonsgegevens voortvloeiende uit een overeenkomst voor het volgen van therapie.

- ☐ *Ik geef hierbij vrij en uitdrukkelijk toestemming voor de verwerking van de persoonsgegevens zoals die hierboven in paragraaf 1 zijn beschreven.*
- ☐ *Ik geef hierbij (vrij en uitdrukkelijk) alléén toestemming voor de verwerking van de volgende persoonsgegevens:*
 - ☐ *Naam, adres en geboortedatum.*
 - ☐ *De verdere gegevens die noodzakelijk zijn om te vermelden op facturen in verband met de (gedeeltelijke) vergoeding van de therapie door een zorgverzekeraar.*
- ☐ *Ik geef toestemming voor het gebruik van de contactgegevens om mij per e-mail of per post te benaderen met informatie die inhoudelijk aansluit bij de therapie.*
- ☐ *Ik geef deze toestemming vrij en uitdrukkelijk in relatie tot de persoonsgegevens van een kind, in mijn hoedanigheid als ouder/verzorger van (naam en geboortedatum):*

.....

(Hierboven aankruisen wat van toepassing is. Let op: er mogen geen vakjes geselecteerd zijn vóórdat u dit document heeft ontvangen ter ondertekening).

Plaats:

Datum:

.....

.....

Handtekening:

Handtekening mede-ouder of verzorger:

.....

.....

Privacy-statement

Inleiding

Indien u in mijn praktijk therapie volgt, registreer en verwerk ik bepaalde persoonsgegevens. Dit gaat om basisgegevens (zoals naam en adres), en bijvoorbeeld gegevens ten behoeve het opstellen van facturen. Ook kan het gaan om informatie over de voorgeschiedenis van therapeutische en medische behandelingen. Daarnaast komen tijdens een therapie ook andere, zeer persoonlijke en ook privacy-gevoelige zaken aan de orde. Ik kan hierover aantekeningen maken, gericht op de inhoudelijke continuïteit en ontwikkeling van de therapie.

Daarnaast kan het voorkomen dat ik de (contact)gegevens gebruik om u per e-mail of schriftelijk te informeren over onderwerpen die zijn gerelateerd aan de therapie die ik geef. Dit doe ik alleen als u hiervoor toestemming geeft (zie hieronder).

Ik verstrek uw persoonsgegevens niet aan een andere partij, met uitzondering van situaties waarin ik de ondersteuning van een andere partij vraag bij het u aanbieden van toepasselijke informatie, zoals hierboven genoemd. In dat geval zal het *nooit* gaan om bijzondere persoonsgegevens zoals medische gegevens, of persoonlijke, emotionele informatie. Als therapeute ben ik gebonden aan het *beroepsgeheim*.

Toestemming

Bij aanvang van de therapie ontvangt u een document met nadere informatie over de persoonsgegevens die ik registreer en verwerk, en kunt u (via ondertekening van dat document) aangeven of u hiervoor toestemming geeft. Uw toestemming vormt voor mij de (wettelijke vereiste) grondslag voor de registratie van uw persoonsgegevens. U kunt er ook voor kiezen om een beperkte toestemming te geven voor de registratie van slechts enkele, voor de uitvoering van de behandelovereenkomst noodzakelijke gegevens. U kunt deze (gehele of gedeeltelijke) toestemming op ieder moment weer intrekken. Ik mag uw persoonsgegevens dan niet meer gebruiken, en geen nieuwe persoonsgegevens meer van u verwerken.

Heeft u in het verleden therapie gevolgd in mijn praktijk? En wilt u meer informatie over de persoonsgegevens die tijdens die therapie zijn geregistreerd? Neem dan contact met mij op.

De Autoriteit Persoonsgegevens

Tijdens het verwerken van persoonsgegevens volg ik de voorschriften zoals deze zijn bepaald in de wet *Algemene Verordening Gegevensbescherming* (AVG) en het wetsvoorstel *Uitvoeringswet AVG*. Dat betekent onder meer dat ik uiterste zorgvuldigheid betracht bij het verwerken en bewaren van persoonsgegevens, en voor zowel de rechtmatigheid als de beveiliging van deze verwerking onder het toezicht sta van de *Autoriteit Persoonsgegevens*.

Uw rechten

U heeft, als betrokkene, ten aanzien van de registratie van uw persoonsgegevens een aantal rechten. Hieronder volgt een kort overzicht van enkele belangrijke rechten. Een volledig overzicht van uw rechten, en aanvullende bepalingen, kunt u vinden op de website van de *Autoriteit Persoonsgegevens*.

Het recht op inzage

U heeft het recht om inzage te vragen in de persoonsgegevens die ik tijdens de therapie heb geregistreerd. U kunt vragen om een schriftelijke, of digitale inzage in uw gegevens.

Het recht op verwijdering

U heeft het recht om uw persoonsgegevens die ik heb geregistreerd te laten verwijderen, uitgezonderd de gegevens die ik vanuit andere wettelijke verplichtingen dien te bewaren (bijvoorbeeld gegevens op facturen), of gegevens die ik op basis van voorschriften van mijn beroepsvereniging(en) en/of geschillencommissies dien te bewaren.

Het recht op wijziging

Indien u het vermoeden heeft dat uw persoonsgegevens die ik verwerk niet correct zijn, dan wel incompleet, kunt u een verzoek indienen tot wijziging of aanvulling van deze gegevens.

Het recht op beperking

U heeft het recht om te eisen dat ik als therapeute (tijdelijk of permanent) elke verwerking (wijziging, aanvulling en toepassing etc.) van uw gegevens staak.

Het recht op het indienen van een klacht bij de toezichthouder

U heeft het recht om ten aanzien van mijn verwerking van uw persoonsgegevens een klacht in te dienen bij de Autoriteit Persoonsgegevens.

Bewaartermijn

Een deel van de persoonsgegevens *bewaar* ik tenminste 10 jaar, voortvloeiende uit mijn verplichtingen aan de belastingdienst. De overige informatie kan ik minimaal 15 jaar bewaren, vanuit het door mijn beroepsvereniging aangegeven advies ter ondersteuning van eventuele geschillen over de behandeling. Ik kan echter oordelen dat het bewaren van de informatie niet noodzakelijk is.

Uitnodiging

De bescherming van uw privacy is voor mij erg belangrijk. En ook, of u zich als cliënt prettig en zeker voelt bij de manier waarop ik omga met toch zeer persoonlijke informatie. De bescherming van persoonsgegevens is sinds 25 mei 2018 nadrukkelijk(er) geregeld dan voorheen via de *Algemene Verordening Gegevensbescherming* (AVG), en dat betekent meer waarborgen, en meer rechten voor u. Toch is 'privacy' meer dan alleen de handhaving van regels. Ik nodig u daarom van harte uit om, indien u hierover vragen, opmerkingen of wensen heeft, hierover contact met mij op te nemen.

Overeenkomst met betrekking tot de verwerking van persoonsgegevens

De ondergetekenden:

Anna Jansen, Praktijk voor Regressie-therapie, Stationsweg 1, 1772 AB Gelderdorp
(hierna te noemen: HV (Hoofd-gegevensverantwoordelijke),

en

W. Kregmeyer, Worldwider Websites, stationsweg 2, 2388 HK Brabantstad
(hierna te noemen: MV (Mede-gegevensverantwoordelijke),

Gezamenlijk te noemen: *partijen*, komen overeen, met inachtneming van de begrippen zoals omschreven in artikel 3:

Artikel 1. Overzicht

1.1

De overeenkomst is gebaseerd op een rolverdeling waarbij HV op hoofdlijnen, qua intentie en doelstelling, vast stelt welke persoonsgegevens zullen worden verwerkt, en waarbij MV deze verwerking op detailniveau inricht, in goed vertrouwen handelend naar de intentie en doelstellingen van HV.

1.2

HV stelt een aantal persoonsgegevens waarvoor HV gegevensverantwoordelijk is in de zin van de AVG, ter beschikking aan MV, en/of verleent toestemming voor de verwerving, en/of het beheer en/of de verwerking van persoonsgegevens waarvoor HV gegevensverantwoordelijk is, ten behoeve van de tijdelijke verwerking van die persoonsgegevens. Aangezien MV in de zin van de AVG niet als 'verwerker' kan worden aangeduid, is MV eveneens gegevensverantwoordelijk, vanaf het moment van overdracht, voor deze persoonsgegevens.

1.3

Deze overeenkomst treedt in werking op het moment waarop deze door partijen is ondertekend, en eindigt nadat MV alle persoonsgegevens heeft gewist of terugbezorgd. MV verplicht zich de persoonsgegevens te wissen, terug te bezorgen of maatregelen te nemen die de toegang van MV tot deze persoonsgegevens voorkomt, indien HV aangeeft de samenwerking te willen beëindigen.

Artikel 2. Waarborgen

2.1

MV verplicht zich te streven naar de toepassing van passende technische en organisatorische maatregelen, opdat de verwerking aan de vereisten van de AVG voldoet en de bescherming van de rechten van de betrokkenen is gewaarborgd. MV verplicht zich tevens om te streven naar het voldoen aan de vereisten van de toepasselijke wet- en regelgeving betreffende de verwerking van persoonsgegevens. MV zal, indien daartoe verzocht door HV, aanvullende beschermingsmaatregelen treffen.

2.2

MV zal de persoonsgegevens niet ter beschikking stellen aan derden zonder toestemming van HV, en hanteert (voor zichzelf, en voor alle aan MV verbonden medewerkers) een *geheimhoudingsplicht* ten aanzien van deze gegevens.

2.3

MV ondersteunt HV bij het faciliteren van de rechten van betrokkenen voor zover deze betrekking hebben op de persoonsgegevens die MV vanuit de opdracht van HV verwerkt. MV ondersteunt HV bij het indien nodig aantonen van het uitoefenen van de benodigde zorgvuldigheid ten aanzien van de verwerking van persoonsgegevens, bij een audit, of onderzoek door de Autoriteit Persoonsgegevens.

2.4

MV informeert HV zonder onredelijke vertraging als MV kennis neemt van de onrechtmatige verwerking van persoonsgegevens of een inbreuk op de beveiligingsmaatregelen. MV ondersteunt tevens HV bij het melden van deze inbreuk aan de Autoriteit Persoonsgegevens en de betrokkenen.

Artikel 3. Begrippen

3.1

Betrokkenen: de personen op wie de persoonsgegevens betrekking hebben.

3.2

AVG: de wetgeving *Algemene Verordening Gegevensbescherming* en de daarbij geldende bepalingen van het wetsvoorstel *Uitvoeringswet AVG*.

3.3

Inbreuk: een inbreuk op de beveiliging die per ongeluk of op onrechtmatige wijze leidt tot de vernietiging, het verlies, de wijziging of de ongeoorloofde verstrekking van of de ongeoorloofde toegang tot doorgezonden, opgeslagen of anderszins verwerkte persoonsgegevens.

3.4

Verwerking: een bewerking of een geheel van bewerkingen met betrekking tot persoonsgegevens, of een geheel van de persoonsgegevens, al dan niet uitgevoerd via geautomatiseerde procedés, zoals het verzamelen, vastleggen, ordenen, structureren, opslaan, bijwerken of wijzigen, opvragen, raadplegen, gebruiken, verstrekken door middel van doorzending, verspreiding of op andere wijze ter beschikking stellen, aligneren of combineren, afschermen, wissen of vernietigen.

Aldus overeengekomen en in tweevoud ondertekend,

Gelderdorp, 25 mei 2018,

Anna Jansen, Praktijk voor Regressie-therapie

Brabantstad, 25 mei 2018,

W. Kregmeyer, Worldwider Websites

.....

.....