VERWERKERSOVEREENKOMST

Samenvatting
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. 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 Praktijk Vitalution moet voldoen omdat gegevens worden vastgelegd 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.
- Het bijhouden van een register van datalekken die zijn opgetreden.
- Het aantonen dat een cliënt daadwerkelijk toestemming heeft gegeven voor het vastleggen van gegevens in het cliëntendossier.

Privacy
Voor een goede behandeling is het noodzakelijk dat Praktijk Vitalution een dossier aanlegt. Dit is ook een wettelijke plicht opgelegd door de WGBO. Het dossier bevat aantekeningen over de gezondheidstoestand van de cliënt en gegevens over de behandelingen. Ook kunnen in het dossier gegevens opgenomen zijn die voor de behandeling noodzakelijk zijn en die na expliciete toestemming van de cliënt zijn opgevraagd bij een andere zorgverlener. Praktijk Vitalution doet haar uiterste best om de privacy van de cliënt te waarborgen. Dit betekent onder meer dat zij:

- Zorgvuldig omgaat met persoonlijke en medische gegevens.
- Ervoor zorgt dat onbevoegden geen toegang hebben tot gegevens van de cliënt.
- Als therapeut als enige toegang heeft tot de gegevens in het dossier van de cliënt.
- Een wettelijke geheimhoudingsplicht (beroepsgeheim) heeft.

De gegevens uit het cliëntendossier kunnen ook voor de volgende doelen gebruikt worden:

- Bij een verwijzing naar een andere behandelaar. Dit gebeurt alleen met expliciete toestemming van de cliënt.
- Voor het gebruik voor waarneming, tijdens afwezigheid van de therapeut, zoals bij ziekte, verlof of vakantie.
- Voor het geanonimiseerde gebruik tijdens intercollegiale toetsing.
- Een klein deel van de gegevens uit het dossier wordt gebruikt voor de financiële administratie, zodat facturen opgesteld kunnen worden.
- Wanneer Praktijk Vitalution vanwege een andere reden gebruik wil maken van cliëntengegevens, dan zal zij eerst de betreffende cliënt informeren en expliciet om toestemming vragen.

Deze gegevens in het cliëntendossier blijven, zoals in de wet op de behandelovereenkomst wordt vereist, 15 jaar bewaard. Bij minderjarigen gaat dit bewaartermijn in vanaf 18 jaar.

De verwerkersovereenkomst

De ondergetekenden:

De cliënt (hierna: "Verwerkingsverantwoordelijke"); en Praktijk Vitalution, gevestigd aan Orion 45, 2665 WB te Bleiswijk en ingeschreven in het register van de Kamer van Koophandel onder nummer 57660131, in deze rechtsgeldig vertegenwoordigd door Marijke Moes, Praktijkhouder (hierna: "Verwerker"). Hierna gezamenlijk ook aan te duiden als: "Partijen" en afzonderlijk als "Partij".

Overwegende dat:

Verwerker diensten verricht ten behoeve van Verwerkingsverantwoordelijke, zoals beschreven in de in Bijlage 1 omschreven overeenkomsten.
De diensten meebrengen dat Persoonsgegevens worden verwerkt, waaronder gegevens betreffende de gezondheid.
Verwerker de betreffende gegevens louter in opdracht van Verwerkingsverantwoordelijke verwerkt en niet voor eigen doeleinden.
Per 25 mei 2018 van toepassing zal zijn Verordening (EU) 2016/679 van het Europees Parlement en de Raad van 27 april 2016 (Algemene verordening gegevensbescherming).
Partijen in deze Verwerkersovereenkomst de afspraken met betrekking tot de verwerking van Persoonsgegevens in het kader van de diensten wensen vast te leggen.
Deze Verwerkersovereenkomst, indien van toepassing, alle eerdere Overeenkomst(en) van gelijke strekking tussen Partijen vervangt.

Verklaren te zijn overeengekomen als volgt:

Artikel 1. Definities

1.1 In deze Verwerkersovereenkomst wordt onder de volgende met een hoofdletter aangeduide begrippen het volgende verstaan:

Algemene Verordening Gegevens Bescherming of AVG
Algemene Verordening Gegevens Bescherming of AVG Verordening (EU) 2016/679 van het Europees Parlement en de Raad van 27 april 2016 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens en tot intrekking van Richtlijn 95/46/EG.

Betrokkene
Een geïdentificeerde of identificeerbare natuurlijke persoon (artikel 4 sub 1 AVG).

Derde
Een derde als bedoeld in artikel 4 sub 10 AVG.

Functionaris voor de Gegevensbescherming
Een functionaris als bedoeld in artikel 37 e.v. AVG.

Incident
Een klacht of (informatie)verzoek van een Betrokkene met betrekking tot de verwerking van Persoonsgegevens door Verwerker;
Een onderzoek naar of beslaglegging door overheidsfunctionarissen op de Persoonsgegevens of een vermoeden dat dit gaat plaatsvinden;
Een inbreuk in verband met Persoonsgegevens als bedoeld in artikel 4 onder 12 AVG;
Iedere ongeautoriseerde toegang, verwijdering, verminking, verlies of enige andere vorm van onrechtmatige verwerking van de Persoonsgegevens.

Medewerker
De door Partijen voor de uitvoering van deze Verwerkersovereenkomst betrokken natuurlijke persoon die werkzaam is bij of voor een van de Partijen.

Overeenkomst(en)
De in Bijlage 1 vermelde overeenkomst(en) betreffende de levering van producten en/of diensten.

Partij
Verwerkingsverantwoordelijke of Verwerker.

Partijen
Verwerkingsverantwoordelijke en Verwerker.

Persoonsgegevens
Alle informatie over een geïdentificeerde of identificeerbare natuurlijke persoon in de zin van artikel 4 onder 1 AVG.

Subverwerker
Iedere niet-ondergeschikte derde partij die door Verwerker is betrokken bij de verwerking van Persoonsgegevens in het kader van de Overeenkomst, niet zijnde Medewerkers.

Verwerker
De verwerker als bedoeld in artikel 4 sub 8 AVG.

Verwerkersovereenkomst
De onderhavige overeenkomst.

Verwerkingsverantwoordelijke
De verwerkingsverantwoordelijke als bedoeld in artikel 4 sub 7 AVG.

Wet bescherming persoonsgegevens of Wbp
Wet van 6 juli 2000, houdende regels inzake de bescherming van persoonsgegevens (Wet bescherming persoonsgegevens), inclusief latere wijzigingen.

1.2 Voornoemde en overige begrippen worden geïnterpreteerd overeenkomstig de AVG. Tot aan 25 mei 2018 worden begrippen geïnterpreteerd overeenkomstig de vergelijkbare bepaling uit de Wbp.

1.3 Waar in deze Verwerkersovereenkomst naar bepaalde normen wordt verwezen (zoals NEN7510) wordt daarmee steeds gedoeld op de meest actuele versie daarvan. Voor zover de betreffende norm niet meer wordt onderhouden, dient in de plaats daarvan de meest actuele versie van de logische opvolger van de betreffende norm gelezen te worden.

Artikel 2. Onderwerp van deze Verwerkersovereenkomst

2.1 Deze Verwerkersovereenkomst heeft betrekking op de verwerking van Persoonsgegevens door Verwerker in opdracht van de Verwerkingsverantwoordelijke in het kader van de uitvoering van de Overeenkomst(en).

2.2 Deze Verwerkersovereenkomst maakt onverbrekelijk deel uit van de Overeenkomst(en). Voor zover het bepaalde in de Verwerkersovereenkomst strijdig is met het bepaalde in de Overeenkomst(en), prevaleren de Algemene Voorwaarden van Verwerker.

Artikel 3. Uitvoering verwerking

3.1 Verwerker garandeert dat hij ten behoeve van Verwerkingsverantwoordelijke uitsluitend Persoonsgegevens zal verwerken voor zover:

Dit nodig is voor de uitvoering van de Overeenkomst; of
Verwerkingsverantwoordelijke daartoe nadere schriftelijke instructies heeft gegeven;
3.2 Verwerker zal alle redelijke instructies van Verwerkingsverantwoordelijke in verband met de verwerking van de Persoonsgegevens opvolgen. Verwerker stelt Verwerkingsverantwoordelijke op de hoogte indien naar zijn oordeel instructies in strijd zijn met de toepasselijke wetgeving met betrekking tot de verwerking van Persoonsgegevens.

3.3 Onverminderd het bepaalde in het eerste lid van dit artikel 3, is het Verwerker toegestaan om Persoonsgegevens te verwerken indien een wettelijk voorschrift (waaronder begrepen daarop gebaseerde rechterlijke of bestuurlijke bevelen) hem tot een verwerking verplicht. In dat geval stelt de Verwerker voorafgaand aan de verwerking Verwerkingsverantwoordelijke in kennis van de beoogde verwerking en het wettelijk voorschrift, tenzij die wetgeving deze kennisgeving om gewichtige redenen van algemeen belang verbiedt. Verwerker zal Verwerkingsverantwoordelijke, waar mogelijk, in staat stellen zich te verweren tegen deze verplichte verwerking en ook overigens de verplichte verwerking beperken tot het strikt noodzakelijke.

3.4 Verwerker zal de Persoonsgegevens aantoonbaar, op behoorlijke en zorgvuldige wijze verwerken en in overeenstemming met de op haar als Verwerker rustende verplichtingen op grond van de AVG, voor zover nog van toepassing de Wbp.

3.5 De dienstverlening door Verwerker betreft de verwerking van gezondheidsgegevens en andere bijzondere Persoonsgegevens. Verwerkingsverantwoordelijke stemt ermee in dat deze door Verwerker verwerkt mogen worden.

3.6 Verwerker mag Persoonsgegevens verwerken of laten verwerken door haarzelf of door derden in landen buiten de Europese Economische Ruimte ("EER").

3.7 Verwerker waarborgt dat betrokken Medewerkers een geheimhoudingsovereenkomst hebben getekend en geeft Verwerkingsverantwoordelijke op verzoek inzage in deze geheimhoudingsovereenkomst.

Artikel 4. Beveiliging Persoonsgegevens en controle

4.1 Verwerker passende en doeltreffende technische en organisatorische beveiligingsmaatregelen nemen ter bescherming van de Persoonsgegevens tegen verlies, onbevoegde kennisname, verminking of enige vorm van onrechtmatige verwerking, alsmede om de (tijdige) beschikbaarheid van de gegevens te garanderen. In deze beveiligings-maatregelen zijn de mogelijk in de Overeenkomst reeds bepaalde maatregelen begrepen. De maatregelen omvatten in ieder geval:

Maatregelen om te waarborgen dat enkel bevoegde Medewerkers toegang hebben tot de relevante Persoonsgegevens;
Maatregelen waarbij de Verwerker zijn Medewerkers uitsluitend toegang geeft tot Persoonsgegevens via op naam gestelde accounts, waarbij het gebruik van die accounts adequaat gelogd wordt en waarbij de betreffende accounts alleen toegang geven tot die Persoonsgegevens waartoe de toegang voor de betreffende (rechts)persoon noodzakelijk is;
Maatregelen om de Persoonsgegevens te beschermen tegen onopzettelijke of onrechtmatige vernietiging, onopzettelijk verlies of wijziging, onbevoegde of onrechtmatige opslag, verwerking, toegang of openbaarmaking;
Maatregelen om de tijdige beschikbaarheid van de Persoonsgegevens te garanderen;
De overige maatregelen die Partijen zijn overeengekomen zoals vastgelegd in Bijlage 2.

Artikel 5. Informatieplichten en incidentenmanagement

5.1 Zodra zich een Incident voordoet is Verwerker verplicht Verwerkingsverantwoordelijke daarvan binnen 72 uur in kennis te stellen en daarbij alle relevante informatie te verstrekken over:

De aard van het Incident;
De (mogelijk) getroffen Persoonsgegevens;
De geconstateerde en de vermoedelijke gevolgen van het Incident; en
De maatregelen die getroffen zijn of zullen worden om het Incident op te lossen dan wel de gevolgen/schade zoveel mogelijk te beperken.

5.2 Verwerker is, onverminderd de overige verplichtingen uit dit artikel, verplicht om maatregelen te treffen die redelijkerwijs van hem kunnen worden verwacht om het Incident zo snel mogelijk te herstellen dan wel de verdere gevolgen zoveel mogelijk te beperken.

5.3 Het is Verwerker toegestaan informatie te verstrekken over Incidenten aan derde partijen of Sub-verwerkers.

Artikel 6. Medewerkingsverplichtingen

6.1 Een door Verwerker ontvangen klacht of een verzoek van een Betrokkene met betrekking tot verwerking van Persoonsgegevens wordt door Verwerker zonder uitstel doorgestuurd naar Verwerkingsverantwoordelijke.

6.2 Op het eerste daartoe strekkende verzoek van Verwerkingsverantwoordelijke zal Verwerker aan Verwerkingsverantwoordelijke alle relevante informatie verstrekken betreffende de aspecten van de door haar verrichte verwerking van Persoonsgegevens zodat Verwerkingsverantwoordelijke, mede aan de hand van die informatie, aan kan tonen dat zij de toepasselijke (privacy) wetgeving naleeft. Alle gemaakte kosten hiervoor mogen doorbelast worden aan Verwerkingsverantwoordelijke.

Artikel 7. Inschakeling subverwerkers

7.1 Verwerker mag haar activiteiten die bestaan uit het verwerken van Persoonsgegevens of vereisen dat Persoonsgegevens verwerkt worden, uitbesteden aan een Subverwerker uit bijlage 1 of aan een andere Subverwerker 30 dagen nadat Verwerkingsverantwoordelijke hierover in kennis is gesteld.

7.2 Indien een collega van Verwerker waarneemt tijdens bijvoorbeeld een vakantie voor Verwerker, mag Verwerker, na in kennisstelling van Verwerkingsverantwoordelijke, het dossier worden overgedragen aan deze collega.

Artikel 8. Aansprakelijkheid

8.1 Verwerker spant zich in de privacy en bescherming van Persoonsgegevens te waarborgen, maar Verwerkingsverantwoordelijke vrijwaart Verwerker van iedere vorm van aansprakelijkheid, schade en/of boetes.

8.2 Verwerkingsverantwoordelijke overhandigt op eigen initiatief en voor eigen rekening en risico (bijzondere) Persoonsgegevens aan Verwerker, ook als deze vereist zijn om de diensten van Verwerker uit te kunnen voeren. Het staat Verwerkingsverantwoordelijke te allen tijde vrij geen gebruik te maken van de diensten van Verwerker en zodoende geen (bijzondere) Persoonsgegevens te overhandigen aan Verwerker.

8.3 Een eventuele schadevergoeding bedraagt maximaal honderd euro.

Artikel 9. Kosten

9.1 De kosten voor de verwerking van gegevens die inherent zijn aan de normale uitvoering van de Overeenkomst, worden geacht besloten te liggen in de op grond van de

Overeenkomst reeds verschuldigde vergoedingen, met uitzondering van specifiek benoemede kosten in deze Verwerkersovereeenkomst.

9.2 Enige ondersteuning of enige andere aanvullende dienstverlening die Verwerker op grond van deze Verwerkersovereenkomst dient te verlenen, of die wordt verzocht door Verwerkingsverantwoordelijke, inclusief alle verzoeken tot aanvullende informatie, zullen in rekening worden gebracht bij Verwerkingsverantwoordelijke.

Artikel 10. Duur en beëindiging

10.1 Deze Verwerkersovereenkomst gaat in nadat het intakeformulier is toegestuurd per mail/post of ingevuld op de website of op de datum van ondertekening. Deze Verwerkersovereenkomst maakt onderdeel uit van de behandelovereenkomst. Bij het tekenen van de behandelovereenkomst wordt ook akkoord gegaan met deze Verwerkersovereenkomst. De duur van deze Verwerkersovereenkomst is gelijk aan de periode dat Verwerkingsverantwoordelijke gebruikt maakt van de diensten van Verwerker en nog niet heeft aangegeven de behandeling te willen staken of Verwerker nog niet heeft aangegeven dat de behandeling voltooid is. Als de behandeling voltooid is en Verwerkingsverantwoordelijke maakt later opnieuw gebruik van de diensten van Verwerker, dan is deze Verwerkersovereenkomst weer van kracht en wordt deze automatisch verlengd conform de bovengenoemde criteria.

10.2 De Verwerkersovereenkomst maakt integraal en onlosmakelijk deel uit van de Overeenkomst(en). Beëindiging van de Overeenkomst(en), op welke grond dan ook, heeft tot gevolg dat de Verwerkersovereenkomst eveneens op dezelfde grond beëindigd wordt (en vice versa), tenzij Partijen in voorkomend geval anders overeenkomen.

10.3 Verplichtingen welke naar hun aard bestemd zijn om ook na beëindiging van deze Verwerkersovereenkomst voort te duren, blijven na beëindiging van deze Verwerkersovereenkomst gelden. Tot deze bepalingen behoren bijvoorbeeld die welke voortvloeien uit de bepalingen betreffende geheimhouding, aansprakelijkheid, geschillenbeslechting, toepasselijk recht en een wettelijke bewaarplicht door Verwerker.

10.4 Deze Verwerkersovereenkomst kan niet los van de behandelovereenkomst worden opgezegd.

Artikel 11. Bewaartermijnen, teruggave en vernietiging van Persoonsgegevens

11.1 Verwerker bewaart de Persoonsgegevens niet langer dan strikt noodzakelijk, waaronder begrepen de wettelijke bewaartermijnen of een eventueel tussen Partijen gemaakte afspraak over bewaartermijnen zoals vastgelegd in Bijlage 1.

11.2 Bij beëindiging van de Verwerkersovereenkomst, of indien van toepassing aan het einde van de overeengekomen bewaartermijnen, of op schriftelijk verzoek van Verwerkingsverantwoordelijke zal Verwerker, tegen redelijke kosten, naar keuze van Verwerkingsverantwoordelijke, de Persoonsgegevens onherroepelijk (doen) vernietigen of teruggeven aan Verwerkingsverantwoordelijke. Eventuele teruggave van de gegevens zal in

een algemeen gangbaar, gestructureerd en gedocumenteerd gegevensformaat langs elektronische weg plaatsvinden. Indien teruggave, onherroepelijke vernietiging of verwijdering niet mogelijk is, stelt Verwerker Verwerkingsverantwoordelijke daarvan onmiddellijk op de hoogte. In dat geval garandeert Verwerker dat hij de Persoonsgegevens vertrouwelijk zal behandelen en niet langer zal verwerken.

Artikel 12. Intellectuele eigendomsrechten

12.1 Voor zover de (verzameling van) Persoonsgegevens wordt beschermd door enig intellectueel eigendomsrecht, verleent Verwerkingsverantwoordelijke toestemming aan Verwerker de Persoonsgegevens te gebruiken in het kader van de uitvoering van deze Verwerkersovereenkomst.

Artikel 13. Slotbepalingen

13.1 De overwegingen maken onderdeel uit van deze Verwerkersovereenkomst.

13.2 In geval van nietigheid c.q. vernietigbaarheid van een of meer bepalingen uit deze Verwerkersovereenkomst, blijven de overige bepalingen onverkort van kracht.

13.3 In alle gevallen waarin deze Verwerkersovereenkomst niet voorziet beslissen Partijen in onderling overleg.

13.4 Op deze Verwerkersovereenkomst is Nederlands recht van toepassing.

13.5 Partijen zullen zich inspannen conflicten in onderling overleg op te lossen. Hierbij is inbegrepen de mogelijkheid het geschil te beëindigen door een in onderling overleg vast te stellen mediation of arbitrage.

13.6 Geschillen over of in verband met deze Verwerkersovereenkomst worden uitsluitend voorgelegd aan de daartoe in de Overeenkomst aangewezen rechtbank of arbiter(s).

Bijlage 1: Overeenkomsten, omschrijving Persoonsgegevens, aard verwerkingen en meer

Deze Verwerkersovereenkomst is een bijlage bij de volgende Overeenkomsten en heeft betrekking op de volgende verwerkingen van Persoonsgegevens.

Categorieën persoonsgegevens
De volgende persoonsgegevens van cliënten worden door Praktijk Vitalution verwerkt:

- Naam, adres, postcode en woonplaats
- Geboortedatum
- Telefoonnummer en e-mailadres
- Aanvullend bij minderjarige cliënten worden de volgende gegevens verwerkt: Naam, adres, postcode, woonplaats, telefoonnummer en e-mailadres van beide ouders

Indien dit in belang is van de begeleiding/ behandeling, worden de volgende bijzondere persoonsgegevens van cliënten vastgelegd:

Informatie over de gezondheid
Indien dit in belang is van de begeleiding/ behandeling van de cliënt, worden de volgende verdere gegevens vastgelegd voor de zorgnota:

Zorgverzekeraar en polisnummer
Doeleinden van de persoonsgegevens die worden verwerkt
Behalve de AVG, zijn de WGBO (Wet op de geneeskundige behandelingsovereenkomst) en de beroepscode van de beroepsvereniging Maatschappij ter Bevordering van de Orthomoleculaire Geneeskunde (MBOG) en van de Koepel Klachtenafhandeling Alternatieve Behandelwijzen (KAB) van toepassing voor Praktijk Vitalution. Deze zijn van invloed op de doeleinden waarvoor persoonsgegevens worden vastgelegd. Om die reden wordt als volgt omgegaan met persoonsgegevens:

Dossierplicht: Op grond van de Wet op de geneeskundige behandelingsovereenkomst (WGBO) is de therapeut verplicht een medisch dossier bij te houden.

Goede dienstverlening: Om een goede dienstverlening van de therapeut naar cliënt(en) te kunnen waarborgen, wordt een medisch dossier bijgehouden.

Bewaartermijn: De hoofdregel voor het bewaren van medische dossiers staat in de WGBO. Dat is 15 jaar, gerekend vanaf de datum van vastlegging van ieder afzonderlijk gegeven. De termijn kan langer zijn indien dit noodzakelijk is met het oog op de behandeling (bijvoorbeeld indien iemand een chronische ziekte heeft). Voor minderjarigen geldt dat de bewaartermijn van 15 jaar ingaat, vanaf het achttiende levensjaar. Deze gegevens moeten dus bewaard blijven tot het 34e levensjaar behalve bij eerder overlijden van de minderjarige. Dan geldt de bewaartermijn van 15 jaar vanaf de datum van overlijden. Voor overleden volwassenen dient het dossier 15 jaar bewaard te blijven vanaf de laatste wijziging in het dossier over de behandeling of vanaf de datum van overlijden.

Beroepsgeheim: Voor de therapeut geldt op grond van de beroepscode en het wettelijk geregeld medisch beroepsgeheim een geheimhoudingsplicht.

Minderjarigen: Volgens de patiëntenrechten uit de WGBO komen de wilsbekwame minderjarige tussen 12-16 jaar zelf en de ouder(s) het 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 therapeut 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.

Rechten van de cliënt(en) van Praktijk Vitalution

Cliënten worden bij de intake schriftelijk geïnformeerd over de dossierplicht en hun recht op inzage, wijzigen, wissen en het ontvangen van alle geregistreerde gegevens tijdens de intake. Deze informatie ligt vast in een schriftelijke behandelovereenkomst.
Op de website van Praktijk Vitalution staat informatie over de 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.
Toegang tot en inzage in de cliëntdossiers

De therapeut is ZZP-er en is de enige die toegang heeft tot de dossiers. Vanuit de beroepscode heeft de therapeut een beroepsgeheim. Tijdens afwezigheid of vakantie wordt waargenomen door verschillende collega's. Deze hebben toegang tot patiëntendossiers. Zij vallen eveneens onder het beroepsgeheim en hanteren dezelfde regels.
De therapeut bepreekt wel eens casuïstiek uit de praktijk met collega's of in intervisiegroepen. Dat gaat altijd anoniem en onherkenbaar. Toegang tot de persoonsgegevens door externe personen of bedrijven Verwerkers waarmee Praktijk Vitalution een verwerkersovereenkomst heeft afgesloten zijn:

- iMuis boekhoudsoftware voor het maken van facturen
- Administratiekantoor Oostland voor het verwerken van de administratie
- ING voor het uitvoeren van betalingen
- Sepay pinautomaat
- De webhost (Weebly) omdat in de website persoonsgegevens worden opgeslagen, bijvoorbeeld bij het invullen van een contactformulier invult .
- iCloud voor online opslag
- Microsoft Outlook en A1 Internethosting voor de zakelijke e-mailhosting
- HRM CellCare voor het versturen van de anamnese vragenlijst en het Neuro4Profiel
- Orthomoleculaire Apotheek de Roode Roos bij bestelling van supplementen
- Online Afspraken Agenda tool voor het boeken van consulten

Bijlage 2: Omschrijving nadere beveiligingsmaatregelen

Beveiliging van de persoonsgegevens

Verwerker werkt met een digitaal cliëntendossier op een laptop. Deze is beveiligd door een wachtwoord. Verwerker maakt regelmatig een back-up van cliëntbestanden. Deze is online opgeslagen en beveiligd door een tweestaps verificatie.Een virusscanner en Firewall zijn geïnstalleerd op de laptop waarop het digitaal cliëntendossier wordt bewaard.
Een deel van het patiëntendossier beslaat een papieren dossier. Die dossiers worden bewaard in een afgesloten kast in een afgesloten ruimte, waar alleen de therapeut toegang toe heeft. Doorlopende beveiligingsupdates voor de webserver, computers, facturatieprogramma, mailserver, clouddiensten, emailmarketingsoftware en digitale agenda. Voor de cloudopslag, zakelijke e-mail en het facturatiesysteem wordt gebruik gemaakt van een beveiligde verbinding (https) en een tweestaps verificatie.

Datalekken
Sinds 1 januari 2016 geldt de meldplicht datalekken. Deze meldplicht houdt in dat Praktijk BioBalans direct (binnen 72 uur na het datalek) een melding moeten doen bij de Autoriteit Persoonsgegevens zodra er een ernstig datalek is. In sommige gevallen moet het datalek ook gemeld worden aan de betrokkenen (de mensen van wie de persoonsgegevens zijn gelekt).

Wanneer moet een datalek worden gemeld?
Een datalek hoeft alleen gemeld te worden aan de Autoriteit Persoonsgegevens als dit leidt tot ernstige nadelige gevolgen voor de bescherming van persoonsgegevens, of als er een aanzienlijke kans bestaat dat dit gebeurt. Dat is het geval als er bij het datalek ofwel persoonsgegevens verloren zijn gegaan, 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 ik had geen controle over wat diegene met de gegevens heeft gedaan of nog zal doen).

De betrokkenen worden alleen geïnformeerd 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.