BV Innoveren van nieuwe wetgeving omtrent privacygegevens

Gemaakt door:
Cas Smits
Emmy Jansen
Ijaz Khan
Jeanine Schut 500700612
Nick van den Nieuwenhof 500712395
Shereen Negm

Inhoud

BV Innoveren van nieuwe wetgeving omtrent privacygegevens 1
Algemene oriëntatie AVG 3
Wat is de AVG? 3
Waarom verandering van de wet? 3
Nieuwe privacy rechten 3
Belangrijke veranderingen voor organisaties 3
Wat levert de AVG organisaties op? 4
Implementatie plan het toepassen van de AVG vanuit het 10 stappenplan 4
Uitwerking 4
Bibliografie 13

Algemene oriëntatie AVG

Wat is de AVG?

De Algemene verordening gegevensbescherming (AVG) is een privacywet die geldt in de hele Europese Unie (EU). Op 4 mei 2016 is de AVG gepubliceerd in het publicatieblad van de Europese Unie. De AVG is 20 dagen na de publicatie in werking getreden. De AVG vervangt de Wet bescherming persoonsgegevens (Wbp) en is op 25 mei 2018 van toepassing. De Wbp geldt dan niet meer. De AVG staat ook bekend onder de Engelse naam: General Data Protection Regulation (GDPR). Dankzij de AVG is de bescherming van persoonsgegevens in alle landen van de EU op dezelfde manier geregeld en gelden in elke lidstaat dezelfde regels (Autoriteit Persoonsgegevens, 2018).

Waarom verandering van de wet?

In 1995 had iedere lidstaat van de EU nog een eigen privacywet. Deze Europese wetgeving werd vastgesteld toen internet net bestond. Doordat mensen nu steeds vaker internet gebruiken waarbij websites gebruiksgegevens kunnen gebruiken wordt de Europese privacywetgeving herzien.

Nieuwe privacy rechten

Recht op vergetelheid
Mensen krijgen hierbij het recht om een organisatie te vragen de persoonsgegevens te verwijderen. Vanaf 25 mei 2018 kunnen mensen eisen dat de organisatie de verwijderingen doorgeeft aan andere organisaties die de gegevens hebben verkregen.

Recht op dataportabiliteit
Hierbij hebben mensen het recht om (onder bepaalde voorwaarden) het recht om via een organisatie de persoonsgegevens in een standaardformaat te ontvangen. Een voorbeeld hiervan is wanneer mensen zich uitschrijven bij een sociale netwerksite en zich inschrijven bij een andere netwerksite de mensen kunnen eisen dat de organisatie hun persoonsgegevens direct doorstuurt aan de nieuwe dienstverlener. Een voordeel hiervan is dat mensen gemakkelijker hun gegevens door kunnen geven aan een andere leverancier van dezelfde soort dienst (Autoriteit Persoonsgegevens, 2017).

Belangrijke veranderingen voor organisaties

Tijdens de veranderingen van de Wbp naar de AVG hebben organisaties/bedrijven meer verplichtingen bij het verwerken van persoonsgegevens. De AVG zorgt voor meer nadruk op de verantwoordelijkheid van bedrijven/organisaties om aan te tonen dat zij zich aan de wethouden. Voor bedrijven/organisaties is dit de verantwoordingsplicht.

De verantwoordingsplicht houdt in dat bedrijven en organisaties zich met documenten kunnen verantwoorden dat de juiste organisatorische en technische maatregelen zijn genomen om aan de AVG te voldoen. Hierbij worden er vanuit de AVG instrumenten aangeboden die bedrijven/organisaties kunnen helpen om zich aan de wet te houden. Een voorbeeld hiervan is een modelbepaling voor doorgifte van persoonsgegevens. Vanaf 25 mei 2018 hoeven organisaties verwerkingen van persoonsgegevens niet meer te melden bij de Autoriteit Persoonsgegevens. Organisaties kunnen verplicht zijn een Data Protection Impact Assessment (DPIA) uit te voeren, kunnen verplicht zijn een functionaris voor de gegevensbescherming (FG) aan te stellen (Autoriteit Persoonsgegevens, 2018).

DPIA
De DPIA is een instrument om vooraf de privacy risico's van een gegevensverwerking in kaart te brengen. En vervolgens maatregelen te kunnen nemen om de risico's te verkleinen. De uitvoering hiervan is te zien in stap 4 van het stappenplan (Autoriteit Persoonsgegevens, 2017).

Wat levert de AVG organisaties op?
Doordat mensen steeds meer internetten zorgt deze wet voor één privacy wet over de gehele Europese Unie (EU) in plaats van 28 verschillende nationale wetten. De wet is meer gericht op de hedendaagse gedigitaliseerde samenleving. Het levert het volgende voor bedrijven/organisaties op:

- Er zijn minder administratieve kosten en nalevingskosten
- Er is sprake van meer rechtszekerheid
- Iedereen heeft in de EU dezelfde regels.
- Er is één toezichthouder om zaken mee te doen (onetopshop)

Onetopshop: de Algemene verordening gegevensbescherming (AVG) gaat uit van de zogeheten onetopshop-regel. Onetopshop houdt in dat organisaties die zogeheten grensoverschrijdende gegevensverwerkingen uitvoeren, nog maar met één privacy toezichthouder zaken hoeven te doen. Dit wordt de 'leidende toezichthouder' genoemd verdere informatie is te lezen in stap 9 van het stappenplan (lead supervisory authority) (Falque-Pierrotin, 2017).

Implementatie plan het toepassen van de AVG vanuit het 10 stappenplan

Uitwerking
Stap 1: bewustwording
Iedereen van de organisatie dient op de hoogte te worden gebracht van de nieuwe privacy regels. Hierbij is het belangrijk dat er een schatting wordt gedaan over de impact van de AVG op de huidige processen, diensten en goederen en welke aanpassingen er gedaan moeten worden om aan de AVG te voldoen. Hierbij biedt de Autoriteit Persoonsgegevens (AP) verschillende instrumenten die kunnen ondersteunen om de AVG na te leven. Een belangrijk detail is dat de AP organisatie een boete kan opleggen van maximaal 20 miljoen euro of 4% van de wereldwijde omzet als er niet voldaan wordt aan de nieuwe privacywetgeving.

De instrumenten die ondersteunen bij het goed uitvoeren van de AVG zijn:
- Website genaamd: hulpbijprivacy.nl
- Guidelines namelijk:
    - Guidelines on data protection officers (uitwerking stap 6)
    - Guidelines leidende toezichthouder (uitwerking bij stap 9)
    - Guidelines recht op dataportabiliteit (uitwerking bij stap 2)
- Data protection impact assessment (DPIA) (uitwerking stap 4)
- Meldplicht datalekken (uitwerking stap 7)
- Profiling (uitwerking bij contracten)
- Toestemming (uitwerking stap 10)
- Transparantie (uitwerking stap 3 en contracten)

Stap 2: rechten van betrokkene
Door de nieuwe wetregeling zijn er ook nieuwe privacy rechten (recht van dataportabiliteit en recht van vergetelheid). In oefentherapeutische organisaties wordt er gebruik gemaakt van digitale dossiers die zijn beveiligd. Dit zorgt ervoor dat bij patiënten die hun persoonsgegevens willen inzien of over willen dragen naar een andere instantie de gegevens gestructureerd zijn en een machine leesbaar format heeft. Voorafgaand aan de dossiervorming die volgens de VvOCM wordt gehanteerd, krijgen de patiënten de informatie over hun persoonlijke rechten en hierbij ook de controle over hun betreffende persoonsgegevens. Dit kan wel een bijdrage leveren aan de patiënt/therapeut vertrouwensrelatie.
Privacy wetten die al bestonden en blijven bestaan onder de AVG zijn

- Recht op inzage → patiënten hebben recht om gegevens die worden verwerkt in te zien
- Recht op rectificatie en aanvulling → patiënten hebben het recht om gegevens die worden verwerkt te wijzigen.
- Het recht op beperking van de verwerking→ patiënten hebben het recht om minder gegevens te laten verwerken
- Het recht om bezwaar te maken tegen de gegevens verwerking (Autoriteit Persoonsgegevens, 2018).

Stap 3: Overzicht verwerkingen
Onder deze stap wordt beschreven hoe de gegevensverwerkingen in kaart worden gebracht in de organisatie. Hierbij wordt aangegeven met welk doel de gegevens worden verwerkt, waar de gegevens vandaan komen en met wie de gegevens worden gedeeld.
De organisatie verwerkt je persoonsgegevens doordat je gebruik maakt van onze diensten en/of omdat je deze gegevens zelf aan ons verstrekt. Hieronder vind je een overzicht van de

Persoonsgegevens die wij verwerken:
- Voor- en achternaam
- Geslacht
- Geboortedatum
- Burger Service Nummer (BSN)
- Adresgegevens
- Telefoonnummer
- E-mailadres

Bijzondere en/of gevoelige persoonsgegevens die wij verwerken:

De organisatie verwerkt de volgende bijzondere en/of gevoelige persoonsgegevens van jou:

- Gezondheidsgegevens.
- Gegevens van personen jonger dan 16 jaar. Onze website en/of dienst heeft niet de intentie gegevens te verzamelen over websitebezoekers die jonger zijn dan 16 jaar. Tenzij ze toestemming hebben van ouders of voogd. We kunnen echter niet controleren of een bezoeker ouder dan 16 is. Wij raden ouders dan ook aan betrokken te zijn bij de online activiteiten van hun kinderen, om zo te voorkomen dat er gegevens over kinderen verzameld worden zonder ouderlijke toestemming. Als je ervan overtuigd bent dat wij zonder die toestemming persoonlijke gegevens hebben verzameld over een minderjarige, neem dan contact met ons op via de klantenservice, dan verwijderen wij deze informatie.
- Burger Service Nummer (BSN)
- Genetische gegevens
- Geslacht

Met welk doel en op basis van welke grondslag wij persoonsgegevens verwerken

Voor oefentherapie verwerken wij ook persoonsgegevens als wij hier wettelijk toe verplicht zijn, zoals gegevens die wij nodig hebben voor declaratieverkeer, kwaliteitsdoeleinden, onderzoeksgegevens en onze belastingaangifte. De persoonsgegevens worden voor de volgende doelen verwerkt:
- Het afhandelen van jouw betaling.
- Je te kunnen bellen of e-mailen indien dit nodig is om onze dienstverlening uit te kunnen voeren.
- Je te informeren over wijzigingen van onze diensten en producten.
- Verzenden van onze nieuwsbrief en/of reclamefolder.

Geautomatiseerde besluitvorming

De organisatie neemt wel op basis van geautomatiseerde verwerkingen besluiten over zaken die (aanzienlijke) gevolgen kunnen hebben voor personen. Het gaat hier om besluiten die worden genomen door computerprogramma's of -systemen, zonder dat daar een mens (bijvoorbeeld een therapeut oefentherapie) tussen zit. Er wordt gebruikt van de volgende computerprogramma's of -systemen: Winmens (Fairware), declaratie (via Vecozo), verslaglegging, kwaliteitsdoeleinden.

Hoe lang we persoonsgegevens bewaren

De organisatie bewaart je persoonsgegevens niet langer dan strikt nodig is om de doelen te realiseren waarvoor je gegevens worden verzameld. Wij hanteren de volgende bewaartermijnen voor de volgende (categorieën) van persoonsgegevens:

- Persoonsgegevens > Bewaartermijn: 7 jaar
- Personalia > Bewaartermijn 7 jaar
- Adres > Bewaartermijn 7 jaar
- Verzekeringsgegevens > Bewaartermijn 7 jaar
- Verwijzingen papier/digitaal > Bewaartermijn 7 jaar
- Brieven/verslaglegging verwijzers/derden > Bewaartermijn 7 jaar

Reden van bewaartermijn:
Met de duur van het bewaartermijn zoals hierboven bij de categorieën is aangegeven, voldoen wij aan onze wettelijke verplichting tot bewaarplicht van dossiers.
De bewaartermijn gaat in vanaf het moment dat de behandeling officieel is beëindigd, middels een uitbehandelingsbrief naar de verwijzer/huisarts en/of overlijden en hierdoor sluiten van het dossier.

Delen van persoonsgegevens met derden

De organisatie deelt jouw persoonsgegevens met verschillende derden als dit noodzakelijk is voor het uitvoeren van de overeenkomst en om te voldoen aan een eventuele wettelijke verplichting. Met bedrijven die je gegevens verwerken in onze opdracht, sluiten wij een bewerkersovereenkomst om te zorgen voor eenzelfde niveau van beveiliging en vertrouwelijkheid van jouw gegevens. De organisatie blijft verantwoordelijk voor deze verwerkingen. Daarnaast verstrekt de organisatie jouw persoonsgegevens aan andere derden. Dit doen wij alleen met jouw nadrukkelijke toestemming.

Derden	Jurisdictie	Doel	Welke gegevens
Huisartsen/verwijzers	AVG en WGBO	Medisch dossier bijhouden	NAP en dossier
Vecozo/ zorgverzekeraars	AVG	Declaratie behandelingen	NAP
Winmens/EPD	WGBO en AVG	Dossier vormingsplicht	NAP en dossier
LDO	AVG	Inzicht krijgen in kwaliteit van behandelen	Behandeldoel, behandelfrequentie. Volledig anoniem
Nivel	AVG	Inzicht krijgen in kwaliteit van behandelen	Behandeldoel, behandelfrequentie. Volledig anoniem
Qualizorg	AVG	Inzicht krijgen in kwaliteit van behandelen	Emailadres

*NAP = Naam, adres en Persoonsgegevens
*NIVEL = Het NIVEL (Nederlands instituut voor onderzoek van de gezondheidszorg) onderzoekt de effectiviteit en kwaliteit van de gezondheidszorg in Nederland en de relaties tussen zorgaanbieders, zorgconsumenten, zorgverzekeraars en de overheid (NIVEL, 2018).
*Qualizorg = Patiënt/klanttevredenheid onderzoek aan de hand van een vragenlijst (Qualizorg, 2018).
*LDO = De Landelijke Database Oefentherapie (LDO) is een initiatief van de VvOCM. In de database wordt informatie verzameld over de zorg die oefentherapeuten Cesar/Mensendieck bieden aan hun patiënten en informatie over de praktijken van deze oefentherapeuten (VvOCM, 2016).
*WGBO = De Wet op de geneeskundige behandelingsovereenkomst (WGBO) ligt aan de basis van alle zorgverlening. In de WGBO staan de rechten en plichten van cliënten die zorg krijgen (Ministerie van Volksgezondheid, Welzijn en Sport, Z.J.).

Cookies, of vergelijkbare technieken, die wij gebruiken op de website
U kunt anoniem de website bezoeken en op die manier meer te weten te komen over de organisatie. De website verzamelt regelmatig gegevens omtrent de gebruikers van onze website, zoals browser type, duur van het bezoek en het aantal gebruikte pagina's. aan de hand van deze gegevens kunnen wij u niet identificeren en wordt er geen gebruik gemaakt van persoonsgegevens.

Gegevens inzien, aanpassen of verwijderen
Je hebt het recht om je persoonsgegevens in te zien, te corrigeren of te verwijderen. Daarnaast heb je het recht om je eventuele toestemming voor de gegevensverwerking in te trekken of bezwaar te maken tegen de verwerking van jouw persoonsgegevens door de organisatie en heb je het recht op gegevensoverdraagbaarheid. Dat betekent dat je bij ons een verzoek kan indienen om de persoonsgegevens die wij van jou beschikken in een computerbestand naar jou of een ander, door jou genoemde organisatie, te sturen. Je kunt een verzoek tot inzage, correctie, verwijdering, gegevensoverdraging van je persoonsgegevens of verzoek tot intrekking van je toestemming of bezwaar op de verwerking van jouw persoonsgegevens doorgeven aan de klantenservice. Om er zeker van te zijn dat het verzoek tot inzage door jou is gedaan, vragen wij jou een kopie van je identiteitsbewijs met het verzoek mee te sturen. Maak in deze kopie je pasfoto, MRZ (machine readable zone, de strook met nummers onderaan het paspoort), paspoortnummer en Burgerservicenummer (BSN) zwart. Dit ter bescherming van je privacy. We reageren zo snel mogelijk, maar binnen vier weken, op jouw verzoek. Onze organisaties willen je er tevens op wijzen dat je de mogelijkheid hebt om een klacht in te dienen bij de nationale toezichthouder, de Autoriteit Persoonsgegevens. Dat kan via de website: https://autoriteitpersoonsgegevens.nl/nl/contact-met-de-autoriteit-persoonsgegevens/tip-ons

Hoe wij persoonsgegevens beveiligen
Alle gegevens van cliënten, patiënten en medewerkers waren altijd al veilig bij de organisatie.
Met de per 25 mei ingaande "Algemene Verordening Persoonsgegevens" staat het nu ook in deze verklaring.
De organisatie neemt de bescherming van jouw gegevens serieus en neemt passende maatregelen om misbruik, verlies, onbevoegde toegang, ongewenste openbaarmaking en ongeoorloofde wijziging tegen te gaan. Als jij het idee hebt dat jouw gegevens toch niet goed beveiligd zijn of er aanwijzingen zijn van misbruik, neem dan contact op met de klantenservice.

Stap 4: data protection impact assessment
Onder de AVG kunnen bedrijven binnenkort verplicht zijn een zogeheten data protection impact assessment uit te voeren. Het is nog niet verplicht om deze stap toe te passen bij alle organisaties, om de privacy risico in kaart te brengen is het van belang de vragenlijst die is bijgevoegd in te vullen. Om vervolgens de risicofactoren te verminderen is er een checklist opgesteld om risicofactoren aan te pakken. De gehele vragenlijst met extra toelichting kan worden ingevuld op https://www.norea.nl/download/?id=522.
Vragenlijst:

1. Het type project?
2. De gegevens die u wilt gebruiken
3. De partijen die betrokken zijn bij de uitvoering van het project
4. Verzamelen van gegevens
5. Gebruik van gegevens
6. Bewaren en vernietigen van gegevens
7. Beveiligen van gegevens

Checklist:

Risicofactoren	**Aanpak**
1. Limitering van het verzamelen van gegevens	Het verminderen van de hoeveelheid gegevens, door de gegevens niet op te slaan of niet te bewaren (tenzij verplichting vanuit vak domein)
2. Gegevenskwaliteit	Introduceren van (geautomatiseerde) controles op gegevens
3. Doelbinding	De doelen voor het verzamelen en de verenigbaarheid van verdere verwerking nader specificeren en hierover communiceren
4. Limitering van gebruik van gegevens	Het beperken van de mogelijkheid om grote hoeveelheden gegevens in een keer binnen en buiten de organisatie te verspreiden door gefragmenteerde opslag in plaats van concentreren van alle gegevens in één database.
5. Beveiliging van gegevens	Het toepassen van encryptie en logische toegangsbeveiliging
6. Transparantie	Het opstellen van een privacy beleid, gedragscode of het laten certificeren van de verwerking (beroepscode/profiel van de VvOCM)
7. Rechten van betrokkenen	Betrokkenen zeggenschap geven over zijn gegevens door de invoer van een ‘self service’ bijvoorbeeld via een beveiligd internet portal
8. Verantwoordelijkheid en Verantwoording	Invoeren van periodieke externe controle. (kan gebeuren door iemand van de organisatie kan

	hiervoor ook iemand aannemen)

(Norea, 2015)

Stap 5: privacy by design & privacy by default

- Privacy by design wil zeggen dat er tijdens het ontwerpen van producten en diensten er zorg gedragen, moet worden dat de persoonsgegevens goed worden beschermd voorbeelden hiervan zijn bijvoorbeeld een beveiligd dossiervorming. Privacy by design moet er ook voor zorgen dat gegevens die verzamelt zijn of worden niet langer dan noodzakelijk bewaart worden of extra gegevens worden toegevoegd die niet bijdrage aan het doel van de verwerking.
- Privacy by default gaat meer in op de technische en organisatorische maatregelen die moeten worden genomen om ervoor te zorgen dat er als standaard alleen persoonsgegevens worden verwerkt die noodzakelijk zijn voor een specifiek doel. Acties die hiervoor genomen kunnen worden zijn:
    1. Een app toevoegen die u aanbiedt niet de locatie van gebruikers te laten registeren als dat niet nodig is
    2. Op de website het vakje ja, ik wil gebruik maken van aanbiedingen of een nieuwsbrief niet vooraf aan hoeven te vinken
    3. Tijdens het abonneren op een nieuwsbrief niet meer gegevens opvragen dan nodig is. → alleen een emailadres is voldoende (Nederlandict, 2017).

Stap 6: Functionaris voor de gegevensbescherming

Deze stap geeft aan of het voor bedrijven/organisatie verplicht is om een functionaris voor de gegevensbescherming aan te stellen. Een functionaris is iemand die binnen de organisatie toezicht houdt op de toepassing en naleving van de AVG. Hieronder kunt u lezen of u verplicht bent als organisatie om een functionaris aan te stellen vanuit de AVG is dit in drie situaties verplicht namelijk:

- Overheden en publieke organisaties

Overheidsinstanties en publieke organisaties zijn altijd verplicht om een FG aan te stellen, ongeacht het type gegevens dat er verwerkt moet worden. Voorbeelden van overheidsinstanties en publieke organisatie zijn: de rijksoverheid, gemeenten en provincies en zorg- en onderwijsinstellingen. Voor rechtbanken geldt het aanstellen van een FG niet.

- Observatie

Het is ook verplicht om een FG aan te stellen voor organisaties/bedrijven die vanuit hun kernactiviteiten op grote schaal individuen volgen. Een voorbeeld hiervan is de profilering van mensen voor het maken van risico-inschattingen, cameratoezicht en monitoring van iemands gezondheid. Hierbij is het van belang hoeveel personen de organisatie volgt, de hoeveelheid gegevens die de organisatie moet verwerken en hoelang de mensen gevolgd worden door de organisatie.

- Bijzondere persoonsgegevens

Organisatie zijn verplicht om een FG aan te stellen als de organisatie/bedrijf op grote schaal bijzondere persoonsgegevens verwerken en dit als belangrijkste taak van hun werk wordt gezien. Bijzondere gegevens zijn gegevens over iemands gezondheid, ras, politieke opvattingen, geloofsovertuiging of strafrechtelijke verleden.

- Onderbouwing FG aanstellen

Wanneer na het lezen van de eventuele bijgevoegde richtlijn het nog onduidelijk is of er voor de organisatie verplicht een FG aan gesteld moet worden, dient de organisatie/bedrijf goed te kunnen onderbouwen waarom ervoor gekozen is om de FG wel of niet aan te stellen (Autoriteit Persoonsgegevens, 2017).

Voor nadere informatie kan er gebruiken worden gemaakt van de richtlijn van de AP: https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/wp243rev01_nl.pdf

Stap 7: meldplicht datalekken
Vanaf 1 januari 2016 is de meldplicht datalekken in gegaan. Dit houdt in dat bedrijven/organisatie bij een ernstig data lek dit meteen moetne melden aan de AP. Hierbij komt ook kijken dat de data lek doorgeven moet worden aan de betrokkenen om wie de data lek kan gaan. Omtrent het datalekken in de AVG blijft het ongeveer hetzelfde als de Wbp. De AVG stelt wel strengere regels aan de eigen registratie van bedrijven/organisatie betreft het data lekken. Alle data lekken moeten worden gedocumenteerd. Aan de hand van de documentatie moet de AP kunnen controleren of er voldaan wordt aan de meldplicht. Het verschil van de AVG ten opzichte van de Wbp is dat de Wbp alleen betrekking had op de gemelde data lekken (Autoriteit Persoonsgegevens, 2015).
Mocht er een data lek plaats vinden dan kunnen de organisaties dat doen bij het Meldloket datalekken AP op https://datalekken.autoriteitpersoonsgegevens.nl/actionpage?0

Mocht de organisatie/bedrijven er achter willen komen of er sprake is van een data lek dat gemeld moet worden kan dan uitgevoerd worden aan de hand van beleidsregels die zijn op gesteld door de Autoriteit Persoonsgegevens. Hierbij is een richtlijn van toepassing: https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/richtsnoeren_meldplicht_datalekken_0.pdf

Stap 8: verwerkersovereenkomsten
Wanneer de AVG van toepassing is op organisaties/bedrijven en er is sprake van een zogenoemde ‘’verwerker’’ dat dienen de volgende onderwerpen te worden vastgelegd:

- Algemene beschrijving: Dit houdt in dat er een omschrijving moet zijn van het onderwerp, de duur, de aard en het doel van de werking. Daarnaast moet het soort persoonsgegevens worden vermeld, de categorieën van betrokkene en uw rechten en verplichtingen als verwerkingsverantwoordelijke.
- instructies verwerking: Hierbij gaat het erom dat de verwerking uitsluitend gebeurt op basis van schriftelijke instructies en mogen niet door de verwerker zelf als doeleinden worden gebruikt.
- Geheimhoudingsplicht: mensen die werk verrichten of in dienst zijn voor de verwerker hebben een geheimhoudingsplicht.
- Beveiliging: pas bij het verwerken van persoonsgegevens een versleuteling toe waardoor er door de organisatie/bedrijf passende organisatorische en technische maatregelen worden genomen om verwerking te beveiligen.
- Subverwerkers: dit zijn mensen die werken in opdracht van een verwerker. De subwerkers zijn verplicht om dezelfde verplichtingen aan te gaan als die de verwerker heeft met het bedrijf/organisatie. Mocht hierbij toch sprake zijn dat de subwerker zijn verplichtingen niet nakomt dan blijft de verwerker volledig aansprakelijk richting de bedrijven/organisaties.
- Privacy rechten: Een verwerker helpt bedrijven/organisaties om andere verplichtingen na te komen. Hierbij kunnen bedrijven/organisaties geholpen worden bij het uitvoeren van een data protection impact assessment (DPIA) of bij het melden van een data lek.
- Gegevens verwijderen: na de verplichtingen van de verwerker is het de verwerker zijn taak om de gegevens te verwijderen. Hierbij is de verwerker ook verplicht de kopieën te verwijderen tenzij het wettelijk verplicht is om de gegevens een bepaalde tijd te bewaren.
- Audits: Een verwerker kan controleren of hij zich aan de hierboven genoemde verplichten houdt door het beschikbaar stellen van relevante informatie. Hierbij werkt de verwerker mee aan audits of aan die van een derde partij (Rijksoverheid, 2018).

Stap 9: leidende toezichthouder

Een leidend toezichthouder heeft de verantwoordelijkheid om toezicht te houden over organisaties/bedrijven met grensoverschrijdende gegevensverwerkingen. Grensoverschrijdende gegevensverwerkingen zijn van toepassing wanneer een organisatie/bedrijf gegevens verwerkt in verschillende EU-lidstaten. Het kan ook voorkomen dat de verwerking van de gegevens voor meerdere EU-lidstaten een impact kan hebben. De leidende toezichthouder moet zijn diensten afstemmen met andere privacy toezichthouders in andere Europese landen waar de eventuele gegevensverwerking een impact kan geven. De leidende toezichthouder coördineert de activiteiten/diensten en zorgt ervoor dat de andere toezichthouders betrokken zijn door conceptbeslissingen voor te leggen. Voor extra informatie over de leidende toezichthouder kan de richtlijn van AP worden bezocht (Autoriteit Persoonsgegevens, 2017).
Voor snelle toegang van de richtlijn kunt u gebruik maken van onderstaande link:
https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/vertaling_guidelines_leidende_toezichthouder.pdf

Stap 10: toestemming
Voor bepaalde verwerkingen van persoonsgegevens moet er toestemming zijn van de patiënten of betrokkenen. De AVG stelt strengere eisen omtrent de toestemming namelijk:

- Vrijelijk gegeven: personen mogen niet onder druk gezet worden
- Ondubbelzinnig: van belang dat het document van toestemming duidelijk is dit kan een digitale verklaring zijn, een schriftelijke verklaring of een mondelinge verklaring. Het moet in ieder geval voor de patiënten duidelijk zijn dat hun toestemming verlenen.
- Geïnformeerd: betrokkenen moeten worden geïnformeerd over de volgende punten:
- 1. De beschrijving van de organisatie → naam, adres, postcode.
- 2. Wat het doel is van de gegevensverwerking
- 3. Welke persoonsgegevens worden verzameld en gebruikt
- 4. Recht om de toestemming in te trekken.
- Specifiek: hierbij is het van belang dat er voor elke toestemming duidelijk is dat het voor een specifieke verwerking gaat met een specifiek doel. Mochten er meerdere doeleinden zijn betrokkenen dan moet de betrokkenen worden geïnformeerd en voor elk doeleinde moet toestemming worden gevraagd
- Organisaties/bedrijven die patiënten behandelen jonger dan 16 jaar moeten toestemming krijgen van de ouders. De AVG geeft hierbij extra bescherming aan mensen met een leeftijd onder de 16 omdat hun een minder tot niet kunnen inschatten wat de risico's zijn van een gegevensverwerking.

De vernieuwing omtrent de toestemming is dat organisaties/bedrijven aan moeten kunnen tonen dat er een geldige toestemming is verkregen van patiënten. Daarnaast is het van belang dat patiënten de toestemming ook weer gemakkelijk moeten kunnen intrekken. Hieronder is een contract uitgewerkt wat toepasbaar is gemaakt voor de stageplekken (Europa decentraal, 2017).

Geachte heer/ mevrouw ….,

Welkom bij ……..*(naam bedrijf)*
Hartelijk dank voor het maken van uw afspraak bij *(naam bedrijf)*
Op.....dag (dd) om... (tijd) zal ……, oefentherapeut Mensendieck, u behandelen.

Het adres is van de praktijk waar u in behandeling bent is:

……..(*Adres gegevens praktijk)*
Hieronder vindt u belangrijke aanvullende informatie. Leest u deze alstublieft aandachtig door. Zodat u deze in de praktijk kunt ondertekenen.

Afspraak wijzigen of annuleren;
Tot 24 uur voor de afspraak kunt u deze kosteloos afzeggen of wijzigen. Om een afspraak af te zeggen of te wijzingen kunt u bellen naar (*…….) telefoonnummer praktijk.* Afspraken die u niet tijdig afzegt en/of afspraken waarbij u niet verschijnt, moeten wij bij u persoonlijk in rekening brengen. Uw zorgverzekeraar vergoedt deze afspraken niet.

Vergoeding voor oefentherapie Mensendieck;
Oefentherapie Mensendieck wordt vergoed uit de aanvullende verzekering (AV). Het aantal behandelingen dat wordt vergoed verschilt per verzekeringsmaatschappij, het type aanvullende verzekering en de aandoening waarvoor u wordt behandeld.
Bij 'chronische indicaties' waarvoor veel Mensendieck nodig is, vindt vergoeding vanaf de 21e behandeling plaats vanuit de basisverzekering.
Het is uw eigen verantwoordelijkheid erop te letten of u het aantal behandelingen waarop u recht heeft binnen uw AV overschrijdt.

Declaratie oefentherapie Mensendieck;
Uw Mensendieck behandelingen worden door ons rechtstreeks bij uw zorgverzekeraar gedeclareerd. Als u geen of een beperkte aanvullende verzekering heeft afgesloten, worden bepaalde kosten van uw behandeling mogelijk niet door uw verzekeraar vergoed. Hierbij worden de kosten in dat geval bij u persoonlijk in rekening gebracht.

Medewerkers;
Alle oefentherapeuten Mensendieck bij Movement Therapy zijn geregistreerd in het kwaliteitsregister van hun beroepsgroep en zijn aangesloten bij VvOCM.

Klachtenregeling;
Als u niet tevreden bent over de behandeling door uw oefentherapeut, of u heeft klachten over de gang van zaken binnen de praktijk, maakt u dat dan a.u.b. kenbaar en bespreek het met uw behandelend therapeut. Voor meer informatie hierover kunt u kijken op
https://www.kwaliteitsregisterparamedici.nl/

Afsluiting;
Wij streven naar een kortdurend traject van hoge kwaliteit waarbij de patiënt weet waar hij/ zij aan toe is of wat hem/ haar te wachten staat. Daaronder valt een duidelijke beginfase en om de behandeling zo goed mogelijk af te sluiten vindt er een afsluitende evaluatie plaats tussen u en de therapeut.

Zorgkwaliteit;
Om de kwaliteit van de zorg te blijven verbeteren zouden wij u willen vragen een enquête over de zorgkwaliteit in te vullen wanneer u uitbehandeld bent. Mocht u hieraan mee willen werken graag uw emailadres onderaan invullen.

Privacy verklaring:
Alle gegevens van cliënten, patiënten en medewerkers waren altijd al veilig bij Movement Therapy. Met de per 25 mei 2018 ingaande "Algemene Verordening Persoonsgegevens" (AGV) staat het nu ook in deze verklaring. Deze verklaring is in zijn geheel in te zien op de site
www.autoriteitpersoonsgegevens.nl
Met het tekenen van dit formulier gaat u akkoord met onze AVG.

Mocht u na het lezen van deze brief nog vragen hebben kunt u ons bereiken op …….
(*telefoonnummer praktijk)*
Wij wens u een succes volle behandeling toe.

Met vriendelijke groet,
(naam bedrijf……..)

☐ Door het invullen van de onder staande gegevens ga ik akkoord met de boven genoemde informatie inclusief AVG.

Naam : _____

Email : _____

Datum :_____

Handtekening:

☐ Hierbij ga ik akkoord met het verstrekken van mijn gegevens aan derden indien noodzakelijk. Dit wordt vooraf altijd nogmaals met u overlegd.

Handtekening:

Bibliografie

Autoriteit Persoonsgegevens. (2015, December 8). *Meldplicht datalekken*. Opgeroepen op Mei 10, 2018, van Autoriteit Persoonsgegevens: https://autoriteitpersoonsgegevens.nl/nl/onderwerpen/beveiliging/meldplicht-datalekken

Autoriteit Persoonsgegevens. (2017, Oktober). *Data protection impact assessment (DPIA)*. Opgehaald van AutoriteitPersoonsgegevens: https://autoriteitpersoonsgegevens.nl/nl/onderwerpen/avg-nieuwe-europese-privacywetgeving/data-protection-impact-assessment-dpia

Autoriteit Persoonsgegevens. (2017, April). *Functionaris voor de gegevensbescherming (FG)*. Opgeroepen op Mei 10, 2018, van Autoriteit Persoonsgegevens: https://autoriteitpersoonsgegevens.nl/nl/onderwerpen/avg-nieuwe-europese-privacywetgeving/functionaris-voor-de-gegevensbescherming-fg

Autoriteit Persoonsgegevens. (2017, April). *Leidende toezichthouder*. Opgeroepen op Mei 10, 2018, van Autoriteit Peroonsgegevens: https://autoriteitpersoonsgegevens.nl/nl/onderwerpen/avg-nieuwe-europese-privacywetgeving/leidende-toezichthouder

Autoriteit Persoonsgegevens. (2017, April). *Wat houdt het recht van dataportabiliteit in?* Opgeroepen op Mei 10, 2018, van Autoriteit Persoonsgegevens: https://autoriteitpersoonsgegevens.nl/nl/onderwerpen/avg-nieuwe-europese-privacywetgeving/rechten-van-betrokkenen

Autoriteit Persoonsgegevens. (2018). *Algemene informatie AVG.* Autoriteit Persoongegevens. Opgeroepen op Mei 10, 2018, van https://autoriteitpersoonsgegevens.nl/nl/onderwerpen/avg-nieuwe-europese-privacywetgeving/algemene-informatie-avg

Autoriteit Persoonsgegevens. (2018). *De AVG-privacyrechten*. Opgeroepen op Mei 10, 2018, van AutoriteitPersoonsgegevens: https://autoriteitpersoonsgegevens.nl/nl/onderwerpen/avg-nieuwe-europese-privacywetgeving/rechten-van-betrokkenen

Europa decentraal. (2017). *Toestemming gegevensverwerking*. Opgeroepen op Mei 10, 2018, van Europadecentraal: https://europadecentraal.nl/onderwerp/informatiemaatschappij/gegevensbescherming-en-de-avg/rechtmatigheid-en-transparantie/toestemming/

Falque-Pierrotin. (2017). *Groep gegevensbescherming artikel 29.* Brussel: Autoriteit Persoonsgegevens. Opgeroepen op Mei 10, 2018, van https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/vertaling_guidelines_leidende_toezichthouder.pdf

Ministerie van Volksgezondheid, Welzijn en Sport. (Z.J.). *WGBO*. Opgeroepen op Mei 05, 2018, van Informatielangdurigezorg: https://www.informatielangdurigezorg.nl/wgbo

Nederlandict. (2017, April 5). *De AVG uitgelegd deel 3: privacy by design en privacy by default*. Opgeroepen op Mei 10, 2018, van Nederlandict: https://www.nederlandict.nl/news/avg-uitgelegd-deel-3-privacy-by-design-privacy-by-default/

NIVEL. (2018). *Onderzoeksprogramma*. Opgeroepen op Mei 05, 2018, van NIVEL: https://www.nivel.nl/nl/onderzoeksprogramma

Norea. (2015, November). *Privacy Impact Assessment (PIA)*. Opgeroepen op Mei 05, 2018, van Norea: https://www.norea.nl/download/?id=522

Qualizorg. (2018). *Achtergrond Qualizorg*. Opgeroepen op Mei 5, 2018, van Qualizorg: https://qualizorg.nl/over-qualizorg/organisatie/

Rijksoverheid. (2018, Januari 25). *Model verwerkersovereenkomst*. Opgeroepen op Mei 10, 2018, van Rijksoverheid: https://www.rijksoverheid.nl/documenten/publicaties/2018/01/25/model-verwerkersovereenkomst-avg

Verhagen, P., & Haarsma-den Dekker, C. (2014). *Ondernemen en innoveren in zorg en welzijn.* Bussum: Coutinho. Opgeroepen op Mei 05, 2018

VvOCM. (2016, September 6). *Start pilot Landelijke Database Oefentherapie*. Opgeroepen op Mei 05, 2018, van VvOCM: https://vvocm.nl/Oefentherapeut/Nieuws/ID/763/Start-pilot-Landelijke-Database-Oefentherapie