AVG verklaring

Hierbij verklaart de Stichting AVG voor Verenigingen dat Fysio-s het AVG-programma geheel of gedeeltelijk heeft doorlopen. Fysio-s verklaart hiermee dat de inspanningen zijn verricht zoals die voortvloeien uit de Algemene Verordening Gegevensbescherming (AVG).

Indien niet alle programmaonderdelen zijn afgewerkt en de verklaring toch wordt aangevraagd, dan is geen volledige invulling gegeven aan de eisen van de wetgever. De Stichting AVG voor Verenigingen adviseert de openstaande punten alsnog zo snel mogelijk af te werken en in elk geval in het programma een aantekening te maken wanneer dit zal gebeuren.

In de hierna volgende verklaring staan alle onderdelen/stappen die Fysio-s heeft doorlopen om te voldoen aan de AVG-wetgeving. Per onderdeel is duidelijk aangegeven welke gegevens en onderdelen van de wet van toepassing zijn en hoe daar aan voldaan is. Waar nodig is additionele informatie verstrekt ter verduidelijking van de situatie.

Fysio-s begrijpt dat AVG-wetgeving continu van toepassing is en dat wij regelmatig de gegevens moeten controleren en updaten.

Met het volledig doorlopen van het AVG-programma van de Stichting AVG voor Verenigingen heeft Fysio-s kennis over de materie ontvangen die door de AVG wordt geraakt, en verklaart zelf naar eer en geweten aan de wet te voldoen. De onderdelen van de zelfverklaring door Fysio-s zijn te vinden op de volgende pagina('s) van deze verklaring.

Aldus opgemaakt te Gorinchem,

d.d. 30-1-2020,

door Stichting AVG voor Verenigingen

gevestigd aan de Stephensonweg 14 te Gorinchem.

2.1 Inventarisatie persoonsgegevens.

Geef hieronder aan welke persoonsgegevens binnen de organisatie gebruikt worden.

Gewone persoonsgegevens

- [x] Naam/ voorletters/ tussenvoegsel
- [x] Titels
- [x] Adres
- [x] Postcode
- [x] Plaats
- [ ] Provincie
- [ ] Land
- [x] Woonplaats
- [x] Telefoonnummer
- [ ] Faxnummer
- [x] E-mailadres
- [ ] Website
- [x] Geslacht
- [x] Geboortedatum
- [ ] Geboorteplaats
- [ ] Overlijdensdatum
- [x] Burgerlijke staat
- [ ] LinkedIn
- [ ] Facebook
- [ ] Twitter
- [x] Werkzaam bij organisatie
- [x] Bankrekeningnummer
- [x] Inloggegevens (gebruikersnaam/wachtwoord)
- [ ] Voertuig kentekenplaat
- [x] Salarisgegevens Salarisgegevens worden niet gezien als bijzondere gegevens.

Andere gewone persoonsgegevens:

Bijzondere persoonsgegevens

- [ ] Etnische afkomst
- [ ] Politieke opvattingen of voorkeur
- [ ] Religieuze opvatting of overtuiging
- [ ] Lidmaatschap van een vakbond
- [ ] Genetische of biometrische gegevens met het oog op unieke identificatie
- [x] Gegevens over gezondheid
- [ ] Gegevens over seksuele geaardheid
- [ ] Strafrechtelijke gegevens of veroordelingen of daarmee verband houdende veiligheidsmaatregelen
- [x] Kopie identiteitsbewijs/paspoort, zonder voorlegger gekopieerd
- [x] BSN-nummer Organisaties buiten de overheid mogen het BSN alleen gebruiken als dat wettelijk is bepaald. Dit geldt bijvoorbeeld voor werkgevers, zorgverleners, zoals huisartsen, apotheken en zorgverzekeraars. Ook in het onderwijs en kinderopvang wordt het BSN gebruikt.

Aantekeningen bijzondere persoonsgegevens:

Wij zijn een fysiotherapiepraktijk en gebruiken het BSN voor het opvragen van de juiste adresgegevens en zorgverzekeraar gegevens. Wij zijn verplicht de identiteit van de patiënten vast te stellen aan de hand van een geldig identiteitsbewijs. Deze gegevens worden ook geregistreerd door ons.Verder worden door de patiënten gegevens verstrekt over hun gezondheidstoestand. Deze worden door ons samen met onderzoek en behandelgegevens geregistreerd in elektronisch patiëntendossier.

3.1 Inventarisatie doelbinding.

Welke persoonsgegevens verwerk je, met welk doel en heb je ze daar ook voor gekregen? Dat noemen we ‘doelbinding’. Het is belangrijk dat je persoonsgegevens alleen verwerkt (dus opslaat en gebruikt) voor de doeleinden waarvoor je deze hebt verkregen.
Voor de inventarisatie van de vormen van doelbinding binnen de onderneming hebben wij onderstaand schema gemaakt. Voor doelbindingen die veel voorkomen, hebben wij het schema al ingevuld en die kun je dus zo aanvinken. Komen er binnen je onderneming nog andere doelbindingen voor, dan kun je deze in de open vorm noteren bij 3.3.

Grondslag: Grondslag is een reden op basis waarvan je de persoonsgegevens mag verwerken. Een reden kan zijn een verkregen toestemming (b.v. het krijgen van een visitekaartje of een inschrijving voor een nieuwsbrief). Een reden kan ook zijn dat je deze persoonsgegevens nodig hebt voor het uitvoeren van een overeenkomst (b.v. een koopcontract of een lidmaatschapsovereenkomst).

LET OP: Het is verstandig zo min mogelijk persoonsgegevens te hanteren. Vraag dus alleen de gegevens die je echt nodig hebt voor het goed functioneren van je organisatie.

(N = Naam, A = Adres, W = Woonplaats, T = Telefoon, E = e-mailadres)

☐ **Klant of leverancier**

Persoonsgegevens: NAWTE.

Grondslag: Opdracht of contract.

Verwerkingen: Administratie, bevestiging, uitlevering.

Verwerkt door: Afdeling administratie, afdeling sales en afdeling inkoop.

Bewaartermijn: Gedurende de looptijd van de overeenkomst.

Beschrijf hieronder kort uw situatie:

n.v.t.

☑ **Klant en BSN**

Organisaties buiten de overheid mogen het BSN (burger-servicenummer) alleen gebruiken als dat volgens de wet is toegestaan. Anders mag het niet! Het is toegestaan voor bijvoorbeeld werkgevers, zorgverleners, zoals huisartsen en apotheken en ook voor zorgverzekeraars. Ook in het onderwijs wordt het BSN gebruikt. Hier heet het ook wel onderwijsnummer of persoonsgebonden nummer. Organisaties kunnen niet onder het verbod uitkomen door mensen toestemming te vragen voor het gebruik van hun BSN!

Persoonsgegevens: NAWTE + BSN.

Grondslag: Overeenkomst met handtekening op papier.

Verwerkingen: Interactie met de overheid in het belang van (en met toestemming van) de klant.

Verwerkt door: Afdeling administratie.

Bewaartermijn: Gedurende de looptijd van de overeenkomst.

Beschrijf hieronder kort uw situatie:

Fysio-s is een zorgverlenend bedrijf. Fysiotherapie, manuele therapie en fitness bieden wij aan aan onze klanten. Elke fysiotherapeut is verantwoordelijk voor de eigen administratie van de klantgegevens. Wij gebruiken het BSN voor opvragen van naam- en adresgegevens via het UZI-register en voor opvragen verzekerkeringsgegevens bij de zorgverzekeraar van de klant. Gegevens worden geregistreerd in elektronisch patiëntendossier en op papieren patiëntenkaarten. Patiëntengegevens worden in principe levenslang bewaard. Zorgverzekeraars en onze administrateurs hebben een duidelijk priviaybeleid en daarmee hebben overeenkomsten afgesloten.

☐ **VvE-leden en -gebruikers**

Het bestuur van de VvE dient op grond van het reglement ex artikel 5:112 BW een register bij te houden van eigenaars en een register van gebruikers. In dit register zijn persoonsgegevens opgenomen.

Persoonsgegevens: NAWTE + bankgegevens + kentekengegevens.

Grondslag: Akte van splitsing en het reglement ex artikel 5:112 BW.

Verwerkingen: Beheeractiviteiten van de VvE in de breedste zin van het woord in het belang van(en met toestemming van) de (gezamenlijke) eigenaars.

Verwerkt door: Bestuur en beheerder.

Bewaartermijn: Gedurende lidmaatschap of gebruik en 12 maanden daarna en voorts alleen in de financiële administratie voor maximaal 7 jaar.

Beschrijf hieronder kort uw situatie:

n.v.t.

☐ **Aanmelden voor nieuwsbrief**

Persoonsgegevens: Naam en e-mailadres.

Grondslag: Aanmelding voor nieuwsbrief (formulier op de website).

Verwerkingen: Informatie verstrekking in de vorm van nieuwsbrieven.

Verwerkt door: Afdeling communicatie.

Bewaartermijn: Gedurende de periode dat men aangemeld is.

Beschrijf hieronder kort uw situatie:

Wij sturen geen nieuwsbrieven.

☐ **Prospect, stakeholder-/lobbycontacten en geïnteresseerde**

Persoonsgegevens: NAWTE.

Grondslag: Mondelinge toestemming, afgifte visitekaartje en/of via LinkedIn.

Verwerkingen: Informatieverstrekking in de vorm van nieuwsbrieven of gerichte contacten.

Verwerkt door: Afdeling communicatie, directie, vakkennisafdelingen en/of relatie beheerder.

Bewaartermijn: Gedurende de periode dat men contact heeft.

Beschrijf hieronder kort uw situatie:

n.v.t.

☐ **Stakeholder-/lobbycontacten met politieke voorkeur**

Persoonsgegevens: NAWTE + politieke voorkeur.

Grondslag: Mondelinge toestemming, afgifte visitekaartje en/of via LinkedIn.

Verwerkingen: Persoonlijke contacten en nieuwsvoorziening.

Verwerkt door: Afdeling communicatie, directie.

Bewaartermijn: Gedurende de periode dat men contact heeft.

Beschrijf hieronder kort uw situatie:

n.v.t.

☑ **Medewerkers**

Persoonsgegevens: NAWTE + geboortedatum, kopie ID en bankgegevens.

Grondslag: Arbeidsovereenkomst.

Verwerkingen: Salariëring.

Verwerkt door: HRM-afdeling.

Bewaartermijn: Gedurende de periode dat men een contract heeft.

Beschrijf hieronder kort uw situatie:

Medewerkers hebben een arbeidsovereenkomst met Fysio-s. In het kader daarvan is het onze wettelijke plicht een kopie ID in onze administratie op te nemen. Dit wordt met de overige gegevens bij praktijkeigenaar (Hans Mandemaker) thuis opgeborgen. De loonadministratie wordt verwerkt door Hans Mandemaker en de loonberekeningen worden gedaan door Verhulst en Van Gestel accountancy, Hoofdstraat 37, 5481 AA Schijndel . Zij verzorgen ook de jaaropgave van de medewerkers. De loongegevens worden verstuurd via de mail, maar via een beveiligde omgeving. Ook de salarisstroken van het personeel gaat rechtstreeks naar het personeel via beveiligde website met eigen inlogcodes. De loonbetalingen worden gedaan door Manuela van Nuland.

☑ **Medewerkersfoto’s op de website**

Persoonsgegevens: Naam + foto.

Grondslag: Aanvullende personeelsovereenkomst.

Verwerkingen: Medewerkersfoto’s op website.

Verwerkt door: Administratie, afdeling communicatie.

Bewaartermijn: Gedurende de periode dat men een contract heeft.

Beschrijf hieronder kort uw situatie:

Verwerking gebeurt door praktijkeigenaren. Hans Mandemaker beheert de website en zorgt dat gegevens actueel zijn. Medewerkers hebben toestemming verleend voor het plaatsen van hun foto op de website. Ook naam en foto van in pand aanwezige podotherapeuten worden met hun toestemming op de website vermeld.

☐ **Vrijwilligers**

Persoonsgegevens: NAWTE.

Grondslag: Vrijwilligersovereenkomst.

Verwerkingen: Informatieverstrekking.

Verwerkt door: Afdeling communicatie, vakkennisafdelingen en/of relatie beheerder.

Bewaartermijn: Gedurende de periode dat men een contract heeft.

Beschrijf hieronder kort uw situatie:

n.v.t.

☐ **Direct marketing (alleen bellen of papier)**

Persoonsgegevens: NAWTE.

Grondslag: Geen overeenkomst nodig.

Verwerkingen: Toesturen van (of bellen over) informatie over de organisatie en/of producten/diensten.

Verwerkt door: Afdeling marketing/communicatie.

Bewaartermijn: Gedurende de periode dat men gezien wordt als prospect voor de organisatie of haar diensten/producten.

Beschrijf hieronder kort uw situatie:

n.v.t.

☑ **Digitale direct marketing (e-mail, facebook, LinkedIn, fax, SMS etc.)**

Persoonsgegevens: NAWTE.

Grondslag: Digitale toestemming vooraf, b.v. bij aanvragen van informatie of inschrijven voor een nieuwsbrief.

Verwerkingen: Digitaal toesturen van (of benaderen over) informatie over de organisatie en/of producten/diensten.

Verwerkt door: Afdeling marketing/communicatie.

Bewaartermijn: Gedurende de periode dat men gezien wordt als prospect voor de organisatie of haar diensten/producten.

Beschrijf hieronder kort uw situatie:

Wij gebruiken e-mailadressen van onze klanten voor patiëntenenquête via Qualiview, onderdeel van Qualizorg B.V., Maagdenburgstraat 22, 7421 ZC Deventer. Dit wordt door de zorgverzekeraars aan ons opgedragen en wij moeten hieraan meewerken. Met Qualizorg B.V. hebben we een verwerkersovereenkomst afgeloten. We hebben een Facebookpagina en daarop wordt door ons informatie verstrekt aan zij die onze pagina hebben "geliked". Er worden op onze website geen persoonsgegevens van anderen gebruikt.

3.3 Beschrijving van extra doelbinding.

Als je meer persoonsgegevens, verwerkingen en/of overeenkomsten hebt dan bij 3.1 beschreven, voeg deze dan hieronder toe. Voeg de extra beschrijving over doelen en doelbinding hieronder toe zodat we die kunnen opnemen in de AVG-verklaring.

Groepen van personen Persoonsgegevens Grondslag verwerking Verwerking Bewaartermijn Verwerking door wie Verwerking door derden Verwerking buiten de EU ICT-systemen Technische en organisatorische beveiligingsmaatregelen Toelichting
Deze velden worden gebruikt voor het opstellen van de privacy policy Deze velden zijn voor intern gebruik om o.a. de autorisatie matrix op te stellen
Benoem groepen van personen van wie je persoonsgegevens ontvangt. Benoem de persoonsgegevens die je ontvangt. Maak de bijzondere persoonsgegevens vetgedrukt. Wat is de basis die van toepassing is: Uitvoering van een overeenkomst of toestemming of wettelijke verplichtingetc. Beschrijf in globale termen wat je met de persoonsgegevens doet. Beschrijf hoe lang je de gegevens bewaart nadat de overeenkomst is beeindigd. Beschrijf met globale rollen wie de gegevens verwerkt. Als een deel van de verwerkingen door derden wordt uitgevoerd, beschrijf dan hier welke partijen dat zijn. Geef aan of gegevens worden doorgegeven landen buiten de EU. In welke ICT-systemen worden de persoonsgegevens opgeslagen of verwerkt. Beschrijf hoe de persoonsgegevens beveiligd zijn, zowel technisch als organisatorisch
Hieronder zijn al een aantal voorbeelden ingevuld. Wat niet van toepassing is kun je verwijderen of aanpassen. Ook kun je nieuwe regels toevoegen. Probeer de beschrijving globaal te houden.
Als je meer dan 10 doelbindingen nodig hebt, kijk dan nog even goed of je deze niet kunt samenvoegen.
Klant (patiënt) Naam, Adres, Woonplaats, Telefoon, E-mailadres, BSN, Zorgverzekeraar, Zorgverzekeraarsnummer, Huisarts, Identiteitsgegevens en in een patiëntendossier worden alle gegevens genoteerd die relevant zijn voor de therapie (anamnese (incl. medische voorgeschiedenis en medicijngebruik), onderzoek en behandelgegevens). Vraag van klant (patiënt) om professionele therapeutische hulp Gegevens worden vastgelegd in administratie. Een patiëntendossier wordt gemaakt, deels op papier en deels op de computer. Gegevens op papier worden gedurende de behandelingen bewaard in de behandelkamer van de behandelaar en gearchiveerd bij de praktijkeigenaren thuis. Op de computer wordt het beheerd door Intramed-online. In principe blijven ze bewaard voor altijd. Patiënt kan zelf verzoeken om vernietiging van gegevens. Bij beëindiging praktijk worden de gegevens overgedragen aan opvolger of vernietigd. Praktijkeigenaren en medewerkers. Ieder administreert eigen klanten (patiënten). Manuela van Nuland verzorgt een deel van de patiëntenadministratie van Frank van Nuland. n.v.t. In praktijkadministratie van Intramed en Fysioroadmap, via Intramed-online. Iedere medewerker heeft eigen gebruikersnaam en wachtwoord op alle systemen. Autorisatie procedure en Back-up procedure wordt uitgevoerd door Intramed-online.
Klant (fitnesser) Naam, adres, woonplaats, telefoonnummer, e-mailadres, evt bankrekeningnummer bij automatische incasso, geboortedatum, leeftijd en gewicht. Trainingsgegevens. Schriftelijke overeenkomst die door klant (fitnesser) wordt ingevuld en ondertekend.Wordt in administratie thuis bij praktijkeigenaar bewaard. Gegevens worden vastgelegd in administratie op papier. Trainingsgegevens op papier worden gedurende de trainingen bewaard en zijn voor de klant (fitnesser) beschikbaar wanneer hij komt trainen. Gegevens op papier worden gedurende de trainingen bewaard en na beeindiging van de overeenkomst vernietigd. In de financiele administratie worden de gegevens minimaal 7 jaar bewaard. Praktijkeigenaren en medewerkers. Manuela van Nuland verzorgt de automatisch incasso van de klant (fitnesser). n.v.t. Alles uitsluitend op papier. De automatische incasso's online via ING bank. n.v.t.
Klant (fitnesser) die mededelingen en/of nieuwsbrief wil ontvangen per e-mail Naam, E-mailadres Mondelinge toestemming en door klant (fitnesser) zelf verstrekt e-mailadres. Informatie verstrekking in de vorm van nieuwsbrieven. Gedurende de periode dat men een overeenkomst heeft met Fysio-s om te sporten en kan op verzoek van klant (fitnesser) op ieder moment worden stopgezet. Praktijkeigenaren en medewerkers n.v.t. n.v.t. Wordt alleen schriftelijk vastgelegd. Contracten worden door praktijkeigenaren thuis opgeborgen.
Medewerker. Naam, Adres, Woonplaats, Telefoon, E-mailadres, Geboortedatum, kopie ID, BSN, Bankgegevens en foto('s) voor website. Arbeidsovereenkomst, geheimhoudingsverklaring en toestemmingsovereenkomst voor gebruik van gegevens en foto op website en Facebookpagina van praktijk. Worden gebruik voor salarisadministratie. Verder worden enkele persoonsgegevens vermeld op de website van de praktijk, inclusief foto van medewerker. Gedurende de periode dat medewerker een contract heeft en daarna alleen in de financiële administratie voor maximaal 7 jaar. Praktijkeigenaren. Extern bureau: Verhulst en Van Gestel Accountancy, Hoofdstraat 37, 5481 AA Schijndel. Manuela van Nuland verzorgt de loonuitbetaling. n.v.t. Loongegevens worden via de mail verstuurd en ontvangen. Arbeidsovereenkomsten en persoonsgegevens worden door praktijkeigenaren thuis opgeborgen.

4.1 Privacy policy vindbaar, verwijzing in documenten.

De privacy policy van de organisatie moet voor iedereen waarvan je persoonsgegevens verwerkt vindbaar zijn. Het eenvoudigste is om deze op de website van de organisatie te zetten en op elke pagina (onderaan) een link hier naartoe te leggen.

- [x] Wij als organisatie hebben onze privacy policy zichtbaar gemaakt op onze website.
- [ ] Wij als organisatie hebben onze privacy policy niet vindbaar gemaakt op onze website.

Beschrijf hieronder kort uw situatie:

Website is aangepast en privacy policy is nu via de website te downloaden.

In alle overeenkomsten (documenten waarin persoonsgegevens gevraagd worden) moet een verwijzing staan naar de privacy policy.

- [ ] Wij als organisatie verwijzen in al onze documenten (contract, overeenkomst, aanmeldingsformulier, etc.) waarin persoonsgegevens staan naar onze privacy policy op de website van de organisatie.
- [x] Wij als organisatie verwijzen in documenten (contract, overeenkomst, aanmeldingsformulier, etc.) waarin persoonsgegevens staan niet naar onze privacy policy op de website van de organisatie.

Beschrijf hieronder kort uw situatie:

We zijn onze folders aan het herschrijven. In komende uitgave zal privacy policy worden vermeld.

5.1 Werken met verwerkersovereenkomst.

Als organisatie mag je persoonsgegevens niet doorgeven aan een andere partij welke ten behoeve van jou persoonsgegevens verwerkt zonder een verwerkersovereenkomst. In een verwerkersovereenkomst spreek je af wat de ander met de gegevens mag doen én ook vooral wat niet.

- ○ Wij als organisatie verklaren dat wij nooit persoonsgegevens doorgeven aan andere partijen waarmee we geen verwerkersovereenkomst hebben afgesloten als dit noodzakelijk is voor uitvoering van de doeleinden waarvoor we ze hebben gekregen.
- ⊘ Wij als organisatie verklaren dat wij ook persoonsgegevens doorgeven aan andere partijen waarmee we geen verwerkersovereenkomst hebben afgesloten.
- ○ Wij als organisatie verklaren dat wij geen persoonsgegevens doorgeven aan andere partijen.

Beschrijf hieronder kort uw situatie:

Wij communiceren met verwijzers en zorgverzekeraars, waarbij er vanuit gaan dat zij de gegevens zorgvuldig hanteren. De persoonsgegevens worden geminimaliseerd. Communicatie met huisartsen verloopt via Zorgmail. Met diverse partijen waar we mee communiceren t.a.v. patiëntgegevens hebben we wel verwerkingsovereenkomsten afgesloten.

6.1 Toegangsbeveiliging.

Om zeker te weten dat alleen geautoriseerde personen de persoonsgegevens kunnen inzien en bewerken, moeten deze altijd beveiligd zijn met een wachtwoord en als het kan ook met een gebruikersnaam. Zo kun je een Excel-bestand beveiligen met een wachtwoord en een PC voorzien van een gebruikersnaam en een wachtwoord. Zorg er dus voor dat je altijd minimaal één keer een wachtwoord moet weten voordat je de persoonsgegevens van jouw organisatie kunt inzien of bewerken.

- [x] Wij als organisatie hebben persoonsgegevens altijd opgeslagen achter de beveiliging van minimaal een gebruikersnaam en een wachtwoord.
- [ ] Wij als organisatie hebben persoonsgegevens niet altijd opgeslagen achter de beveiliging van minimaal een gebruikersnaam en een wachtwoord.
- [ ] Wij als organisatie hebben geen persoonsgegevens elektronisch opgeslagen en hebben daarom geen toegangsbeveiliging.

Beschrijf hieronder kort uw situatie:

Onze patiënten administratie loopt via Intramed en Fysioroadmap en daarvoor hebben we ieder apart een inlognaam, een wachtwoord en een token dat een code doorgeeft. Deze administratie loopt via Intramed online via hun beveiligde server. Daarna moeten we voor ieder pakket opnieuw inloggen met een gebruikersnaam en wachtwoord. We hebben met deze leveranciers een verwerkingsovereenkomst afgesloten.

7.1 Software en antivirussoftware up-to-date.

Om systemen zo veilig mogelijk te laten zijn, moet je ze up-to-date houden. Dit doe je door het aanzetten van het automatisch ophalen en installeren van updates van de software. Zorg ook voor goede antivirussoftware. Zorg ervoor dat alle software ingesteld is op het automatisch ophalen en uitvoeren van updates. Maak goede afspraken met al je softwareleveranciers.

- [x] Wij als organisatie hebben de persoonsgegevens alleen opgeslagen op computers/servers met beveiligingssoftware waarbij zowel de beveiligingssoftware als het besturingssysteem ingesteld zijn om automatisch updates op te halen en te installeren.
- [ ] Wij als organisatie hebben de persoonsgegevens niet alleen opgeslagen op computers/servers met beveiligingssoftware waarbij zowel de beveiligingssoftware als het besturingssysteem ingesteld zijn om automatisch updates op te halen en te installeren.
- [ ] Wij als organisatie hebben geen persoonsgegevens elektronisch opgeslagen en hebben daarom geen software updates.

Beschrijf hieronder kort uw situatie:

Dit gebeurt allemaal via Intramed-online.

8.1 Opslaan alleen binnen de EU.

Binnen de EU is het niveau van gegevensbescherming gelijk. Dat komt omdat alle EU-lidstaten moeten voldoen aan de AVG. Als je persoonsgegevens verwerkt buiten de EU, bijvoorbeeld door deze te laten verwerken door een partij buiten de EU of er een passend beschermingsniveau bestaat voor dat land , bijvoorbeeld door een adequaatheidbesluit van de Europese Commissie. Je moet ook weten en kunnen aantonen dat er passende of geschikte waarborgen zijn, en hoe er een kopie van kan worden verkregen of waar ze kunnen worden geraadpleegd.

De wetgever is dus extra streng als je persoonsgegevens wilt verwerken/opslaan buiten de EU. Als je dat toch zou willen, dan moet er heel veel geregeld worden bovenop de normale AVG-verplichtingen. Dus check of je dienstverlener (drukker, verspreider, enz.) de toevertrouwde persoonsgegevens binnen de EU opslaat.

Het is dus het makkelijkste om persoonsgegevens alleen te verwerken binnen de EU, dit raden wij daarom ook sterk aan.

- [x] Wij als organisatie verklaren dat wij nooit persoonsgegevens overdragen aan of opslaan bij partijen die gevestigd zijn buiten de EU.
- [ ] Wij als organisatie verklaren dat wij ook persoonsgegevens overdragen aan of opslaan bij partijen die gevestigd zijn buiten de EU.

Beschrijf hieronder kort uw situatie:

Wij werken uitsluitend in Nederland, Schijndel.

9.1 Data back-up.

Om de persoonsgegevens te beschermen tegen het verlies of diefstal moet je back-ups maken. Het is noodzakelijk om dat regelmatig te doen. Zorg ervoor dat deze back-up veilig wordt opgeborgen.

- [x] Wij als organisatie hebben de opgeslagen persoonsgegevens beveiligd met een back-up.
- [ ] Wij als organisatie hebben de persoonsgegevens niet beveiligd met een back-up.
- [ ] Wij als organisatie hebben geen persoonsgegevens elektronisch opgeslagen en hebben daarom geen back-up.

Beschrijf hieronder kort uw situatie:

Intramed-online zorgt hiervoor meerder keren per dag en er draaien altijd 2 systemen gelijktijdig. Er kan niets fout gaan.

10.1 Geautoriseerde medewerkers.

Via autorisatie regel je wie binnen de organisatie welke persoonsgegevens mag verwerken.

- ☑ In onze organisatie hebben alleen geautoriseerde personen toegang tot de persoonsgegevens van de organisatie.
- ○ In onze organisatie hebben ook niet geautoriseerde personen toegang tot de persoonsgegevens van de organisatie.

Beschrijf hieronder kort hoe jullie de autorisatie geregeld hebben:

Echtgenoot van Frank van Nuland doet een deel van de administratie en heeft via toegangscodes van Frank van Nuland toegang tot Intramed-online.
Medewerkers in loondienst en waarnemers die in onze vakantie werken hebben toegang tot de administratie. Zij gebruiken dan onze inloggegevens.
We hebben dit nog niet schriftelijk vastgelegd. Geheimhoudingsverklaring is aanwezig.

Onderstaande vragen zijn alleen ter bewustwording en hoeven niet precies ingevuld te worden!
Wij als organisatie hebben 1 personen geautoriseerd om de persoonsgegevens van de organisatie in te zien en te verwerken indien dit nodig in voor de uitoefening van hun functie.

Wij als organisatie hebben van ongeveer 5000 personen de persoonsgegevens geregistreerd.

11.1 Vernietigen persoonsgegevens.

Geef hieronder aan dat je organisatie alle persoonsgegevens vernietigt door bijvoorbeeld een regel te wissen in Excel en/of het versnipperen van een aanmeldingsformulier als er geen overeenkomst meer is.
Persoonsgegevens mogen niet langer worden bewaard dan voor verwezenlijking van de doeleinden waarvoor ze worden verwerkt. Dus: na beëindiging van een overeenkomst worden de persoonsgegevens van die persoon vernietigd.
Wijs aan wie verantwoordelijk is voor het vernietigen van persoonsgegevens of de controle op de vernietiging.

NB: Verscheuren en weggooien is onvoldoende. Schaf daarom een versnipperaar aan.

Let op: In de financiële administratie mogen (of eigenlijk: moeten!) deze persoonsgegevens nog wel blijven staan, want daar geldt een (wettelijke) bewaarplicht van 7 jaar.

- [x] Wij als organisatie verklaren dat wij alle persoonsgegevens vernietigen als de overeenkomst op grond waarvan ze verkregen zijn verlopen is of de toestemming is ingetrokken.
- [ ] Wij als organisatie verklaren dat wij geen persoonsgegevens vernietigen als de overeenkomst op grond waarvan ze verkregen zijn verlopen is of de toestemming is ingetrokken.

Beschrijf hieronder kort uw situatie:

Wij bewaren patiëntengegevens in principe oneindig lang. Deze informatie is nodig om de klachtengeschiedenis van patiënten te kunnen overzien. Alles wat op papier staat wordt in archieven bij praktijkeigenaren bewaard. Bij beëindiging van de praktijk zullen deze patiëntengegevens worden overgedragen aan opvolger of op de daarvoor geëigende manier worden vernietigd door gecertificeerd bedrijf. Wanneer de klant zelf het dossier wil vernietigen dan wordt dat ook gedaan.

12.1 Toestemming voor direct marketing en bij minderjarigheid.

Bij direct marketing.

De wetgever maakt onderscheid tussen gewone direct marketing (bellen en post sturen) of digitale marketing (via e-mail, fax, Facebook, LinkedIn of sms). Doordat gewone direct marketing een organisatie geld kost zal dat altijd beperkt blijven. Juist digitale marketing is nagenoeg gratis en kan daardoor heel veel toegepast worden met alle gevolgen van dien.

- ○ Wij als organisatie vragen vooraf altijd toestemming voordat we iemand benaderen via digitale direct marketing.
- ○ Wij als organisatie vragen vooraf geen toestemming voordat we iemand benaderen via digitale direct marketing.
- ⊘ Wij als organisatie maken geen gebruik van digitale direct marketing.

Beschrijf hieronder kort uw situatie:

Bij minderjarigheid (jonger dan 16 jaar).

Als je persoonsgegevens online verwerkt van personen jonger dan 16 jaar via bijvoorbeeld een app, online game, webwinkel of via sociale media, dan moet je daarvoor altijd schriftelijk een toestemming hebben van de ouder, verzorger of wettelijke vertegenwoordiger. Geef hieronder aan dat je organisatie dat ook altijd zo doet.

- ⊘ Wij als organisatie verklaren dat wij alleen online persoonsgegevens van minderjarigen verwerken bijvoorbeeld een app, online game, webwinkel of via sociale media als daarvoor schriftelijke toestemming is gegeven door de ouder, verzorger of wettelijke vertegenwoordiger.
- ○ Wij als organisatie verklaren dat wij persoonsgegevens van minderjarigen online verwerken bijvoorbeeld een app, online game, webwinkel of via sociale media zonder dat daarvoor schriftelijke toestemming is gegeven door de ouder, verzorger of wettelijke vertegenwoordiger.
- ○ Wij als organisatie verklaren dat wij geen persoonsgegevens van minderjarigen online verwerken bijvoorbeeld een app, online game, webwinkel of via sociale media.

Beschrijf hieronder kort uw situatie:

Van personen onder de 16 jaar die naar ons worden verwezen worden momenteel de persoonsgegevens en behandelgegevens zonder toestemming van ouder, verzorger of wettelijke vertegenwoordiger geregistreerd. Wanneer wij jongeren onder de 18 jaar een patiëntenenquête toesturen gebeurt dat uitsluitend met schriftelijke toestemming van een van de ouders.

13.1 Papieren documenten en beveiliging.

Als persoonsgegevens ook vastliggen op papier (denk aan contracten), dan moeten die papieren met persoonsgegevens achter slot en grendel zijn opgeslagen. Praktisch: bewaar dus alle papieren met persoonsgegevens in een kast die je steeds op slot doet. Alleen personen die voor hun werk voor de organisatie daarvoor toestemming hebben, mogen in die kast komen.

- ○ Wij als organisatie hebben papieren documenten waarop de persoonsgegevens staan, opgeslagen achter slot en grendel.
- ◉ Wij als organisatie hebben niet alle papieren documenten waarop de persoonsgegevens staan, opgeslagen achter slot en grendel.
- ○ Wij als organisatie hebben geen papieren documenten waarop de persoonsgegevens staan.

Beschrijf hieronder kort uw situatie:

Wij gebruiken naast computerprogramma's ook nog papieren patiëntenkaarten. Deze worden op de praktijk bewaard achter slot. De sleutels worden beheerd door ieder praktijkhouder en de sleutels worden mee naar huis genomen. Deze kaarten worden thuis gearchiveerd en daar heeft dan verder niemand toegang tot de kaarten. Verder worden alle personeelsadministratie en financiële administratie ook thuis bewaard. Trainingsformulieren van sporters liggen niet achter slot. Deze zijn vrij toegankelijk voor de klanten.

14.1 Datalekken.

Iedereen in de organisatie moet op de hoogte zijn wat een een datalek is en wat je eraan moet doen. Geef aan wat voor jullie van toepassing is:

- ☑ Binnen onze organisatie is iedereen op de hoogte van wat een datalek is. Ook is bekend waar dit intern gemeld moet worden zodat wij als organisatie adequaat het datalek kunnen afhandelen en documenteren.
- ○ Binnen onze organisatie is niet iedereen op de hoogte van wat een datalek is. Ook is niet bekend waar dit intern gemeld moet worden zodat wij als organisatie adequaat het datalek kunnen afhandelen en documenteren.

Beschrijf hieronder kort hoe jullie met datalekken omgaan:

De kans op een datalek is binnen onze organisatie uitermate klein. Er zou inderdaad patiëntenkaarten of andere gegevens moeten worden verloren of gestolen. Iedereen werkzaam in de praktijk weet hoe te handelen in deze situatie. De persoon waarvan de gegevens zijn gelekt wordt direkt door ons op de hoogte gesteld.

15.1 Medewerkers geïnstrueerd

Wij hebben onze medewerkers als volgt geïnstrueerd:

- ☐ Alle medewerkers hebben de video van de Stichting AVG bekeken.
- ☑ We hebben het onderwerp privacy bescherming in alle afdelingsoverleggen besproken.
- ☐ We hebben uitlegposters opgehangen.
- ☐ We hebben alle medewerkers een brief gestuurd met uitleg en instructie.
- ☐ We hebben met alle medewerkers een workshop over privacy bescherming gevolgd.
- ☐ We hebben een nieuwsbrief voor alle medewerkers waarin we regelmatig aandacht besteden aan privacy bescherming.
- ☐ Onze directeur/voorzitter heeft alle medewerkers opgeroepen extra aandacht te besteden aan privacy bescherming.

Hieronder is ruimte om te beschrijven hoe jullie de medewerkers geïnstrueerd hebben:

Onze medewerkers hebben nauwelijks toegang tot de persoonsgegevens. Zij werken alleen met sporters. Wij moeten hen nog nader informeren over de AVG.

16.3 Afronding.

Naam organisatie:	Fysio-s
Plaats:	Schijndel
Datum:	30-1-2020

De AVG-verklaring is een automatische samenvatting van alle vragen en antwoorden in het stappenplan. De AVG-verklaring is geen juridisch document maar een verklaring waarin je zelf verklaart dat je alle inspanningen hebt gepleegd om aan de Algemene Verordening Gegevensbescherming te voldoen. Wij zien in de praktijk dat sommige gebruikers de AVG-verklaring regelmatig opvragen en gebruiken als een todolijst.
Je kunt de AVG-verklaring zo vaak opvragen als je wilt.