AVG verklaring

AVG PROGRAMMA

MTC de Viergang

Uitgegeven op 19-2-2024

Geldig tot 19-5-2024

De bescherming van persoonlijke gegevens is geen eenmalige zaak.

Ook al heb je het eenmalig goed ingericht, de wet vereist dat je met een actueel document kunt aantonen dat je voldoet aan de AVG. De Autoriteit Persoonsgegevens (AP) controleert dat steekproefsgewijs.

Deze AVG-verklaring laat zien dat je alle verplichtingen vanuit de wet AVG hebt uitgevoerd (mits je alle onderdelen hebt ingevoerd). Als er iets verandert in jouw organisatie kun je de stappen opnieuw bekijken en eventueel aanpassen. Daarna vraag je de AVG-verklaring opnieuw op door op de "Verklaring Aanmaken" knop te klikken.

Ook ontvang je elk kwartaal automatisch een nieuwe AVG-verklaring. Bewaar deze digitaal of print hem uit. Zo ben je altijd up-to-date!

AVG verklaring

Hierbij verklaart de Stichting AVG voor Verenigingen dat MTC de Viergang het AVG-programma geheel of gedeeltelijk heeft doorlopen. MTC de Viergang 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 MTC de Viergang 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.

MTC de Viergang begrijpt dat AVG-wetgeving continu van toepassing is en dat zij regelmatig de gegevens moeten controleren en updaten.

Met het volledig doorlopen van het AVG-programma van de Stichting AVG voor Verenigingen heeft MTC de Viergang 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 MTC de Viergang zijn te vinden op de volgende pagina('s) van deze verklaring.

Aldus opgemaakt te Den Haag,

d.d. 19-2-2024,

door Stichting AVG voor Verenigingen

gevestigd aan de Doctor Kuyperstraat 10 te Den Haag.

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
- [x] Provincie
- [x] Land
- [x] Woonplaats
- [x] Telefoonnummer
- [x] Faxnummer
- [x] E-mailadres
- [x] Website
- [x] Geslacht
- [x] Geboortedatum
- [x] Geboorteplaats
- [x] Overlijdensdatum
- [x] Burgerlijke staat
- [ ] LinkedIn
- [x] Facebook
- [x] Twitter
- [x] Werkzaam bij organisatie

- [x] Bankrekeningnummer
- [x] Inloggegevens (gebruikersnaam / wachtwoord)
- [x] Voertuig kentekenplaat
- [x] Salarisgegevens

Andere gewone persoonsgegevens

Ook sla ik telefoonnummers op van partners/ouders van medewerkers om te waarschuwen in geval van nood. 2 voertuigen kentekenplaten staan opgeslagen i.v.m. 2 bedrijfsauto's.

Bijzondere persoonsgegevens

- [ ] Ras of etnische afkomst
- [ ] Politieke opvattingen
- [ ] Religieuze of levensbeschouwelijke overtuiging
- [x] Lidmaatschap van een vakbond
- [ ] Genetische of biometrische gegevens met het oog op unieke identificatie
- [x] Gegevens over gezondheid
- [x] Gegevens over seksueel gedrag of seksuele gerichtheid
- [ ] Strafrechtelijke veroordelingen en strafbare feiten of daarmee verband houdende veiligheidsmaatregelen
- [x] Kopie identiteitsbewijs/paspoort, zonder voorlegger gekopieerd
- [x] BSN-nummer

Aantekeningen bijzondere persoonsgegevens

Mijn medewerkers zijn aangesloten bij de beroepsorganisatie van fysiotherapeuten, het KNGF. Daarnaast zijn ze BIG geregistreerd, VEKTIS geregistreerd op openbare site AGB webzoeker en staan ze in het KRF-NL (beroepsgroep). Ik betaal hun lidmaatschapsgelden. De BIG nummers staan op onze website vermeld. Verder zijn wij een gezondheidsinstelling 1e lijn fysiotherapie en verwerken wij dus bijzondere persoonsgegevens. Elk personeelslid moet een VOG verklaring afgeven bij indienst treding, dit staat geregistreerd.

3.1 Inventarisatie doelbinding

Grondslag

Je moet een goede reden hebben om persoonsgegevens te mogen verwerken. De juridische naam voor die redenen is grondslagen. Je hebt dus een grondslag nodig om persoonsgegevens te mogen verwerken. In de AVG staan de volgende 6 grondslagen voor het verwerken van persoonsgegevens:

- U heeft toestemming van de persoon om wie het gaat,
- Het is noodzakelijk om gegevens te verwerken,
  - om een overeenkomst uit te voeren,
  - omdat u dit wettelijk verplicht bent,
  - om vitale belangen te beschermen,
  - om een taak van algemeen belang of openbaar gezag uit te oefenen.
- Het is noodzakelijk om gegevens te verwerken om uw gerechtvaardigde belang te behartigen.

Voorbeelden van grondslagen zijn:

- Toestemming = ondertekening van een toestemmingsformulier of een inschrijving door middel van een opt-in voor een nieuwsbrief,
- Overeenkomst = je hebt deze persoonsgegevens nodig voor het uitvoeren van een overeenkomst (b.v. een koopcontract of een lidmaatschapsovereenkomst),
- Gerechtvaardigd belang = bestaande klanten na een aankoop te informeren over soortgelijke, eigen producten of diensten.

Doelbinding

Welke persoonsgegevens verwerk je, met welk doel en heb je ze daar ook voor gekregen (grondslag)? Dat noemen we ‘doelbinding’. Het is belangrijk dat je persoonsgegevens alleen verwerkt (dus opslaat en gebruikt) voor de doeleinden waarvoor je deze hebt verkregen. In de doelbinding beschrijf je dus welke gegevens, met welke grondslag en wat je met die gegevens doet.

Voor de inventarisatie van de vormen van doelbinding binnen de organisatie 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 organisatie nog andere doelbindingen voor, dan kun je deze in de open vorm noteren bij 3.3.

Bewaartermijn

Het uitgangspunt is dat je persoonsgegevens niet langer mag bewaren dan noodzakelijk. Wat noodzakelijk is hangt af van de situatie. Dit staat niet concreet beschreven in de AVG en dus moet je bepalen wat in jouw situatie passend is.

Wel zijn er andere wettelijke termijnen waar je je aan moet houden. Bijvoorbeeld op grond van belastingwetgeving of de Archiefwet. Zo moet je voor de belastingdienst je administratie 7 jaar bewaren.

LET OP: Je bent wettelijk verplicht zo min mogelijk persoonsgegevens te verwerken. 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

We zijn een praktijk voor fysiotherapie . We hebben te maken met cliënten c.q. patiënten, met medewerkers, stagiaires en leveranciers. Daarnaast versturen we informatie over patiënten (na toestemming patiënten) naar andere zorgverleners en anoniem naar zorgverzekeraars (LDF) en ontvangen we van hen visa versa gegevens (polisgegevens m.b.t. vergoedingen voor fysiotherapie).

Daarnaast hebben wij een zeer streng persoonlijk contract afgesloten om BRP gegevens van de gemeentes te mogen overnemen ter controle van persoonsgegevens. Deze gegevens worden verwerkt en staan onder strikte geheimhouding binnen onze organisatie. Elk personeelslid heeft een strikte geheimhouding en boeteclausule getekend om hier mee om te mogen gaan.

Gegevens van medewerkers delen we met onze accountant, salarisverwerkingsbedrijf en boekhouder en voor een deel die noodzakelijk zijn voor de verwerking met onze beroepsvereniging en zorgverzekeraars.

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

Van alle medewerkers vragen we het BSN nummer voor onze administratie die we delen met de zorgverzekeraars, de accountant en de beroepsvereniging.
Van alle patienten vragen we het BSN nummer op en registreren we dat in ons patienten volgsysteem. Als de patient zijn of haar BSN nummer niet geeft kunnen we dat opvragen via een digitaal hoog beveiligd certificaat dat we in de beschermde cloud van Intramed BV hebben staan a.d.h.v. adres gegevens en achternaam die de patiënt wel levert. En waarmee we gerechtigd zijn om patient gegevens op te halen uit de Gemeentelijk Basis Administratie. Wel moeten we dit bij het contact met de patient controleren op juistheid van de opgevraagde gegevens door controle van een geldig NL ID bewijs.

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

Wij huren dit pand van Vastgoed Viergang B.V. Dit betekent dat de NAWTE en bankgegevens van Ruud Lindenburg (eigenaar eenmanszaak MTC) bekend zijn bij de verhuurders.

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

Wij vragen aan patiënten hun e-mailadres om hen mailingen te versturen, echter alleen na expliciete toestemming te hebben gegeven worden er vragenlijsten via Intramed verzonden. Indien dit niet wordt gegeven wordt het e-mail adres alleen gebruikt voor reguliere vragen over behandelafspraken maken in onze praktijk, versturen van beveiligde medische rapportages en huiswerkoefeningen. Patiënt is ten alle tijde bevoegd om de toestemming in te trekken voor alle bovenstaande genoemde acties.

☐ 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

☐ 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

☑ 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

Ons bedrijf heeft medewerkers waarvan we de NAWTE gegevens met geboorte datum, BSN en kopie ID en bankgegevens opvragen en vastleggen in onze administratie en we delen deze met onze accountant Syfers en ons salarisadministratiekantoor People&Payment. We delen enkele NAW gegeven sook met ons ARBO kantoor PP ARBO. Ook leggen we een stamkaart vast met daarop de burgerlijke staat en de NAW gegevens van partners in het beveiligde programma Intramed Online. We hebben ook personeelsmappen fysiek achter slot en alarm staan in archiefkasten.

☑ 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

We hebben een bedrijfswebsite waarop de medewerkers staan met naam, BIG nummer (wettelijke verplichting), foto en hun werkdagen/tijden en specialisaties. Op de bedrijfsfacebookpagina/twitter verschijnen soms nieuwsberichten over medewerkers indien zij een bepaalde specialisatie cursus volgen, dan gebruiken wij ook hun naam en foto na toestemming van de medewerker. Ook staan onze medewerkers met naam en foto op enkele andere websites van bijvoorbeeld: www.fysiotherapiepraktijken.nl

☐ 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

☑ 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

Wij bellen en worden gebeld door mogelijke patiënten. Zij willen graag afspraken maken met onze therapeuten om van hun klachten af te komen. Wij bellen mensen die al bij ons onder behandeling zijn ook regelmatig op om afspraken in te plannen, of informatie te geven over de behandeling, tijdstip of locatie van de afspraak. Sommige patiënten zijn niet aanvullend verzekerd, maar betalen particulier. Dan krijgen ze van ons per post soms een nota indien dit niet per e-mail gedaan kan worden.

☑ 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.

Ons bedrijf stuurt aan patiënten de CQ index PREM vragenlijsten (verplichting vanuit zorgverzekeraars voor hulpverleners), zij mogen uiteraard hierop bezwaar maken (OPT out optie), ook sturen wij huiswerkoefeningen op via mail en sturen wij gestandaardiseerde vragenlijsten via Intramed en zivver op per mail.

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.

Toelichting:

NAW gegevens partners van medewerkers. Alleen in geval van nood of alarmsituaties willen wij contact op kunnen nemen met deze partner. Als de medewerker geen partner heeft slaan we de NAWTE gegevens op van ouders of ander familieleden.

4.1 Privacy policy vindbaar, verwijzing in documenten

De privacy policy van de vereniging moet voor iedereen vindbaar zijn. Het eenvoudigste is om deze op de website van de vereniging te zetten en op elke pagina (onderaan) een link hier naar toe 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:

Wij hebben een kopje "Uw Privacy"gemaakt op de Home Pagina van onze website over onze verwerking van persoonsgegevens en medische gegevens.
Bij elke pagina staat een link naar deze pagina. Bovenaan deze privacyverklaring hebben wij ook de AVG verklaring toegevoegd in .pdf format.

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

- [x] 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.
- [ ] 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:

Alle verslagen (tussentijds, eindrapportages, etc.) die naar medische specialisten en/of naar de patiënt zelf gaan worden ondertekend met de afzender + een link naar onze website die verwijst naar de privacy policy en verwerking.

Alle afspraakbevestigingen die worden verstuurd staat een link in die verwijst naar onze privacy verklaring.

In alle mailings over invullen van medische vragenlijsten, verwijzen wij naar de zorgvuldige verwerking van hun gegevens via een link op onze website: https://www.mtcdeviergang.nl/uw-privacy

Voor het gebruik van onze "MijnZorgApp" moeten gebruikers eerst akkoord verklaren omtrent onze privacyvoorwaarden/verklaring.

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.

- [x] 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 geven patiënt gegevens aan de zorgverzekeraars via Vecozo (hoog beveiligde online dienst die alle hulpverleners en zorgverzekeraars gebruiken). Ook gebruikt Qualizorg gegevens van onze patiënt. We denken daarbij ook aan ARBO diensten en verzuimverzekeraars, alles met het oog op noodzakelijkheid en worden geen gegevens verstrekt die onnodig zijn.

Wij verstrekken uitsluitend op verzoek van de patiënt persoonsgegevens en medische gegevens met huisartsen, specialist, collega fysiotherapeuten en overige paramedische beroepen.

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:

Wachtwoord van de gebruiker bij de pc. Daarna nog een wachtwoord om in Intramed in te loggen op elk werkstation is dit een andere gebruiker en inlogcode. Hierna heeft elke fysiotherapeut en administratief medewerker een eigen naam en inlogcode om in Intramed in te loggen. Daarna is er een verplichting om een code in te voeren die gegenereerd wordt door Authenticator app. Hierna kan er pas gewerkt worden met de patiëntgegevens. Elk werkstation vergrendelt zichzelf na 5 min geen actief gebruik. En elke fysiotherapeut vergrendelt het station actief wanneer hij/zij klaar is op het station.

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:

Alle intramedgegevens over NAW en medische info staat in de cloud op de servers van Intramed. Alle werkstations hebben anti virus programma's en zijn voorzien van automatische updates.

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.

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.
- [ ] Wij als organisatie verklaren dat wij ook persoonsgegevens overdragen aan of opslaan bij partijen die gevestigd zijn buiten de EU. Wij hebben hiervoor de correcte maatregelen en overeenkomsten afgesloten. Onze situatie hebben wij hieronder beschreven.

Beschrijf hieronder kort uw situatie:

Wij slaan gegevens op in Intramed B.V. in de cloud, gegevens van medewerkers in en op de beveiligde servers van de accountant en salarisverwerker. En alle gegevens op onze eigen afgesloten NAS servers.

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:

Alle gegevens van patiënten worden opgeslagen en bijgehouden in ons software pakket Intramed. We gebruiken Intramed in een online omgeving. Intramed zelf zorgt voor backup van deze data. Gegevens van personeel worden opgeslagen in online software pakketten die beheerd worden door onze accountant en salarisverwerker en ook zijn maken backup's op hun beveiligde servers online. Ook maken we als bedrijf zelf backup's van data die op onze harde schijven staat. Deze backup wordt gemaakt op een harde schijf die met encryptie beveiligd ligt in een datakluis die op het bedrijf achter slot en grendel ligt.

10.1 Geautoriseerde medewerkers

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

- [x] 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 uw situatie:

Onze patiënten melden zich bij onze receptie. Deze receptie medewerkers vragen de voor het zorgproces benodigde persoonsgegevens uit en leggen die vast in het dossier van de patiënten en vragen de patiënten toestemming om deze gegevens doelbestendig te mogen gebruiken. De patiënten worden tijdens het zorgproces gezien en behandeld door een of meerdere fysiotherapeuten. Zowel deze fysiotherapeuten als de receptie medewerkers zijn geautoriseerd voor deze taken en hebben een geheimhoudingsverklaring ondertekend. Deze geheimhoudingsverklaring maakt onderdeel uit van hun arbeidsovereenkomst. Dit zelfde geldt ook voor onze fysiofitbegeleiders.
De directie heeft ook toegang tot alle data van het bedrijf, zij zijn gebonden aan de geheimhouding van het bedrijf m.b.t. medische gegevens.

Onderstaande vragen zijn alleen ter bewustwording en hoeven niet precies ingevuld te worden!

Wij als organisatie hebben 16 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 18000 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 (na de bewaartermijn) 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 als organisatie hebben de wettelijke plicht om medische gegevens 20 jaar te bewaren, met ingang vanaf de laatste behandeling. Op het moment dat een patiënt actief verzoekt aan ons om zijn gegevens te vernietigen / dan wel te verwijderen zullen wij zijn of haar dossier uit alle actieve verwerkingen/database halen. Dan komt haar/zijn dossier in ons archief terecht en alle papieren documenten worden verzameld en achter slot en grendel in een aparte map gezet. Op dit moment bestaan we ongeveer 15 jaar, zodra we de 20 jaar halen, moeten we dossiers ook actief gaan vernietigen. Op dit moment is dat niet aan de orde.

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 bij de verspreiding veel 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.

Op grond van de Telecommunicatiewet mag je bestaande klanten benaderen via digitale direct marketing zonder toestemming (maar met een opt-out).

- [x] 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 de intake vragen we heel specifiek aan de patiënten/cliënten of wij hun mailadres mogen noteren en leggen we uit waarom we deze opslaan (afspraken maken, medische vragenlijsten en of enquête over de kwaliteit van onze zorg). Patiënten krijgen deze automatisch indien zij akkoord gaan met afgeven van hun mailadres. Indien ze dit niet willen en dit aangeven dan vinken wij per keuze dit aan in de patiëntenkaart. Dit geldt ook voor het gebruik van de mobiele telefoon.

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/elektronisch een toestemming hebben van de ouder, verzorger of wettelijke vertegenwoordiger. Geef hieronder aan dat je organisatie dat ook altijd zo doet.

- [x] 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:

Indien wij een medische rapportage moeten verzenden bij minderjarigen vragen wij schriftelijk aan ouders of wij een eenmalige rapportage en/of echobeelden mogen versturen via het software programma Zivver (beveiligde 2-staps authenticatie programma) naar de ouders en/of een andere zorgverlener. De gegevens die gebruikt worden voor het melden van afspraken en huiswerkoefeningen worden verwerkt door mijnzorgapp, dit wordt vooraf altijd gemeld. Indien dit niet gewenst is door de ouders dan kunnen wij dit handmatig uitzetten in de app portal.

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.

- [x] 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:

Alle medische en (bijzondere) persoonsgegevens liggen bij ons achter slot en grendel. Alle geautoriseerde personen (met sleutelcontracten) hebben hier toegang toe via sleutels. Cliënten/patiënten kunnen hier niet bijkomen, meerdere sloten en 's avonds/ 's nachts een automatisch alarm.

14.1 Datalekken

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

- [x] 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:

Alle medewerkers zijn goed op de hoogte van wat datalekken zijn. Ze weten dat ze een eventuele datalek moeten melden bij Ruud Lindenburg en Koen Ruigrok. Wij gaan dan actief aan de slag om het datalek zo klein mogelijk te houden, de betrokkenen te informeren en melding te doen bij de autoriteit Persoonsgegevens. Wij gaan aan de slag om onze medewerkers nog beter te informeren/instrueren hoe om te gaan met datalekken. Update 2019; bijna elke dag hebben we te maken met informeren van de medewerkers op allerlei kleine zaken in kader van de privacy wetgeving, aangezien we dagelijks met patiënten werken is dit ook normaal.
Update 2024: Datalekken worden uiteraard bijgehouden in ons incidentenregister. Ook datalekken die niet verplicht te hoeven worden gemeld aan de AP. Deze is voor één ieder van onze medewerkers inzichtelijk.

15.1 Medewerkers geïnstrueerd

Wij hebben onze medewerkers als volgt geïnstrueerd:

- [ ] Alle medewerkers hebben de video van de Stichting AVG bekeken.
- [x] We hebben het onderwerp privacy bescherming in alle afdelingsoverleggen besproken.
- [ ] We hebben uitlegposters opgehangen.
- [x] We hebben alle medewerkers een brief gestuurd met uitleg en instructie.
- [ ] We hebben met alle medewerkers een workshop over privacy bescherming gevolgd.
- [x] We hebben een nieuwsbrief voor alle medewerkers waarin we regelmatig aandacht besteden aan privacy bescherming.
- [x] 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:

Elke keer als er privacy gevoelige zaken worden besproken en/of over de AVG wet wordt gesproken wordt de medewerker op het hart gedrukt om met de gegevens van patiënten zorgvuldig om te gaan, als ze iets niet zeker weten worden ze aangemoedigd om dit te vragen bij ons. Daarnaast hebben ze ook medische geheimhouding en een geheimhoudingsverklaring getekend.

16.3 Afronding

Naam organisatie:

MTC de Viergang

Plaats:

Pijnacker

Datum:

19-2-2024

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.