Beleid (AVG)

AVG onderdeel

Directieverklaring

De directie van ***Podotherapeut Schrama*** is verantwoordelijk voor de veiligheid van de door haar verwerkte gegevens. Zij zorgt voor een privacy beleid of Information Security Management System (ISMS) dat passend is voor de organisatie. De doelstellingen van dat systeem stellen zeker dat de belangen van derden bij informatiebeveiliging voldoende worden beschermd. Zij verbindt zich eraan om het privacy beleid of ISMS continu te verbeteren en aan de (wettelijke) eisen te laten voldoen. Zij stelt voldoende middelen ter beschikking (binnen de mogelijkheden van de praktijk) om de veiligheid van gegevens te beschermen.

De directie van ***Podotherapeut Schrama*** zorgt ervoor dat haar medewerkers zich bewust zijn van de vertrouwelijkheid van de (patiënten)-gegevens waarmee zij werkt en beschermt deze gegevens passend. Daarom werkt ***Podotherapeut Schrama*** met een privacy beleid op basis van de Algemene Verordening Gegevensbescherming (AVG), of een ISMS op basis van de norm ISO27001, Informatiebeveiliging.

Het managementsysteem voor privacy- en informatiebeveiliging van ***Podotherapeut Schrama*** beschermt de vertrouwelijkheid, de integriteit en de beschikbaarheid van informatie doordat zij een risicobeheerproces toepast, en geeft belanghebbenden het vertrouwen dat zij risico's adequaat beheert.

De directie van ***Podotherapeut Schrama*** ondersteunt dit beleid, en voor de toepassing ervan stelt zij voldoende middelen ter beschikking (binnen de mogelijkheden van de praktijk). Het beleid van ***Podotherapeut Schrama*** maakt zij blijvend bekend aan alle medewerkers van ***Podotherapeut Schrama*** en relevante externe partijen.

De directie van ***Podotherapeut Schrama*** zorgt ervoor dat het privacy beleid of ISMS op regelmatige wijze wordt gecontroleerd op zijn goede werking.

Werkingsgebied van het AVG privacybeleid en ISMS

Het werkingsgebied van het privacy beleid of ISMS van ***Podotherapeut Schrama*** strekt zich uit tot de verantwoordelijkheden voor informatiebeveiliging van interne belanghebbenden (de bedrijfsgegevens van de praktijk zelf) en externe belanghebbenden (klanten, relaties, patiënten informatie).

Doel van gegevensverwerking

De gegevensverwerking door ***Podotherapeut Schrama*** vindt plaats om de goede behandeling van patiënten mogelijk te maken.

Gevolg van het niet voldoen aan het AVG privacy beleid en ISMS

Kan ***Podotherapeut Schrama*** via de controlemechanismen van het privacy beleid of ISMS de veiligheid van door haar beheerde informatie niet voldoende waarborgen, dan kan ***Podotherapeut Schrama*** van die belanghebbende(n) geen gegevens beheren. Deze blokkade wordt opgeheven op het moment dat de directie de dataveiligheidswaarborgen op basis van het privacy beleid of ISMS kan weergeven.

Interne en externe communicatie over het AVG privacy beleid en ISMS

Intern besteedt de directie regelmatig aandacht aan het privacy beleid of ISMS van ***Podotherapeut Schrama***. Tijdens bijeenkomsten communiceert zij op regelmatige basis over dataveiligheids onderwerpen.

Podotherapeut Schrama vermeldt extern in de uitingen en communicatie waar dat opportuun is dat ***Podotherapeut Schrama*** via haar privacy beleid of ISMS werkt aan continue informatieveiligheid.

Eisen en verwachtingen van belanghebbenden

De belanghebbenden verwachten van ***Podotherapeut Schrama*** dat zij gecontroleerd en op de meest veilige wijze met de (patiënten-) gegevens omgaat. Om die reden werkt ***Podotherapeut Schrama*** volgens haar privacy beleid of ISMS. Dat privacy beleid of ISMS is gebaseerd op de wet AVG of ISO 27001 Informatieveiligheid. Het gehele privacy beleid of

ISMS is erop gericht blijvend de informatieveiligheid te waarborgen, te monitoren, corrigerende maatregelen te nemen en het privacy beleid of ISMS aan te passen indien nodig.

Privacy beleid (op basis van de AVG, voortvloeiend uit de Algemene Verordening Gegevensbescherming 2016/679)

Podotherapeut Schrama gebruikt patiëntengegevens alleen voor het doel waarvoor de gegevens zijn opgeslagen. ***Podotherapeut Schrama*** deelt patiëntengegevens niet met derden, tenzij dit voor het opslagdoel nodig is. ***Podotherapeut Schrama*** bewaart patiëntengegevens niet langer dan nodig is op basis van het opslagdoel van de gegevens. ***Podotherapeut Schrama*** houdt met alle mogelijke middelen en maatregelen patiëntengegevens veilig voor inzage van onbevoegden. ***Podotherapeut Schrama*** vraagt toestemming aan de patiënten voor het opslaan van persoonsgegevens, als er *geen* behandelcontract gesloten is. ***Podotherapeut Schrama*** informeert patiënten over de rechten van de patiënten ten aanzien van zijn persoonsgegevens. ***Podotherapeut Schrama*** informeert haar patiënten over het doel van de verwerking van persoonsgegevens. ***Podotherapeut Schrama*** informeert patiënten indien ***Podotherapeut Schrama*** bijzondere handelingen met de persoonsgegevens gaat verrichten.

Risico-beoordeling (Data Protection Impact Assesment-DPIA)

Risico's bestaan in het door ***Podotherapeut Schrama*** onbedoeld wijzigen of lekken of zoekraken van informatie waardoor schade ontstaat aan de externe belanghebbenden (patiënten en (oud-) patiënten van ***Podotherapeut Schrama***.

Tegen dit risico neemt ***Podotherapeut Schrama*** de maatregelen in dit privacy beleid of ISMS, voert deze uit en beoordeelt deze op effectiviteit. De procedures van het privacy beleid of ISMS zijn onderwerp van continu onderzoek en verbetering. Alle medewerkers worden bij de veiligheids-procedures betrokken, op de wijzen als in dit privacy beleid of ISMS beschreven.

Procedure risico beoordeling

Podotherapeut Schrama reduceert bovenstaande gevaren doordat zij werkt op basis van haar privacy beleid of ISMS. Bij iedere interne audit en management review wordt een risico-beoordeling dataveiligheid uitgevoerd.

Buiten het beheer van het privacy beleid of ISMS blijft een rest-risico bestaan. De bekende risico's voor ***Podotherapeut Schrama*** worden via de interne audits en management reviews geanalyseerd. Maatregelen voor die risico's zijn in het privacy beleid of ISMS opgenomen en worden beheerd en uitgevoerd. Rest-risico's bestaan uit extreem wijzigende omstandigheden die ***Podotherapeut Schrama*** niet voorziet. Die risico's acht ***Podotherapeut Schrama*** onvermijdelijk. Na een onvoorzien incident wordt een nieuwe risico beoordeling uitgevoerd. Eventuele remedies neemt ***Podotherapeut Schrama*** in het privacy beleid of ISMS op.

Creatie van AVG/ISMS documenten en procedures

De documenten voor het privacy beleid of ISMS worden voor ***Podotherapeut Schrama*** gemaakt en beheerd door het dataveiligheidspakket van Waveland. Binnen ***Podotherapeut Schrama*** zorgt de directie voor een verantwoordelijke voor het uitvoeren van de taken volgens het privacy beleid of ISMS.

De praktijk houdt zich bezig met:*
Podotherapie
De podotherapeut behandelt personen met voetklachten of klachten aan het houdings- en bewegingssysteem, die voortvloeien uit een afwijkend functioneren en/of afwijkende stand van de voeten. Sinds 2015 voert de podotherapeut diabetes screenings uit in verband met de vergoedingen voor pedicure behandelingen vanuit het basispakket van de zorgverzekeringen. De bevoegdheid tot het voeren van de titel podotherapeut is voorbehouden aan degenen die een door het ministerie van Onderwijs, Cultuur en Wetenschap (OCW)geaccrediteerde HBO-opleiding (met bachelor degree) voor podotherapeuten hebben afgerond, zoals geregeld in art.34 van de wet BIG.

Informatie aan betrokkenen (AVG)

Podotherapeut Schrama informeert haar patiënten over de verwerking van persoonsgegevens en de rechten die de AVG aan de patiënten toekent.
Als patiënten **geen** 'behandelovereenkomst' sluiten met ***Podotherapeut Schrama***, vraagt ***Podotherapeut Schrama*** uitdrukkelijke toestemming tot die verwerking.

Dit doet ***Podotherapeut Schrama*** in overeenstemming met de Algemene Verordening Gegevensbescherming EU 2016/679 (AVG). ***Podotherapeut Schrama*** gebruikt hiervoor haar document 'informatie aan cliënten'.

Bij de toepassing van de privacy wetgeving (AVG) houdt ***Podotherapeut Schrama*** zich ook aan de WGBO, de Wet aanvullende bepalingen verwerking persoonsgegevens in de zorg, Besluit elektronische gegevensverwerking in de zorg, en overige toepasselijke wetgeving. Deze wetten kunnen afwijken van de AVG.

Bij een toegekend verzoek tot verwijdering van persoongegevens zal ***Podotherapeut Schrama*** de gegevens verwijderen of opslaan in een inactief archief waarmee het onzichtbaar is voor de gewone gebruiker binnen ***Podotherapeut Schrama***.
Podotherapeut Schrama reageert op een verzoek zo spoedig mogelijk, maar in ieder geval binnen 3 maanden na de aanvraag.
In het geval ***Podotherapeut Schrama*** een verzoek over de persoonsgegevens afwijst, informeert ***Podotherapeut Schrama*** de patiënten over de redenen voor de afwijzing.

Verwerkingsregister en informatie classificatie (AVG)

AVG onderdeel

Informatie classificatie

Podotherapeut Schrama classificeert informatie met betrekking tot wettelijke eisen, waarde, belang en gevoeligheid voor onbevoegde bekendmaking of wijziging en de bewaartermijn. ***Podotherapeut Schrama*** maakt onderscheid tussen openbare informatie en gevoelige informatie.

Informatie over de behandeling van patiënten van ***Podotherapeut Schrama*** is altijd gevoelige informatie.

Informatie over medewerkers van ***Podotherapeut Schrama*** is altijd gevoelige informatie.
Medische informatie is altijd gevoelige informatie.

Bedrijfsmiddelen (waaronder ook 'data' behoort) worden behandeld in overeenstemming met het informatieclassificatieschema dat is vastgesteld door ***Podotherapeut Schrama***.

Podotherapeut Schrama bewaart de (persoons) gegevens in het behandeldossier volgens de wettelijke bewaartermijn van de WGBO. ***Podotherapeut Schrama*** vernietigt gegevens na het verstrijken van de wettelijke bewaartermijn.

Podotherapeut Schrama **is in staat de volgende acties uit te voeren met haar informatiepakket:**

- Gegevens laten **inzien** door onze patiënten. Alleen de gegevens van de bewuste patiënten mogen dan inzichtelijk zijn. (de patiënten mogen geen wijzigingen in ons systeem kunnen aanbrengen tijdens het inzien.)
- **Correcties** (en wijzigingen) aanbrengen, alleen mogelijk door een geautoriseerde verwerker van ***Podotherapeut Schrama***.
- Gegevens van één persoon **overdragen.**
- **Verwijderen** van alle, of een deel van de gegevens van één persoon (een persoon heeft het recht om 'vergeten te worden' op basis van de AVG, dit recht wordt opzij gezet door de WGBO bepalingen). ***Podotherapeut Schrama*** beoordeelt het verzoek met in achtneming van de eisen van de WGBO. Als er goede redenen zijn om het verzoek af te wijzen, legt ***Podotherapeut Schrama*** dit vast in het patiëntendossier en brengt ***Podotherapeut Schrama*** de patiënten van de beslissing op de hoogte.

Verwerkingsregister van *Podotherapeut Schrama*:

Per verwerkingsactiviteit staan mogelijk de volgende gegevens geregistreerd:

- Naam van de dataverantwoordelijke is vastgelegd bij onderdeel 'praktijksamenstelling'
- ***Podotherapeut Schrama*** slaat de noodzakelijke gegevens van medewerkers op in het personeelsdossier.
- ***Podotherapeut Schrama*** slaat de volgende data van patiënten op:
  -NAW gegevens,
  -BSN nummer,
  -Geslacht,
  -Leeftijd,
  -Telefoonnummer,
  -Emailadres van patiënten,
  -Medische gegevens, het gehele patiëntendossier,
  -(Rontgen) -foto's gericht op de medische behandeling,
  - Laboratorium uitslagen,
  - Sexueel verleden, indien dat voor het verlenen van de zorg nodig en/of relevant is,
  - Etnische afkomst, indien dat voor het verlenen van de zorg nodig en/of relevant is,
  - Godsdienst, indien dat voor het verlenen van de zorg nodig en/of relevant is,
  - Opleidingsniveau, indien dat voor het verlenen van de zorg relevant is.

- Medische gegevens van ***Podotherapeut Schrama*** zijn 'bijzondere gegevens' volgens de AVG wetgeving.
- Informatie wordt opgeslagen om behandeling van de patiënten mogelijk te maken.
- Informatie wordt verwerkt door behandelaars en hun assistenten en praktijkondersteunende diensten.
- Informatie wordt verwerkt van patiënten die de ***Podotherapeut Schrama*** behandelt.
- Informatie wordt bij verwijzing uitgewisseld met een volgende behandelaar (bijvoorbeeld een specialist). Iedere specialist is zelf verwerkingsverantwoordelijke. Hij verwerkt de persoonsgegevens ter uitvoering van de behandelovereenkomst die hij zelf is aangegaan met de patiënten.
- De informatie wordt uitgewisseld met andere behandelaars die nodig zijn voor de goede behandeling.
- Informatie wordt uitgewisseld met verzekeraars of hun vertegenwoordigers (Vecozo). Als die niet gebeurt op grond van een wettelijke verplichting, vraagt ***Podotherapeut Schrama*** hiervoor toestemming aan de patiënten.
- ***Podotherapeut Schrama*** verstrekt geen Informatie aan buitenlandse organisaties, tenzij de goede behandeling dit nodig maakt.
- De bewaartermijn is zo lang als de informatie nodig is voor de goede behandeling, met in achtneming van de WGBO.
- De beveiligingsmaatregelen zijn in de afdeling van het DataVeiligheidsportaal te vinden, in de AVG- of ISMS vastlegging van ***Podotherapeut Schrama***.

Per verwerker: (daaronder verstaat ***Podotherapeut Schrama*** onderaannemers van ***Podotherapeut Schrama*** die gevraagd worden een handeling uit te voeren met persoons***gegevens*** in opdracht van ***Podotherapeut Schrama***. Daaronder vallen *niet* de zorgverleners die onderdeel uitmaken van de medische behandeling. Die behandelaars zijn zelf verantwoordelijk voor de beveiliging van de privacy van de patiënten.

- Informatie wordt door derden verwerkt (verwerkers) met als doel de goede behandeling van patiënten.
- ***Podotherapeut Schrama*** deelt persoonsgegevens van medewerkers met derden als dat nodig is voor de goede uitvoering van het arbeidscontract.
- ***Podotherapeut Schrama*** sluit met verwerkers een verwerkingcontract. Daarin staan de voorwaarden voor de verwerking.

De categorieën van het verwerkingsregister van ***Podotherapeut Schrama*** zijn in haar dataveiligheids portaal te vinden onder 'beheer van bedrijfsmiddelen'.

Andere persoonsgegevens die u opslaat:
-

Beleid bewustwording (AVG)

AVG onderdeel

Het contract van iedere medewerker bij ***Podotherapeut Schrama*** bevat bepalingen over geheimhouding van gegevens en de verantwoordelijkheid om veilig met data om te gaan.

Om dit te onderstrepen organiseert ***Podotherapeut Schrama*** regelmatig, minimaal 4 keer per jaar via bewustwordingssessies en interne audits over dataveiligheid, samen met alle medewerkers van ***Podotherapeut Schrama***. Ontwikkelingen op het gebied van dataveiligheid (breed) worden verspreid en besproken binnen ***Podotherapeut Schrama***.

Podotherapeut Schrama plant regelmatig bijeenkomsten waarin het privacy beleid en/of ISMS en dataveiligheid worden besproken. Hierbij gebruikt ***Podotherapeut Schrama*** onderstaand schema.

Indien anders:**
-

Toegangsbeveiliging van data (AVG)

AVG onderdeel

Autorisatie matrix

Toegang tot informatie verstrekt ***Podotherapeut Schrama*** op basis van de directe taken en bezigheden van betreffende medewerker. Dit wordt weergegeven in de autorisatiematrix van de verschillende informatiesystemen.

De toegang tot informatie van ***Podotherapeut Schrama*** is te vinden in de rollen en/of profielen in het informatiepakket dat ***Podotherapeut Schrama*** gebruikt.

Wachtwoorden

De toegang tot het (draadloze) netwerk en netwerkdiensten wordt afgedwongen met persoonlijke wachtwoorden.

Gebruikers hebben een persoonlijk wachtwoord te kiezen dat minimaal 8 karakters bevat, en;

• gemakkelijk te onthouden is.

• niet gebaseerd is op iets dat iemand anders gemakkelijk zou kunnen raden of verkrijgen door gebruik te maken van persoons-gerelateerde informatie, zoals namen, telefoonnummers en geboortedata.

• niet kwetsbaar is voor woordenboekaanvallen (d.w.z. niet bestaande uit woorden die in het woordenboek voorkomen).

• geen opeenvolgende gelijke tekens bevat en niet uitsluitend uit numerieke of uitsluitend uit alfabetische tekens bestaat.

Informatiebeveiliging met derden en in leveranciersrelaties (AVG)

AVG onderdeel

Podotherapeut Schrama houdt een lijst bij van categorieën van organisaties waarmee zij patiëntengegevens deelt. (zie het verwerkingsregister afd. 3/7 - 19/37).

Podotherapeut Schrama sluit verwerkingsovereenkomsten met organisaties waarmee zij patiënteninformatie deelt om die patiëntengegevens te verwerken. (Voorbeeld). ***Podotherapeut Schrama*** vult haar verwerkersovereenkomst aan met het contract waarin de opdracht aan de verwerker nauwkeurig wordt omschreven. Indien ***Podotherapeut Schrama*** dit wenst voegt zij beide overeenkomsten samen.

Podotherapeut Schrama houdt een leverancierslijst bij van leveranciers die mogelijk patiëntengegevens van de praktijk kunnen inzien, en met welke organisaties zij een verwerkerscontract heeft gesloten. ***Podotherapeut Schrama*** houdt die leverancierslijst actueel. De betreffende leverancier tekent de verwerkersovereenkomst (daarin is geheimhouding opgenomen)

Ondanks deze verwerkersovereenkomst, deelt ***Podotherapeut Schrama*** niet meer informatie dan strikt noodzakelijk is om gevraagde dienst/service/behandeling uit te voeren.

Podotherapeut Schrama sluit een geheimhoudingsverklaring met personen die onbedoeld persoonsgegevens kunnen inzien. Dit kan in de serviceovereenkomst staan, of in een aparte geheimhoudingsverklaring.

Beheer van informatiebeveiligingsincidenten (datalek) (AVG)

AVG onderdeel

Beleid bij data veiligheidsincidenten (datalek)

Een datalek (of: data incident) is voor ***Podotherapeut Schrama***: iedere inbreuk op de dataveiligheid die per ongeluk of op onrechtmatige wijze leidt tot:
• vernietiging van data of informatie,
• verlies van persoonsgegevens,
• wijziging van persoonsgegevens,
• ongeoorloofde verstrekking van persoonsgegevens,
• ongeoorloofde toegang tot opgeslagen persoonsgegevens,
• ongeoorloofde toegang tot doorgezonden persoonsgegevens.

Een datalek ontstaat onder andere als ***Podotherapeut Schrama*** het slachtoffer wordt van ransomware of een andere vorm van kwaadwillige hacking.

In het geval dat zich een dataveiligheids incident voordoet of een zwakte in de databeveiliging geconstateerd wordt door een medewerker, meldt hij dit zo spoedig mogelijk bij zijn of haar leidinggevende en de verantwoordelijke voor databeveiliging van ***Podotherapeut Schrama***.

Na een incident analyseert ***Podotherapeut Schrama*** de oorzaak, de aanpak en de mogelijkheden om een dergelijk incident te voorkomen. Zij legt haar bevindingen vast in het formulier 'dataveiligheidsincident'. De maatregelen *ter voorkoming* van het incident worden na invoering geëvalueerd.

Procedure bij een incident (datalek)

Wanneer er sprake is van een incident, wordt de volgende procedure doorlopen:

• incident direct melden bij leidinggevende en verantwoordelijke voor informatiebeveiliging.

• intern meldingsformulier invullen en opslaan in het dataveiligheids portaal.

• melder, leidinggevende en verantwoordelijke voor informatiebeveiliging stellen vast welke actie genomen dient te worden op basis van het soort informatie, de hoeveelheid informatie en welke belanghebbenden door dit incident geraakt zouden kunnen worden.

• actie toewijzen aan uitvoerder(s).

• ***Podotherapeut Schrama*** beoordeelt het incident door zich (intern) de volgende vraag te stellen:

Levert het data incident risico op voor de aantasting van de rechten en vrijheden van patiënten?
(Als aangetoond kan worden dat het datalek **geen** gevolgen heeft voor de rechten en vrijheden van patiënten, doet ***Podotherapeut Schrama*** geen melding bij de Autoriteit Persoonsgegevens.)

Als het antwoord **NEE** is, wordt er niet gemeld bij de AP, en wordt ***alleen*** het interne formulier 'dataveiligheidsincident' ingevuld en opgeslagen onder dossier.
Als het antwoord **JA** is wordt binnen 72 uur gemeld bij de Autoriteit Persoonsgegevens --> Meldingsformulier datalek: klik hier --> **Autoriteit Persoonsgegevens.**

• W*ave***land** treedt op als **Collectieve Functionaris Gegevensbescherming (FG)** namens ***Podotherapeut Schrama***, tenzij ***Podotherapeut Schrama*** ervoor heeft gekozen een eigen, interne medewerker als eigen FG aan te wijzen. Deze wordt *in dat geval* genoemd onder 'praktijksamenstelling' als dataverantwoordelijke voor ***Podotherapeut Schrama***. Bij 'functie' staat dan 'FG'. Hij of zij is dan de *interne* dataverantwoordelijke **EN** de FG voor ***Podotherapeut Schrama***.

• controle door de verantwoordelijke voor dataveiligheid op uitvoering van acties door de FG.

• dataverantwoordelijke meldt aan de betrokken patiënten het incident, de maatregelen die genomen worden. ***Podotherapeut Schrama*** meldt het incident alleen aan betrokkene indien na de genomen maatregelen toch nog een risico bestaat voor de rechten en vrijheden van de betrokkene of betrokkenen. Let op: een melding kan ook vereist zijn op basis van de Wkkgz.

• verantwoordelijke voor dataveiligheid documenteert het incident, de actie en de correctieve maatregel(-en) en publiceert deze aan de betrokkenen binnen de organisatie.

• ***Podotherapeut Schrama*** trekt lering uit het incident en stelt maatregelen vast ter voorkoming van een dergelijk incident.