Beleid (AVG)

AVG onderdeel

Directieverklaring

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

De directie van Ergotherapie Hoeksche Waard 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 Ergotherapie Hoeksche Waard strekt zich uit tot de verantwoordelijkheden voor informatiebeveiliging van interne belanghebbenden (de bedrijfsgegevens van de praktijk zelf) en externe belanghebbenden (klanten, relaties, patiënteninformatie).

Doel van gegevensverwerking

De gegevensverwerking door Ergotherapie Hoeksche Waard vindt plaats om de goede behandeling van patiënten mogelijk te maken.

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

Kan Ergotherapie Hoeksche Waard via de controlemechanismen van het privacy beleid of ISMS de veiligheid van door haar beheerde informatie niet voldoende waarborgen, dan kan Ergotherapie Hoeksche Waard 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 Ergotherapie Hoeksche Waard. Tijdens bijeenkomsten communiceert zij op regelmatige basis over dataveiligheids onderwerpen.

Ergotherapie Hoeksche Waard vermeldt extern in de uitingen en communicatie waar dat opportuun is dat Ergotherapie Hoeksche Waard via haar privacy beleid of ISMS werkt aan continue informatieveiligheid.

Eisen en verwachtingen van belanghebbenden

De belanghebbenden verwachten van Ergotherapie Hoeksche Waard dat zij gecontroleerd en op de meest veilige wijze met de (patiënten-) gegevens omgaat. Om die reden werkt Ergotherapie Hoeksche Waard 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)

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

Risico-beoordeling (Data Protection Impact Assesment-DPIA)

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

Tegen dit risico neemt Ergotherapie Hoeksche Waard 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

Ergotherapie Hoeksche Waard 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 Ergotherapie Hoeksche Waard 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 Ergotherapie Hoeksche Waard niet voorziet. Die risico's acht Ergotherapie Hoeksche Waard onvermijdelijk. Na een onvoorzien incident wordt een nieuwe risico beoordeling uitgevoerd. Eventuele remedies neemt Ergotherapie Hoeksche Waard in het privacy beleid of ISMS op.

Creatie van AVG/ISMS documenten en procedures

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

De praktijk houdt zich bezig met:*
het voeren van een ergotherapiepraktijk

In onze ergotherapie praktijk behandelen we en adviseren we cliënten die problemen ervaren in de uitvoering van de dagelijkse handelingen. Dit kan plaatsvinden in de praktijk, thuis, op school/ werk.

Informatie aan patiënten (AVG)

Ergotherapie Hoeksche Waard informeert haar patiënten over de verwerking van persoonsgegevens en de rechten die de AVG aan de patiënt toekent.
Als een relatie/patiënt **geen** 'behandelovereenkomst' sluit met Ergotherapie Hoeksche Waard, vraagt Ergotherapie Hoeksche Waard uitdrukkelijke toestemming tot die verwerking.

Dit doet Ergotherapie Hoeksche Waard in overeenstemming met de Algemene Verordening Gegevensbescherming EU 2016/679 (AVG). Ergotherapie Hoeksche Waard gebruikt hiervoor haar document 'informatie aan patienten'.

Bij de toepassing van de privacy wetgeving (AVG) houdt Ergotherapie Hoeksche Waard 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 Ergotherapie Hoeksche Waard de gegevens verwijderen of opslaan in een inactief archief waarmee het onzichtbaar is voor de gewone gebruiker binnen Ergotherapie Hoeksche Waard.
Ergotherapie Hoeksche Waard reageert op een verzoek zo spoedig mogelijk, maar in ieder geval binnen 3 maanden na de aanvraag.
In het geval Ergotherapie Hoeksche Waard een verzoek over de persoonsgegevens afwijst, informeert Ergotherapie Hoeksche Waard de patiënt over de redenen voor de afwijzing.

Verwerkingsregister en informatie classificatie (AVG)

AVG onderdeel

Informatie classificatie

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

Informatie over de behandeling van patiënten van Ergotherapie Hoeksche Waard is altijd gevoelige informatie.

Informatie over medewerkers van Ergotherapie Hoeksche Waard 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 Ergotherapie Hoeksche Waard.

Ergotherapie Hoeksche Waard bewaart de (persoons) gegevens in het behandeldossier volgens de wettelijke bewaartermijn van de WGBO. Ergotherapie Hoeksche Waard vernietigt gegevens na het verstrijken van de wettelijke bewaartermijn.

Ergotherapie Hoeksche Waard is in staat de volgende acties uit te voeren met haar informatiepakket:

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

Verwerkingsregister van Ergotherapie Hoeksche Waard:

Per verwerkingsactiviteit staan de volgende gegevens geregistreerd:

-Naam van de dataverantwoordelijke is vastgelegd bij onderdeel 'praktijksamenstelling'
-Ergotherapie Hoeksche Waard slaat de noodzakelijke gegevens van medewerkers op in het personeelsdossier.
-Ergotherapie Hoeksche Waard slaat de volgende data van de patiënt op:
-NAW gegevens,
-BSN nummer,
-Geslacht,
-Leeftijd,
-Telefoonnummer,
-Emailadres van de patiënt,
-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 Ergotherapie Hoeksche Waard zijn 'bijzondere gegevens' volgens de AVG wetgeving.
-Informatie wordt opgeslagen om behandeling van de patiënt mogelijk te maken.
-Informatie wordt verwerkt door behandelaars en hun assistenten en praktijkondersteunende diensten.
-Informatie wordt verwerkt van patiënten die de Ergotherapie Hoeksche Waard 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 patiënt.
-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 Ergotherapie Hoeksche Waard hiervoor toestemming aan de patiënt.
-Ergotherapie Hoeksche Waard 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 Ergotherapie Hoeksche Waard.

Per verwerker: (daaronder verstaat Ergotherapie Hoeksche Waard onderaannemers van Ergotherapie Hoeksche Waard die gevraagd worden een handeling uit te voeren met persoons***gegevens*** in opdracht van Ergotherapie Hoeksche Waard. 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 patiënt).

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

De categorieën van het verwerkingsregister van Ergotherapie Hoeksche Waard zijn in haar dataveiligheids portaal te

vinden onder 'beheer van bedrijfsmiddelen'.

-

Beleid bewustwording (AVG)

AVG onderdeel

Het contract van iedere medewerker bij Ergotherapie Hoeksche Waard bevat bepalingen over geheimhouding van gegevens en de verantwoordelijkheid om veilig met data om te gaan.

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

Ergotherapie Hoeksche Waard plant regelmatig bijeenkomsten waarin het privacy beleid en/of ISMS en dataveiligheid worden besproken. Hierbij gebruikt Ergotherapie Hoeksche Waard onderstaand schema.

Datum	Locatie	Aanwezig	Agenda	Email medewerkers

-

Toegangsbeveiliging van data (AVG)

AVG onderdeel

Autorisatie matrix

Toegang tot informatie verstrekt Ergotherapie Hoeksche Waard 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 Ergotherapie Hoeksche Waard is te vinden in de rollen en/of profielen in het informatiepakket dat Ergotherapie Hoeksche Waard 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.

24-04-2018

-

Informatiebeveiliging met derden en in leveranciersrelaties (AVG)

AVG onderdeel

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

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

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

Ondanks deze verwerkersovereenkomst, deelt Ergotherapie Hoeksche Waard niet meer informatie dan strikt noodzakelijk is om gevraagde dienst/service/behandeling uit te voeren.

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

Naam	Kunnen informatie zien	Mogen informatie zien	Deelt informatie met praktijk	Verwerkersovereenkor getekend
Hulpmiddelencentrum	Ja	Ja	Ja	Nee
Livit	Ja	Ja	Ja	Nee
MHG	Ja	Ja	Ja	Nee
Sarkow	Ja	Ja	Ja	Nee
WMO Hoeksche Waard	Ja	Ja	Ja	Nee
WMO Barendrecht	Ja	Ja	Ja	Nee
Innocare	Ja	Ja	Ja	Nee
Atlas kidtech	Ja	Ja	Ja	Nee
Peerenboom	Ja	Ja	Ja	Nee
Medipoint	Ja	Ja	Ja	Nee
Vegro	Ja	Ja	Ja	Nee
van der Mark	Ja	Ja	Ja	Nee
Stichting MEE	Ja	Ja	Ja	Nee

Aan-slag belastingadviesbureau	Ja	Ja	Ja	Nee
Raymond van Noort ICT	Ja	Ja	Ja	Nee
Esmeralda Kuiper Grafisch vormgever	Ja	Ja	Ja	Nee
Listesso	Ja	Ja	Ja	Nee
Bijzonder handig	Ja	Ja	Ja	Nee

Beheer van informatiebeveiligingsincidenten (datalek) (AVG)

AVG onderdeel

Beleid bij data veiligheidsincidenten (datalek)
Een datalek (of: data incident) is voor Ergotherapie Hoeksche Waard: 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 Ergotherapie Hoeksche Waard 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 Ergotherapie Hoeksche Waard.

Na een incident analyseert Ergotherapie Hoeksche Waard 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).

• Ergotherapie Hoeksche Waard 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 de patiënt?
(Als aangetoond kan worden dat het datalek **geen** gevolgen heeft voor de rechten en vrijheden van de patiënt, doet Ergotherapie Hoeksche Waard 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.**

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

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

•dataverantwoordelijke meldt aan de betrokkene patiënt (of patiënten) het incident, de maatregelen die genomen worden. Ergotherapie Hoeksche Waard 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.

•Ergotherapie Hoeksche Waard trekt lering uit het incident en stelt maatregelen vast ter voorkoming van een dergelijk incident.

functionaris gegevensbescherming Ergotherapie Hoeksche Waard en Barendrecht is KS van Domburg