Beleid (AVG)

AVG onderdeel

Directieverklaring

De directie van Stichting Nedereind 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 Stichting Nedereind zorgt ervoor dat haar medewerkers zich bewust zijn van de vertrouwelijkheid van de (cliënten)-gegevens waarmee zij werkt en beschermt deze gegevens passend. Daarom werkt Stichting Nedereind 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 Stichting Nedereind 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 Stichting Nedereind ondersteunt dit beleid, en voor de toepassing ervan stelt zij voldoende middelen ter beschikking (binnen de mogelijkheden van de praktijk). Het beleid van Stichting Nedereind maakt zij blijvend bekend aan alle medewerkers van Stichting Nedereind en relevante externe partijen.

De directie van Stichting Nedereind 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 Stichting Nedereind 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 Stichting Nedereind vindt plaats om de goede behandeling van cliënten mogelijk te maken.

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

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

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

Eisen en verwachtingen van belanghebbenden

De belanghebbenden verwachten van Stichting Nedereind dat zij gecontroleerd en op de meest veilige wijze met de (cliënten-) gegevens omgaat. Om die reden werkt Stichting Nedereind 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)

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

Risico-beoordeling (Data Protection Impact Assesment-DPIA)

Risico's bestaan in het door Stichting Nedereind onbedoeld wijzigen of lekken of zoekraken van informatie waardoor schade ontstaat aan de externe belanghebbenden (cliënten en (oud-) cliënten van Stichting Nedereind.

Tegen dit risico neemt Stichting Nedereind 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

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

Creatie van AVG/ISMS documenten en procedures

De documenten voor het privacy beleid of ISMS worden voor Stichting Nedereind gemaakt en beheerd door het dataveiligheidspakket van Waveland. Binnen Stichting Nedereind 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 leveren van zorg op maat aan mensen met een licht-verstandelijke beperking en/of psychische stoornis/gedragsproblemen.

Stichting Nedereind is een instelling met een WTZi-toelating en levert zorg op maat aan mensen met een licht-verstandelijke beperking en/of psychische stoornis/gedragsproblemen. De begeleiding van de jong volwassenen wordt verzorgd door een klein en vast team van ervaren medewerkers, dat daarbij wordt ondersteund door het hoofd en een orthopedagoog als zorginhoudelijk adviseur.

Informatie aan betrokkenen (AVG)

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

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

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

Onze aanvullende procedure:
-

Verwerkingsregister en informatie classificatie (AVG)

AVG onderdeel

Informatie classificatie

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

Informatie over de behandeling van cliënten van Stichting Nedereind is altijd gevoelige informatie.

Informatie over medewerkers van Stichting Nedereind 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 Stichting Nedereind.

Stichting Nedereind bewaart de (persoons) gegevens in het behandeldossier volgens de wettelijke bewaartermijn van de WGBO. Stichting Nedereind vernietigt gegevens na het verstrijken van de wettelijke bewaartermijn.

Stichting Nedereind is in staat de volgende acties uit te voeren met haar informatiepakket:

-Gegevens laten **inzien** door onze cliënten. Alleen de gegevens van de bewuste cliënten mogen dan inzichtelijk zijn. (de cliënten mogen geen wijzigingen in ons systeem kunnen aanbrengen tijdens het inzien.)
-**Correcties** (en wijzigingen) aanbrengen, alleen mogelijk door een geautoriseerde verwerker van Stichting Nedereind.
-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). Stichting Nedereind beoordeelt het verzoek met in achtneming van de eisen van de WGBO. Als er goede redenen zijn om het verzoek af te wijzen, legt Stichting Nedereind dit vast in het cliëntendossier en brengt Stichting Nedereind de cliënten van de beslissing op de hoogte.

Verwerkingsregister van Stichting Nedereind:

Per verwerkingsactiviteit staan mogelijk de volgende gegevens geregistreerd:

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

Per verwerker: (daaronder verstaat Stichting Nedereind onderaannemers van Stichting Nedereind die gevraagd worden een handeling uit te voeren met persoons***gegevens*** in opdracht van Stichting Nedereind. 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 cliënten.

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

De categorieën van het verwerkingsregister van Stichting Nedereind zijn in haar dataveiligheids portaal te vinden onder 'beheer van bedrijfsmiddelen'.

Andere persoonsgegevens die wij opslaan:
-

Beleid bewustwording (AVG)

AVG onderdeel

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

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

Stichting Nedereind plant regelmatig bijeenkomsten waarin het privacy beleid en/of ISMS en dataveiligheid worden besproken. Hierbij gebruikt Stichting Nedereind onderstaand schema.

Datum	Locatie	Aanwezig	Agenda	Email medewerkers
12-06-2018				

Onze aanvullende procedure:
-

Toegangsbeveiliging van data (AVG)

AVG onderdeel

Autorisatie matrix

Toegang tot informatie verstrekt Stichting Nedereind 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 Stichting Nedereind is te vinden in de rollen en/of profielen in het informatiepakket dat Stichting Nedereind 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.

Datum laatste overleg:**
02-05-2018

Indien u zelf uw IT organisatie doet:**
-

Informatiebeveiliging met derden en in leveranciersrelaties (AVG)

AVG onderdeel

Stichting Nedereind houdt een lijst bij van categorieën van organisaties waarmee zij cliëntengegevens deelt. (zie het verwerkingsregister afd. 3/7 - 19/37).

Stichting Nedereind sluit verwerkingsovereenkomsten met organisaties waarmee zij cliënteninformatie deelt om die cliëntengegevens te verwerken. (Voorbeeld). Stichting Nedereind vult haar verwerkersovereenkomst aan met het contract waarin de opdracht aan de verwerker nauwkeurig wordt omschreven. Indien Stichting Nedereind dit wenst voegt zij beide overeenkomsten samen.

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

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

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

Naam	Kan informatie zien	Mag informatie zien	Is verwerker voor praktijk	Verwerkerscontract getekend	Geheimhoudingsverkl getekend
AGZ	Ja	Ja	Nee	Nee	Nee
NEDAP	Ja	Ja	Ja	Ja	Nee
Arbo-butler	Ja	Ja	Nee	Ja	Nee
VVAA	Ja	Ja	Nee	Ja	Nee

Beheer van informatiebeveiligingsincidenten (datalek) (AVG)

AVG onderdeel

Beleid bij data veiligheidsincidenten (datalek)
Een datalek (of: data incident) is voor Stichting Nedereind: 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 Stichting Nedereind 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 Stichting Nedereind.

Na een incident analyseert Stichting Nedereind 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).

• Stichting Nedereind 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 cliënten?
(Als aangetoond kan worden dat het datalek **geen** gevolgen heeft voor de rechten en vrijheden van cliënten,
doet Stichting Nedereind 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 Stichting Nedereind, tenzij Stichting Nedereind ervoor heeft gekozen een eigen, interne medewerker als eigen FG aan te wijzen. Deze wordt *in dat geval* genoemd onder 'praktijksamenstelling' als dataverantwoordelijke voor Stichting Nedereind. Bij 'functie' staat dan 'FG'. Hij of zij is dan de *interne* dataverantwoordelijke **EN** de FG voor Stichting Nedereind.

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

•dataverantwoordelijke meldt aan de betrokken cliënten het incident, de maatregelen die genomen worden. Stichting Nedereind 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.

•Stichting Nedereind trekt lering uit het incident en stelt maatregelen vast ter voorkoming van een dergelijk incident.

-