

Privacybeleid

In dit document wordt het beleid aangaande de omgang met gegevens en privacy van de organisatie verduidelijkt. Het [privacyreglement](#), hetgeen een uitwerking is van dit beleid, sluit hierop aan.

Om dit beleid leesbaar te houden voor de doelgroep is gekozen om zo min mogelijk juridische taal te gebruiken zodat deze toegankelijk en begrijpelijk is voor iedereen.

Indien er vragen zijn met betrekking tot privacy gerelateerde onderwerpen kan contact worden opgenomen met

- Privacy officer;
- Functionaris gegevensbescherming;
- Information Security Officer;

Via: privacy@mgzl.nl

Inleiding

In het kader van de Algemene Verordening Gegevensbescherming (AVG) is het voor MGZL noodzakelijk dat de gehele organisatie wettig en op een verantwoorde wijze omgaat met persoonsgegevens. Dat geldt ook voor de diensten die door MGZL geleverd worden. In dit privacy beleid staan alle medewerkers van de organisatie MGZL en haar klanten / bewoners en potentiële klanten / bewoners centraal. Voor leveranciers en partners is dit document tevens bruikbaar om te begrijpen hoe MGZL omgaat met privacy en hoe het daaraan verbonden securityaspect wordt ingevuld.

Visie

MGZL heeft als visie haar dienstverlening aantoonbaar veilig en zorgvuldig te leveren aan haar klanten / bewoners. Dat geldt voor zowel de intra- als extramurale zorg. Zodra een klanten / bewoner diensten afneemt van MGZL, dient privacy te worden gewaarborgd conform AVG-wetgeving zonder dat zij daar om hoeven te vragen. Van de intake tot het stopzetten van de dienstverlening, dient de klanten / bewoner erop te kunnen vertrouwen dat zorgvuldig omgegaan wordt met de persoonsgegevens die toevertrouwd worden aan MGZL. Datzelfde geldt voor de verwerkingen van persoonsgegevens van medewerkers van MGZL.

Doel

Het privacy beleid heeft als doel ervoor te zorgen dat elke informatie, in elke vorm, is voorzien van een passend veiligheidsniveau.

Dit document heeft ook het doel om betrokkenen inzicht te verschaffen in:

- welke persoonsgegevens worden bewaard;
- hoe deze gegevens zijn verkregen;
- wie toegang heeft tot welke gegevens en aan wie deze gegevens (eventueel) worden verstrekt;
- de rechten die een betrokkene heeft;
- de persoonlijke levenssfeer van ieder van wie persoonsgegevens zijn opgenomen in een of meer bestanden te beschermen tegen misbruik van de gegevens en opslag van onjuiste gegevens;
- te voorkomen dat persoonsgegevens die in een bestand zijn opgenomen voor een ander doel worden gebruikt dan waarvoor dat bestand is bestemd;
- de rechten van de betrokkene te waarborgen.

Scope

- Dit beleid is van toepassing op de geheel of gedeeltelijk geautomatiseerde verwerking van persoonsgegevens, en daarbij de niet geautomatiseerde verwerking van persoonsgegevens die in een bestand zijn opgenomen of die bestemd zijn om daarin te worden opgenomen.

- Dit beleid is van toepassing binnen elk onderdeel van MGZL en heeft betrekking op het door de organisatie-eenheid op te stellen overzicht van genoemde verwerkingen van persoonsgegevens. Dit overzicht vormt één geheel met dit beleid.

Raakvlakken en overlap met andere beleidsthema's

De naleving van privacy is sterk verbonden met informatiebeveiliging. Het informatiebeveiligingsbeleid beschrijft de informatiebeveiligings controls die voor MGZL relevant zijn.

- De verwerkingsverantwoordelijke zorgt voor de voorzieningen van fysieke, technische en organisatorische aard ter beveiliging van de verwerkingen en registraties tegen verlies of aantasting van de gegevens en tegen onbevoegde kennisneming, wijziging of verstrekking daarvan.
- Dezelfde verantwoordelijkheid rust op de beheerder voor het geheel of het gedeelte van de apparatuur die hij beheert. Deze maatregelen garanderen, rekening houdende met de stand van de techniek en de kosten van, een passend beveiligingsniveau.
- Vanuit de AVG is bepaald dat duidelijk moet zijn welke categorieën persoonsgegevens worden verwerkt, met welk doel, hoe de gegevens worden beveiligd, welke rechten betrokkenen hebben en hoe zij die rechten kunnen uitoefenen. Deze gegevens worden vastgelegd in het verwerkingsregister en is op verzoek in te zien door de Autoriteit Persoonsgegevens (AP).

1. Wettelijke kaders voor de omgang met gegevens

De organisatie is verantwoordelijk voor het opstellen, uitvoeren en handhaven van dit privacy beleid. Hiervoor geldt sinds 25 mei 2018 de Europese Verordening; de Algemene Verordening Gegevensbescherming (AVG) en de Uitvoeringswet AVG (UAVG). Als zorginstelling dient MGZL eveneens te handelen conform de (privacyregels in de) Wet op de Geneeskundige Behandelingsovereenkomst (WGBO), de Wet kwaliteit, klachten en geschillen zorg (Wkkgz), de Wet op de beroepen in de individuele gezondheidszorg (Wet BIG), de Zorgverzekeringswet (Zvw), de Wet marktordening gezondheidszorg (Wmg) en de Wet aanvullende bepalingen verwerking persoonsgegevens in de zorg. Daarnaast gelden de regels voor het medisch beroepsgeheim.

2. Definities

De meest fundamentele definities met betrekking tot dit beleid zijn de volgende:

- Persoonsgegevens
De AVG geeft aan dat een persoonsgegeven alle informatie is over een geïdentificeerd of identificeerbaar natuurlijk persoon ("de betrokkene"). Dit betekent dat informatie ofwel direct over iemand gaat, ofwel naar deze persoon te herleiden is. Gegevens van overleden personen of van organisaties zijn geen persoonsgegevens volgens de AVG. MGZL verwerkt alleen persoonsgegevens als daar een wettelijke grondslag voor is (artikel 6 AVG).
- Bijzondere persoonsgegevens
Bijzondere persoonsgegevens zijn gegevens over iemands:
 - o ras of etnische afkomst;
 - o politieke opvattingen;
 - o godsdienst of levensovertuiging;
 - o lidmaatschap van een vakbond;
 - o genetische of biometrische gegevens met oog op unieke identificatie;
 - o gezondheid;
 - o seksuele leven;
 - o strafrechtelijk verleden.Een organisatie mag geen bijzondere persoonsgegevens gebruiken, tenzij daarvoor in de wet een uitzondering is. MGZL verwerkt alléén bijzondere persoonsgegevens als hiervoor een wettelijke uitzondering (artikel 9 lid 2 AVG) geldt.
- Verwerking
Een verwerking van gegevens is elke bewerking of elk geheel van bewerkingen van persoonsgegevens.

- Verwerkingsverantwoordelijke
De verwerkingsverantwoordelijke bepaalt het doel van en de middelen voor de verwerking. De verwerkingsverantwoordelijke is verplicht passende en effectieve maatregelen te nemen om te zorgen dat de verwerkingen in lijn met de AVG plaatsvinden. Daarbij dienen de te nemen maatregelen in verhouding te staan tot de verwerking
- Verwerker
De verwerker verwerkt persoonsgegevens ten behoeve van de verwerkingsverantwoordelijke.

3. Privacyfunctionarissen

Binnen het kader van de gegevensbescherming die relevant is voor de naleving van de AVG en overige privacyrechtelijke regelgeving, zijn de volgende belangrijke rollen gedefinieerd en toegewezen binnen MGZL:

- Chief Information Security Officer;
- Information Security Officer;
- Functionaris gegevensbescherming.

De specifieke verantwoordelijkheden van elk van deze rollen worden in Bijlage A: Rollen en verantwoordelijkheden toegelicht.

Daarnaast zijn er specifieke verantwoordelijkheden op het gebied van gegevensbescherming die worden uitgevoerd door de bestaande interne rollen binnen de organisatie en deze worden ook samengevat in dit document. Deze rollen zijn:

- Afdelingsmanagers;
- Medewerkers.

In het algemeen worden de verantwoordelijkheden die gelden voor alle werknemers, aannemers en andere belanghebbenden uiteengezet binnen het relevante organisatiebeleid.

4. Privacymanagement

De algemene verordening gegevensbescherming (AVG) eist van de organisaties die persoonsgegevens verwerken dat zij deze adequaat beschermen.

De verordening is niet alleen van toepassing op organisaties die binnen de EU zijn gevestigd, maar ook op organisaties buiten de EU die de gegevens van EU-burgers bewaren en verwerken.

De invoering van deze verordening vereist dat zorgvuldig omgegaan wordt met de persoonsgegevens die verzameld en verwerkt worden en dat ervoor gezorgd wordt dat dit op een gepaste transparante en eerlijke manier gebeurt, waarbij rekening wordt gehouden met de rechten van de betrokkenen in het kader van de AVG.

Privacy is een aspect dat nageleefd en uitgedragen dient te worden door iedere medewerker uit de gehele organisatie. Iedere medewerker is dus verantwoordelijk en aansprakelijk voor de naleving van de privacywetgeving. De eindverantwoordelijkheid ligt echter bij de raad van bestuur.

5. Proces eigenaarschap, rechten en plichten van de verwerkingsverantwoordelijke

5.1 Proceseigenaarschap

Privacy is een continue proces, waarbij het van belang is dat het eigenaarschap hiervan aan de juiste personen is toegewezen. In onderstaande opsomming zijn de verantwoordelijkheden en het eigenaarschap van het privacybeleid beschreven:

1. Alle door, of namens MGZL gevoerde verwerkingen en registraties van persoonsgegevens, vallen onder dit reglement.
2. MGZL heeft de dagelijkse zorg voor de persoonsregistraties neergelegd bij één of meer beheerders.

3. De raad van bestuur draagt de eindverantwoordelijkheid voor de naleving van de AVG en de bepalingen van dit reglement en voor de juistheid en de volledigheid van de opgenomen gegevens.
4. MGZL draagt zorg voor de nodige voorzieningen van fysieke, technische en organisatorische aard ter beveiliging van de verwerkingen en registraties tegen verlies of aantasting van de gegevens en tegen onbevoegde kennisneming, wijziging of verstrekking daarvan. Gelijke plicht rust op de beheerder voor het geheel of het gedeelte van de apparatuur die hij onder zich heeft. Deze maatregelen garanderen, rekening houdende met de stand van de techniek en de kosten van ten uitvoerlegging, een passend beveiligingsniveau gelet op de risico's die de verwerking en de aard van de te beschermen gegevens met zich meebrengen.
5. MGZL bepaalt in de rol van verwerkingsverantwoordelijke wie de gebruiker is. De gebruiker is verantwoordelijk voor de naleving van de bepalingen in dit reglement voor zover het geheel of gedeelte van de apparatuur waarmee de verwerking wordt gevoerd bij hem rust.

5.2 Plichten

Verwerking van persoonsgegevens dient plaats te vinden binnen de kaders die beschreven staan in de AVG. Iedere verwerking dient te voldoen aan de verwerkingsbeginselen (art. 5 AVG) en daarmee rechtmatig, behoorlijk en transparant te zijn. Een verwerking is rechtmatig en behoorlijk wanneer deze plaatsvindt op basis van een zogenaamde grondslag.

De rechtmatige grondslag van MGZL voor de verwerking van persoonsgegevens is gelegen in:

1. De verwerking is noodzakelijk voor de uitvoering van een overeenkomst waarbij de betrokkene partij is, of om op verzoek van de betrokkene vóór de sluiting van een overeenkomst maatregelen te nemen;
2. De verwerking is noodzakelijk om te voldoen aan een wettelijke verplichting die op MGZL rust;
3. De verwerking is noodzakelijk om de vitale belangen van de betrokkene of van een andere natuurlijke persoon te beschermen;
4. De verwerking is noodzakelijk voor de behartiging van de gerechtvaardigde belangen van MGZL of van een derde, behalve wanneer de belangen of de grondrechten en de fundamentele vrijheden van de betrokkene die tot bescherming van persoonsgegevens nopen, zwaarder wegen dan die belangen, met name wanneer de betrokkene een kind is.
5. Uitsluitend indien sub 1 t/m 4 niet van toepassing is, betrokkene de ondubbelzinnige (en voor zover vereist uitdrukkelijke) toestemming heeft verleend.

Tevens dient de verwerking gebonden te zijn aan specifieke verzameldoelen en toereikend te zijn, ter zake dienend te zijn, en zich te beperken tot wat noodzakelijk is. MGZL dient te zorgen dat de gegevens juist zijn en gegevens niet langer te bewaren dan nodig. In het kader van een veilige omgang met persoonsgegevens, dienen deze passend beveiligd te zijn en vertrouwelijk te blijven.

Persoonsgegevens worden zoveel mogelijk verzameld bij de betrokkene zelf en zodra persoonsgegevens worden verzameld bij derden volgens de grondslag "toestemming", wordt dat alleen toegestaan zodra ondubbelzinnige toestemming van de betrokkene is ontvangen.

5.3 Toezicht

De functionaris gegevensbescherming (FG) heeft een brede functie. Enerzijds is het de taak om te informeren en adviseren, anderzijds ziet de FG toe op de naleving van de AVG. Om deze taken goed uit te voeren, heeft de FG een beschermd positie. Deze mag niet worden ontslagen of gestraft voor de uitvoering van zijn taken en mag daarover geen instructies ontvangen. Formeel is de FG dus onafhankelijk. Tegelijkertijd heeft de FG geen handhavingsbevoegdheden.

De handhaving van de AVG is neergelegd bij de nationale toezichthouders, in Nederland de Autoriteit Persoonsgegevens (AP). Het samenwerken met de AP en het optreden als contactpunt voor de AP behoort tot de taken van de FG, evenals het plegen van overleg met de AP.

De FG beschikt over de bevoegdheid om te rapporteren aan de hoogste leidinggevende van de organisatie. Dit betekent dat de FG de hoogste leidinggevende op de hoogte brengt van de stand

van zaken aangaande privacy. Deze kan dat naast zich neerleggen, maar neemt daarmee wel de verantwoording voor gerapporteerde misstanden.

Een geheel of gedeeltelijk geautomatiseerde verwerking van persoonsgegevens die voor de verwezenlijking van een bepaald doel of samenhangende doeleinden bestemd is, wordt voor aanvang van de verwerking, gemeld bij de FG.

6. Privacybeleid

Binnen de organisatie wordt dagelijks gewerkt met (bijzondere) persoonsgegevens van betrokkenen. Persoonsgegevens worden voornamelijk verzameld bij de klanten / bewoners van MGZL zodat het uitvoeren van de dagelijkse werkzaamheden mogelijk is. De klanten / bewoners van de organisatie kunnen erop vertrouwen dat de organisatie zorgvuldig en veilig met de persoonsgegevens omgaat. Daarnaast worden de persoonsgegevens van medewerkers verwerkt ten behoeve van de arbeidsrelatie.

6.1 Algemeen

Het bestuur en management spelen een cruciale rol bij het waarborgen van privacy. MGZL geeft middels dit beleid een duidelijke richting aan privacy en laat zien dat zij de privacy waarborgt, beschermt en handhaaft. Dit beleid is van toepassing op de gehele organisatie, alle processen, onderdelen, objecten en gegevensverzamelingen van de organisatie. Dit privacybeleid van organisatie is in lijn met het algemene beleid van MGZL en de relevante lokale, regionale, nationale en Europese wet- en regelgeving.

Bij de naleving van de AVG behoort tevens het toepassen van passende organisatorische en technische maatregelen. Deze maatregelen worden in detail beschreven in het informatiebeveiligingsbeleid. Het informatiebeveiligingsbeleid is conform NEN7510 en is direct gelinkt aan dit privacybeleid. In het Statement Of Applicability van het informatiebeveiligingsbeleid is vastgelegd welke controls van toepassing zijn op de organisatie van MGZL.

6.2 Noodzakelijke gegevensverwerking

De verwerking van persoonsgegevens is elke handeling of elk geheel van handelingen met persoonsgegevens, al dan niet uitgevoerd via geautomatiseerde processen. In de AVG valt onder een verwerking:

- Verzamelen, vastleggen en ordenen;
- bewaren, bijwerken en wijzigen;
- opvragen, raadplegen, gebruiken;
- verstrekken door middel van doorzending;
- verspreiding of enige andere vorm van ter beschikkingstellen;
- samenbrengen, met elkaar in verband brengen;
- afschermen, uitwissen of vernietigen van gegevens.

Uit bovenstaande opsomming blijkt dat alles wat met een persoonsgegeven gedaan wordt een verwerking is. De organisatie verwerkt per definitie enkel persoonsgegevens indien daar een wettelijke grondslag voor is zoals beschreven in artikel 6 AVG of indien er sprake is van een uitzonderingsgrond zoals beschreven is in artikel 9 AVG indien het bijzondere persoonsgegevens betreft.

6.3 Verwerking van bijzondere persoonsgegevens

De verwerking van persoonsgegevens waaruit iemands ras of etnische afkomst, politieke opvattingen, religieuze of levensbeschouwelijke overtuigingen, of het lidmaatschap van een vakbond blijken en verwerking van genetische gegevens, biometrische gegevens met het oog op de unieke identificatie van een persoon, of gegevens over gezondheid, of gegevens met betrekking tot iemands seksueel gedrag of seksuele gerichtheid zijn verboden. Het verwerken van bijzondere persoonsgegevens is wél toegestaan indien hier een wettelijke uitzondering voor bestaat, zoals beschreven in art. 9 AVG.

Delen van gevoelige gegevens met anderen wordt gezien als het doorbreken van de geheimhoudingsplicht en wordt door MGZL alleen gedaan indien:

- Vrijelijk gegeven, ondubbelzinnige en vooraf goed geïnformeerde toestemming is ontvangen voor de specifieke datadeling;
- Een wettelijk voorschrift dit vereist;

- Een conflict van plichten bestaat;
- De gegevens gedeeld worden met de directe betrokkenen (zover dit noodzakelijk is voor hun werkzaamheden).
- De toestemming benodigd is van de wettelijke vertegenwoordigers.
- De gegevens (volledig!!) geanonimiseerd zijn en benodigd zijn voor statistisch onderzoek.

6.4 Gedragsnorm voor proceseigenaren

Het management kan ervan op aan dat proceseigenaren zich bewust zijn van hun verantwoordelijkheid en de nodige maatregelen treffen. Door de organisatie wordt een data protection information assessment (DPIA) uitgevoerd indien dat op grond van artikel 35 AVG vereist is. Met name is een DPIA vereist indien de organisatie:

- Systematisch en uitgebreid persoonlijke aspecten evalueert gebaseerd op geautomatiseerde verwerking, waaronder profiling, en daarop besluiten baseert die gevolgen hebben voor mensen;
- Op grote schaal bijzondere persoonsgegevens verwerkt;
- Op grote schaal en systematisch mensen volgt in een publiek toegankelijk gebied (bijvoorbeeld met cameratoezicht).

6.5 Evenwichtige aanpak

Vanuit een Gegevensbeschermingseffectbeoordeling dient een score te worden vastgesteld door de proceseigenaar, waar de maatregelen voor de privacy borging op afgestemd worden. Er zijn belangen en (mogelijke) nadelen bij een verwerking van persoonsgegevens, zowel voor de organisatie als voor de betrokkene.

6.6 Beheer procesbeschrijving

Op basis van de risico-scores op de DPIA-matrix blijkt welke eisen er zijn aan een procesbeschrijving, aan het toezicht op het betreffende proces, en aan de frequentie waarmee de procesbeschrijving geëvalueerd dient te worden. Ook wordt de verhouding tussen incidenten en procesevaluatie beschreven.

7. Privacy rechten van de betrokkene

Indien MGZL persoonsgegevens verkrijgt bij de betrokkene zelf, wordt de betrokkene op het moment van verkrijging zijn identiteit voorzien van het doel van de verwerking waarvoor de gegevens zijn bestemd, tenzij de betrokkene hiervan reeds op de hoogte is. MGZL verstrekt in het voorgaande bedoelde informatie op een zodanige wijze dat de betrokkene er daadwerkelijk de beschikking over krijgt.

Indien de persoonsgegevens niet rechtstreeks bij de betrokkene worden verkregen deelt MGZL de betrokkene dat mede op het moment van vastlegging van hem betreffende gegevens of, wanneer de gegevens bestemd zijn voor derden, uiterlijk op het moment van eerste verstrekking, tenzij deze reeds daarvan op de hoogte is, de volgende informatie mede:

- zijn identiteit
- de doeleinden van de verwerking waarvoor de gegevens zijn bestemd.

Om de rechten van de betrokkene na te leven heeft MGZL hiervoor een proces ingericht. Vragen over de rechten van de betrokkene worden beantwoord via privacy@mgzl.nl.

7.1 Recht op informatie (artikel 13 en 14 AVG)

Een betrokkene wordt op de hoogte gesteld van het feit dat verwerking van zijn persoonsgegevens plaatsvindt of zal plaatsvinden en wat de doeleinden hiervan zijn. Gegevens die altijd verstrekt worden zijn: informatie over de periode, de rechten van betrokkene, de bron van gegevens en de juridische grondslag voor de verwerking. Verandert het doel van de verwerking, dan wordt ook daarover informatie verstrekt.

7.2 Recht van inzage (artikel 15 AVG)

Betrokkenen hebben het recht te weten of hun betreffende persoonsgegevens worden verwerkt door MGZL. MGZL verstrekt de betrokkene een kopie van de persoonsgegevens die worden verwerkt mits het validatieproces juist wordt doorlopen.

7.3 Recht op rectificatie (artikel 16 AVG)

Betrokkene heeft recht op rectificatie van hem betreffende onjuiste persoonsgegevens dan wel het recht een aanvullende verklaring te verstrekken wanneer de verwerking plaatsvindt op basis van onvolledige gegevens. Deze rectificatie vindt meteen plaats. MGZL stelt iedere ontvanger aan wie persoonsgegevens zijn verstrekt in kennis van elke rectificatie, tenzij dit onmogelijk is of onevenredig veel inspanning vraagt.

7.4 Recht op gegevenswissing / vergetelheid (artikel 17 AVG)

MGZL wist persoonsgegevens van de betrokkene zonder onredelijke vertraging, onder andere indien:

- Persoonsgegevens niet langer nodig zijn voor de doeleinden waarvoor zij zijn verzameld of anderszins verwerkt;
- De betrokkene zijn toestemming intrekt en er geen andere rechtsgrond voor verwerking bestaat;
- Betrokkene bezwaar maakt tegen de verwerking;
- De persoonsgegevens onrechtmatig verwerkt zijn.

7.5 Recht op beperking van de verwerking (artikel 18 AVG)

Het recht op beperking houdt in dat de persoonsgegevens (tijdelijk) niet verwerkt mogen worden en niet gewijzigd mogen worden. Het feit dat de verwerking van de persoonsgegevens beperkt is, wordt door MGZL duidelijk in het bestand aangegeven zodat dit ook duidelijk is voor ontvangers van de persoonsgegevens. Wanneer de beperking weer wordt opgeheven, wordt de betrokkene hiervan op de hoogte gebracht.

7.6 Recht op overdraagbaarheid / dataportabiliteit (artikel 20 AVG)

Dit recht houdt in dat een betrokkene de gegevens van een Verwerkingsverantwoordelijke verkrijgt in gestructureerde, gangbare en machine leesbare vorm en het recht heeft deze gegevens aan een andere Verwerkingsverantwoordelijke over te dragen of rechtstreeks te laten overdragen, zonder daarbij te worden gehinderd tenzij dit afbreuk doet aan rechten en vrijheden van anderen. Een betrokkene heeft recht op overdraagbaarheid voor zover het gaat om door hem zelf verstrekte gegevens.

7.7 Recht van bezwaar (artikel 21 AVG)

Een betrokkene kan vanwege redenen die verband houden met zijn specifieke situatie gebruik maken van dit recht van bezwaar (dat niet vergelijkbaar is met bezwaar op grond van de Awb) tegen de verwerking van hem betreffende persoonsgegevens, als voldaan aan de in de verordening genoemde eisen. Als een betrokkene bezwaar maakt staakt MGZL de verwerking, tenzij dwingende gerechtvaardigde gronden anders bepalen.

7.8 Recht niet te worden onderworpen aan geautomatiseerde individuele besluitvorming / Profiling (artikel 22 AVG)

Bij dit recht kan bijvoorbeeld gedacht worden aan de automatische weigering van een online ingediende kredietaanvraag of aan de verwerking van sollicitaties via internet zonder menselijke tussenkomst. In drie gevallen is geautomatiseerde individuele besluitvorming wel mogelijk:

- A. het is noodzakelijk voor de totstandkoming of de uitvoering van een overeenkomst;
- B. het is toegestaan bij een Unierechtelijke of lidstaatrechtelijke bepaling;
- C. het berust op de uitdrukkelijke toestemming van de betrokkene. Beschrijving van rechten van betrokkenen/burgers.

8. Klachten

Indien de betrokkene van mening is dat de bepalingen van dit beleid niet worden nageleefd of andere reden heeft tot klagen, kan hij zich wenden tot :

- MGZL;
- de binnen MGZL functionerende regeling voor onafhankelijke klachtenbehandeling; hier wordt verwezen naar de "Klachtenregeling medewerkers MGZL" voor medewerkers en "Klachtenbehandeling klanten / bewoners MGZL", voor klanten / bewoners.
- de FG of de autoriteit persoonsgegevens met het verzoek een onderzoek in te stellen of de wijze van gegevensverwerking door MGZL in overeenstemming is met de AVG;
- De Autoriteit Persoonsgegevens, op grond van artikel 77 AVG.

9. Privacy programma

9.1 Bewustwording en training

MGZL vindt privacy dusdanig belangrijk, dat zij ervoor zorgt dat het personeel voorzien wordt van training in de omgang van persoonsgegevens en andere informatie. Middels een user awareness campagne en diverse online trainingen in de vorm van een spel wordt het personeel voorzien van een hoger user awareness niveau. Daarnaast wordt een quiz ingezet om het kennisniveau van het personeel te toetsen, hieraan hangen vooralsnog geen consequenties.

9.2 Archiefbeleid, managementinformatie, gegevensvernietiging

Meander bewaart de persoonsgegevens alleen zo lang als nodig is om de doelen te realiseren waarvoor de gegevens worden verzameld en overeenkomstig haar bewaartermijnenbeleid. Het bewaartermijnenbeleid is uitgewerkt in het [privacyreglement](#) van Meander.

10. Informatiebeveiliging

Vanuit de AVG dient iedere organisatie passende maatregelen te treffen. Het treffen hiervan wordt binnen MGZL toegepast via het informatiebeveiligingsbeleid. In het kader van informatieveiligheid en privacy heeft Meander zichzelf als doel gesteld om informatie, in elke vorm, te voorzien van een passend veiligheidsniveau. In het Informatiebeveiligingsbeleid is hiervan de exacte invulling beschreven.

10.1 Security incident- en datalekprocedure

Security incidenten komen in iedere organisatie voor, maar niet iedereen herkent ze. In het document "[Procedure securityincident en datalek](#)" is beschreven wanneer sprake is van een security incident en wanneer dit geclassificeerd wordt als een datalek.

10.2 Handhaving

De organisatie hanteert de standaard arbeidsvoorwaarden bij niet-nakoming van afspraken volgens dit privacybeleid.

10.3 Beleidsevaluatie

Proceseigenaren doen binnen de planning en control cyclus verslag aan de portefeuillehouder privacy van de werkzaamheden aan het privacybeleid, oplossingen en incidenten die onder hun verantwoordelijkheid hebben voorgedaan met afschrift aan de FG. De FG doet jaarlijks verslag aan het bestuur en geeft aanbevelingen die strekken tot verdere optimalisering van de privacy beleidsvoering. Het college besluit over bijsturing van de organisatie haar privacybeleid met inachtneming van de aanbevelingen van de FG.

Bijlage A: Rollen en verantwoordelijkheden

Verwerkingsverantwoordelijke

De verwerkingsverantwoordelijke heeft de volgende aansprakelijkheid:

- Ervoor zorgen dat de beginselen met betrekking tot de verwerking van persoonsgegevens zoals beschreven in artikel 5 van de AVG worden nageleefd de naleving aan te tonen. Oftewel: ervoor zorgen dat de eisen aan de verwerking van persoonsgegevens worden nageleefd:
 - rechtmatig, eerlijk en transparant worden verwerkt.
 - Verzameld voor specifieke, expliciete en legitieme doeleinden
 - Adequaate, relevant en beperkt tot wat nodig is
 - Nauwkeurig en, waar nodig, bijgewerkt.
 - Opgeslagen in een vorm die het mogelijk maakt de betrokkenen niet langer dan nodig te identificeren.
 - Verwerkt op een manier die de nodige veiligheid garandeert.
- Ervoor zorgen dat, indien nodig, de toestemming van de betrokkene voor de verwerking van de persoonsgegevens wordt verkregen, met inbegrip van de toestemming van de ouders voor de kinderen.
- Alle informatie die op grond van de AVG vereist is, in een beknopte, transparante, begrijpelijke en gemakkelijk toegankelijke vorm aan de betrokkene te verstrekken, in duidelijke en begrijpelijke taal.
- De uitoefening van de rechten van de betrokkene uit hoofde van de AVG vergemakkelijken en de betrokkene op de hoogte houden van de voortgang van zijn of haar verzoek.
- Passende technische en organisatorische maatregelen treffen om ervoor te zorgen en aan te kunnen tonen dat de verwerking in overeenstemming met de AVG plaatsvindt.
- Ervoor zorgen dat alleen verwerkers worden gebruikt die voldoende garanties bieden voor de uitvoering van passende technische en organisatorische maatregelen om aan de AVG te voldoen en om persoonsgegevens te beschermen.
- Een register bijhouden van de verwerkingsactiviteiten met betrekking tot persoonsgegevens die onder de verantwoordelijkheid van de voor de verwerking verantwoordelijke vallen.
- Op verzoek met de toezichthoudende autoriteit samenwerken bij de uitvoering van haar taken
- Ervoor zorgen dat eenieder die onder het gezag van de voor de verwerking verantwoordelijke handelt en toegang heeft tot persoonsgegevens, deze niet verwerkt, behalve in opdracht van de voor de verwerking verantwoordelijke.
- Een inbreuk in verband met persoonsgegevens melden aan de toezichthoudende autoriteit, tenzij het onwaarschijnlijk is dat de inbreuk in verband met persoonsgegevens een risico voor de rechten en vrijheden van natuurlijke personen inhoudt, in overeenstemming met de organisatorische procedures.
- Het documenteren van alle inbreuken in verband met persoonsgegevens, met inbegrip van de feiten met betrekking tot de inbreuk in verband met persoonsgegevens, de gevolgen ervan en de genomen corrigerende maatregelen.
- In voorkomend geval de betrokkene onverwijld in kennis stellen van een inbreuk in verband met persoonsgegevens.
- Indien nodig een effectbeoordelingen uitvoeren met betrekking tot gegevensbescherming uit overeenkomstig de procedures.
- Een functionaris voor gegevensbescherming aanwijzen, indien de GDPR dit voorschrijft, de gegevens ervan publiceren en aan de toezichthoudende autoriteit mededelen.
- De functionaris voor gegevensbescherming te ondersteunen bij de uitvoering van zijn taken door de nodige middelen ter beschikking te stellen om deze taken uit te voeren en toegang

te krijgen tot persoonsgegevens en verwerkingsoperaties, en om zijn of haar deskundige kennis op peil te houden

- Persoonsgegevens alleen naar een derde land of een internationale organisatie doorgeven indien de voor de verwerking verantwoordelijke of de verwerker passende waarborgen heeft geboden en op voorwaarde dat afdwingbare rechten van de betrokkene en doeltreffende rechtsmiddelen voor de betrokkenen beschikbaar zijn.

Verwerker

De gegevensverwerker heeft de volgende aansprakelijkheid:

- Ervoor zorgen dat elke verwerking van persoonsgegevens wordt geregeld door een contract of een andere rechtshandeling waarin het onderwerp en de duur van de verwerking, de aard en het doel van de verwerking, het soort persoonsgegevens en de categorieën van betrokkenen en de verplichtingen en rechten van de verantwoordelijke voor de verwerking zijn vastgelegd.
- Alleen persoonsgegevens te verwerken op gedocumenteerde instructies van de verantwoordelijke voor de verwerking, ook met betrekking tot de doorgifte van persoonsgegevens naar een derde land of een internationale organisatie.
- Ervoor zorgen dat personen die bevoegd zijn om de persoonsgegevens te verwerken, zich tot geheimhouding hebben verplicht of onder een passende wettelijke verplichting tot geheimhouding vallen.
- Passende technische en organisatorische maatregelen treffen om te zorgen voor een beveiligingsniveau dat is afgestemd op het risico dat aan de verwerking van persoonsgegevens is verbonden.
- Verkrijg de voorafgaande specifieke of algemene schriftelijke toestemming van de voor de verwerking verwerkingsverantwoordelijke voordat u een andere verwerker in dienst neemt.
- de voor de verwerking verwerkingsverantwoordelijke helpen bij het nakomen van de verplichting van de voor de verwerking verwerkingsverantwoordelijke om te reageren op verzoeken tot uitoefening van de rechten van de betrokkene
- Alle persoonsgegevens verwijderen of terugsturen naar de verwerkingsverantwoordelijke voor de verwerking na afloop van de dienstverlening met betrekking tot de verwerking
- De controleur alle informatie ter beschikking stellen die nodig is om aan te tonen dat de verplichtingen van de AVG worden nageleefd en om audits, met inbegrip van inspecties, door de controleur of een andere door de controleur gemandateerde auditor mogelijk te maken en daaraan bij te dragen.
- Het bijhouden van een register van alle categorieën van verwerkingsactiviteiten die worden uitgevoerd voor rekening van een voor de verwerking verwerkingsverantwoordelijke.
- Op verzoek met de toezichthoudende autoriteit samenwerken bij de uitvoering van haar taken
- Ervoor zorgen dat eenieder die onder het gezag van de verwerker handelt en toegang heeft tot persoonsgegevens, deze niet verwerkt, behalve in opdracht van de voor de verwerking verwerkingsverantwoordelijke.
- Stel de verwerkingsverantwoordelijke voor de verwerking zonder onnodige vertraging op de hoogte van een inbreuk in verband met persoonsgegevens.
- Een functionaris voor gegevensbescherming aanwijzen, indien de GDPR dit voorschrijft, de gegevens ervan publiceren en aan de toezichthoudende autoriteit mededelen.
- de functionaris voor gegevensbescherming te ondersteunen bij de uitvoering van zijn taken door de nodige middelen ter beschikking te stellen voor de uitvoering van die taken en de toegang tot persoonsgegevens en verwerkingsoperaties, en om zijn of haar deskundige kennis op peil te houden

Functionaris gegevensbescherming:

– **Chief Information Security Officer**

De Chief Information Security Officer (CISO) is verantwoordelijk voor beveiliging van gezondheidsinformatie binnen de organisatie

– **Information Security Officer**

De Information Security Officer (ISO) is verantwoordelijk voor uitvoering van de beveiliging van gezondheidsinformatie binnen de organisatie