Gegevensbeschermingsbeleid

Veiligheids- en Gezondheidsregio Gelderland-Midden

Versie 1.01
Maart
Auteu [redacted]

Versiebeheer

Datum	Versie	Auteur	Omschrijving
27-11-2020	1.0	[redacted]	Final document vastgesteld
8-3-2021	1.01		Artikel 4.3 aangepast. Vernietiging vanuit de archiefwet toegevoegd. Rol management bij vaststellen bewaartermijnen verwijderd.

Inhoud

1 Inleiding 4
1.1 Visie op gegevensbescherming 4
1.2 Reikwijdte 4
1.3 Juridisch kader 5
1.4 Begripsbepalingen 5
1.5 Ingangsdatum 7
2 Organisatie 8
2.1 De wettelijke verantwoordelijkheden 8
2.2 Verantwoording 8
2.3 Organisatorische borging 8
2.4 Sturing en monitoring 8
3 Uitgangspunten zorgvuldige gegevensbescherming 10
3.1 Omgaan met persoonsgegevens 10
3.2 Rechtmatige grondslag van de verwerking 10
3.3 Verkrijging van gegevens 10
3.4 Toegang tot en verstrekking van persoonsgegevens 10
3.5 Gebruik van gegevens voor onderzoek en statistische doelen 11
4 Bescherming van gegevens 12
4.1 Data Protection Impact Assessment (DPIA) 12
4.2 Dataminimalisatie 12
4.3 Bewaren en vernietigen van gegevens 12
4.4 Dataclassificatie 12
4.5 Logging van gegevensgebruik 12
4.6 Verwerkersovereenkomst 13
4.7 Bewust omgaan met persoonsgegevens 13
4.8 Meldplicht voor inbreuken in verband met persoonsgegevens (datalekken) 13
5 Rechten van betrokkenen 15
5.1 Rechten en plichten aangaande het medisch dossier 15
5.2 Rechten van betrokkenen 15
5.3 Recht op informatie en toegang tot gegevens 16
5.4 Recht op inzage en afschrift van gegevens 16
5.5 Recht op rectificatie (correctie, aanvulling) van gegevens 16
5.6 Recht op gegevenswissing 16

5.7 Recht op beperking van de verwerking 17
5.8 Recht op overdraagbaarheid van gegevens (dataportabiliteit) 17
5.9 Recht van bezwaar tegen verwerking 17
5.10 Recht niet te worden onderworpen aan geautomatiseerde individuele besluitvorming waaronder profilering 17
5.11 Klachten en vragen 18
5.12 Informeren van (keten)partners 18
6 Functies en verantwoordelijkheden 19
7 Toezicht op de gegevensvewerking 21

1 Inleiding

Privacy is volop in ontwikkeling waardoor de Veiligheids- en Gezondheidsregio Gelderland-Midden (VGGM) een nog belangrijkere verantwoordelijkheid krijgt waar het gaat om de verwerking van persoonsgegevens van haar cliënten, patiënten en medewerkers. Daarnaast wordt de bescherming van persoonlijke gegevens steeds complexer. Zwakke beveiliging en/of niet adequate verwerking van persoonsgegevens kan leiden tot misbruik of verlies.Een zorgvuldige omgang met de gegevens van haar cliënten, patiënten en medewerkers is essentieel voor het vertrouwen in VGGM. VGGM hecht er dan ook veel waarde aan dat de verwerkingen van persoonsgegevens zorgvuldig, rechtmatig en veilig gebeurt.

Dit beleid gaat primair om naleving van de wet- en regelgeving welke voorziet in de verwerking van persoonsgegevens. VGGM zorgt hiermee voor een goed gedocumenteerd stelsel van interne afspraken waarmee de belangen kunnen worden gewaarborgd. Daarnaast leidt het mogelijk ook tot efficiënter werken omdat inzicht geboden wordt in de verwerking van gegevens.
In dit beleid staan kaders beschreven voor het verwerken en het beschermen van persoonsgegevens en de omgang met deze gegevens. In gevallen waarin dit beleid niet voorziet, beslist het hoger management. Dit beleid geldt niet enkel ten aanzien van de medewerkers van VGGM en derden die betrokken zijn bij de gegevensverwerking, maar ook ten aanzien van alle personen waarvan VGGM over gegevens beschikt.
Om het beschermen van persoonsgegevens te borgen is een adequate informatiebeveiliging beschikbaar. Hiervoor wordt verwezen naar het Informatiebeveiligingsbeleid zoals dit binnen VGGM geformaliseerd is.

1.1 Visie op gegevensbescherming

De verwerking van persoonsgegevens is een essentieel onderdeel van het bestaansrecht van VGGM. De verwerking van gegevens gaat gepaard met de verantwoordelijkheid om effectieve bescherming van gegevens te bieden. Het uitgangspunt hierbij is, dat we respect hebben voor de persoonlijke levenssfeer van alle betrokkenen. Daarbij houdt VGGM zich aan de wettelijke regels op het gebied van de verwerking van de persoonsgegevens.

1.2 Reikwijdte

Dit beleid is van toepassing op alle geheel of gedeeltelijk geautomatiseerde verwerkingen van persoonsgegevens binnen de administratieve organisatie van VGGM. Daarnaast is het van toepassing op de niet geautomatiseerde verwerking van persoonsgegevens die in een bestand zijn opgenomen. De kaders die in dit beleid staan beschreven gelden voor iedereen (zowel interne als externe verwerkers) die namens VGGM gegevens verwerken.

Wanneer in dit document gesproken wordt over VGGM wordt bedoeld:

- Brandweer
- Gemeentelijke GezondheidsDienst (GGD)
  - Jeugd & gezondheid
  - Infectieziekten & hygiëne
  - Milieu & gezondheid
  - Reizen & gezondheid
  - Seks & gezondheid
  - Openbare Geestelijke Gezondheidszorg
  - Tuberculosebestrijding
  - Technische Hygiënezorg
  - Forensische geneeskunde
  - Onderzoek, Informatie en Advies
  - Wmo-toezicht
  - Ambulancezorg
  - Corona
- Geneeskundige Hulpverleningsorganisatie in de Regio (GHOR)
- Bedrijfsvoering

Dit gegevensbeschermingsbeleid is ook van toepassing op de Stichting Publieke Gezondheid Gelderland-Midden en de Stichting Veilig Thuis Gelderland-Midden.

1.3 Juridisch kader

Bij de verwerking van persoonsgegevens staat respect voor de persoonlijke levenssfeer van de betrokkenen voorop. Er moet voorkomen worden dat er onnodig inbreuk wordt gemaakt. De Algemene Verordening Gegevensbescherming (AVG) welke sinds 25 mei 2018 van kracht is, biedt hiervoor het wettelijk kader. De AVG heeft als doel om de privacy van burgers in Europa beter te beschermen. Sinds 1 januari 2016 bestaat ook al de meldplicht datalekken. Daarnaast is er zorg-specifieke wetgeving van kracht waarin ook een kader voor privacy is weggelegd. Bij dit beleid wordt in aanmerking genomen:

- Algemene Verordening Gegevensbescherming (“AVG”);
- Uitvoeringswet Algemene Verordening Gegevensbescherming (“UAVG”);
- Burgerlijk Wetboek, Boek 7 (Wet op de geneeskundige behandelingsovereenkomst, ”WGBO”);
- Wet op de Beroepen in de individuele gezondheidszorg (Wet Big);
- Wet kwaliteit, klachten en geschillen zorg (“Wkkgz”);
- Wet aanvullende bepalingen verwerking persoonsgegevens in de zorg (“Wabvpz”);
- Besluit elektronische gegevensverwerking door zorgaanbieders (Besluit egz);
- Wet en besluit publieke gezondheid (“Wpg”);
- Burgerlijk Wetboek, Boek 1; Jeugdwet (“Jw”);
- Wet maatschappelijke ondersteuning 2015 (“Wmo”);
- Wet verplichte meldcode huiselijk geweld en kindermishandeling;
- Wet op de lijkbezorging;
- Wet toetsing levensbeëindiging op verzoek en hulp bij zelfdoding;
- Vreemdelingenwet in verband met de Regeling verstrekkingen asielzoekers en andere categorieën vreemdelingen 2005;
- Wet op het bevolkingsonderzoek;
- Wet verplichte geestelijke gezondheidszorg (“Wvggz”);
- Wet op de Veiligheidsregio’s (“Wvr”)
- KNMG-richtlijn Omgaan met medische gegevens;
- KNMG-meldcode Kindermishandeling en huiselijk geweld;
- KNMG/GGD GHOR NL/GGZ NL-handreiking Gegevensuitwisseling in de bemoeizorg;
- KNCV-richtlijn Archivering tuberculosegegevens (Commissie voor Praktische Tuberculosebestrijding);
- GGD NL-handreiking Privacybescherming epidemiologie;
- FMWV-gedragscode Gezondheidsonderzoek (Federatie Medisch Wetenschappelijke Verenigingen);

Het doel van dit gegevensbeschermingsbeleid is om invulling te geven aan de manier waarop binnen VGGM wordt omgegaan met privacy en gegevensbescherming.
Als algemene regel geldt dat persoonsgegevens binnen VGGM op een zorgvuldige wijze moeten worden verwerkt. Persoonsgegevens mogen enkel en alleen voor een specifiek beschreven doel worden verwerkt. Daarbij geldt dat deze gegevens niet langer mogen worden bewaard dan noodzakelijk om het doel waarvoor ze zijn verzameld, te realiseren. De betrokkene kan altijd inzage of wijziging van de verwerkte persoonsgegevens vragen. Dit wordt in de volgende hoofdstukken nader uitgewerkt.

1.4 Begripsbepalingen

Persoonsgegeven
Elk gegeven betreffende een geïdentificeerde of identificeerbare natuurlijke persoon.

- *Personalia en identificatiegegevens*
  Persoonsgegevens, die betrekking hebben op persoonlijke bijzonderheden van betrokkene (naam,

adres, woonplaats e.d.)

- *Medische, psychologische en/of sociale gegevens*
  Persoonsgegevens, direct of indirect betrekking hebbend op de lichamelijke of geestelijke gesteldheid van betrokkene, verzameld door een beroepsbeoefenaar op het gebied van de gezondheidszorg in het kader van zijn beroepsuitoefening.

- *Financiële en administratieve gegevens*
  Gegevens die in de administratie van de Veiligheids- en Gezondheidsregio Gelderland-Midden en de persoonsdossiers zijn opgenomen, niet zijnde personalia, identificatie, medische, psychologische of sociale gegevens, die noodzakelijk zijn voor de financiering en/of administratieve afhandeling.

- *Gegevens derden*
  Gegevens van derden die in de administratie van Veiligheids- en Gezondheidsregio Gelderland-Midden en de persoonsdossiers zijn opgenomen, die noodzakelijk zijn voor de zorgverlening.

Verwerking van persoonsgegevens
Elke handeling of geheel van handelingen met betrekking tot persoonsgegevens, waaronder in ieder geval het verzamelen, vastleggen, ordenen, bewaren, bijwerken, wijzigen, opvragen, raadplegen, gebruiken, verstrekken door middel van doorzending, verspreiding of enige vorm van terbeschikkingstelling, samenbrengen, met elkaar in verband brengen, alsmede het afschermen, uitwissen of vernietigen van gegevens.

Bestand
Elk gestructureerd geheel van persoonsgegevens, ongeacht of dit geheel van gegevens gecentraliseerd is of verspreid is op een functioneel of geografische wijze, dat volgens bepaalde criteria toegankelijk is en betrekking heeft op verschillende personen.

Verantwoordelijke
Het bestuur dat het doel van en de middelen voor de verwerking van persoonsgegevens vaststelt: het dagelijks betuur van Veiligheids- en Gezondheidsregio Gelderland-Midden.

Verwerker
Externe persoon of organisatie die ten behoeve van de verantwoordelijke persoonsgegevens verwerkt, zonder aan zijn rechtsgezag te zijn onderworpen.

Veiligheids- en Gezondheidsregio Gelderland-Midden
Veiligheids- en Gezondheidsregio Gelderland-Midden, het rechtspersoonlijkheid bezittend openbaar lichaam, ingesteld op grond van de Wet gemeenschappelijke regelingen. De Algemene Verordening Gegevensbescherming is van toepassing op alle gegevensverwerkingen binnen Veiligheids- en Gezondheidsregio Gelderland-Midden.

Betrokkene
Degene op wie een persoonsgegeven betrekking heeft.

Derde
Ieder ander dan de betrokkene, de verantwoordelijke, de verwerker, of degene(n) die onder gezag van de verantwoordelijke of de verwerker gemachtigd is (zijn) om persoonsgegevens te verwerken.

Ontvanger
Degene aan wie de persoonsgegevens worden verstrekt.

Toestemming van betrokkene
Elke vrije, specifieke en op informatie berustende wilsuiting waarmee de betrokkene aanvaardt dat zijn persoonsgegevens worden verwerkt. Deze toestemming moet vrij en ondubbelzinnig zijn. Dat betekent dat

betrokkenen in vrijheid hun wil moeten kunnen uiten. Ook mag er geen twijfel zijn of betrokkenen hun toestemming hebben gegeven en voor welke specifieke verwerking zij dit hebben gedaan.

Gebruiker
Degene die geautoriseerd is gegevens in een persoonsregistratie in te voeren en/of te muteren, dan wel van enigerlei uitvoer van de persoonsregistratie kennis te nemen.

Beheerder
Degene die binnen de organisatie belast is met de inrichting en de beveiliging van een bestand binnen een organisatieonderdeel of, in een hiërarchische lijn daarboven, een cluster van bestanden.

Autoriteit Persoonsgegevens
De toezichthouder die tot taak heeft toe te zien op de verwerking van persoonsgegevens overeenkomstig de Algemene Verordening Gegevensbescherming.

Verstrekken van persoonsgegevens
Het bekend maken of ter beschikking stellen van persoonsgegevens.

Verwerking van persoonsgegevens
Elke handeling of elk geheel van handelingen met betrekking tot persoonsgegevens, waaronder in ieder geval het verzamelen, vastleggen, ordenen, bewaren, bijwerken, wijzigen, opvragen, raadplegen, gebruiken, verstrekken door middel van doorzending, verspreiding of enige andere vorm van terbeschikkingstelling, samenbrengen, met elkaar in verband brengen, evenals het afschermen, uitwissen of vernietigen van gegevens.

Verwerkingsregister
Een overzicht van alle verwerkingen van persoonsgegevens die plaatsvinden binnen de Veiligheids- en Gezondheidsregio Gelderland-Midden. Het register dient actueel te zijn en wordt zodoende aangepast zodra verwerkingen worden aangepast of wanneer sprake is van nieuwe verwerkingen. Ten minste jaarlijks vindt een review plaats.

Data Protection Impact Assessment (DPIA)
Een instrument om de privacyrisico's in kaart te brengen wanneer er sprake is van een verwerking van persoonsgegevens. Ook wel genoemd Gegevensbeschermingseffectbeoordeling of Privacy Impact Assessment (PIA).

Datalek
Een datalek is een inbreuk op de beveiliging die per ongeluk of op onrechtmatige wijze leidt tot de vernietiging, het verlies, de wijziging of de ongeoorloofde verstrekking van of de ongeoorloofde toegang tot doorgezonden, opgeslagen of anderszins verwerkte gegevens

Dataminimalisatie
Bij het verzamelen en verwerken van persoonsgegevens mogen niet meer gegevens worden gebruikt dan nodig is om het doel waarvoor ze gebruikt zullen worden te bereiken.

Anonimiseren
Persoonsgegevens die voor een taakuitvoering niet meer noodzakelijk zijn, worden verwijderd uit een dataset. De dataset bevat dan enkel geanonimiseerde gegevens, die wel worden bewaard voor bijvoorbeeld onderzoeksdoeleinden of om te gebruiken als open data. Geanonimiseerde gegevens zijn geen persoonsgegevens en vallen niet onder dit beleid.

1.5 Ingangsdatum

De laatste versie van dit document dateert van november 2020. Dit beleid treedt in werking nadat het is vastgesteld en gecommuniceerd door de directie van VGGM (december 2020).

2 Organisatie

2.1 De wettelijke verantwoordelijkheden

De manier waarop dit beleid binnen VGGM wordt verankerd, vormt het fundament van de privacyborging. Het hoger management is verantwoordelijk voor juiste gegevensverwerking en informatiebeveiliging. Echter deze verantwoordelijkheid beperkt zich niet enkel tot het management. Zorgvuldige gegevensverwerking geldt voor iedereen die binnen VGGM werkzaam is. Het niet in acht nemen van privacy normen of ernstige schending daarvan kan leiden tot het nemen van maatregelen.

2.2 Verantwoording

Het hoger management is verantwoordelijk voor de juiste naleving van de AVG en het beleid op het gebied van de gegevensverwerking. Ook VGGM geeft privacy een hoge prioriteit. Naast het jaarlijkse verantwoorden, hebben zowel het management als de Functionaris Gegevensbescherming de plicht om het Dagelijks Bestuur te informeren over bijzonderheden (incidenten) ten aanzien van gegevensverwerking.

2.3 Organisatorische borging

De afdelingshoofden zijn verantwoordelijk voor de borging van de uitganspunten van dit beleid binnen hun werkprocessen. Het borgen van de privacy is hierbij onlosmakelijk verbonden met het informatiebeveiligingsbeleid. De afdelingshoofden zullen in veel gevallen werken met een aandachtsfunctionaris privacy. Daar waar een aandachtsfunctionaris privacy is aangesteld, zal hij/zij betrokken worden bij het uitvoeren van de gegevensbeschermingseffectbeoordeling, tevens zal hij/zij als aanspreekpunt dienen voor vragen uit de eigen het eigen team, optreden als sparingspartner voor de Functionaris voor de Gegevensbescherming en bij relevante veranderingen in het verwerken van persoonsgegevens, dit signaleren en benoemen richting de Functionaris voor de Gegevensbescherming.

De Functionaris voor de Gegevensbescherming (FG) heeft een toetsende rol en houdt zodoende toezicht op het nakomen van het opgestelde gegevensbeschermingsbeleid. De FG adviseert hierin onafhankelijk richting directie en management. Daarnaast heeft de FG nog een aantal andere verantwoordelijkheden zoals adviseren over privacy vragen en klachten, het toetsen op de aanwezigheid van een verwerkingsregister, het overzicht houden op de verwerkers die namens VGGM zijn aangesteld en het toetsen van de uitgevoerde gegevensbeschermingseffectbeoordelingen (DPIA). De FG is onafhankelijk, maar rapporteert periodiek en wanneer hier aanleiding toe is, aan de directie van VGGM.

De Adviseur Informatiebeveiliging en Gegevensbescherming is verantwoordelijk voor het actualiseren van het informatiebeveiligingsbeleid en dit gegevensbeschermingsbeleid. Daarnaast wordt de Adviseur Informatiebeveiliging en Gegevensbescherming geconsulteerd bij diverse projecten waarbij security of privacy mogelijk een rol speelt. De Adviseur Informatiebeveiliging en Gegevensbescherming richt zich voornamelijk op de organisatorische kant van informatiebeveiliging, de technische aspecten worden door de afdeling ICT invulling gegeven. De Adviseur Informatiebeveiliging en Gegevensbescherming rapporteert aan het afdelingshoofd Mens en Organisatie van de sector Bedrijfsvoering.

2.4 Sturing en monitoring

Met een reeks maatregelen wordt geborgd dat er continu gewerkt wordt aan het optimaliseren en borgen van de kwaliteit van de werkprocessen waarbij privacy een rol speelt. Elke afdelingsmanager is verantwoordelijk voor de zorgvuldige verwerking van persoonsgegevens die binnen zijn of haar werkprocessen plaatsvindt. Het is daarom ook hun verantwoordelijkheid om te monitoren of persoonsgegevens zorgvuldig verwerkt worden, en dit zo nodig bij te sturen. Daarnaast zijn zij verplicht om incidenten te melden bij de FG[1]. De FG heeft de verantwoordelijkheid om structureel te toetsen of de wettelijke eisen en richtlijnen op het gebied van gegevensbescherming zijn geïmplementeerd en worden

[1] Binnen de Veiligheids- en Gezondheidsregio Gelderland-Midden is de Adviseur Informatiebeveiliging en Gegevensbescherming tevens aangesteld als Functionaris Gegevensbescherming.

uitgevoerd.

Juist omdat gegevensbescherming voor een belangrijk deel mensenwerk is, moet op alle niveaus binnen VGGM over gegevensbescherming worden nagedacht. Door dit onderwerp vast op de diverse agenda's te plaatsen, ontstaat een continu proces van veranderen en verbeteren. Door vanuit verschillende niveaus en rollen binnen VGGM naar de kwaliteit van de uitvoering van privacy te kijken, ontstaat een evenwichtig systeem. De belangrijkste elementen van deze borging zijn:

- Vaststellen van dit beleid
- Uitvoering van dit beleid
- Gegevensbescherming als onderwerp in werkoverleggen
- Toezicht op gegevensbescherming
- Gegevensbescherming in het plan- en controlproces (PDCA)
- Interne (en externe) audit

3 Uitgangspunten zorgvuldige gegevensbescherming

3.1 Omgaan met persoonsgegevens

Persoonsgegevens worden bij VGGM in overeenstemming met de wet en op zorgvuldige wijze verwerkt. Dit houdt in dat persoonsgegevens alleen voor specifieke, uitdrukkelijke en legitieme doeleinden worden verzameld en dat er niet meer persoonsgegevens worden verwerkt dan voor dat doel noodzakelijk is. Daarbij wordt tenminste rekening gehouden met de wettelijke grondslag, de aard van de gegevens, de gevolgen van de verdere verwerking voor de betrokkene, de wijze waarop de gegevens zijn verkregen en de gestelde waarborgen ter bescherming van de persoonlijke levenssfeer.

3.2 Rechtmatige grondslag van de verwerking

De verwerking van persoonsgegevens mag alleen gebeuren wanneer er sprake is van een rechtmatige grondslag voor de verwerkingen is gelegen in:

- De toestemming van de betrokken persoon.
- De gegevensverwerking is noodzakelijk voor de uitvoering van een overeenkomst.
- De gegevensverwerking is noodzakelijk voor het nakomen van een wettelijke verplichting.
- De gegevensverwerking is noodzakelijk ter bescherming van de vitale belangen.
- De gegevensverwerking is noodzakelijk voor de vervulling van een taak van algemeen belang of uitoefening van openbaar gezag.
- De gegevensverwerking is noodzakelijk voor de behartiging van de gerechtvaardigde belangen.

Vanuit VGGM zijn er verschillende grondslagen aan te reiken om gegevens te verwerken. Binnen de Publieke Gezondheid gaat het in veel gevallen om het voldoen aan een wettelijke verplichting, binnen de brandweer worden gegevens verwerkt om een taak van algemeen belang goed te vervullen. Maar ook alle andere grondslagen zijn op specifieke verwerkingen van toepassing. De grondslag voor verwerking wordt in het verwerkingsregister vastgelegd.

3.3 Verkrijging van gegevens

De persoonsgegevens worden door de betrokkene zelf verstrekt, of vanuit een landelijke administratie ontsloten (zoals BRP = Basisregistratie Personen). Wat er precies met de verzamelde gegevens gebeurt, is afhankelijk van het doel waarvoor ze verzameld worden. Meestal worden ze in een informatiesysteem opgenomen waar ze alleen toegankelijk zijn voor de medewerkers die belast zijn met het uitvoeren van een specifieke taak. Gegevens worden niet zonder toestemming van de betrokkene of wettelijke grondslag gedeeld. Informatiesystemen moeten voldoen aan de gestelde eisen. De herkomst van de gegevens wordt vastgelegd in het verwerkingsregister.

3.4 Toegang tot en verstrekking van persoonsgegevens

Alle medewerkers, intern en extern zijn verplicht tot geheimhouding van de persoonsgegevens, waarvan zij kennis nemen. Uitsluitend de taakverantwoordelijke heeft ten behoeve van een juiste verwerking rechtstreekse toegang tot persoonsgegevens. Gegevens uit de gegevensverwerking en uit de bestanden die gebruikt worden voor het verwerken van gegevens kunnen worden verstrekt aan binnen VGGM werkzame personen, die rechtstreeks betrokken zijn bij de dienstverlening aan en begeleiding van de betrokkene, voor zover dit voor hun taakuitoefening noodzakelijk is. Indien de werkzame persoon niet direct toegang zou hoeven hebben voor het uitvoeren van zijn/haar taak, wordt ook geen toegang verleend.

Aan derden worden de gegevens enkel verstrekt indien:

1. Een wettelijk voorschrift ertoe verplicht de gegevens te verstrekken;
2. De betrokkene schriftelijk toestemming heeft verleend tot gegevensverstrekking voor een kenbaar specifiek doel;
3. Daarnaast worden de gegevens verstrekt aan de verwerkers, indien dit voor de uitoefening van de taken van de verantwoordelijke noodzakelijk is.

Derden, die op vastgestelde wijze bepaalde persoonsgegevens verwerken, worden door het management van VGGM ingelicht over de daaraan gestelde voorwaarden en beperkingen. De afspraken hierover worden vastgelegd in de verwerkersovereenkomst.
Extra aandacht is er voor de processen rondom in- door en uitstroom. Toegang tot gegevens wordt verschaft wanneer dit voor het uitvoeren van de functie noodzakelijk is. Bij door- en uitsroom is het management verantwoordelijk dat accounts tijdig worden geblokkeerd. Door de functioneel beheerders dient er actief gecontroleerd te worden op d toegang en autorisaties.

3.5 Gebruik van gegevens voor onderzoek en statistische doelen

Het gebruik van persoonsgegevens voor wetenschappelijk of historisch onderzoek of statistische doeleinden mag, mits betrokkene van wie de data voor het onderzoek wordt gebruikt hierover is geïnformeerd en passende waarborgen zijn genomen. Binnen VGGM wordt de data zodoende minimaal gepseudonimiseerd voor gebruik.

Wanneer persoonsgegevens worden gedeeld met derde partijen voor onderzoek of statische doeleinden moet toestemming aan betrokkenen worden gevraagd.

Het delen van de gegevens van de patiënt kan enkel zonder toestemming indien gegevens worden verstrekt ten behoeve van statistisch of wetenschappelijk onderzoek op het gebied van de volksgezondheid. Hierbij opgemerkt dat het onderzoek dan een algemeen belang dient, het onderzoek niet zonder de desbetreffende gegevens kan worden uitgevoerd, en voor zover de betrokken patiënt tegen een verstrekking niet uitdrukkelijk bezwaar heeft gemaakt. Bij een verstrekking wordt een aantekening bijgehouden in het dossier.
Daarbij geldt wel dat het vragen van toestemming in redelijkheid niet mogelijk is en met betrekking tot de uitvoering van het onderzoek is voorzien in zodanige waarborgen, dat de persoonlijke levenssfeer van de patiënt niet onevenredig wordt geschaad. Het kan ook zijn dat het vragen van toestemming, gelet op de aard en het doel van het onderzoek, in redelijkheid niet kan worden verlangd en de hulpverlener zorg heeft gedragen dat de gegevens in zodanige vorm worden verstrekt dat herleiding tot individuele natuurlijke personen redelijkerwijs wordt voorkomen. Ook in dat geval kunnen gegevens zonder toestemming worden gedeeld.

4 Bescherming van gegevens

VGGM treft passende technische en organisatorische maatregelen ter bescherming, bevordering van de juistheid en volledigheid van de persoonsgegevens en ter voorkoming van inbreuk, verlies en onrechtmatige verwerking van de persoonsgegevens. De AVG geeft aan dat er technische en organisatorische maatregelen getroffen moeten worden. De AVG bevat geen verplichtingen over de manier waarop de gegevensbescherming geborgd moeten worden. De maatregelen dienen een passend niveau van beveiliging, met inbegrip van vertrouwelijkheid, te waarborgen, rekening houdend met de stand van de techniek en de uitvoeringskosten afgezet tegen de risico's en de aard van de te beschermen persoonsgegevens. Er zijn verschillende instrumenten beschikbaar om gegevensbescherming te waarborgen.

4.1 Data Protection Impact Assessment (DPIA)

Eén van de instrumenten om de gegevensbescherming te borgen is de uitvoering van een Data Protection Impact Assessment (DPIA). De DPIA wordt ook wel de gegevensbeschermingseffectbeoordeling of de Privacy Impact Assessment (PIA) genoemd. Bij het aanpassen van een bestaande verwerking of het starten van een nieuwe verwerking moet een DPIA worden uitgevoerd indien de verwerking een hoog risico voor de gegevensbescherming bevat. De DPIA wordt gebruikt om risico's in kaart te brengen en om de maatregelen te nemen om deze risico's in de gegevensverwerking te minimaliseren.

4.2 Dataminimalisatie

Met de komst van de AVG worden de beginselen *Privacy by design* en *Privacy by default* geïntroduceerd. Om te waarborgen dat binnen VGGM wordt gehandeld in overeenstemming met Privacy by design en Privacy by default, moet met name dataminimalisatie voldoende gewaarborgd zijn.
Dataminimalisatie houdt in dat bij het verzamelen en verwerken van persoonsgegevens niet meer gegevens mogen worden gebruikt dan nodig is om het doel waarvoor ze gebruikt zullen worden te bereiken. Om dataminimalisatie goed toe te passen, is het belangrijk om goed vast te leggen op welke manier de gegevens zijn verkregen en voor welk doel de gegevens worden gebruikt, waarbij ook de duur van het gebruik een bepalende factor is.

4.3 Bewaren en vernietigen van gegevens

Om ervoor te zorgen dat persoonsgegevens niet langer worden bewaard dan noodzakelijk is, dient VGGM termijnen vast te stellen voor het wissen van gegevens of voor een periodieke toetsing ervan.
De bewaartermijnen van persoonsgegevens lopen uiteen. In diverse wetten zijn minimale en maximale bewaartermijnen opgenomen. Daarnaast geldt de Archiefwet voor het bewaren en vernietigen van papieren en elektronische documenten. Dit betekent ook dat gegevens aan het einde van de bewaartermijn opgeschoond moeten worden. Indien gegevens nog gebruikt worden voor statistische- of onderzoeksdoeleinden, dan dienen de gegevens geanonimiseerd te worden.

4.4 Dataclassificatie

De maatregelen die getroffen moeten worden om de gegevensbescherming te kunnen borgen, is niet voor elk proces en informatiesysteem hetzelfde. Daarom is het nodig dat alle processen en informatiesystemen die gegevens verwerken een dataclassificatie krijgen. Dataclassificatie heeft als doel om de beschikbaarheid, integriteit en vertrouwelijkheid van het proces en het informatiesysteem te benoemen. Zo wordt inzichtelijk welke maatregelen genomen moeten worden om de gegevens die verwerkt worden passend te beschermen.

4.5 Logging van gegevensgebruik

Elk geautomatiseerde systeem dat persoonsgegevens verwerkt, moet logging bijhouden van de verwerkingen. In deze logging staat minimaal vermeld welke gebruiker, op welke moment, welke gegevens heeft verwerkt. Logging:

- van chronologische registratie van gegevens over van belang zijnde gebeurtenissen, die zich gedurende een periode in een verwerking voordoen,
- houdt in het vastleggen in een log, bijvoorbeeld een systeem log of een security log, van feitelijk uitgevoerde bewerkingen en/of pogingen daartoe.

4.6 Verwerkersovereenkomst

In specifieke situaties schakelt VGGM derden in om gegevens te verwerken. Het uitbesteden van werkzaamheden aan derden brengt risico's met zich mee op het gebied van gegevensverwerking en informatiebeveiliging. Het hoger management blijft verantwoordelijk voor de verwerking van de gegevens. Zij moeten er daarom op toezien dat gegevens juist verwerkt en beveiligd worden. Met het oog op de omgang met privacy door alle partijen waar VGGM mee samenwerkt en waarbij persoonsgegevens worden verwerkt, worden verwerkersovereenkomsten afgesloten.

4.7 Bewust omgaan met persoonsgegevens

VGGM streeft naar een cultuur waarbij iedereen elkaar in alle openheid aanspreekt op het eigen gedrag rondom privacy en daarmee van elkaar leert. Communicatie, openheid en toetsing zijn belangrijke randvoorwaarden om een optimaal gegevensbeschermingsbeleid te realiseren.
Het management en alle binnen VGGM werkzame personen behandelen alle informatie over individuele personen die hij/zij ten behoeve van de uitvoering van met opdrachtgevers gesloten overeenkomsten verkrijgt, vertrouwelijk en draagt er zorg voor dat deze informatie niet aan derden bekend wordt.

Een medewerker van VGGM moet zich bij de uitoefening van zijn/haar taken voortdurend bewust zijn van het belang van het waarborgen van de rechten van betrokkenen. Hij/Zij moet persoonsgegevens op een zorgvuldige manier verwerken, zoals omschreven in dit beleid.

Om bewustwording te realiseren is kennisdeling over het onderwerp noodzakelijk. De AIG zorgt er samen met de verschillende aandachtsfunctionarissen voor dat de informatie over informatiebeveiliging en gegevensbescherming herhaaldelijk onder de aandacht wordt gebracht bij medewerkers van VGGM.

Opgemerkt wordt dat een groot deel van de gegevens vallen onder het medisch beroepsgeheim. Deze gegevens dienen met uiterste zorg behandeld te worden. Dit betekent dat gegevens niet zomaar gebruikt mogen worden voor andere doeleinden. Het verwerken van de gegevens is voorbehouden aan de arts en de ondersteuning van de arts, die een directe behandelrelatie heeft met betrokkene. Inzage voor anderen dient afgeschermd te worden en daar waar dit (technisch of organisatorisch) dit niet mogelijk is, maakt het management helder afspraken over het verwerken. In alle gevallen is inzage in het dossier pas mogelijk na toestemming van de behandelend arts.

4.8 Meldplicht voor inbreuken in verband met persoonsgegevens (datalekken)

Indien zich een informatiebeveiligingsincident voordoet, waarbij bijvoorbeeld gegevens van personen in verkeerde handen kunnen komen of zijn gekomen, handelt VGGM in overeenstemming met de vastgestelde werkwijze in het Protocol Meldplicht en Afhandeling van (vermoedelijke) datalekken. Dit protocol bevat een vastgesteld proces van te doorlopen stappen om de eventuele schade of de kans hierop, bij een 'datalek' te beperken en de getroffen perso(o)n(en) te beschermen.

Het gaat bij een 'datalek' om situaties waarbij een onrechtmatige verwerking van persoonsgegevens heeft plaatsgevonden of kan plaatsvinden, waarbij beveiligingsmaatregelen (on)bewust zijn omzeild of doorbroken of dat geen of onvoldoende beveiligingsmaatregelen zijn genomen. Het gaat ook om situaties waarbij persoonsgegevens verloren zijn gegaan, waardoor ze niet meer beschikbaar zijn, en om situaties waarin gegevens in handen kunnen komen of zijn gekomen van derden die geen toegang tot die gegevens mogen hebben.

De plicht tot het melden van een (vermoeden van een) 'datalek' geldt als er sprake is van een aanzienlijke

kans op ernstige nadelige gevolgen voor betrokkene, dan wel ernstige nadelige gevolgen voor de bescherming van persoonsgegevens. Het betreft situaties van het (mogelijk) lekken van persoonsgegevens uit bestanden en/of gegevens waarvoor VGGM verantwoordelijkheid draagt.

Wanneer er een dergelijk 'datalek' heeft plaatsgevonden, wordt dit zonder onredelijke vertraging, uiterlijk 72 uur nadat er kennis van de inbreuk is vernomen, gemeld aan de AP. Als dit later dan 72 uur is wordt er een motivering voor de vertraging bij de melding gevoegd. Indien de inbreuk een hoog risico voor de rechten en vrijheden van de betrokkenen met zich meebrengt, word de inbreuk ook in eenvoudige en duidelijke taal aan de betrokkenen gemeld.

VGGM maakt de afweging of het informeren van de betrokkene in diens belang is of dat dit beter achterwege kan blijven om de betrokkene zelf of anderen te beschermen. Indien van informeren wordt afgezien zal VGGM dit besluit registreren en duidelijk motiveren. De FG houdt namens VGGM een overzicht bij waarin alle datalekken zijn opgenomen. VGGM maakt haar register van informatiebeveiligingsincidenten niet openbaar.

Jaarlijks legt het MT in haar bestuursrapportage verantwoording af over naleving van de AVG.
In betreffende verantwoording zijn ten minste de volgende onderdelen opgenomen:

- Het aantal geregistreerde datalekken en de opvolging hiervan, incl. resultaat;
- Het aantal medewerkers dat heeft deelgenomen aan het bewustwordingstraject;
- Status certificering(en) op het gebied van informatiebeveiliging (bijv. NEN 7510);
- Gesignaleerde knelpunten en geplande/voorgestelde aanpak incl. tijdspad van implementatie.

5 Rechten van betrokkenen

5.1 Rechten en plichten aangaande het medisch dossier

De Wet op de geneeskundige behandelingsovereenkomst (“WGBO”) verplicht de hulpverlener binnen de GGD om een medisch dossier in te richten. In het medisch dossier neemt de hulpverlener alle gegevens op over de gezondheid van de betrokkene en over de uitgevoerde verrichtingen, voor zover dit voor een goede hulpverlening noodzakelijk is.
De betrokkene kan de hulpverlener niet van deze verplichting ontheffen. De gegevens vallen onder het medisch beroepsgeheim: de hulpverlener heeft een geheimhoudingsplicht.
Een hulpverlener van de GGD mag uitsluitend een (medisch) dossier aanleggen in de hiervoor bestemde en door de GGD aangewezen (zorg)informatiesystemen.

Een hulpverlener kan alleen gegevens aan een derde verstrekken als dat mag op basis van de AVG én als er een grond is om het medisch beroepsgeheim te doorbreken. Doorbreking van deze zwijgplicht is toegestaan op grond van:

(1) expliciete toestemming van de betrokkene;
(2) een wettelijke bepaling;
(3) (noodtoestand in de zin van) conflict van plichten;
(4) zwaarwegend belang;
(5) zeer uitzonderlijke omstandigheden.

Ieder heeft het recht om zijn (medisch)dossier in te zien, gegevens te laten corrigeren c.q. te verwijderen. In de WGBO is bepaald dat wanneer een kind jonger dan 12 jaar is de ouder(s)/wettelijk vertegenwoordiger(s) bevoegd zijn en het dossier van het kind mogen inzien.

Jeugdigen van 12,13,14 of 15 jaar kunnen zelfstandig deze rechten uitoefenen en moeten toestemming verlenen aan de ouder(s). Jeugdigen van 16 of 17 jaar oefenen de rechten zelfstandig uit, ouders hebben geen recht op informatie zonder toestemming van de jeugdige.

5.2 Rechten van betrokkenen

De AVG brengt betrokkenen sterkere privacyrechten; organisaties die persoonsgegevens verwerken krijgen juist meer verplichtingen. De nadruk ligt op de verantwoordelijkheid van VGGM om te kunnen aantonen dat de organisatie zich aan de wet houdt. De rechten van de betrokkene zijn binnen VGGM op transparante wijze ingericht. Betrokkenen hebben recht op:

- informatie en toegang tot gegevens (artikel 13 AVG en 14 AVG);
- inzage van gegevens (artikel 15 AVG);
- rectificatie van gegevens (artikel 16 AVG);
- gegevenswissing, oftewel op "vergetelheid" (artikel 17 AVG);
- beperking van de verwerking (artikel 18 AVG);
- kennisgevingplicht inzake rectificatie, wissing of beperking (artikel 19 AVG);
- overdraagbaarheid van gegevens, dataportabiliteit (artikel 20 AVG);
- het niet onderworpen worden aan geautomatiseerde besluitvorming (artikel 22 AVG).

VGGM geeft hieraan onder andere uitvoering door betrokkenen op haar diverse websites helder te informeren over hoe van deze rechten gebruik gemaakt kan worden.
Om gebruik te maken van hun rechten kunnen de betrokkenen een verzoek indienen. Alvorens het verzoek te kunnen behandelen moet de identiteit van de verzoeker op deugdelijke wijze worden vastgesteld.

5.3 Recht op informatie en toegang tot gegevens

Tijdens het eerste contact met een cliënt informeert de hulpverlener betrokkenen over de wijze waarop zijn persoonsgegevens worden verwerkt. Als het niet mogelijk is om de betrokkene tijdens het eerste contact te informeren, dan zorgt de hulpverlener dat de betrokkene zo spoedig als de situatie toe laat, alsnog over de gegevensverwerking wordt geïnformeerd. Van het (uitstellen of niet) informeren van de betrokkene kan een aantekening worden gemaakt in het dossier.

VGGM verzamelt gegevens om haar taken te kunnen uitvoeren. Indien het persoonsgegevens betreft en betrokkenen is hiervan niet op de hoogte, dan informeert VGGM de betrokkene actief over de verwerking van hun persoonsgegevens. Hierbij dient in ieder geval gecommuniceerd te worden wat het doel is, welke persoonsgegevens worden verwerkt, wie daarvoor verantwoordelijk is en of de gegevens aan derden worden verstrekt. VGGM informeert betrokkene, uiterlijk binnen vier weken na de verzameling van persoonsgegevens, indien de persoonsgegevens van derden afkomstig zijn.

5.4 Recht op inzage en afschrift van gegevens

Patiënten, medewerkers en andere betrokkenen kunnen altijd hun persoonsgegevens inzien wanneer zij hier om vragen en kunnen er op vertrouwen dat deze gegevens correct zijn dan wel worden aangepast wanneer noodzakelijk of door de betrokkene is aangegeven dat deze aangepast dienen te worden, voor zover een (wettelijke) verplichting dit niet onmogelijk maakt.
Betrokkene heeft de mogelijkheid om te controleren of en op welke manier zijn/haar gegevens worden verzameld en verwerkt. Ook heeft betrokkene het recht op inzage en een afschrift van zijn/haar dossier. Uitzondering op deze regel is als de persoonlijke levenssfeer van een ander daardoor wordt geschaad. Bijvoorbeeld informatie die een partner aan een hulpverlener heeft verstrekt in het vertrouwen dat betrokkene deze informatie niet te zien krijgt.

VGGM verstrekt de betrokkene, binnen vier weken na ontvangst van het verzoek, kosteloos een kopie van de persoonsgegevens die worden verwerkt. Indien de termijn van vier weken onhaalbaar blijkt, verlengt VGGM de termijn met twee maanden en brengt de betrokkene hier schriftelijk van op de hoogte.
Indien de betrokkene om bijkomende kopieën vraagt, kan de VGGM een vergoeding rekenen niet hoger dan de kostprijs.

5.5 Recht op rectificatie (correctie, aanvulling) van gegevens

Als VGGM persoonsgegevens van betrokkenen verwerkt die naar hun oordeel onjuist zijn, kunnen zij een verzoek indienen bij VGGM om feitelijke onjuistheden in het dossier te corrigeren. Het gaat dan bijvoorbeeld om onjuiste adresgegevens. Niet wordt bedoeld dat de bijvoorbeeld de diagnose mag worden gewijzigd.
Er kan ook een verklaring aan het medisch dossier worden toegevoegd, bijvoorbeeld wanneer het gaat om de eigen visie van de betrokkene. Ook als de hulpverlener het niet eens is met de verklaring moet deze worden opgenomen.

5.6 Recht op gegevenswissing

Betrokkenen hebben het recht persoonsgegevens te laten verwijderen indien VGGM niet langer een goede grond heeft voor het gebruik hiervan, bijvoorbeeld indien betrokkene een eerder gegeven toestemming intrekt, indien de gegevens onjuist zijn of de gegevens niet langer nodig zijn.

Het recht op gegevenswissing geldt in principe niet voor het medisch dossier. De betrokkene heeft het recht om op hem betrekking hebbende gegevens te laten verwijderen en op grond van de WGBO heeft hij bovendien het recht dossiergegevens te laten vernietigen ongeacht of dit relevante gegevens zijn.

Het recht op vernietiging geldt alleen voor gegevens die de hulpverlener in het kader van zijn dossierplicht heeft opgeslagen. Het geldt niet voor andere gegevens, zoals financiële gegevens die de hulpverlener op andere gronden moet bewaren.

VGGM hanteert drie uitzonderingen op het recht op vernietiging:

(1) Een andere wet schrijft een afwijkende bewaartermijn voor waarbinnen de gegevens niet vernietigd mogen worden;
(2) Een ander dan de betrokkene heeft een aanmerkelijk belang bij het bewaren van de gegevens;
(3) 'Goed hulpverlenerschap' staat vernietiging in de weg.

5.7 Recht op beperking van de verwerking

Het recht op beperking van de verwerking van persoonsgegevens houdt in dat de gegevens wel beschikbaar blijven in het medisch dossier, maar dat ze tijdelijk niet gebruikt mogen worden. De persoonsgegevens mogen dan alleen nog worden gebruikt met toestemming van de betrokkene, of als dat nodig is voor het instellen, uitoefenen of onderbouwen van een rechtsvordering of ter bescherming van de rechten van andere natuurlijke personen of rechtspersonen. Voorbeeld: als de juistheid van de persoonsgegevens worden betwist en voor een periode die de verwerkingsverantwoordelijke in staat stelt om de juistheid van die persoonsgegevens te controleren.

5.8 Recht op overdraagbaarheid van gegevens (dataportabiliteit)

VGGM is vanuit de AVG niet verplicht invulling te geven aan overdraagbaarheid van gegevens voor zover het werkzaamheden betreft in het kader van algemeen belang, op basis van een wettelijke verplichting of het verstrekken van gezondheidszorg.

Het recht om gegevens te mogen meenemen geldt voor een deel van de gegevens van medische dossiers. Persoonsgegevens die de cliënt zelf actief en bewust heeft verstrekt (eigen data) vallen onder het recht op dataportabiliteit. Dit geldt ook voor de gegevens die de betrokkene indirect heeft verstrekt door het gebruik van een dienst of een apparaat. Gegevens die niet (in)direct door het gebruik van een dienst of een apparaat door de betrokkene zijn verstrekt vallen hier niet onder. Bijvoorbeeld conclusies, diagnoses, vermoedens of behandelplannen die de hulpverlener op basis van de door de betrokkene verstrekte gegevens vaststelt.

5.9 Recht van bezwaar tegen verwerking

Betrokkenen hebben het recht aan VGGM te vragen hun persoonsgegevens niet meer te gebruiken en bezwaar te maken tegen de verwerking van hun persoonsgegevens. VGGM moet hieraan voldoen, tenzij er gerechtvaardigde gronden zijn voor de verwerking.

5.10 Recht niet te worden onderworpen aan geautomatiseerde individuele besluitvorming waaronder profilering

Bij geautomatiseerde individuele besluitvorming is geen sprake van (noemenswaardige) menselijke tussenkomst zodat eventuele uitkomst kunnen worden gecorrigeerd. Het is uitsluitend gebaseerd op geautomatiseerde verwerking van persoonsgegevens.

VGGM past geen geautomatiseerde individuele besluitvorming, waaronder profilering, toe als daaraan rechtsgevolgen voor de betrokkene (degene wiens persoonsgegevens het betreft) aan zijn verbonden of het besluit hem/haar in aanmerkelijke mate treft. Daarbij kan gedacht worden aan een indicatie van een medisch oordeel op basis van karakteristieken uit het digitaal dossier of het verwerken van sollicitaties via internet zonder menselijke tussenkomst.

5.11 Klachten en vragen

Onverminderd de rechten die de betrokkenen worden toegekend in de WGBO en de AVG, kan iedere betrokkene schriftelijk een klacht indienen bij VGGM indien hij meent dat door (een hulpverlener van) VGGM persoonsgegevens worden verwerkt op een wijze die in strijd is met de wet of met dit beleid.

Binnen vier weken beoordeelt VGGM of het verzoek ontvankelijk is. VGGM laat binnen die termijn weten wat er met het verzoek gaat gebeuren, waaronder of VGGM de behandeling van het verzoek met twee maanden verlengt. VGGM behandelt het verzoek volgens de daarvoor door haar vastgestelde en bekendgemaakte klachtenregeling .

Als het verzoek niet tijdig kan worden opgevolgd, deelt VGGM uiterlijk binnen vier weken mee waarom het verzoek zonder gevolg is gebleven. De betrokkene heeft dan de mogelijkheid om bezwaar te maken bij VGGM of een klacht in te dienen bij de Autoriteit Persoonsgegevens.

5.12 Informeren van (keten)partners

VGGM informeert relevante ketenpartners indien het verzoek wordt ingewilligd. Dit betreft o.a. organisaties met wie een verwerkersovereenkomst dan wel een gebruiksovereenkomst of een overeenkomst tot derdenverstrekking is afgesloten. Indien relevant vraagt VGGM actief om bevestiging van de betreffende ketenpartner(s) dat aan het betreffende verzoek is voldaan.

6 Functies en verantwoordelijkheden

VGGM heeft gegevensbescherming ingebed in de organisatie. Voor alle medewerkers, op ieder niveau, is duidelijk welke rollen er zijn op het gebied van gegevensbescherming. Medewerkers kennen hun rol en verantwoordelijkheid op het gebied van gegevensbescherming zoals hierna uiteengezet.

Dagelijks- en Algemeen bestuur
- verantwoordelijke in de zin van AVG (Kaders stellen tav privacy beleid)
- eindverantwoordelijk voor uitvoering en controle op naleving van het beleid

De directie
- gemandateerd door het DB;
- vaststellen van gewenste niveau van informatiebeveiliging en privacy, implementatie, en aanwijzing van procesverantwoordelijke/systeemeigenaar per informatiesysteem;
- bevordert de beschikbaarheid van voldoende middelen om gegevensbescherming passend te waarborgen.

Afdelingshoofden
- Verantwoordelijk voor de borging van de beschikbaarheid, integriteit en vertrouwelijkheid van de door het team verwerkte persoonsgegevens;
- In voorkomend geval verantwoordelijk voor de uitvoering van een (door de FG getriggerde) DPIA en borging van de hieruit voortvloeiende (verbeter)maatregelen;
- Verantwoordelijk voor aanmelden van nieuwe (of veranderde) verwerkingen van persoonsgegevens;
- Het behandelen van verzoeken in het kader van de rechten van betrokkenen;
- Het afsluiten van verwerkersovereenkomsten en andere regelingen.

Aandachtsfunctionaris gegevensbescherming (per team of afdeling)
- Onderhouden van het register van de verwerkingsactiviteiten;
- Bevorderen van privacy- en informatiebeveiligingsbewustzijn;
- Aanspreekpunt per team of afdeling voor vragen op het gebied van gegevensbescherming.

Functionaris voor de gegevensbescherming (FG)
- Actueel houden- en coördineren van de uitvoering van dit gegevensbeschermingsbeleid;
- Toezichthouder op de verwerking van persoonsgegevens (naleving van privacywetgeving);
- Informeren, adviseren, bewustmaking over AVG verplichtingen, verwerking, incidenten, klachten, DPIA, opstellen van beleid;
- Beheert het register van verwerkingsactiviteiten;
- Ziet toe op de uitvoering van de maatregelen voor gegevensbescherming;
- Rapporteert tenminste jaarlijks aan het MT over de manier waarop VGGM de afgelopen periode met gegevensbescherming is omgegaan;
- Onderhoudt het contact met de Autoriteit Persoonsgegevens;
- Beheert het overzicht van datalekken.

Privacy officer (Team Juridische Zaken)
- Advisering, uitvoering en naleving van privacy wetgeving;
- Beoordelen van- en adviseren over de verwerking van persoonsgegevens;
- Aanspreekpunt voor privacyvragen;
- Coördineren van privacy werkzaamheden, inzage- en correctie verzoeken;
- Advisering en ondersteuning bij het afsluiten van verwerkersovereenkomsten.

Aandachtsfunctionaris infromatiebeveiliging (per team of afdeling)

- Adviezen uit veiligheidsincidenten implementeren, onder supervisie van de CISO;
- Verbeteren van de informatiebeveiliging binnen team, afdeling en organisatie conform normenkaders;
- Bevorderen van informatiebeveiligingsbewustzijn;
- Aanspreekpunt per team of afdeling voor vragen op het gebied van informatiebeveiliging.

CISO (Chief Information Security Officer) of Adviseur Informatiebeveiliging en Gegevensbescherming

- Actueel houden- en coördineren van de uitvoering van het informatiebeveiligingsbeleid;
- Aanspreekpunt voor informatiebeveiliging;
- Bevorderen van informatiebeveiligingsbewustzijn;
- Verantwoordelijk voor de afhandelen van informatiebeveiligingsincidenten;
- (Pro) actief adviseren over informatiebeveiliging en het informatiebeveiligingsbeleid;
- Uitvoeren van gapanalyse (nulmeting) en advies over NEN7510/BIO (minimaal benodigde aanpassingen);
- Ondersteunen bij het uitvoeren van risicoanalyses;
- Adviseren en ondersteunen van VGGM om het benodigde niveau van informatiebeveiliging te bereiken dat minimaal voldoet aan de wet- en regelgeving;
- Ervoor zorgdragen dat ondersteunende systemen en processen voldoen aan wet- en regelgeving (en de behaalde NEN7510 certificering behouden).

Functioneel beheerders informatiesystemen

- Verantwoordelijk voor de uitvoering van het gegevensbeschermings- en informatiebeveiligingsbeleid voor de betreffende applicaties.

7 Toezicht op de gegevensvewerking

VGGM heeft een Functionaris voor de Gegevensverwerking aangesteld. Deze functionaris fungeert als vraagbaak en heeft als taak binnen de organisatie toezicht te houden op de verwerking van persoonsgegevens en daarmee op de toepassing en naleving van de AVG. De Functionaris voor de Gegevensbescherming (FG) die binnen VGGM toezicht houdt op de toepassing en naleving van de AVG is: [redacted]

Hij is geregistreerd bij de Autoriteit Persoonsgegevens onder nummer [redacted], waarbij aangetekend is dat hij tevens als Functionaris voor de Gegevensbescherming optreedt voor de Stichting Publieke Gezondheid Gelderland-Midden en de Stichting Veilig Thuis Gelderland-Midden.

Datum:

De verantwoordelijke,

Het Dagelijks Bestuur van Veiligheids- en Gezondheidsregio Gelderland-Midden,
namens deze,

A. Slofstra
H. Bril
directie