9.7

Privacybeleid GGD GHOR Nederland

Versiebeheer

Versie	Datum	Auteurs	Opmerkingen
0.1	02-06-2021	[redacted]	Eerste opzet
0.2	11-06-2021	[redacted]	Tweede concept + kwaliteitscheck [redacted]
0.3	18-06-2021	[redacted]	Opmerkingen [redacted] en klankbordgroep waar mogelijk verwerkt
0.4	21-06-2021	[redacted]	Diverse (kleine) tekstuele aanpassingen
0.5	07-07-2021	[redacted]	Verwerken feedback Stuurgroep
0.6	07-07-2021	[redacted]	Verwerken feedback [redacted]
0.7	28-07-2021	[redacted]	Verwerken feedback [redacted] en [redacted]
0.8	03-08-2021	[redacted]	Finaliseren privacybeleid
0.9	17-09-2021	[redacted]	Finale versie na stuurgroepoverleg van 15-09-2021.
1.0	19-12-2021	[redacted]	Verwerken feedback [redacted].

Inhoudsopgave

1 Inleiding

In een gedigitaliseerde maatschappij waar snelle technologische ontwikkelingen en globalisering nieuwe uitdagingen voor de bescherming van persoonsgegevens met zich meebrengen, krijgen privacy en gegevensbescherming meer aandacht. De verwerking van persoonsgegevens dient met de grootste zorgvuldigheid te gebeuren, omdat misbruik grote schade kan toebrengen aan de betrokkenen. GGD GHOR Nederland hecht dan ook veel waarde aan het beschermen van de persoonsgegevens die aan haar worden verstrekt en aan de wijze waarop deze persoonsgegevens worden verwerkt.

Met dit privacybeleid wil GGD GHOR Nederland de kwaliteit van de verwerking en de beveiliging van persoonsgegevens vastleggen en optimaliseren en daarmee voldoen aan de relevante privacywet- en regelgeving. Hetgeen is gesteld in dit privacybeleid, dient als uitgangspunt te worden gebruikt in processen, werkinstructies en richtlijnen binnen GGD GHOR Nederland.

Bij de verwerking van persoonsgegevens, dient aandacht te worden besteed aan de bijzondere rol van GGD GHOR Nederland. GGD GHOR Nederland is een belangenorganisatie voor de GGD'en en GHOR-bureaus, die GGD'en en GHOR-bureaus ondersteunt in onder meer technische oplossingen, waardoor persoonsgegevens worden verwerkt. Bovendien is GGD GHOR Nederland een centrale landingsplaats voor landelijke projecten en programma's waarvoor GGD GHOR Nederland de coördinatie verzorgt. GGD GHOR Nederland kan dit vanuit diverse hoedanigheden doen, namelijk als (gezamenlijk) verwerkingsverantwoordelijke of als verwerker. Bij iedere verwerking wordt beoordeeld wat de rol van GGD GHOR Nederland is en worden de juiste maatregelen getroffen met betrekking tot de vastgestelde rol en de verwerking.

1.1 Reikwijdte en doelstellingen privacybeleid

GGD GHOR Nederland acht privacy en gegevensbescherming en daarmee het privacybeleid van zeer groot belang. Het privacybeleid heeft betrekking op het verwerken van persoonsgegevens van betrokkenen binnen (de systemen van) GGD GHOR Nederland, waaronder in ieder geval medewerkers, externe relaties en derden. GGD GHOR Nederland beoogt om de rechten en vrijheden van deze betrokkenen adequaat te waarborgen.

Bij GGD GHOR Nederland wordt het beschermen van persoonsgegevens breed geïnterpreteerd. Er is een belangrijke relatie en gedeeltelijke overlap met informatiebeveiliging, waarbij het gaat om de beschikbaarheid, integriteit en de vertrouwelijkheid van data, waaronder persoonsgegevens. Op strategisch niveau wordt aandacht geschonken aan deze en andere raakvlakken en wordt zowel planmatig als inhoudelijk afstemming gezocht met de juiste afdelingen/lijnverantwoordelijke, zoals het CISO office.

Dit privacybeleid heeft als doel om de kwaliteit van de verwerking en de beveiliging van persoonsgegevens te optimaliseren, waarbij een goede balans moet worden gevonden tussen gegevensbescherming, functionaliteit en veiligheid.

GGD GHOR Nederland beoogt de persoonlijke levenssfeer en het recht op privacy van de betrokkenen zoveel mogelijk te respecteren. Persoonsgegevens dienen beschermd te worden tegen misbruik, onwettelijk en onrechtmatig gebruik. Dit brengt met zich mee dat het verwerken van persoonsgegevens dient te voldoen aan relevante wet- en regelgeving en dat persoonsgegevens adequaat zijn beveiligd bij GGD GHOR Nederland.

Het privacybeleid geeft medewerkers en ingehuurde externen van GGD GHOR Nederland inzicht in hoe privacy en gegevensbescherming zijn geregeld binnen GGD GHOR Nederland. Daarnaast draagt het bij aan bewustwording (awareness) over het belang en de noodzaak van het beschermen van persoonsgegevens. Medewerkers worden geacht het privacybeleid te kennen, zodat zij de standpunten van GGD GHOR Nederland met betrekking tot het verwerken van persoonsgegevens kennen en weten wat van hen wordt verwacht bij de verwerking van persoonsgegevens. Het privacybeleid is een intern stuk, dat wordt uitgewerkt in overeenkomsten, privacyverklaringen en, indien nodig, andere stukken die informatie bieden over de verwerking van persoonsgegevens binnen GGD GHOR Nederland.

De doelstelling van het privacybeleid voor GGD GHOR Nederland is concreet het volgende:

- **Het bieden van een kader om tot verbeterde compliance te komen**: het privacybeleid biedt een kader om (toekomstige) verwerkingen van persoonsgegevens te toetsen aan relevante wet- en regelgeving, een vastgestelde 'best practice' of norm en om de taken, bevoegdheden en verantwoordelijkheden in de organisatie te beleggen.

Het bovenstaande wordt door GGD GHOR Nederland gerealiseerd door onder meer:

- **Het stellen van normen en het nemen van maatregelen:** de basis voor de bescherming en beveiliging van persoonsgegevens is het privacy- en informatiebeveiligingsbeleid van GGD GHOR Nederland.
- **Het nemen van verantwoordelijkheid:** het nemen van verantwoordelijkheid door zowel de directie als iedere medewerker, zowel intern als extern, in de verwerking van persoonsgegevens.
- **Daadkrachtige communicatie van het privacybeleid in GGD GHOR Nederland:** iedere medewerker, zowel intern als extern, is op de hoogte van het privacybeleid.

Naast voormelde concrete doelstellingen, is een algemeen doel het creëren van bewustwording van het belang en de noodzaak van de bescherming van persoonsgegevens bij de medewerkers en externen van GGD GHOR Nederland. Daarnaast wordt met dit privacybeleid de lijn gezet voor het voldoen aan relevante wet- en regelgeving, waardoor het risico van het niet volgen van deze wet- en regelgeving vermindert.

1.2 Indeling GGD GHOR Nederland

Het privacybeleid geldt voor alle entiteiten binnen GGD GHOR Nederland, namelijk de vereniging, de stichting projectenbureau, de stichting verenigingsbureau en de stichting Landelijke Coördinatie Covid-19 Bestrijding (hierna: "LCCB"). De stichting projectenbureau, de stichting verenigingsbureau en de stichting LCCB voeren elk andere taken uit. Het grootste verschil tussen beide entiteiten is de kwalificatie in het kader van de AVG.

De vereniging is in (bijna) alle gevallen verwerkingsverantwoordelijke. De stichting projectenbureau vervult echter taken waarbij de kwalificatie, afhankelijk van de taak en opdracht, anders kan zijn naar gelang de situatie in de praktijk, namelijk verwerker, gezamenlijk verwerkingsverantwoordelijk en verwerkingsverantwoordelijke. Bij iedere project en iedere verwerking die wordt gestart, wordt bepaald wat de kwalificatie van GGD GHOR Nederland voor die verwerking is, en welke maatregelen daarbij moeten worden genomen. In dit beleid worden de standpunten van GGD GHOR Nederland uitgewerkt. In dat kader treft GGD GHOR Nederland de maatregelen die van een (gezamenlijk) verwerkingsverantwoordelijke die (bijzondere) persoonsgegevens verwerkt mag worden verwacht. Hetzelfde geldt indien GGD GHOR Nederland verwerker is. Contractueel zal daarnaast altijd worden vastgelegd wat de eisen met betrekking tot de verwerking van persoonsgegevens inhouden, onfhankelijk van de kwalificatie van GGD GHOR Nederland.

1.3 Stichting Landelijke Coördinatie Covid-19 Bestrijding

De stichting LCCB zal per 1 januari 2022 voor de activiteiten op het gebied van de coronabestrijding de status van Rechtspersoon met een Wettelijke Taak (RWT) krijgen: een zelfstandige organisatie op afstand van de Rijksoverheid, die een taak uitvoert die in de wet geregeld is en wordt gefinancierd met publiek geld.

Voor het onderbrengen van deze wettelijke taak gaan de stichting LCCB in het leven roepen. Allereerst om ervoor te zorgen dat de leden niet het (financiële) risico dragen, dat samenhangt met de werkzaamheden in de Corona Programma Organisatie. En ten tweede omdat een dergelijke wettelijke taak om een nieuwe manier van besturen vraagt. De minister van Volksgezondheid, Welzijn en Sport (hierna: "VWS") is immers opdrachtgever en verantwoordelijk voor deze wettelijke taak en dus kan er maar één verantwoordingslijn bestaan en die is richting VWS. De Stichting Projectenbureau, waaruit de CPO-activiteiten worden afgesplitst,

legt verantwoording af aan het bestuur (Presidium) van GGD GHOR Nederland. De nieuwe stichting krijgt een Raad van Toezicht en een deelnemersraad, waarin de DPG'en zitten hebben.

2 Juridisch kader

2.1 Wet- en regelgeving

Dit privacybeleid is opgesteld overeenkomstig met de daarvoor geldende wet- en regelgeving. Voor GGD GHOR Nederland zijn, ongeacht de rol van GGD GHOR Nederland, een aantal wetten van toepassing. Dit is afhankelijk van de werkzaamheden die GGD GHOR Nederland uitvoert of waarbij zij ondersteunt. Wetgeving die altijd relevant is, is:

- Algemene verordening gegevensbescherming;
- Uitvoeringswet AVG:
- Telecommunicatiewet (TW).

Afhankelijk van de ondersteunende werkzaamheden van GGD GHOR Nederland, zijn daarbij nog sectorspecifieke wetgeving en richtlijnen van toepassing. Deze zal altijd worden vastgesteld bij de werkzaamheden die worden uitgevoerd door GGD GHOR Nederland. Het betreft onder andere:

- Wet op de geneeskundige behandelovereenkomst (WGBO);
- Wet publieke gezondheid (Wpg) en daarbij behorende gedelegeerde regelgeving;
- Wet veiligheidsregio's.

2.2 Gehanteerde begrippen

In dit privacybeleid worden een aantal begrippen regelmatig gebruikt. Hieronder worden deze begrippen uitgelegd, zodat duidelijk is wat met deze begrippen wordt bedoeld.

Persoonsgegevens
Alle informatie over een geïdentificeerde of identificeerbare natuurlijke persoon ("de betrokkene"); als identificeerbaar wordt beschouwd een natuurlijke persoon die direct of indirect kan worden geïdentificeerd. Een natuurlijke persoon kan onder andere worden geïdentificeerd door middel van een naam, een identificatienummer, locatiegegevens, een online identificator of van een of meer elementen die kenmerkend zijn voor de fysieke, fysiologische, genetische, psychische, economische, culturele of sociale identiteit van die natuurlijke persoon, zoals lengte, haarkleur, afkomst en politieke voorkeuren of een combinatie van persoonsgegevens. Dit betekent dat als met gegevens iemand direct kan worden herkend, zoals met een naam, of niet direct, maar wel kan worden achterhaald om wie het gaat met een gegeven of een combinatie van gegevens, zoals een cliëntnummer, maar ook een combinatie van bijvoorbeeld een functie binnen een organisatie, er wordt gesproken van een persoonsgegeven/persoonsgegevens.

Betrokkene(n)
De betrokkene is de geïdentificeerde of identificeerbare natuurlijk persoon op wie de verwerkte en/of de te verwerken persoonsgegevens betrekking hebben. Dit betekent dat de betrokkene de persoon is van wie de persoonsgegevens worden verwerkt.

Verwerking
Onder een verwerking of een geheel van verwerkingen valt elke activiteit met betrekking tot het vastleggen, ordenen, structureren, opslaan, bijwerken of wijzigen, opvragen, raadplegen, gebruiken, verstrekken door middel van doorzending, verspreiden of op andere wijze ter beschikking stellen, aligneren of combineren, afschermen, wissen of vernietigen van persoonsgegevens. Dit betekent dat (bijna) alles wat met persoonsgegevens wordt gedaan, een verwerking is.

Verwerkingsverantwoordelijke
De partij die (zelf of samen met anderen) de doeleinden en middelen voor de verwerking van persoonsgegevens bepaalt. In sommige gevallen bepaalt de wet wie een verwerkinsverantwoordelijke is.

Gezamenlijke verwerkingsverantwoordelijke
De partijen die samen de doeleinden en middelen voor de verwerking van persoonsgegevens bepalen. Het bestaan van een gezamenlijke verantwoordelijkheid betekent niet een verantwoordelijkheid op gelijke voet. Deze verantwoordelijken kunnen in diverse fasen en in verschillende mate betrokken zijn bij een verwerking van persoonsgegevens. Dit geldt ook voor de mate waarin doel en middelen worden vastgesteld.

Verwerker
De partij die persoonsgegevens alleen verwerkt op uitdrukkelijke instructie van een verwerkingsverantwoordelijke.

Derde
Een natuurlijke persoon of rechtspersoon, een overheidsinstantie, een dienst of een ander orgaan, die niet tot een van de volgende groepen behoort:

- Betrokkene;
- Verwerkingsverantwoordelijke;
- Verwerker;
- Personen die onder rechtstreeks gezag van de verwerkingsverantwoordelijke of de verwerker gemachtigd zijn om de persoonsgegevens te verwerken.

Dit betekent dat een derde niet rechtstreeks betrokken is bij de verwerking van persoonsgegevens, maar wel op een bepaalde manier kennis zou kunnen nemen van die persoonsgegevens. Hier kan onder andere gedacht worden aan:

- Politie;
- Samenwerkingspartners;
- Belastingdienst;
- Burgemeester.

Datalek
Bij een datalek gaat het om toegang tot of vernietiging, verlies, wijziging of vrijkomen van persoonsgegevens bij een organisatie, zonder dat dit de bedoeling is van de organisatie. Voorbeelden zijn:

- Gestolen laptop;
- Onrechtmatige inzage door een medewerker;
- Verlies van een USB-stick of notitieboekje;
- Onnodig uitprinten/exporten van (complete) bestanden;
- Maken van foto's/screenshots van persoonsgegevens;
- Het (on)bedoeld wissen/ vernietigen van bestanden.

Privacy by Default (gegevensbescherming door standaardinstellingen)
Een gegevensverwerking waarbij de standaardinstellingen van producten en diensten zo zijn ingesteld dat de privacy van betrokkenen maximaal wordt gewaarborgd. Dit betekent onder meer dat er zo min mogelijk persoonsgegevens worden gevraagd en verwerkt.

Privacy by Design (gegevensbescherming door ontwerp)
Voorafgaand aan de gegevensverzameling wordt het beheer van de gehele levenscyclus van persoonsgegevens, vanaf het verzamelen tot het verwerken en verwijderen, zo ontworpen dat zij zo veel mogelijk rekening houden met de privacy van betrokkenen. Hierbij wordt stelselmatig aandacht besteed aan allesomvattende waarborgen met betrekking tot nauwkeurigheid, vertrouwelijkheid, integriteit, fysieke veiligheid en verwijdering van de persoonsgegevens.

Data Protection Impact Assessment (DPIA)
Een beoordeling die helpt bij het identificeren van risico's in de verwerking van persoonsgegevens. De DPIA levert daarnaast handvatten om de geïdentificeerde risico's te verkleinen tot een acceptabel niveau door maatregelen voor te stellen en deze uit te voeren.

3 Beleidsprincipes verwerking persoonsgegevens

3.1 Beleidsprincipes

Algemeen beleidsuitgangspunt is dat persoonsgegevens in overeenstemming met de relevante wet- en regelgeving op behoorlijke en zorgvuldige wijze worden verwerkt. Bij de verwerking van persoonsgegevens is het belangrijk dat de belangen van de betrokkenen worden afgewogen tegen de belangen die de organisaties hebben bij het verwerken van de persoonsgegevens. De organisaties die hier voornamelijk worden bedoeld zijn GGD GHOR Nederland, de GGD'en en de GHOR-bureaus. De belangen van zowel de betrokkene als de organisaties kunnen tegenstrijdig zijn. Een adequate afweging van deze belangen is hier altijd noodzakelijk en moet altijd worden gemotiveerd.

Om aan bovenstaand beleidsuitgangspunt te voldoen gelden, in overeenstemming met de AVG, de volgende principes:

- Een verwerking van persoonsgegevens is gebaseerd op een van de wettelijke grondslagen zoals genoemd in artikel 6 van de AVG ("rechtmatigheid").
- Het verwerken van bijzondere persoonsgegevens is op grond van de AVG verboden, tenzij ten minste één van de uitzonderingsgronden van artikel 9 lid 2 van de AVG van toepassing is.
- Persoonsgegevens worden alleen verwerkt op een manier die ten aanzien van de betrokkene behoorlijk en transparant is. Dit houdt in dat het voor betrokkenen inzichtelijk moet zijn in hoeverre en op welke manier persoonsgegevens worden verwerkt. Informatie en communicatie hierover moet eenvoudig, toegankelijk en begrijpelijk zijn ("behoorlijkheid en transparantie"). Dit kan onder andere door te verwijzen naar de voor de materie relevante privacyverklaring van GGD GHOR Nederland.
- Persoonsgegevens worden alleen verwerkt voor welbepaalde, uitdrukkelijk omschreven en gerechtvaardigde doeleinden. Het gaat hier om specifieke en gerechtvaardigde doeleinden, die zijn vastgelegd en omschreven voordat men begint met de verwerking. Persoonsgegevens worden niet verder verwerkt op een wijze die onverenigbaar is met de doeleinden waarvoor ze zijn verkregen ("doelbinding").
- Bij een verwerking van persoonsgegevens blijft de hoeveelheid en het soort gegevens beperkt tot de persoonsgegevens die daadwerkelijk noodzakelijk zijn voor het specifieke doeleinde. De persoonsgegevens dienen met het oog op dat doel toereikend, ter zake dienend en niet bovenmatig te zijn. Indien de verwerking van persoonsgegevens voor het desbetreffende doeleinde niet noodzakelijk is, zullen geen persoonsgegevens worden verwerkt ("minimale gegevensverwerking").
- Verwerking van persoonsgegevens gebeurt op de minst ingrijpende wijze en dient in redelijke verhouding te staan tot het beoogde doeleinde ("proportionaliteit en subsidiariteit").
- Er worden maatregelen getroffen om zoveel mogelijk te waarborgen dat de persoonsgegevens die worden verwerkt door GGD GHOR Nederland juist en actueel zijn ("juistheid"). Het up-to-date houden van de persoonsgegevens is hierbij relevant.
- Persoonsgegevens binnen GGD GHOR Nederland worden adequaat beveiligd volgens de geldende beveiligingsnormen op het gebied van beschikbaarheid, integriteit en vertrouwelijkheid. Daarnaast worden gepaste organisatorische maatregelen genomen om persoonsgegevens te beschermen.
- Persoonsgegevens worden niet langer verwerkt dan noodzakelijk is voor de doeleinden waarvoor ze zijn verzameld. Hierbij worden de van toepassing zijnde bewaar- en vernietigtermijnen in acht genomen ("opslagbeperking").
- Bij de inrichting van systemen, procedures en werkprocessen of bij het ontwikkelen van systemen, producten en diensten wordt uitgegaan van de principes 'Privacy by Design' en 'Privacy by Default'.
- Persoonsgegevens worden alleen op grond van toestemming van betrokkene verwerkt als er geen andere grondslag conform de AVG aanwezig is.

- Iedere betrokkene heeft recht op inzage respectievelijk verbetering, aanvulling, verwijdering of afscherming van de in de afzonderlijke verwerkingen hem betreffende persoonsgegevens en heeft het recht op bezwaar, zoals geformuleerd in hoofdstuk 8 van dit privacybeleid.
- Bij alle registraties die gebaseerd zijn op toestemming van de betrokkene zal het intrekken van de toestemming net zo eenvoudig zijn als het geven ervan.
- Indien het voor een specifieke toepassing niet noodzakelijk is om persoonsgegevens te herleiden tot het individu zullen die persoonsgegevens worden verwijderd en/of waar mogelijk het principe van anonimiseren worden toegepast.
- Het delen van persoonsgegevens, zowel intern als extern, zal alleen plaatsvinden voor zover dat strikt noodzakelijk voor het doeleinde van de bewerking en alleen met diegene die rechtstreeks betrokken is. Daarbij dient de grootste zorgvuldigheid en terughoudendheid in acht te worden genomen als het gaat om het verstrekken van persoonsgegevens aan derden.
- Persoonsgegevens worden niet onbeheerd en in open zicht achtergelaten.
- Daar waar sprake is van verwerking van persoonsgegevens worden werkwijzen vastgesteld en op professionele wijze uitgevoerd conform protocollen en procesbeschrijvingen.
- Inbreuken in verband met persoonsgegevens (datalekken) worden te allen tijde gemeld via privacyoffice@ggdghor.nl. Het is medewerkers niet toegestaan zelfstandig melding doen van een datalek bij de Autoriteit Persoonsgegevens en de betrokkenen.
- Afhandeling van klachten, verzoeken en bezwaren over privacyaspecten vindt door de daartoe verantwoordelijke medewerker tijdig en op een toegankelijke, laagdrempelige wijze plaats.
- GGD GHOR Nederland is onder andere een belangenorganisatie voor de GGD'en en GHOR-bureaus. Om die reden zal altijd worden beoordeeld in welke rol GGD GHOR Nederland persoonsgegevens voor de GGD'en en GHOR-bureaus verwerkt. Daarvoor wordt gezorgd voor adequate onderlinge communicatie en afspraken. De communicatie vindt plaats door het projectleider of directie voor strategische zaken en via het Privacy Office voor inhoudelijke zaken. De te maken afspraken bevatten ten minste een uitsplitsing van de verantwoordelijkheden. Indien de verwerking meerdere fasen heeft, wordt per fase vastgelegd welke rol de partijen hebben.
- Bij samenwerking met partners, waar sprake is van verwerking van persoonsgegevens, worden afspraken gemaakt over de voorwaarden voor een zorgvuldige en adequaat beveiligde verwerking van persoonsgegevens en de controle daarop.
- Er wordt intern gewerkt aan awareness met betrekking tot privacy, gegevensbescherming en informatiebeveiliging.
- GGD GHOR Nederland geeft uitvoering aan het privacybeleid. De directie en het management draagt het privacybeleid uit binnen de organisatie en maakt privacy, gegevensbescherming en informatiebeveiliging bespreekbaar bij de uitvoering van de taken van GGD GHOR Nederland. De FG van GGD GHOR Nederland houdt toezicht en stelt de directie op de hoogte indien blijkt dat het privacybeleid niet op een juiste wijze wordt uitgevoerd.
- Schendingen van wetgeving, voorschriften en regels op het gebied van privacy en gegevensbescherming binnen GGD GHOR Nederland kunnen leiden tot corrigerende maatregelen door of namens GGD GHOR Nederland.

4 De gegevensverwerking

Tijdens de uitvoering van haar taken en de werkzaamheden die binnen GGD GHOR Nederland plaatsvinden, worden verschillende soorten persoonsgegevens verwerkt. Hierbij valt te denken aan verwerkingen in het kader van werkgeverschap, verwerking van medische gegevens van cliënten van een regionale GGD en het behandelen van bezwaren of klachten. In bepaalde gevallen kan het ook voorkomen dat de GGD GHOR Nederland persoonsgegevens deelt met andere partijen of derden. Dit is bijvoorbeeld het geval als een verwerker wordt ingeschakeld, GGD GHOR Nederland werknemersgegevens aan de Belastingdienst moet verstrekken of dit kan ook het geval zijn als een verzoek tot gegevensdeling door de toezichthoudende autoriteit (Autoriteit Persoonsgegevens) wordt gedaan.

4.1 Aard en omvang persoonsgegevens

GGD GHOR Nederland verwerkt bij haar werkzaamheden alle mogelijke categorieën van persoonsgegevens, waaronder gewone persoonsgegevens met een gevoelig karakter en bijzondere persoonsgegevens. GGD GHOR Nederland heeft haar verwerkingen in een verwerkingsregister opgenomen, waarin van ieder afzonderlijke verwerking nadere informatie wordt gegeven over onder meer:

- De verwerkingsdoeleinden;
- De categorieën betrokkenen;
- De categorieën persoonsgegevens;
- De categorieën ontvangers;
- De grondslag van de verwerking;
- De herkomst van de persoonsgegevens;
- De bewaartermijn van de persoonsgegevens;
- De beveiligingsmaatregelen.

Het verwerkingsregister is beschikbaar bij het Privacy Office en is toegankelijk voor de medewerkers van het Privacy Office en directie. De verwerkingen die worden uitgevoerd, worden beschreven in de privacyverklaringen van GGD GHOR Nederland.

4.1.1 Gewone persoonsgegevens

GGD GHOR Nederland verwerkt bij haar werkzaamheden allerlei categorieën persoonsgegevens. Hier kan gedacht worden aan:

- Persoonlijke identificatiegegevens;
- Persoonlijke kenmerkgegevens;
- Werk gerelateerde gegevens;
- Contactgegevens;

Gewone persoonsgegevens met een gevoelig karakter
Daarnaast verwerkt GGD GHOR Nederland persoonsgegevens met een gevoelig karakter. Dit betekent dat alhoewel het hier om gewone en niet bijzondere persoonsgegevens (zie pararagraaf 4.1.2) conform de AVG gaat, deze persoonsgegevens een gevoelig karakter hebben, waardoor met deze persoonsgegevens integer en vertrouwelijk moet worden omgegaan.

Voorbeelden van persoonsgegevens met een gevoelig karakter zijn:

- Burgerservicenummer (BSN);
- Elektronische identificatiegegevens (locatiegegevens);
- Verslagen van beoordelings- en/of functioneringsgesprekken;
- Financiële gegevens;
- Verklaring omtrent gedrag (VOG);
- Gegevens omtrent de persoonlijke situatie medewerker.

Voor het BSN en strafrechtelijke gegevens worden zeer strenge eisen gesteld, waarbij de mogelijke verwerking is vastgelegd in specifieke wetgeving.

4.1.2 Bijzondere persoonsgegevens

De verwerking van bijzondere persoonsgegevens is verboden, tenzij het verwerkingsverbod op grond van de AVG kan worden opgeheven. Als het verwerkingsverbod is opgeheven, moet de verwerking van bijzondere persoonsgegevens ook voldoen aan alle andere eisen van de AVG en dit privacybeleid. Zo moet voldaan worden aan de beleidsbeginselen van hoofdstuk 3 van dit privacybeleid en moet de verwerking van bijzondere persoonsgegevens een doeleinde (paragraaf 4.2) en een grondslag (paragraaf 4.3) hebben.

GGD GHOR Nederland verwerkt bij haar werkzaamheden bijzondere categorieën persoonsgegevens. Daarbij worden vooral de volgende gegevens verwerkt:

- Gegevens over gezondheid;
- Gegevens die iets zeggen over ras of etnische afkomst;
- Gegevens met betrekking tot iemand seksueel gedrag;
- Gegevens over seksueel gedrag of seksuele gerichtheid.

Voor het verwerken van bijzondere persoonsgegevens gelden zwaardere zorgvuldigheidseisen, waaronder die voor voor de beveiliging. Daar waar de basisbescherming niet voldoende is, moeten voor elk informatiesysteem individueel afgestemde extra maatregelen worden genomen om deze bijzondere persoonsgegevens te beschermen.

Betrek bij het verwerken van bijzondere persoonsgegevens altijd het Privacy Office en/of de Functionaris Gegevensbescherming.

4.1.3 BIV Classificatie GGD GHOR Nederland

GGD GHOR Nederland hanteert een classificatiedocument (‘BIV Classificatie GGD GHOR Nederland’) dat van toepassing is op alle documenten, informatie en informatiesystemen die onder de verantwoordelijkheid van GGD GHOR Nederland vallen. Dit betekent dat gewone persoonsgegevens (4.1.1) en bijzondere persoonsgegevens (4.1.2) hier ook onder vallen.

4.2 Doeleinden verwerkingen persoonsgegevens

GGD GHOR Nederland omschrijft vooraf de doeleinden van de verwerking. Deze doeleinden zijn concreet en specifiek geformuleerd. Bij elke verwerking wordt getoetst in hoeverre het verwerken van persoonsgegevens noodzakelijk is. Hierbij worden de verschillende belangen afgewogen en wordt gekeken naar de doelmatigheid, proportionaliteit en subsidiariteit. Persoonsgegevens worden overeenkomstig de beleidsprincipes niet verwerkt op een wijze die onverenigbaar is met de doeleinden waarvoor ze zijn gekregen.

De doeleinden waarvoor GGD GHOR Nederland persoonsgegevens verwerkt zijn onder andere:

1) Personeelszaken, o.a.:
    - Werving & selectie nieuwe medewerkers;
    - Personeelsadministratie (waaronder beoordelingen en verzuim);
    - Salarisadministratie.
2) Bedrijfsvoering en financiën, o.a.:
    - Financiële administratie;
    - Beheren van het inkoopsystemen en betaalsystemen;
    - Communicatie.
3) Facilitaire zaken, o.a.:
    - Reservering vergaderzalen;
    - Toegang- en beheersystemen;
4) Algemene processen, o.a.:
    - Fysieke en digitale toegang;

- Klachtenprocedure en bezwaar bij de verwerking van persoonsgegvens;

5) Ondersteuning van processen bij GGD'en, o.a.
   - Infectieziektebestrijding;
   - Authenticatiemethoden.

GGD GHOR Nederland heeft een Security Operation Center (SOC). Het SOC monitort en onderzoekt afwijkende gedragingen van medewerkers in systemen. GGD GHOR Nederland zorgt ervoor dat in het kader van de werkzaamheden van het SOC wordt voldaan aan de AVG.

4.3 Grondslag verwerking

GGD GHOR Nederland verwerkt Persoonsgegevens alleen op grond van de wettelijke grondslagen zoals beschreven in artikel 6 of indien het verbod op verwerking van bijzondere persoonsgegevens wordt opgeheven door artikel 9 van de AVG. Het gaat dan specifiek om de volgende grondslagen voor de verwerking van persoonsgegevens:

a. Toestemming van de betrokkene.
b. Noodzakelijk voor de uitvoering van een overeenkomst met de betrokkene.
c. Noodzakelijk om te voldoen aan een wettelijke verplichting die op GGD GHOR Nederland rust.
d. Noodzakelijk om de vitale belangen van de betrokkene of een ander natuurlijk persoon te beschermen.
e. Noodzakelijk voor de vervulling van een taak van algemeen belang of in het kader van uitoefening van openbaar gezag.
f. Noodzakelijk voor de behartiging van het gerechtvaardigd belang van GGD GHOR Nederland of eenderde.

Artikel 9 lid 2 AVG biedt daarbij de uitzonderingsgronden om bijzondere persoonsgegevens te mogen verwerken.

4.4 Bewaartermijn persoonsgegevens

GGD GHOR Nederland bewaart persoonsgegevens niet langer dan redelijkerwijs noodzakelijk is. GGD GHOR Nederland voert als verwerkingsverantwoordelijke en als verwerker daarvoor een bewaartermijnenbeleid waarin zoveel mogelijk de (wettelijke) bewaartermijnen worden gehanteerd.

Persoonsgegevens dienen na het verlopen van de bewaartermijn buiten het bereik van de actieve administratie te worden gebracht. GGD GHOR Nederland zal de persoonsgegevens na het verlopen van de bewaartermijn vernietigen, of in het uiterste geval indien dit niet mogelijk is, anonimiseren. Bij iedere verwerking wordt vooraf bepaald wat de bewaartermijnen zijn of de criteria voor de gebruikstermijn voor verwijdering.

Het bewaartermijnenbeleid van GGD GHOR Nederland staat beschreven in een separaat beleidsdocument.

4.5 Werkprocessen

GGD GHOR Nederland zorgt voor werkprocessen, zodat medewerkers weten wat van hen wordt verwacht in het uitvoeren van de werkzaamheden die zij uitvoeren. In deze werkprocessen wordt daarbij ook aandacht besteed voor hoe de persoonsgegevens dienen te worden verwerkt. Bij iedere verwerking worden de werkprocessen opgesteld voor de verwerking is gestart. Indien blijkt dat werkprocessen niet zijn opgesteld of niet volledig zijn, worden deze werkprocessen zo snel en volledig mogelijk opgesteld door de verantwoordelijke afdeling/projectleider.

4.6 Gegevensuitwisseling (doorgifte)

In bepaalde gevallen kan het voorkomen dat GGD GHOR Nederland persoonsgegevens deelt met andere partijen. Uitgangspunt is dat GGD GHOR Nederland alleen persoonsgegevens deelt als dat noodzakelijk is voor de procedure of als GGD GHOR Nederland hiertoe wettelijk verplicht is. Per geval wordt beoordeeld of het delen van persoonsgegevens noodzakelijk is. GGD GHOR Nederland is verantwoordelijk voor het eindoordeel alsmede het maken van de juiste afspraken hierover. Indien GGD GHOR Nederland niet de verwerkingsverantwoordelijke is van de persoonsgegevens, wordt de uitwisseling eerst afgestemd met de verwerkingsverantwoordelijke(n) (of een door de verwerkingsverantwoordelijke gemachtigd gremium) en wordt daarvoor een opdracht verwacht van de verwerkingsverantwoordelijken (of een door de verwerkingsverantwoordelijke gemachtigd gremium).

4.6.1 Verwerking uitbesteden aan een (sub)verwerker

GGD GHOR Nederland laat namens haar en op grond van haar instructies persoonsgegevens door een (sub)verwerker verwerken. De uitvoering hiervan wordt geregeld in een verwerkersovereenkomst, welke tussen GGD GHOR Nederland en de (sub)verwerker tot stand komt. De verwerkersovereenkomst vormt een aanvulling op een hoofdovereenkomst. Binnen GGD GHOR Nederland is een standaardmodel van de verwerkersovereenkomst ontwikkeld. De verantwoordelijke voor de verwerking, zoals de projectleider bij GGD GHOR Nederland zorgt en waakt ervoor dat daar waar sprake is van een verwerker, een verwerkersovereenkomst wordt aangegaan en nageleefd. Het Privacy Office van GGD GHOR Nederland biedt hierbij ondersteuning. GGD GHOR Nederland ondertekent de verwerkersovereenkomst en zorgt ervoor dat deze ook bij het Privacy Office van GGD GHOR Nederland wordt aangeleverd. Het Privacy Office van GGD GHOR Nederland houdt een overzicht van alle aangeleverde verwerkersovereenkomsten bij, en doet dit enkel voor overzicht en toezicht, niet als de feitelijke beheerder.

4.6.2 Verwerken als een gezamenlijke verantwoordelijke

GGD GHOR Nederland gaat samenwerkingsverbanden aan, waarbij door meerdere organisaties persoonsgegevens kunnen worden verwerkt en uitgewisseld. In dat geval hebben de partijen in een dergelijk samenwerkingsverband vaak een gezamenlijk doel dat zij bepalen en nastreven. Conform artikel 26 van de AVG worden er duidelijke afspraken over de rollen en verantwoordelijkheden die de samenwerkende partijen hebben en moet het voor de betrokkenen eenduidig zijn waar en bij wie zij hun vragen kunnen stellen en zich op hun rechten kunnen beroepen. GGD GHOR Nederland stelt zulke afspraken vast middels een overeenkomst tussen gezamenlijk verantwoordelijken. De verantwoordelijke voor de verwerking, zoals de projectleider bij GGD GHOR Nederland zorgt en waakt ervoor dat daar waar sprake is van gezamenlijke verwerkingsverantwoordelijkheid, een gezamenlijke verantwoordelijkenovereenkomst wordt aangegaan. Het Privacy Office van GGD GHOR Nederland kan hierbij ondersteuning bieden.

4.6.3 Verwerking binnen de Europese Economische Ruimte (EER)[1]

GGD GHOR Nederland verstrekt over het algemeen persoonsgegevens aan organisaties die zich binnen de EER bevinden. Hier kan gedacht worden aan een verwerker, maar ook aan samenwerkingspartner van GGD GHOR Nederland. De AVG is rechtstreeks van toepassing binnen alle lidstaten van de Europese Unie en tevens binnen de EER. De verantwoordelijke voor de verwerking, zoals de projectleider bij GGD GHOR Nederland zorgt ervoor dat bij gegevensuitwisseling binnen de EER wordt voldaan aan de eisen van de AVG.

4.6.4 Verwerking buiten de EER

GGD GHOR Nederland verstrekt in beginsel geen persoonsgegevens aan organisaties (een (sub)verwerker of samenwerkingspartner) die zich buiten de EER bevinden. Indien dit wel gebeurt zorgt GGD GHOR Nederland ervoor dat te allen tijde rekening wordt gehouden met de eisen van de AVG. De AVG is echter niet rechtstreeks van toepassing voor organisaties buiten de EER. Om die reden is GGD GHOR Nederland verplicht een extra controle tot het beschermingsniveau van het desbetreffende land te hanteren. Daarbij hanteert GGD GHOR Nederland als eerste uitgangspunt de lijst met landen met een passend beschermingsniveau van de Europese

[1] De EER bestaat uit alle lidstaten van de Europese Unie en tevens drie EVA-lidstaten, namelijk Noorwegen, IJsland en Liechtenstein.

Commissie, de zogenoemde adequaatheidsbesluiten.[2] Landen buiten de EER waarvoor een adequaatheidsbesluit geldt, worden geacht een passend beschermingsniveau te bieden, waardoor GGD GHOR Nederland geen aanvullende maatregelen hoeft te nemen om de persoonsgegevenste beschermen.

Landen waarvoor geen adequaatheidsbesluit geldt, worden geacht **geen** passend beschermingsniveau te bieden voor de verwerking van persoonsgegevens. GGD GHOR Nederland verstrekt in dat geval alleen persoonsgegevens, indien er passende waarborgen, zoals het afsluiten van de standaard modelcontracten voor veilige doorgifte van persoonsgegevens, conform de AVG zijn genomen. De verantwoordelijke voor de verwerking, zoals de projectleider bij GGD GHOR Nederland zorgt en waakt ervoor dat daar waar nodig passende waarborgen worden genomen om de persoonsgegevens van betrokkene bij gegevensuitwisseling buiten de EER te beschermen. Het Privacy Office kan hierbij ondersteuning bieden.

Daar waar het treffen van passende waarborgen niet mogelijk is, wordt door GGD GHOR Nederland alleen persoonsgegevens doorgegeven naar landen buiten de EER of internationale organisaties conform artikel 49 AVG. Hier kan gedacht worden aan de uitdrukkelijke toestemming van de betrokkene voor de gegevensuitwisseling buiten de EER.

4.7 Geheimhouding

Binnen GGD GHOR Nederland worden alle persoonsgegevens als vertrouwelijk behandeld. Dit betekent onder andere dat persoonsgegevens niet mogen worden gedeeld, gepubliceerd, ingezien of anderszins mogen worden verwerkt, zonder dat daarvoor een geldige noodzaak is. Iedereen hoort de vertrouwelijkheid van persoonsgegevens te kennen en daarnaar te handelen.

Ook personen voor wie niet reeds uit hoofde van ambt, beroep of wettelijk voorschrift een geheimhoudingsplicht geldt, zijn verplicht tot geheimhouding van de persoonsgegevens waarvan zij kennisnemen, behoudens voor zover enig wettelijk voorschrift hen tot mededeling verplicht of uit hun taak de noodzaak tot mededeling voortvloeit. Deze geheimhouding wordt voor interne medewerkers gewaarborgd via de arbeidsovereenkomst en/of de daarbij geldende collectieve arbeidsovereenkomst. Externe medewerkers ondertekenen hiervoor een overeenkomstige geheimhoudingsverklaring. Verwerkers en diens medewerkers of ingeschakelde partijen die namens en op instructie van GGD GHOR Nederland persoonsgegevens verwerken worden middels de verwerkersovereenkomst aan geheimhouding gebonden.

[2] 'Adequacy decisions', zie de website van de Europese Commissie <https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en>.

5 Governance en organisatorische borging gegevensverwerking

GGD GHOR Nederland zorgt ervoor dat alle medewerkers, externen en ingeschakelde partijen op een rechtmatige wijze persoonsgegevens verwerken. De wijze waarop dit binnen GGD GHOR Nederland organisatorisch wordt geborgd, wordt in dit hoofdstuk beschreven.

De feitelijke verwerking van persoonsgegevens wordt binnen allerlei lagen van GGD GHOR Nederland uitgevoerd. Het goed, efficiënt en verantwoord leiden van een organisatie wordt vaak aangeduid met de term governance. Het omvat vooral ook de relatie met de belangrijkste belanghebbenden van GGD GHOR Nederland. Een goed governance draagt bij aan de borging van privacy binnen GGD GHOR Nederland en biedt waarborgen voor de rechten van alle betrokkenen.

5.1 Functies | rollen

In dit gedeelte wordt beschreven welke functies binnen GGD GHOR Nederland een taak en verantwoordelijkheid hebben in de borging van een rechtmatige verwerking van persoonsgegevens binnen de organisatie.

Functies in verschillende lagen
Alle medewerkers binnen GGD GHOR Nederland zijn verantwoordelijk voor een rechtmatige omgang met persoonsgegevens. Er wordt van medewerkers verwacht dat zij zich integer gedragen en geen gedrag vertonen en situaties laten ontstaan die kunnen leiden tot inbreuken op de rechten en vrijheden van de betrokkenen en schade voor GGD GHOR Nederland. Daartoe zijn de beleidsprincipes in hoofdstuk 3 opgesteld. Deze beleidsprincipes vormen ook het kader bij het vaststellen of aanpassen van de procedures en de werkprocessen binnen GGD GHOR Nederland.

Iedere medewerker heeft zijn of haar eigen verantwoordelijkheid voor de rechtmatige omgang met persoonsgegevens. Om dit te controleren en te coördineren, houden een aantal daartoe aangewezen personen zich naast hun reguliere werkzaamheden bezig met de borging van de rechtmatige verwerking van persoonsgegevens door GGD GHOR Nederland. Dit geschiedt in de volgende lagen:

1. Het Privacy Office van GGD GHOR Nederland;
2. Leidinggegevende van de afdeling (lijnverantwoordelijke) of projectmanager;
3. Functionaris Gegevensbescherming (indien er sprake is van informatiebeveiliging wordt ook de CISO betrokken);
4. Directie.

5.1.2 Informatiebeveiliging

Informatiebeveiliging en gegevensbescherming zijn verwante verantwoordelijkheidsgebieden, raken en vinden elkaar in de beveiliging van persoonsgegevens. Privacy ziet vooral toe op juridische aspecten (o.a. behoorlijkheid en legitimiteit), informatiebeveiliging ziet vooral toe op betrouwbaarheid (beschikbaarheid, integriteit en vertrouwelijkheid) van informatie.

Chief Information Security Officer
De Chief Information Security Officer (CISO) voert onafhankelijk regie op en coördineert de informatiebeveiliging, waaronder de beveiliging van de persoonsgegevens die worden verwerkt binnen GGD GHOR Nederland. De Chief Information Security Officer:

- Stelt relevant tactisch en strategisch informatiebeveilingsbeleid voor;

- Adviseert de verantwoordelijke voor de verwerking en de directie van GGD GHOR Nederland gevraagd en ongevraagd over de uitvoering van het informatiebeveiligingsbeleid;
- Controleert namens de directie de naleving van het informatiebeveiligingsbeleid.

Information Security Officer
De Information Security Officer (ISO) is voor de verantwoordelijke voor de verwerking het aanspreekpunt voor de uitvoering en naleving van het organisatiebrede informatiebeveiligingsbeleid. De Information Security Officer:

- Adviseert op operationeel, tactisch niveau over uitvoeringsrichtingen op het gebied van informatiebeveiliging;
- Adviseert bij besluitvorming over gevolgen voor informatiebeveiliging;
- Draagt actief uitvoeringsrichtlijnen op het gebied van informatiebeveiliging uit;
- Voert beveiligingsrisicoanalyses op technisch, proces en business niveau uit.

5.2 Taken en verantwoordelijkheden gegevensverwerking

5.2.1 Presidium

Het Presidium is als bestuur eindverantwoordelijk voor de rechtmatige en zorgvuldige verwerking van persoonsgegevens binnen GGD GHOR Nederland. Het Presidium stelt het beleid, de maatregelen en de procedures op het gebied van gegevensverwerking met dit privacybeleid vast.

5.2.2 Directie

Het Presidium heeft de verantwoordelijkheid voor de uitvoering van het privacybeleid bij de directie belegd. Ten aanzien van de stichting LCCB stelt de directeur van de stichting LCCB het privacybeleid vast en is tevens verantwoordelijk voor de uitvoering hiervan.

5.2.3 Privacy Office

Het privacy Office ondersteunt en controleert alle processen binnen GGD GHOR Nederland waarbij persoonsgegevens worden verwerkt. Met het privacy Office kan GGD GHOR Nederland aantonen dat zij op een verantwoordelijke manier omgaat met persoonsgegevens.

Op verantwoorde wijze persoonsgegevens verwerken gaat verder dan naleving van wet- en regelgeving. Om op zorgvuldige wijze met persoonsgegevens om te gaan moet ook worden nagegaan hoe het belang van gegevensverwerking binnen de eigen organisatie wordt ingevuld en hoe dit naar de buitenwereld wordt gecommuniceerd.

De winst van een Privacy Office is dat het gehele proces van gegevensverwerking binnen GGD GHOR Nederland duidelijk en controleerbaar wordt. Voor de medewerkers van GGD GHOR Nederland schept een Privacy Office zekerheid over de manier waarop invulling moet worden gegeven aan de rechten en vrijheden van de betrokkenen. Hierdoor kunnen fouten (die leiden tot onrechtmatige verwerkingen) beperkt of voorkomen worden. GGD GHOR Nederland loopt hierdoor minder risico op reputatieschade en handhaving door de toezichthouder. Daarnaast draagt het Privacy Office bij aan de zichtbaarheid op de wijze waarop GGD GHOR Nederland omgaat met gegevensverwerking. Hiermee kan GGD GHOR Nederland optimaal verantwoording afleggen over de verwerking van persoonsgegevens aan betrokkenen, media, de toezichthouder en de politiek.

In het Privacy Office van GGD GHOR Nederland zijn drie rollen onderkend die regie voeren over en toezicht houden op het privacybeleid en privacy governance, te weten de Privacy Lead Projecten (5.2.3), de Privacy Officer (5.2.4) en de Functionaris Gegevensbescherming (5.3).

5.2.4 Privacy Lead (Projecten)

De Privacy Lead (Projecten) (PLP) behoort tot het Privacy Office van GGD GHOR Nederland en is verantwoordelijk voor de advisering en ondersteuning om privacy compliance van GGD GHOR Nederland ten aanzien van projecten in de 1ste lijn te realiseren (supportive) en is tevens verantwoordelijk voor privacy compliance in de 2e lijn, waarbij de Privacy Lead (Projecten) hierin vooral een coördineerde rol heeft ten aanzien van het privacyteam (responsible) voor de lopende projecten binnen GGD GHOR Nederland. De Privacy Lead (Projecten) is verantwoordelijk voor de behandeling van organisatiebrede vraagstukken en het privacyproces voor de projecten die lopen binnen GGD GHOR Nederland.

De Privacy Lead (Projecten) (o.a.):

- Ondersteunt projecten bij privacygerelateerde zaken;
- Stuurt behandeling uitvoering rechten van betrokken en privacy vragen (ook ten aanzien van projecten)aan;
- Stuurt behandeling datalekken aan;
- Voert (meer complexe) DPIA's uit;
- Sparringpartner van en met Functionaris Gegevensbescherming.

De rol van de Privacy Lead (Projecten) is van tijdelijke aard en kan in de nabije toekomst worden gewijzigd.

5.2.5 Privacy Officer

De Privacy Officer (PO) behoort tot het Privacy Office van GGD GHOR Nederland en is verantwoordelijk voor de advisering en ondersteuning om privacy compliance van de GGD GHOR Nederland in de 1ste lijn te realiseren (supportive) en is tevens werkzaam in de 2e lijn, middels onder andere het ondersteunen van de Privacy Lead (Projecten) (supportive).

De Privacy Officer (o.a):

- Ondersteunt Privacy Lead (Projecten) bij opstellen privacybeleid en procedures;
- Ondersteunt bij de uitvoering van de rechten van betrokkenen en privacy vragen;
- Wikkelt datalekken af;
- Ondersteunt Privacy Lead (Projecten) bij organisatiebrede vraagstukken;
- Voert DPIA's uit, wordt daarbij ondersteunt door informatiemanagers, beleidsmedewerkers en medewerkers die inhoudelijk in het proces werken;
- Is het aanspreekpunt voor privacygerelateerde vragen voor de informatiemanagers, beleidsmedewerkers en projectondersteuners;
- Ondersteunt de informatiemanagers,managers en projectleiders bij awareness(campagnes);
- Ondersteunt de Functionaris Gegevensbescherming in de uitvoering van haar taken.

5.3 Toezicht

GGD GHOR Nederland heeft een Functionaris Gegevensbescherming aangesteld. De Functionaris Gegevensbescherming is de interne adviseur en toezichthouder (consulted) op de naleving van privacy en gegevensbescherming conform de AVG. De Functionaris Gegevensbescherming handelt onafhankelijk van GGD GHOR Nederland en wordt niet aangestuurd door GGD GHOR Nederland. GGD GHOR Nederland oefent ook geen invloed uit op hetgeen de Functionaris Gegevensbescherming doet. Deze onafhankelijke positie is vastgelegd in de AVG. Alle medewerkers van GGD GHOR Nederland werken volledig mee aan alle verzoeken van de Functionaris Gegevensbescherming.

De taken van de Functionaris Gegevensbescherming worden in de AVG bepaald. De Functionaris Gegevensbescherming:

- Informeert, signaleert en adviseert (gevraagd en ongevraagd), de directie, de lijnverantwoordelijke, alle medewerkers en het Privacy Office over de verwerking van persoonsgegevens en nakoming uit hoofde van de AVG en andere relevante wet- en regelgeving inzake gegevensbescherming;
- Houdt toezicht op de naleving van de AVG, andere wet- en regelgeving inzake gegevensbescherming en het GGD GHOR NL privacybeleid en brengt verslag uit aan de directie;
- Houdt toezicht op de getroffen maatregelen door de Chief Information Security Officer;
- Houdt toezicht op de toewijzing van verantwoordelijkheden, bewustwording en opleiding van de medewerkers;
- Adviseert met betrekking tot DPIA's en ziet toe op de uitvoering daarvan;
- Treedt op als contactpunt en werkt samen met de Autoriteit Persoonsgegevens.

De Functionaris Gegevensbescherming krijgt ruimte voor professionele uitvoering van bovengenoemde taken. Dit gebeurt mede volgens de volgende, door GGD GHOR Nederland gefaciliteerde zaken:

- GGD GHOR Nederland zorgt ervoor dat de Functionaris Gegevensbescherming naar behoren en tijdig wordt betrokken bij de verwerking van persoonsgegevens. Dit betekent dat de Functionaris Gegevensbescherming vanaf de start wordt betrokken bij die aangelegenheid die risico's kunnen hebben vanuit privacy en AVG-perspectief, zoals nieuwe projecten, bestaande projecten waarin de verwerking van persoonsgegevens wordt gewijzigd/uitgebreid, intenties tot aanschaf van applicaties;
- De Functionaris Gegevensbescherming wordt bij de start van de DPIA betrokkenen en ingelicht en op de hoogte gehouden van het DPIA proces;
- De Functionaris Gegevensbescherming krijgt toegang tot alle ruimten, waar een verwerking van persoonsgegevens plaatsvindt en is bevoegd apparatuur, programmatuur, gegevensbestanden, boeken, bescheiden en andere informatie te onderzoeken en zich over de werking van apparatuur en programmatuur doen tonen;
- De Functionaris Gegevensbescherming wordt volledig geïnformeerd over aspecten van de bedrijfsvoering binnen GGD GHOR Nederland waarbij persoonsgegevens worden verwerkt of wanneer daartoe voornemens bestaan;
- De Functionaris Gegevensbescherming is de gesprekspartner en maakt deel uit van relevante werkgroepen die zich ook bezighouden met gegevensverwerking binnen de organisatie;
- De Functionaris Gegevensbescherming heeft standing invitation voor vergaderingen van het hogere en middenmanagement;
- GGD GHOR Nederland (de directie, lijnverantwoordelijken en medewerkers) ondersteunt de Functionaris Gegevensbescherming door op diens verzoek toegang te geven tot de verwerking van persoonsgegevens en haar de middelen te bieden voor professioneel onderzoek;
- De Functionaris Gegevensbescherming kan vrij en onafhankelijk advies geven;
- De Functionaris Gegevensbescherming kan niet ontslagen worden of een sanctie krijgen als gevolg van de uitoefening van haar taken, zoals deze blijken uit de AVG.

De zienswijze van de Functionaris Gegevensbescherming is zwaarwegend en geldt als de geëigende wijze voor naleving van de AVG en andere relevante wet- en regelgeving inzake gegevensbescherming door GGD GHOR Nederland, onverminderd de opvatting van de Autoriteit Persoonsgegevens. Indien GGD GHOR Nederland besluit af te wijken van een advies van de Functionaris Gegevensbescherming, zal hiervoor altijd een schriftelijke motivatie worden vastgelegd.

5.4 Planning & Control cyclus GGD GHOR Nederland

GGD GHOR Nederland hanteert een Planning & Control cyclus.

Er zijn twee formele momenten in het jaar waarin GGD GHOR Nederland zich moet verantwoorden, te weten:

- Voorjaarsrapportage; en
- Najaarsrapportage.

De interne controlecyclus heeft een frequentie van eenmaal per jaar. Elk jaar informeren de lijnverantwoordelijken, het Privacy Office en de Functionaris Gegevensbescherming aan de directie van GGD GHOR Nederland.

6 Risicobeheersing

Het beheersen van risico's is een belangrijk onderdeel van gegevensverwerking en de bescherming van de rechten van betrokkenen. Risicobeheersing is een constant proces dat vanaf het moment dat persoonsgegevens worden verzameld tot aan het moment dat deze worden verwijderd in acht moet worden genomen. Om alle mogelijke risico's ten aanzien van gegevensverwerking in kaart te brengen en deze te kunnen beheersen acht GGD GHOR Nederland Privacy by Design, Privacy by Default, DPIA's, passende maatregelen en awareness noodzakelijk.

6.1 Privacy by Design en Privacy by Default

GGD GHOR NL hanteert bij de inrichting van procedures en werkprocessen of bij het aanschaffen, ontwerpen en inrichten van producten en diensten de principes van 'Privacy by Design' en Privacy by Default'. Hiermee worden privacyaspecten en de bescherming van persoonsgegevens vanaf het begin geborgd, waardoor risico's voor de rechten en vrijheden van de Betrokkene aan de voorkant worden beperkt of voorkomen.

Privacy by Design (gegevensbescherming door ontwerp)
Bij het ontwerpen van een product of dienst of bij de inrichting van procedures en werkprocessen wordt vanaf het begin rekening gehouden met de uitgangspunten van de AVG en de daarbij behorende technische en organisatorische maatregelen, waarbij de aandacht hiervoor tijdens de gehele levensduur blijft bestaan. Zo wordt bij het ontwikkelen van een informatiesysteem rekening gehouden welke persoonsgegevens daadwerkelijk noodzakelijk zijn voor het doel waarvoor ze worden verzameld, of deze persoonsgegevens kunnen worden beveiligd, hoe lang de persoonsgegevens mogen worden bewaard, wie toegang heeft tot het systeem en welke rechten daaraan zijn verbonden, zoals wie mag welke gegevens inzien, kopiëren, verwerken, wijzigen en verwijderen.

Elke nieuwe verwerking wordt onderworpen aan een checklist om ervoor te zorgen dat de privacy van betrokkenen wordt gewaarborgd. Deze checklist wordt voor een verwerking wordt gestart geraapleegd en tijdens het opzetten van de verwerking compleet gevolgd. Voordat de verwerking start, dient de checklist volledig doorlopen te zijn.

Privacy by Default (gegevensbescherming door standaardinstellingen)
GGD GHOR Nederland zorgt ervoor dat technische en organisatorische maatregelen worden genomen waarbij als standaard alleen die persoonsgegevens worden verwerkt die ook daadwerkelijk noodzakelijk zijn voor het specifieke doel van de verwerking. Dit betekent dat bijvoorbeeld bij de instellingen van een programma, een applicatie, een website of een dienst maximale privacy wordt betracht, zonder dat de betrokkene deze instelling zelf AVG-compliant moet instellen.

GGD GHOR Nederland zorgt en waakt ervoor dat deze principes worden nageleefd. Het Privacy Office kan ondersteuning bieden waar nodig.

6.2 Data Protection Impact Assessment (DPIA)

Bij nieuwe verwerkingen, zoals projecten, infrastructurele wijzigingen of de aanschaf van nieuwe systemen, wordt door GGD GHOR Nederland vanaf het begin rekening gehouden met de inrichting van privacy en gegevensbescherming. Dit houdt onder andere in dat GGD GHOR Nederland handelt volgens haar beleidsprincipes (hoofdstuk 3), haar betrokkenen informeert over het doel en de verwerking van persoonsgegevens, haar systemen van beveiliging voorziet en betrokkenen in staat stelt om hun rechten uit te oefenen (hoofdstuk 8).

Bij nieuwe verwerkingen, zoals projecten, infrastructurele wijzigingen of de aanschaf van nieuwe systemen die een mogelijk hoog risico voor de privacy rechten en vrijheden van betrokkenen opleveren, wordt standaard een DPIA uitgevoerd. Dit wordt uitgevoerd door GGD GHOR Nederland of gezamenlijk met één of meerdere

(samenwerkings)partijen De DPIA vindt plaats voorafgaand aan de gegevensverwerking. Bij het vaststellen van de risico's houdt GGD GHOR Nederland rekening met onder andere het aantal betrokkenen, de categorieën persoonsgegevens die worden verwerkt en of het een verwerking betreft waarin persoonsgegevens met derden worden verwerkt/gedeeld. In de DPIA worden de risico's van een voorgenomen verwerking beoordeeld en op een gestandaardiseerd wijze in kaart gebracht. Op basis hiervan worden maatregelen getroffen om de geconstateerde risico's te verlichten of te voorkomen. Wanneer een hoog risico resteert, dient een voorafgaande raadpleging gevraagd te worden bij de Autoriteit Persoonsgegevens. Hoe hoog een risico is en of er sprake is van een verplichting tot het uitvoeren van een DPIA wordt bepaald aan de hand van een aantal vragen. Dit is de pre-DPIA.

De verantwoordelijke voor de nieuwe verwerking zorgt en waakt ervoor dat daar waar sprake is van projecten, infrastructurele wijzigingen of de aanschaf van nieuwe systemen, een pre-DPIA dan wel een DPIA wordt uitgevoerd. De Functionaris Gegevensbescherming wordt door de verantwoordelijke voor de nieuwe verwerking tijdig betrokken bij het DPIA-proces. De Functionaris Gegevensbescherming voorziet de DPIA daarnaast van een formeel advies. Het Privacy Office beschikt over de pre-DPIA vragenlijst en een DPIA register met alle uitgevoerde DPIA's, zodat op deze wijze kan worden voldaan aan de verantwoordingsplicht van GGD GHOR Nederland.

6.3 Passende beveiligingsmaatregelen

In het kader van de uitvoering van haar taak en werkzaamheden vertrouwen medewerkers, betrokkenen en onder andere GGD'en en GHOR-bureaus (gevoelige) persoonsgegevens toe aan GGD GHOR Nederland, die deze verwerkt in haar organisatie en informatiesystemen. GGD GHOR Nederland is verantwoordelijk voor het inrichten, onderhouden en continue verbeteren van passende beveiliging van deze persoonsgegevens. GGD GHOR Nederland draagt daarom zorg voor een passend beveiligingsniveau en legt passende technische en organisatorische maatregelen ten uitvoer, in lijn met de wettelijke verplichting, haar eigen organisatierisico's en het vertrouwen en belangen van de betrokkenen.

Met de getroffen en te treffen passende beveiligingsmaatregelen beoogt GGD GHOR Nederland persoonsgegevens te beveiligen tegen verlies of tegen enige vorm van onrechtmatige verwerking. Deze maatregelen zijn er mede op gericht onnodige c.q. onrechtmatige verzameling en verwerking van persoonsgegevens te voorkomen en materiële en/of immateriële schade van betrokkenen en de organisatie te verkleinen en/of te voorkomen. GGD GHOR Nederland heeft een intern informatiebeveiligingsbeleid en classificatiebeleid geïmplementeerd waarin maatregelen zijn uitgewerkt die de GGD GHOR Nederland hanteert.

6.3.1 Informatiebeveiligingsbeleid

GGD GHOR Nederland hanteert een informatiebeveiligingsbeleid voor het gehele proces van informatievoorziening, inclusief de niet geautomatiseerde stappen waarin nog sprake is van papieren gegevensuitwisseling of dossiers. Informatiebeveiliging is de verzamelnaam voor de processen die GGD GHOR Nederland inricht om de betrouwbaarheid van informatie te beschermen. Het begrip 'informatiebeveiliging' heeft betrekking op:

- Beschikbaarheid: zorgdragen voor het beschikbaar en toegankelijk zijn van informatie en informatie verwerkende informatiesystemen voor de gebruikers;
- Integriteit: waarborgen van de correctheid, volledigheid, tijdigheid en controleerbaarheid van de informatie en informatieverwerking;
- Vertrouwelijkheid: beschermen van informatie tegen kennisname, mutatie, toevoeging of vernietiging door onbevoegden. Informatie is alleen toegankelijk voor degenen die daartoe geautoriseerd zijn.

Het informatiebeveiligingsbeleid en het privacybeleid hebben een duidelijk verband en komen op het gebied van gegevenswerking en de bescherming daarvan samen, waarbij tussen beide gebieden integraal wordt samengewerkt om persoonsgegevens conform de AVG te verwerken en om de rechten en vrijheden van de betrokkene te waarborgen. De CISO ziet toe op de naleving van het informatiebeveiligingsbeleid binnen GGD GHOR Nederland.

6.4 Awareness (bewustwording en training)

Awareness is een belangrijke stap voor AVG-compliance. Een privacybeleid en maatregelen om gegevensbescherming te waarborgen zijn niet voldoende om risico's uit te sluiten. Het is noodzakelijk om bij medewerkers (zowel intern als extern) voortdurend en actief het bewustzijn met betrekking tot privacy, informatiebeveiliging en gegevensbescherming aan te scherpen. Hiermee kan gedragsverandering worden gerealiseerd, veilig en verantwoord gedrag worden aangemoedigd en wordt kennis van gegevensbescherming en de daarmee gepaard gaande risico's verhoogd.

GGD GHOR Nederland wil om die reden de onderwerpen van privacy, gegevensbescherming en informatiebeveiliging in de organisatie levend houden. Terugkerende bewustwordingscampagnes vormt hier een belangrijk onderdeel van. Deze campagnes kunnen aansluiten met andere beveiligingscampagnes.

Awareness zal worden vergroot door:

- Voorlichtende communicatie rond privacy en security thema's in allerlei vormen (presentaties, workshops, periodieke blogs en artikelen, flyer en poster campagne).
- Een Q&A over privacy, gegevensbescherming en informatiebeveiliging op kennisnet plaatsen.
- Organiseren van cursussen en trainingen (kennisniveau verhogen).
- Mystery guest bezoek faciliteren (opzoeken van kwetsbaarheden tijdens bezoek en rapportage opleveren hierover die aan de medewerkers wordt teruggekoppeld) en toepassen van social engineering.
- Opstellen en uitdragen van gedragsregels (gedragsregels privacy en gegevensverwerking).
- Stimuleren van privacy policies (clean desk, clean screen policy).
- Toepassen van procedures (meldingen en afhandelingen van incidenten, inbreuken, verzoeken).
- Online awareness training.

GGD GHOR Nederland zorgt daarnaast ervoor dat de directe en de lijnverantwoordelijke op de hoogte zijn van de AVG, om het hen mogelijk te maken de impact van de AVG op hun bestaande processen, diensten en goederen te kunnen inschatten en daarop de juiste maatregelen te kunnen nemen.

De directie en de lijnverantwoordelijke zijn verantwoordelijk voor de verhoging van awareness op het gebied van privacy, security en gegevensbescherming. Het Privacy Office kan daarbij ondersteuning bieden.

7 Datalekken

GGD GHOR Nederland heeft op grond van de AVG de plicht om datalekken te melden bij de Autoriteit Persoonsgegevens. Als er sprake is van een vermoeden van een datalek of een datalek is ontdekt, dient direct een melding te worden gemaakt bij het Privacy Office, zodat binnen GGD GHOR Nederland zo snel mogelijk acties kunnen worden ondernomen om de melding te registeren, te onderzoeken en af te handelen om zo de rechten en vrijheden van betrokkenen te beschermen. Dit hoofdstuk beschrijft het beleid met betrekking tot de melding, registratie en afhandeling van een datalek of het vermoeden van een datalek binnen de GGD GHOR Nederland.

7.1 Datalek

Bij een datalek[3] gaat het om ongeoorloofde of onbedoelde toegang tot en/of ongeoorloofde of onbedoelde verlies, vernietiging, wijziging en verstrekking van de persoonsgegevens, zoals:

- Diefstal van een laptop of een mobiel met persoonsgegevens die bij de werkzaamheden voor GGD GHOR Nederland worden verwerkt;
- E-mail met Persoonsgegevens versturen naar een verkeerde ontvanger;
- Verlies van een USB-stick;
- Het (on)bedoeld wissen/vernietigen van persoonsgegevens;
- Besmetting met ransomware waarbij persoonsgegevens ontoegankelijk zijn;
- Een ongeautoriseerde persoon toegang heeft tot persoonsgegevens;
- Een geautoriseerd persoon gegevens inziet die niet nodig zijn voor de uitvoering van de werkzaamheden.

De AVG kent de term ‘datalek’ niet. De AVG spreekt in dit geval van ‘een inbreuk in verband met persoonsgegevens’. In het maatschappelijk verkeer wordt de term ‘datalek’ gehanteerd. Ieder vastgesteld datalek of ieder vermoeden van een datalek wordt door de GGD GHOR Nederland gedocumenteerd.

Een vermoeden van een datalek of een datalek wordt direct gemeld volgens de datalekprocedure GGD GHOR Nederland. Alleen op deze wijze kan GGD GHOR Nederland het datalek tijdig onderzoeken en indien nodig melden aan de Autoriteit Persoonsgegevens en indien nodig de betrokkene(n). Medewerkers worden op verschillende manieren op de hoogte gebracht over de procedure.

7.2 Melding en registratie

Een datalek kan binnen GGD GHOR Nederland worden gemeld door alle medewerkers (zowel intern als extern), leveranciers en derden buiten GGD GHOR Nederland van wie de persoonsgegevens binnen GGD GHOR Nederland mogelijk zijn betrokken bij een datalek. Dit gebeurt via de procedure datalekken en voor leverancies en derden via de gemaakte afspraken of verschafte informatie. Vastgestelde of vermoede datalekken, net als waargenomen of verdachte zwakke plekken in systemen of diensten, worden door alle medewerkers, ingehuurd personeel en externe gebruikers per direct gemeld bij de lijnverantwoordelijke dan wel bij de persoon volgens de gemaakte afspraken. Zij melden het vermoedelijke datalek bij het Privacy Office, zoals vastgesteld in de procedure datalekken.

Elk gemelde (vermoedelijke) datalek en de afhandeling daarvan zal worden bijgehouden in het Register datalekken van GGD GHOR Nederland.

7.3 Afhandeling

Indien sprake is van een datalek wordt dit conform de datalekprocedure van GGD GHOR Nederland en in de relevante wet- en regelgeving opgenomen specifieke bepalingen over datalekken afgehandeld, zoals onder

[3] Zie verdere uitleg AP: https://autoriteitpersoonsgegevens.nl/nl/onderwerpen/beveiliging/meldplicht-datalekken#wat-is-een-datalek-precies-5916.

andere beschreven in de beleidsregels meldplicht datalekken van de Autoriteit Persoonsgegevens[4], zodat de melding van het datalek de juiste personen en uiteindelijk de toezichthouder en betrokkenen op tijd bereikt.

Bij een datalek met een medium tot hoog risico-inschatting, in het geval dat de betrokkene(n), de bedrijfsprocessen, de financiën of goede naam van GGD GHOR Nederland ernstig in gevaar zijn, wordt in ieder geval de directie bij de afhandeling van het gemelde datalek betrokkenen.

7.4 Besluitvorming

In het geval dat de beoordeling van het incident leidt tot een meldingswaardig datalek, zal volgens de procedure datalekken een besluit worden genomen omtrent de verplichting om het datalek te melden aan de Autoriteit Persoonsgegevens en indien nodig ook aan de betrokkene(n). De directie is verantwoordelijk (responsible & accountable) voor het besluit om al dan niet de melding te maken aan de Autoriteit Persoonsgegevens en/of de betrokkene(n) ingeval het datalek een medio tot hoog risico-inschatting heeft gekregen.

7.5 Evaluatie – verbeterplan

Het is voor de organisatie van groot belang om te leren van bestaande datalekken, om de waarschijnlijkheid van toekomstige datalekken te verkleinen en bedrijfsprocessen te verbeteren.

Registratie van datalekken, een periodieke rapportage en een verbeterplan daarover horen thuis bij een professionele manier van verwerken van persoonsgegevens. De rapportage over datalekken met betrekking tot persoonsgegevens maakt daarom een vast onderdeel uit van de verslaglegging naar het presidium, de directie en de betrokken verantwoordelijke voor de verwerking. De Functionaris Gegevensbescherming ziet toe op de naleving van het verbeterplan.

[4] Beleidsregels meldplicht datalekken van de Autoriteit Persoonsgegevens: https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/guidelines_meldplicht_datalekken.pdf.

8 Rechten van betrokkenen

8.1 Rechten van betrokkenen

Onder de AVG hebben betrokkenen bepaalde rechten waarmee ze controle kunnen uitoefenen op de persoonsgegevens die GGD GHOR Nederland van hen verwerkt. Een verzoek van een betrokkene kan schriftelijk per e-mail worden ingediend bij de lijnverantwoordelijke van de desbetreffende afdeling.[5] Een verzoek kan ook per brief via de post bij de verantwoordelijke voor de verwerking worden ingediend.

Indien gegevens worden verwerkt door GGD GHOR Nederland ten behoeve van regionale GGD'en, zal in beginsel het verzoek worden voorgelegd aan de verantwoordelijke GGD. Daartoe wordt de betrokkene verwezen naar de GGD, of, indien door de betrokkene toestemming wordt verleend, wordt het verzoek doorgestuurd. GGD GHOR Nederland handelt enkel verzoeken van betrokkenen af voor persoonsgegevens waarvoor GGD GHOR Nederland zelfstandig verwerkersverantwoordelijk is, of indien er afspraken zijn gemaakt over de afhandeling van de verzoeken door GGD GHOR NL.

De volgende rechten van betrokkenen worden in acht genomen:

a) Het recht op informatie;
b) Het recht op inzage;
c) Het recht op rectificatie en aanvulling;
d) Het recht op vergetelheid en verwijderen van gegevens ('recht om te worden vergeten');
e) Het recht om de verwerking te beperken;
f) Het recht op overdraagbaarheid van gegevens (recht op dataportabiliteit);
g) Het recht van bezwaar.

8.1.1 Recht op informatie

Persoonsgegevens moeten rechtmatig, eerlijk en op een transparante manier worden verwerkt. Betrokkenen hebben het recht om daarover te worden geïnformeerd.

8.1.2 Recht op inzage

Betrokkenen hebben het recht om aan GGD GHOR Nederland te vragen of hun persoonsgegevens worden verwerkt. Als dit het geval is hebben betrokkenen het recht op toegang tot (een kopie van) de verwerkte persoonsgegevens.

8.1.3 Recht op rectificatie en aanvulling

Betrokkenen hebben het recht om persoonsgegevens te laten corrigeren als deze onjuist of onvolledig zijn. Dit recht omvat het feit dat onvolledige gegevens mogen worden aangevuld, door middel van een aanvullende verklaring, zodat de persoonsgegevens compleet en juist zijn.

8.1.4 Recht op vergetelheid en verwijderen van gegevens

Het recht om persoonsgegevens te doen verwijderen, ook wel het recht om vergeten te worden, is geen absoluut recht. Betrokkenen hebben het recht om persoonsgegevens te laten verwijderen in het geval dat één van de volgende redenen van toepassing is:

a) De persoonsgegevens zijn niet langer noodzakelijk met betrekking tot het doel waarvoor ze oorspronkelijk zijn verzameld of verwerkt;
b) Betrokkenen de door hen gegeven toestemming intrekken en er geen andere wettelijke grondslag is voor de verwerking;
c) Betrokkenen bezwaar maken tegen de verwerking van hun persoonsgegevens en er geen doorslaggevende legitieme redenen zijn voor de verwerking;
d) De verwerking van de persoonsgegevens onrechtmatig is;
e) De persoonlijke gegevens moeten worden gewist om te voldoen aan een wettelijke verplichting.

[5] Indien nodig of gewenst kan het privacyteam bij moeilijke vraagstukken worden ingeschakeld door de lijnverantwoordelijke.

8.1.5 Recht om de verwerking te beperken

Betrokkenen hebben het recht om de verwerking van hun versoonsgegevens te beperken in het geval dat één van de volgende redenen van toepassing is:

a) De nauwkeurigheid van persoonsgegevens wordt betwist door de betrokkene;
b) De verwerking onrechtmatig is en betrokkenen zich verzetten tegen het verwijderen van de persoonsgegevens;
c) GGD GHOR Nederland heeft de persoonsgegevens niet langer nodig.

8.1.6 Recht op overdraagbaarheid van gegevens

Het recht op overdraagbaarheid van gegevens stelt de betrokkenen in staat hun persoonlijke gegevens voor hun eigen doeleinden te verkrijgen en hergebruiken voor verschillende diensten, maar is alleen van toepassing:

a) Op persoonsgegevens die door de betrokkenen verstrekt zijn aan GGD GHOR Nederland;
b) Wanneer de verwerking is gebaseerd op toestemming van de betrokkenen of voor de uitvoering van een overeenkomst;
c) Wanneer de verwerking op een geautomatiseerde wijze wordt uitgevoerd.

8.1.7 Recht van bezwaar

Op het moment dat de verwerking rechtmatig is, kunnen betrokkenen op elk moment bezwaar maken tegen de verwerking van hun persoonsgegevens, om redenen die samenhangen met hun specifieke situatie.

In geval van twijfel of vragen kunnen vragen/cases worden voorgelegd aan de Privacy Office via privacyoffice@ggdghor.nl of rechtstreeks aan de Functionaris Gegevensbescherming via fg@ggdghor.nl.

8.2 Kosten

Alle informatie, communicatie of acties worden kosteloos verstrekt aan betrokkenen, tenzij een dergelijk verzoek kennelijk ongegrond of buitensporig is, met name vanwege het repetitieve karakter ervan. GGD GHOR Nederland kan in dat geval een redelijke vergoeding in rekening brengen, rekening houdend met de administratieve kosten van de communicatie, of het verzoek weigeren. Voorafgaand aan het inwilligen van het verzoek geeft GGD GHOR Nederland aan de betrokkene de te berekenen kosten op, zodat de betrokkenen toestemming kunnen geven.

GGD GHOR Nederland onderbouwt bij weigering van het verzoek het kennelijk ongegronde of buitensporige karakter van het verzoek.

8.3 Beslistermijn

GGD GHOR Nederland informeert in ieder geval binnen 1 maand aan de betrokkenen zonder onnodige vertraging na ontvangst van het verzoek over het gevolg van het verzoek. De periode kan met 2 maanden worden verlengd, rekening houdend met de complexiteit en het aantal verzoeken. Van zo'n verlenging wordt de betrokkene in voorkomend geval op de hoogte gesteld.

Indien GGD GHOR Nederland geen actie onderneemt op het verzoek van de betrokkenen, zal GGD GHOR Nederland dit zonder onnodige vertraging en uiterlijk binnen 1 maand, of 2 maanden bij een verlenging, na ontvangst van het verzoek aan de betrokkenen gemotiveerd kenbaar maken. Gelijktijdig informeert GGD GHOR Nederland de betrokkenen over de mogelijkheid om een klacht in te dienen bij de Functionaris Gegevensbescherming en/of de Autoriteit Persoonsgegevens.

8.4 Vaststellen identiteit van persoon die het verzoek indient

Een verzoek wordt alleen in behandeling genomen nadat de identiteit van de betrokkene is vastgesteld. Indien GGD GHOR Nederland twijfelt aan de identiteit van de betrokkenen of aan die van degene die namens de betrokkenen een verzoek indient, vraagt GGD GHOR Nederland aanvullende informatie om de identiteit te vast

te stellen. De beslistermijn wordt opgeschort gedurende de periode dat de betreffende betrokkene nalaat gehoor te geven aan het verzoek om de aanvullende informatie te verstrekken.