Document 9.1

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 vereningsbureau 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 persoonsgegevens;

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.

Document 9.2

Procedure meldplicht datalekken GGD GHOR Nederland

Inhoudsopgave

Inleiding

GGD GHOR Nederland heeft als verwerkingsverantwoordelijke op grond van de Algemene Verordening Gegevensbescherming (AVG) een verplichting om datalekken te melden, tenzij het waarschijnlijk is dat de inbreuk in verband met persoonsgegevens een laag risico inhoudt voor de rechten en vrijheden van betrokkenen. Daarnaast is GGD GHOR Nederland verantwoordelijk voor de afhandeling van datalekken wanneer dat expliciet is overeengekomen. Dit betekent dat wanneer een vermoeden van een datalek aanwezig is of een datalek wordt ontdekt[1], GGD GHOR Nederland moet beoordelen of er sprake is van een datalek en of het datalek moet worden gemeld bij de Autoriteit Persoonsgegevens en of de getroffen betrokkenen.

Het datalek moet om die reden direct na ontdekking aan het Privacy Office worden gemeld. Een datalek kan binnen GGD GHOR Nederland door iedereen worden gemeld. Voor sommige verwerkers of projecten bestaan echter specifieke afspraken over de procedure tot melden en dus ook wie meldt. Wanneer een (vermoedelijk) datalek bekend is binnen GGD GHOR Nederland, zal deze binnen een termijn van uiterlijk 72 uur worden beoordeeld en afgehandeld c.q. gemeld bij de Autoriteit Persoonsgegevens. Om die reden wordt onderzocht of een melding aan de Autoriteit Persoonsgegevens noodzakelijk is en of de getroffen betrokkenen op de hoogte moet worden gesteld.

Dit document bevat de procedure hoe een interne datalekmelding door het Privacy Office in behandeling wordt genomen en op welke wijze een (mogelijk) datalek wordt afgehandeld, in overeenstemming met de AVG. In het kader van deze procedure zullen er drie beoordelingen plaatsvinden:

1. Beoordeling of de melding een datalek inhoudt;
2. Indien er sprake is van een datalek, beoordeling of het datalek bij de Autoriteit Persoonsgegevens moet worden gemeld;
3. Daaropvolgend wordt beoordeeld of het datalek eveneens aan de betrokkene moet worden gemeld.

We spreken van een datalek als er een inbreuk is op de beveiliging van persoonsgegevens (beveiligingsincident). Bij een datalek gaat het om onrechtmatige toegang tot, vernietiging (alsook verlies), wijziging of vrijkomen van persoonsgegevens van betrokkenen. Onder een datalek valt dus niet alleen het vrijkomen (lekken) van persoonsgegevens, maar ook de onrechtmatige verwerking van persoonsgegevens.

Voorbeelden van datalekken zijn:

- Een kwijtgeraakte USB-stick met persoonsgegevens (ook als deze is versleuteld);
- Een gestolen laptop;
- Een verkeerd gestuurde e-mail met persoonsgegevens;
- Het verstrekken van persoonsgegevens aan de verkeerde persoon;
- Onrechtmatig inzien van een dossier;
- Een inbraak in een databestand door een hacker.

[1] Dit kan een datalek zijn dat zich binnen GGD GHOR Nederland, bij een verwerker of bij een partij waarmee GGD GHOR Nederland gezamenlijke verwerkingsverantwoordelijke is, heeft plaatsgevonden.

2. Beoordeling aanmelding datalek

Het beoordelen van de aanmelding van een (vermoedelijk) datalek omvat de volgende stappen:

1. De melding dient te worden gedaan bij het Privacy Office[2] (privacyoffice@ggdghor.nl) met een ingevuld intern datalekformulier. Het Privacy Office bevestigt de ontvangst van de melding aan de melder. De periode van 72 uur voor het melden van het datalek bij de Autoriteit Persoonsgegevens gaat in op het moment dat het datalek is dan wel wordt ontdekt.[3]
2. Het Privacy Office registreert de ontvangen melding van het (vermoedelijke) datalek in het datalekregister.

2.1. First Response Team

Het datalek wordt eerst behandeld door het First Response Team. Bij ontvangst van de melding wordt door het Privacy Office het First Response Team direct bij elkaar geroepen. Het First Response Team bestaat uit:

- Privacy Office[4]
- Functionaris voor de Gegevensbescherming
- Chief Information Security Officer (CISO)
- Duty officer (alleen wanneer noodzakelijk)
- Verantwoordelijke manager

1. Het Privacy Office controleert de melding en stelt vast of er sprake is van een datalek conform de AVG. Als nodig, vraagt het Privacy Office de Functionaris Gegevensbescherming om advies. Als in de melding informatie ontbreekt, vraagt het Privacy Office deze informatie op. Indien er sprake is van een datalek, zorgt het Privacy Office dat een afspraak met het First Response Team wordt ingepland.
2. Het First Response Team komt bijeen en bespreekt het datalek. Als extra informatie nodig is, zal gezamenlijk worden bepaald welke informatie nodig is en zal het Privacy Office dit opvragen.
3. Indien blijkt dat er sprake is van een datalek met grote gevolgen voor een of meerdere betrokkenen en/of de organisatie, wordt direct opgeschaald naar het Second Response Team. Zie hiervoor paragraaf 2.2 voor onderhavige procedure.
4. Het First Response Team overweegt of het datalek (voorlopig) bij de Autoriteit Persoonsgegevens moet worden gemeld. De Functionaris Gegevensbescherming geeft hierover advies aan de overige leden van het First Response Team. Indien het First Response Team geen doorslaggevende keuze kan maken, beslist de verantwoordelijke manager. Indien het First Response Team/verantwoordelijke manager afwijkt van het advies van de Functionaris Gegevensbescherming, dient dat door het First Response Team gemotiveerd te worden.
5. Vervolgens wordt besproken welke technische maatregelen genomen dienen te worden om het datalek (beveiligingsincident) te herstellen en/of mogelijke schade te reduceren. Het First Response Team bespreekt ook welke overige organisatorische maatregelen dienen te worden genomen om het datalek in de toekomst te beperken dan wel voorkomen.

---

[2] Het Privacy Office wordt bemand door de volgende rollen: de Privacy Lead en Privacy Officer(s).

[3] De termijn van 72 uur gaat niet in op het moment dat het Privacy Office bevestigt dat de melding een datalek is. Dit kan anders zijn indien de melding van een vermoedelijk datalek zodanig onduidelijk is en uitgebreid onderzoek vergt. In dat geval is er sprake van het ontdekken van het datalek op het moment dat daadwerkelijk bekend wordt dat er sprake is van een datalek.

[4] Behoudens uitzonderingen, sluit per melding slechts één afgevaardigde van het Privacy Office aan bij het overleg van het First Response Team.

6. De verantwoordelijke manager is verantwoordelijk voor de doorvoering van de maatregelen. Hierbij kan de CISO, een informatiemanager en/of het Privacy Office worden geraadpleegd.
7. Daaropvolgend wordt overwogen of het datalek moet worden gemeld aan de betrokkene(n). Dit is slechts het geval als er sprake is van een hoog risico voor de rechten en vrijheden van de betrokkene. De Functionaris Gegevensbescherming geeft hierover advies. Indien het First Response Team geen doorslaggevende keuze kan maken, beslist de verantwoordelijke manager. Als wordt afgeweken van het advies van de Functionaris Gegevensbescherming, dient dat door het First Response Team/verantwoordelijke manager te worden gemotiveerd.
8. Indien de betrokkene over het datalek zal worden geïnformeerd, wordt afgestemd wat de inhoud van de mededeling zal zijn. Dit zal in samenwerking met het Privacy Office, de CISO en de verantwoordelijke manager gebeuren. De verantwoordelijke manager zal contact opnemen met de betrokkene.
9. Als wordt gekozen voor een schriftelijke benadering, stelt het Privacy Office in samenwerking met de CISO en de verantwoordelijke manager een bericht op, waarna deze door een communicatiemedewerker wordt beoordeeld. De communicatiemedewerker laat het bericht een laatste keer beoordelen door het Privacy Office en Functionaris Gegevensbescherming. Het definitieve bericht wordt door of namens de verantwoordelijke manager aan de betrokkene(n) verstuurd.
10. Ten slotte wordt de melding, waarom er wel of geen (voorlopige) melding wordt gemaakt bij de Autoriteit Persoonsgegevens en de afhandeling daarvan vastgelegd in het datalekregister door het Privacy Office.

2.2. Second Response Team

Indien sprake is van een datalek met grote gevolgen voor een of meerdere betrokkenen en/of grote gevolgen voor GGD GHOR NL, wordt direct het Second Response Team bijeengeroepen. Het Second Response Team bestaat uit:

- Privacy Office[5]
- Functionaris Gegevensbescherming
- CISO
- Duty officer (indien noodzakelijk)
- Algemeen directeur
- Verantwoordelijke manager
- Communicatiemedewerker

1. Het Privacy Office zorgt dat het Second Response Team met spoed bijeenkomt om het datalek te bespreken.
2. Het Second Response Team komt bijeen om het gemelde datalek te bespreken. Het Second Response Team overweegt of het datalek (voorlopig) bij de Autoriteit Persoonsgegevens moet worden gemeld. De Functionaris Gegevensbescherming geeft hierover advies aan de overige leden van het Second Response Team. Het aanwezige directielid heeft de doorslaggevende keuze. Als wordt afgeweken van het advies van de Functionaris Gegevensbescherming, dient dat door de aanwezige directielid te worden gemotiveerd.

[5] Behoudens uitzonderingen, sluit per melding slechts één afgevaardigde van het Privacy Office aan bij het overleg van het First Response Team.

3. Vervolgens wordt besproken welke technische maatregelen genomen dienen te worden om het datalek (beveiligingsincident) te herstellen en/of mogelijke schade te reduceren. Tevens wordt afgestemd welke overige organisatorische maatregelen dienen te worden genomen om het datalek in de toekomst te beperken dan wel voorkomen.
4. De verantwoordelijke manager is verantwoordelijk voor de doorvoering van de maatregelen. Hierbij kan de CISO, een informatiemanager en/of het Privacy Office worden geraadpleegd.
5. Daaropvolgend wordt overwogen of het datalek moet worden gemeld aan de betrokkene(n). Dit is slechts het geval als er sprake is van een hoog risico voor de rechten en vrijheden van de betrokkene. De Functionaris Gegevensbescherming geeft hierover advies. Indien wordt afgeweken van het advies van de Functionaris Gegevensbescherming, dient dat door de aanwezige directielid te worden gemotiveerd.
6. Indien de betrokkene over het datalek zal worden geïnformeerd, wordt afgestemd wat de inhoud van de mededeling zal zijn. Dit zal in samenwerking met het Privacy Office, de CISO en de directie gebeuren.
7. Als wordt gekozen voor een schriftelijke benadering, stelt het Privacy Office in samenwerking met de CISO en een communicatiemedewerker een bericht op, waarna deze door de directie wordt beoordeeld. De directie laat het bericht een laatste keer beoordelen door de Functionaris Gegevensbescherming en de CISO. Het definitieve bericht wordt vanuit de directie aan de betrokkene(n) verstuurd.
8. Ten slotte wordt het datalek, waarom er wel of geen (voorlopige) melding wordt gemaakt bij de Autoriteit Persoonsgegevens en de afhandeling daarvan vastgelegd in het datalekregister.

3. Besluit tot melding

In het First Response Team wordt onderling besloten of een (voorlopige) melding bij de Autoriteit Persoonsgegevens wordt ingediend en welke passende maatregelen bij het geconstateerde datalek dienen te worden getroffen. Indien het First Response Team afwijkt van het advies van de Functionaris Gegevensbescherming, dient dit door het First Response Team te worden gemotiveerd. Uitsluitend de algemeen directeur bevoegd is tot het besluiten of een datalek gemeld moet worden bij de Autoriteit Persoonsgegevens, op aangeven van de Teamlead Privacy Office en de Functionaris Gegevensbescherming.

In het Second Response Team wordt in onderling overleg besproken of een (voorlopige) melding bij de Autoriteit Persoonsgegevens wordt ingediend en welke passende maatregelen dienen te worden getroffen. De Algemeen Directeur bepaalt hierbij of het datalek (voorlopig) wordt gemeld en welke vervolgstappen worden ondernomen. Indien door de aanwezige directielid wordt afgeweken van het advies van de Functionaris Gegevensbescherming, dient dat te worden gemotiveerd.

4. Melding aan de Autoriteit Persoonsgegevens

De (voorlopige) melding aan de Autoriteit Persoonsgegevens omvat de volgende stappen.

1. Het Privacy Office vult het online meldformulier van de Autoriteit Persoonsgegevens in op grond van verstrekte informatie op het interne meldformulier en mondelinge of schriftelijke aanvullingen op basis van uitvragen voor extra informatie. Wanneer de informatie nog niet volledig bekend is, wordt eerst een voorlopige melding gedaan.

2. Een kopie van de melding wordt opgeslagen in de hiervoor bestemde map door het Privacy Office binnen de werkomgeving van het Privacy Office.
3. De Functionaris Gegevensbescherming en de directie ontvangen een afschrift van de (voorlopige) melding ter informatie.
4. Bij een voorlopige melding worden later de ontbrekende informatie verzameld en een definitieve melding door het Privacy Office gedaan. Deze melding wordt direct gedaan als de ontbrekende informatie bekend zijn.
5. Ingeval het besluit tot het melden van een datalek door het First Response Team is besloten, zorgt het Privacy Office ervoor dat de verantwoordelijke manager hierover wordt geïnformeerd. De directie ontvangt een kopie van de melding.

5. Melding aan de betrokkenen

Tijdens het overleg wordt in het First Response Team of in het Second Response Team besproken of de betrokkene(n) over het datalek wordt/worden geïnformeerd. Daarbij worden de volgende zaken nagegaan:

- Zijn de betrokkenen en hun bereikbaarheidsgegevens allemaal bekend?
- Op welke manier worden de betrokkenen geïnformeerd (telefonisch en/of schriftelijk)?
- Wanneer worden de betrokkenen geïnformeerd?
- Door wie worden de betrokkenen geïnformeerd?
- Wat wordt de inhoud van de boodschap aan de betrokkenen?

Indien wordt gekozen voor een schriftelijke benadering, stelt het Privacy Office samen met communicatie een bericht op, waarna deze door een communicatiemedewerker wordt beoordeeld. De communicatiemedewerker laat het bericht een laatste keer beoordelen door het Privacy Office en Functionaris Gegevenbescherming. Het definitieve bericht wordt door de verantwoordelijke manager of door de directie aan de betrokkene(n) verstuurt. Wie het bericht zal versturen, is afhankelijk uit welk Response Team het besluit tot mededeling aan de betrokkene(n) is genomen.

Indien niet kan worden gemeld aan de betrokkene(n) of een groot aantal betrokkenen door het datalek zijn getroffen, waardoor de betrokkene(n) niet individueel kunnen worden geïnformeerd, zal gekozen worden voor een algemene verklaring. De algemene verklaring zal op dezelfde wijze worden opgesteld als het bericht aan de betrokkene(n). Waar nodig zal door GGD GHOR Nederland (tijdelijk) een contactpunt voor de betrokkenen worden opgezet, zodat betrokken op een gepaste wijze hun vragen ten aanzien het datalek kunnen stellen.

6. Interne registratie en bewaarplicht melding datalek

6.1. Interne meldingenregistratie

Het Privacy Office houdt een interne registratie bij (incl. nummering) van de ontvangen datalek meldingen. Dit gebeurt in het daarvoor bedoelde datalekregister. Als geen melding aan de Autoriteit Persoonsgegevens of aan de betrokkene(n) wordt gedaan, worden de overwegingen hiervan door het Privacy Office in het datalekregister vastgelegd. In het datalekregister wordt in dat geval ten minste gemotiveerd waarom volgens het First of Second Response Team er geen sprake is van een datalek en/of waarom er geen sprake is van een hoog risico voor de rechten en vrijheden betrokkenen. Deze registratie blijft bewaard.

In geval van melding aan de Autoriteit Persoonsgegevens wordt een kopie hiervan opgeslagen op een daartoe vooraf bepaalde locatie die toegankelijk is voor het Privacy Office en de Functionaris Gegevensbescherming. Een kopie wordt daarnaast verzonden aan de directie.

Het Privacy Office neemt alle relevante informatie over de melding op in het datalekregister, waaronder de berichtgeving aan betrokkenen over het datalek. Het datalekregister bevat ten minste:

- Feiten en omstandigheden van het datalek;
- Gevolgen van het datalek;
- De betrokken persoonsgegevens; en
- De genomen corrigerende technische en/of organisatorische maatregelen.

Het datalekregister is niet openbaar, ook niet voor de organisatie. Geaggregeerde informatie kan worden gebruikt ten behoeve van het verslag van de Functionaris Gegevensbescherming aan de directie.

6.2. Bewaartermijn

De AVG bevat geen specifieke regels over de bewaartermijnen van datalekmeldingen. Om die reden zijn de bewaartermijnen uit de beleidsregels van de Autoriteit Persoonsgegevens ten aanzien van de Wet bescherming persoonsgegevens (Wbp) vooralsnog aangehouden.[6]

Er geldt in beginsel een bewaartermijn van minimaal één jaar (*na melding autoriteit dan wel betrokkenen).* In de volgende gevallen geldt een bewaartermijn van minimaal drie jaar:

- Indien er sprake is geweest van een datalek, maar de beveiligingsmaatregelen bieden voldoende bescherming om de melding aan de betrokkenen achterwege te laten *(evalueer periodiek of de melding aan betrokkene alsnog gedaan moet worden);*
- Indien er zwaarwegende redenen zijn geweest om de melding aan de betrokkene achterwege te laten *(evalueer periodiek of de melding aan betrokkene alsnog gedaan moet worden).*

7. Vervolgstappen

Op grond van de aard en omvang van het datalek worden door de verantwoordelijke vervolgstappen genomen. Deze kunnen betrekking hebben op aanvullende organisatorische en technische beveiligingsmaatregelen. De maatregelen kunnen gericht zijn op het opheffen van het specifieke datalek en/of op het voorkomen van vergelijkbare datalekken op andere plaatsen in de organisatie.

De Functionaris Gegevensbescherming kan toezicht houden of de vervolgstappen en de genomen maatregelen (binnen een redelijke termijn) zijn doorgevoerd.

8. Evaluatie datalekken

De afhandeling van het datalek wordt na een vastgestelde periode geëvalueerd. Deze periode wordt bepaald in onderling overleg tussen de verantwoordelijke voor de melding en het First Response Team.

Het First Response Team evalueert alle gemelde en afgehandelde datalekken jaarlijks.

---

[6] De meldplicht datalekken in de Wet bescherming persoonsgegevens (Wbp), Autoriteit Persoonsgegevens, geraadpleegd op 21 juli 2021: https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/beleidsregels_meldplicht_datalekken_wbp.pdf>

Bijlage 1. Meldingsformulier vermoedelijk datalek GGD GHOR Nederland

Ik wil een mogelijk datalek melden

Aanmelder

Naam:
Vestiging:
Telefoonnummer:
E-mail:
Afdeling:
Plaats:

Beschrijving van het incident:

Wanneer vond de inbreuk plaats? (Kies een of meerdere van de volgende opties en vul waar nodig aan.)

- ○ Op (datum)
- ○ Tussen (begindatum periode) (einddatum periode)
- ○ Nog niet bekend

Duurt de inbreuk nog steeds voort?

- ○ Ja
- ○ Nee
- ○ Niet bekend

Wanneer is het ontdekt en door wie?

Op (datum):
Naam:
Telefoon:
E-mail:

Van hoeveel personen zijn persoonsgegevens mogelijk betrokken bij de inbreuk (Vul de aantallen in)

Minimaal:
Maximaal:

Van wie zijn de persoonsgegevens betrokken bij de inbreuk? Denk hierbij aan werknemers, zakelijke partners, (minderjarige) patiënten, leveranciers, e.d.

Wat is de aard van de inbreuk? (U kunt meerdere mogelijkheden aankruisen)

- ○ Lezen (vertrouwelijkheid)
- ○ Kopiëren
- ○ Veranderen (integriteit)
- ○ Verwijderen of vernietigen (beschikbaarheid)
- ○ Diefstal
- ○ Nog niet bekend

Wat is de aard van het incident waarbij er een inbreuk op de beveiliging van de persoonsgegevens is geweest?

- ○ Apparaat, gegevensdrager (bijv. USB-stick) en/of papier met persoonsgegevens kwijtgeraakt of gestolen
- ○ Brief of postpakket met persoonsgegevens kwijtgeraakt of geopend retour ontvangen
- ○ Hacking, malware (bijv. Ransomware) en/of phishing waarbij persoonsgegevens o.a. ontoegankelijk zijn gemaakt of zijn buitgemaakt
- ○ Onbevoegde toegang (autorisatie) tot het inzien en/of wijzigen en/of aanpassen en/of verwijderen van persoonsgegevens
- ○ Persoonsgegevens bij oud papier gezet
- ○ Persoonsgegevens mondeling gedeeld met onbevoegde ontvanger
- ○ Persoonsgegevens nog aanwezig op afgedankt apparaat of op afgedankte gegevensdrager (bijv. USB stick)
- ○ Persoonsgegevens per ongeluk gepubliceerd
- ○ Persoonsgegevens van verkeerde klant getoond in klantportaal
- ○ Persoonsgegevens verstuurd of afgegeven aan verkeerde ontvanger
- ○ Overig, zoals: _____

Om welk type persoonsgegevens gaat het? (U kunt meerdere mogelijkheden aankruisen)

- ○ Naam
- ○ Adres- en woonplaatsgegevens
- ○ Telefoonnummers
- ○ E-mailadressen of andere adressen voor elektronische communicatie
- ○ Toegangs- of identificatiegegevens (bijvoorbeeld inlognaam / wachtwoord of klantnummer
- ○ Financiële gegevens (bijvoorbeeld rekeningnummer, creditcardnummer)
- ○ Burgerservicenummer (BSN) of sofinummer
- ○ Paspoortkopieën of kopieën van andere legitimatiebewijzen
- ○ Geslacht, geboortedatum en/of leeftijd
- ○ Persoonsgegevens betreffende strafrechtelijke veroordelingen en strafbare feiten of daarmee verband houdende veiligheidsmaatregelen
- ○ Overige gegevens, namelijk (vul aan): _____

Heeft de inbreuk betrekking op bijzondere categorieën persoonsgegevens?

- ○ Persoonsgegevens waaruit iemands ras of etnische afkomst blijkt
- ○ Persoonsgegevens waaruit iemands politieke opvattingen blijken
- ○ Persoonsgegevens waaruit iemands religieuze of levensbeschouwelijke overtuigingen blijken
- ○ Persoonsgegevens waaruit iemands lidmaatschap van een vakbond blijkt
- ○ Gegevens met betrekking tot iemands seksueel gedrag of seksuele gerichtheid
- ○ Gegevens over iemands gezondheid
- ○ Genetische gegevens
- ○ Biometrische gegevens

Waren de persoonsgegevens op het moment van de inbreuk versteuteld (bijv. Bitlocker), gehasht of een andere manier onbegrijpelijk of ontoegankelijk gemaakt voor onbevoegden. (Kies een van de volgende optoes en vul aan waar nodig)

- ○ Ja
- ○ Nee
- ○ Deels, namelijk: (vul aan): _____

Als de persoonsgegevens geheel of gedeeltelijk onbegrijpelijk of ontoegankelijk zijn gemaakt, op welke manier is dit dan gebeurd?

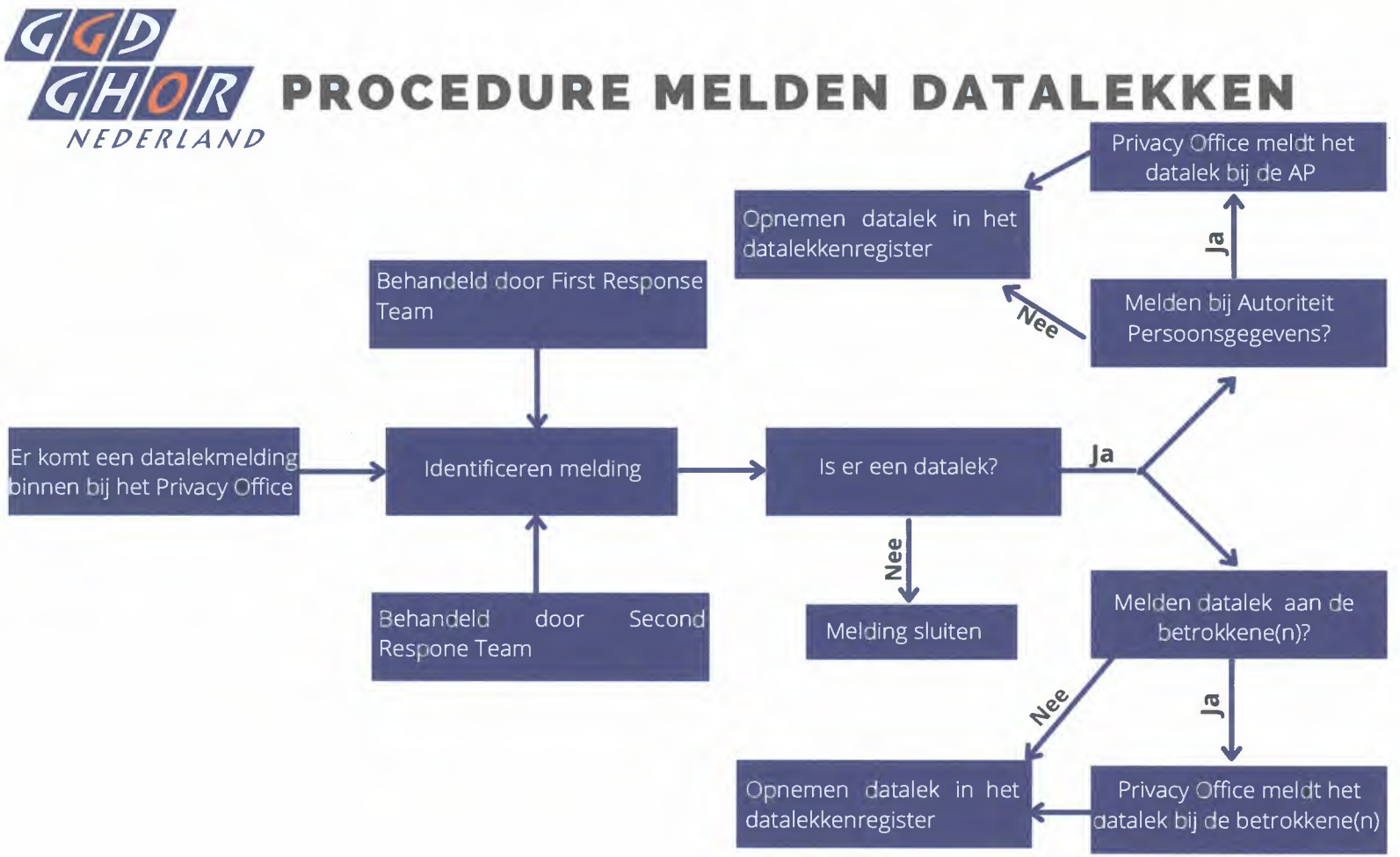
Welke passende maatregelen zijn er in de tussentijd getroffen om de inbreuk aan te pakken en/of om verdere inbreuken te voorkomen?

Was er een andere organisatie betrokken bij de inbreuk?

- ○ Nee
- ○ Ja naam van de andere organisatie is:

In welke hoedanigheid was de organisatie betrokken bij de inbreuk?

Bijlage 2. Stroomdiagram procedure melden datalekken GGD GHOR Nederland



Document 9.3

SOC Team
Zwarte Woud 2
3524 SJ Utrecht
Telefoon 030 252 3004
Email [redacted]

Checklist Onboarding Applicaties

Eerst controleren, daarna aanschaffen

Definitieve versie: 1.02

Opdrachtgever	[redacted]
Auteur	[redacted]
Kwaliteitszorg	
Rapportnummer	
Classificatie	Intern
Status	Definitief
Datum	26 maart 2021
File Naam	Checklist Onboarding Applicaties

Template versie 0.02

Inhoud

Documentbeheer

Versiebeheer

Versie	Datum	Auteur	Omschrijving verandering	Status
0.01	09-03-2021	[redacted]	Initiële opzet	Concept
0.02	10-03-2021	[redacted]	Beveiligingsmaatregelen	Concept
0.90	10-03-2021	[redacted]	Proces	Concept
1.00	11-03-2021	[redacted]	Finaliseren na accordering	Definitief
1.01	25-03-2021	[redacted]	Verbeteren op basis feedback	Concept
1.02	26-03-2021	[redacted]	Finaliseren na accordering	Definitief

Gecontroleerd door

Versie	Datum	Naam	Functie
0.90	10-03-2021	[redacted]	[redacted]
1.01	26-03-2021		

Geautoriseerd door

Versie	Datum	Naam	Functie
1.00	11-03-2021	[redacted]	[redacted]
1.02	26-03-2021	[redacted]	[redacted]

Gerelateerde documenten

Documenttitel	Omschrijving
Algemene Verordening Gegevensbescherming (AVG)	Europese privacy-verordening
Baseline Informatiebeveiliging Overheid (BIO)	Nederlandse richtlijn, gebaseerd op de internationale standaard ISO/IEC 27001:2013
NEN 7510 – Informatiebeveiliging in de Zorg	Nederlandse richtlijn, gebaseerd op de internationale standaard ISO/IEC 27001:2013 en specifiek voor de zorgsector

Volgende review en/of herziening, plus accordering (tenzij eerdere update)

Datum	Functie voor bewaking
01-06-2021	[redacted]

1. Inleiding

Met deze checklist wil GGD GHOR borgen dat applicaties die worden aangeschaft passen binnen de infrastructuur van de GGD'en en op een veilige en betrouwbare wijze gegevens verwerken.

1.1. Scope en doelgroep

Deze checklist is van toepassing op alle applicaties die worden aangeschaft ter ondersteuning van de werkzaamheden van GGD GHOR en de GGD'en.

De doelgroep bestaat uit de GGD'en, partners voor de digitale infrastructuur en leveranciers van SaaS-oplossingen, programmatuur en apparatuur.

1.2. Rollen en verantwoordelijkheden

De Chief Information Officer (CIO) van GGD GHOR is verantwoordelijk voor de inhoud van deze checklist.

De inkopende afdelingsmanager is verantwoordelijk voor het invullen van de checklist en deze toe te zenden aan het Security Operating Center (SOC) van GGD GHOR.

Het SOC is verantwoordelijk om de checklist te verifiëren en te interveniëren als blijkt dat een aan te schaffen applicatie leidt tot risico's voor de beschikbaarheid van de dienstverlening, of de integriteit of vertrouwelijkheid van de te verwerken gegevens.

Interventies door het SOC worden gerapporteerd aan de CIO, de Chief Information Security Officer (CISO) en de Functionaris voor de Gegevensbescherming (FG) van GGD GHOR.

1.3. Richtlijn voor het gebruik van de checklist

De checklist bevat een aantal aandachtspunten. Deze zijn niet voor alle toepassingen relevant en, waar nodig, mogen op 'Niet van toepassing' (Nvt) worden gezet. Van belang is dat wordt nagedacht over de betreffende aandachtspunten en weloverwogen wordt vastgesteld of deze wel of niet van toepassing zijn.

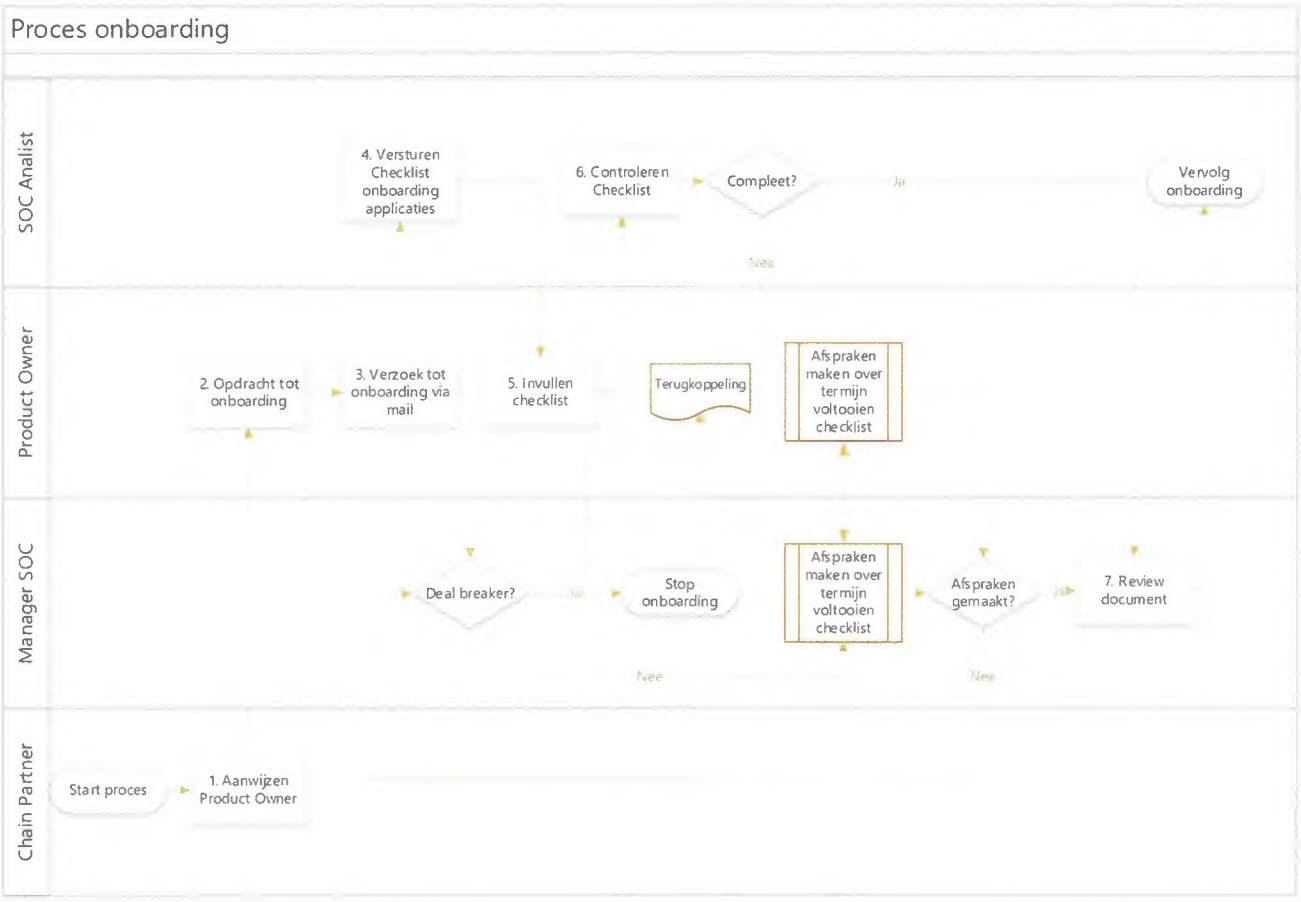
1.4. Review of audit door het SOC

Desgewenst kan het SOC een review of audit uitvoeren op een applicatie. Dit wordt met name geadviseerd voor applicaties die gevoelige persoonsgegevens verwerken of die onderdeel zijn van een essentieel bedrijfsproces bij een GGD.

1.5. Onderhoud van de checklist

Het SOC onderhoudt de checklist en communiceert deze naar de GGD'en.

2. Proces voor controle onboarding



De stappen binnen het proces zijn:

1. **Aanwijzen Product Owner**
   Deze wordt aangewezen door de ketenpartner;

2. **Opdracht tot onboarding**
   De Product Owner besluit dat controle nodig is, gezien een mogelijk risico dat kan worden veroorzaakt door de installatie of het gebruik van de applicatie;

3. **Verzoek tot onboarding via mail**
   De Product Owner licht het SOC in over de voorgenomen aanschaf van de applicatie;

4. **Versturen checklist onboarding applicaties**
   Het SOC stuurt de actuele versie van de checklist aan de Product Owner;

5. **Invullen checklist**
   De Product Owner laat de checklist invullen, bij voorkeur in overleg met de lokale CISO en, indien sprake is van het verwerken van persoonsgegevens, met de lokale Privacy Officer (PO) en/of FG. De ingevulde checklist wordt naar het SOC gestuurd;

6. **Controleren checklist**
   Het SOC controleert de ingevulde checklist op volledigheid en verifieert de risico-inschatting van de Product Owner. Dit kan leiden tot verder overleg, onder andere over aanpassing van de risico-classificatie of over de te treffen mitigerende maatregelen. Dit kan eventueel leiden tot het afwijzen van de applicatie. Als naar de mening van het SOC een getrouw beeld is gevormd van de risico's en risicomitigatie, wordt de review van de ingevulde checklist afgerond;

7. **Review document**
   De Manager SOC neemt het besluit of de onboarding van de applicatie kan worden gecontinueerd.

3. Eisen voor applicaties

In de onderstaande tabel is de 'Vlag' bedoeld om het risico van een eventuele afwijking weer te geven, met:

Vlag	Ernst	Toelichting
H	Hoog	Onacceptabel risico voor integere en vertrouwelijke gegevensverwerking.
M	Midden	Risico voor integere en vertrouwelijke gegevensverwerking, waarvoor complexe compenserende maatregelen nodig zijn.
L	Laag	Risico voor integere en vertrouwelijke gegevensverwerking, waarvoor eenvoudige compenserende maatregelen nodig zijn.

3.1. Werknemers en applicatiegebruikers

Nr.	Beveiligingsmaatregel	J	N	Nvt	Vlag	Toelichting
1.1	Awareness van gebruikers en beheerders voor integriteit en vertrouwelijkheid bij het gebruik is geborgd					
1.2	De gebruiker ziet een notificatie bij opstarten, waarin staat dat de regels moeten worden gevolgd					
1.3	Procedures voor uitgeven, muteren en innemen van accounts en authenticatiemiddelen, uitgeven en resetten van wachtwoorden etc. zijn ingericht					
1.4	Gebruikers zijn ingelicht dat accounts niet mogen worden gedeeld					
1.5	Use cases voor verdacht en onverdacht gebruik (voor analyse in het SIEM) zijn beschikbaar					
1.6	Monitoren van verdachte en onverdachte activiteiten van de gebruiker is mogelijk					

3.2. Coding en systeemdocumentatie

Nr.	Beveiligingsmaatregel	J	N	Nvt	Vlag	Toelichting
2.1	Een formele standaard wordt gevolgd voor ontwerpdocumentatie					
2.2	Het functioneel ontwerp is beschikbaar					
2.3	Het technisch ontwerp is beschikbaar					
2.4	Het autorisatiebeheer in de applicatie kan worden gekoppeld aan het centrale rollenbeheer					
2.5	Logging en monitoring zijn beschikbaar					
2.6	De schaalbaarheid is geborgd, dus capaciteit kan worden uitgebreid					
2.7	Het uitvoeren van op beveiliging gerichte testsessies is mogelijk					
2.8	Formele standaard documentatie over interface(s) is beschikbaar					
2.9	De koppelingen garanderen volledige en correcte gegevensoverdracht					
2.10	Cryptografie is toegepast op de applicatie en API's					

3.3. Testen op kwetsbaarheden in de beveiliging

Nr.	Beveiligingsmaatregel	J	N	Nvt	Vlag	Toelichting
3.1	Kwetsbaarheden bij het verzamelen van informatie, zoals het ontdekken van toepassingen, toegangspunten voor toepassingen en meer zijn in kaart gebracht en gemitigeerd of formeel geaccepteerd door de risico-eigenaar					
3.2	Kwetsbaarheden in configuratiebeheer, zoals toegang tot beheerdersinterfaces, SSL-zwakte, XSS-risico en meer zijn in kaart gebracht en gemitigeerd of formeel geaccepteerd door de risico-eigenaar					
3.3	Autorisatiekwetsbaarheden en authenticatiekwetsbaarheden zoals het opsommen van gebruikers, het doorlopen van paden, het manipuleren van rollen en meer zijn in kaart gebracht en gemitigeerd of formeel geaccepteerd door de risico-eigenaar					
3.4	Kwetsbaarheden in gegevensvalidatie, zoals SQL / LDAP / SMTP / code-injectie zijn in kaart gebracht en gemitigeerd of formeel geaccepteerd door de risico-eigenaar					
3.5	Penetratietests zijn uitgevoerd en gepland					

3.4. Infrastructuur, back-up en monitoring

Nr.	Beveiligingsmaatregel	J	N	Nvt	Vlag	Toelichting
4.1	De continuïteit van de applicatie is geborgd via redundante voorzieningen					
4.2	Een realtime beveiligingsservice is toegepast					
4.3	Back-ups worden regelmatig of realtime geproduceerd en restore-testen worden regelmatig uitgevoerd					
4.4	Maatregelen zijn getroffen om back-ups te beschermen tegen ransomware, via isolatie en controles					
4.5	Monitoring van blootgestelde services					
4.6	Monitoring van interne diensten					
4.7	Gevoelige omgevingen zijn geïsoleerd op netwerkniveau, door een veilige netwerkarchitectuur met VLAN's					
4.8	De toegang tot interne services en IP-adressen is beheerst					
4.9	OS- en docker-images zijn up-to-date					
4.10	Gezag en toezicht op de Data Base Administrators (DBA's) is ingericht					
4.11	Gebruik van een Ontwikkel, Test, Acceptatie en Productie (OTAP)-straat is geborgd					

3.5. Organisatie

Nr.	Beveiligingsmaatregel	J	N	Nvt	Vlag	Toelichting
5.1	De applicatie past binnen de veiligheidscultuur					
5.2	De applicatie draagt bij aan transparantie over diensten en gegevensverzamelingen					
5.3	De applicatie is niet in strijd met het beleid inzake openbare veiligheid					
5.4	De applicatie is niet in strijd met de naleving van het organisatiebeleid en wettelijke vereisten					
5.5	De applicatie past binnen het beleid voor bedrijfscontinuïteit en noodherstel					

3.6. Dienstverlener

Nr.	Beveiligingsmaatregel	J	N	Nvt	Vlag	Toelichting
6.1	De uptime in de SLA, die door dienstverlener wordt verstrekt, is geverifieerd					
6.2	Technische ondersteuning is beschikbaar vanuit de dienstverlener					
6.3	De geldigheid van certificaten, zoals ISO 27001, NEN 7510 etc. is geverifieerd					
6.4	Er is geverifieerd dat uitwijk mogelijk is naar een beveiligde uitwijklocatie					
6.5	Er is geverifieerd dat gegevens worden versleuteld tijdens transport via het interne netwerk					
6.6	Er is geverifieerd dat persoonsgegevens worden verwerkt conform de AVG (dit betreft PII – Personal Identifiable Information)					

Nr.	Beveiligingsmaatregel	J	N	Nvt	Vlag	Toelichting
6.7	Er is geverifieerd dat persoonsgegevens alleen binnen de Europese Economische Ruimte (EER) worden opgeslagen en altijd binnen de EER blijven					

3.7. Beheerprocessen

3.7.1. Autorisatiebeheer

Nr.	Beveiligingsmaatregel	J	N	Nvt	Vlag	Toelichting
7.1	Gedocumenteerde procedures voor autorisatiebeheer zijn beschikbaar					
7.2	Het gezamenlijk gebruik van een account is niet toegestaan (dus geen groepsaccounts, altijd individuele accounts)					
7.3	Rollen zijn gebaseerd op aantoonbare functiescheiding					
7.4	Accounts zijn ingedeeld in logisch opgebouwde groepen (zoals Organizational Units – OU's – in de AD), bijvoorbeeld als eindgebruiker, administrator, mailbox, service-account etc.					
7.5	Het afdwingen van een wachtwoordbeleid dat voldoet aan de BIO is ingericht					
7.6	Een adequate lock-out policy ter voorkoming van brute force aanval met raden van wachtwoorden is ingericht					
7.7	2-Factor Authenticatie is toegepast					
7.8	Periodieke controles op accounts ter voorkoming van vervuiling worden uitgevoerd					
7.9	Rapportage over accounts is beschikbaar					

3.7.2. Configuratiebeheer

Nr.	Beveiligingsmaatregel	J	N	Nvt	Vlag	Toelichting
8.1	Configuratie-items zijn geregistreerd in een Configuratie Management Data Base (CMDB), inclusief hun BIV-classificatie					
8.2	Een procedure voor het beheer en onderhoud van de CMDB is ingericht					
8.3	Rapportagefaciliteiten voor de configuratie-items in de CMDB zijn beschikbaar					

3.7.3. Wijzigingenbeheer

Nr.	Beveiligingsmaatregel	J	N	Nvt	Vlag	Toelichting
9.1	De classificatie van wijzigingen is ingericht					
9.2	De registratie en afhandeling van wijzigingen is ingericht					
9.3	De bewaking en tijdige afhandeling van wijzigingen is ingericht					
9.4	De evaluatie van mislukte wijzigingen is ingericht					
9.5	Rapportage over wijzigingen, wel of niet succesvol geïmplementeerd, en tijdigheid is ingericht					

3.7.4. Incident- en probleembeheer

Nr.	Beveiligingsmaatregel	J	N	Nvt	Vlag	Toelichting
10.1	De classificatie voor reguliere incidenten en beveiligingsincidenten is ingericht					
10.2	De registratie- en afhandeling van incidenten en problemen is ingericht					
10.3	De bewaking van tijdige afhandeling van incidenten en problemen is ingericht					
10.4	Incidentevaluatie en -preventie is ingericht					
10.5	Een reactieplan voor beveiligingsincidenten (incident response plan) is opgesteld en actueel					

3.7.5. Beveiligingsbeheer

Nr.	Beveiligingsmaatregel	J	N	Nvt	Vlag	Toelichting
11.1	De fysieke toegangsbeveiliging is ingericht					
11.2	De bescherming tegen phishing is ingericht					
11.3	De bescherming tegen DDoS-aanvallen is ingericht					
11.4	De bescherming tegen ransomware is ingericht					
11.5	Domeinen zijn afgeschermd, waar nodig					
11.6	De bescherming van domeinnamen is ingericht					
11.7	Het gebruik van beveiligde wifi-verbindingen is geborgd					
11.8	Het gebruik van Virtual Private Network (VPN), waar noodzakelijk, is geborgd					
11.9	De Demilitarized Zone (DMZ) is ingericht					
11.10	Intrusion Detection System (IDS) en Intrusion Prevention System (IPS) zijn ingericht					
11.11	De web application firewall en reverse proxy zijn ingericht					

Bijlage A Lijst van afkortingen

Afkorting	Toelichting
AD	Active Directory, Microsoft
API	Application Programming Interface
AVG	Algemene Verordening Gegevensbescherming
BIO	Baseline Informatiebeveiliging Overheid
BIV	Beschikbaarheid, Integriteit en Vertrouwelijkheid
CIO	Chief Information Officer
CISO	Chief Information Security Officer
CMDB	Configuration Management Data Base
DBA	Data Base Administrator
DMZ	Demilitarized Zone. Dit is een nul-netwerk met een binnen-firewall en een buiten-firewall, om te zorgen voor isolatie tussen netwerken.
DDoS	Distributed Denial of Service
EER	Europese Economische Ruimte
FG	Functionaris voor de Gegevensbescherming
IAM	Identity and Access Management
IDS	Intrusion Detection System
IP	Internet Protocol
IPS	Intrusion Prevention System
LDAP	Lightweight Directory Access Protocol. Het netwerkprotocol dat beschrijft hoe gegevens uit directoryservices moeten worden benaderd.
OS	Operating System
OTAP	Ontwikkel, Test, Acceptatie en Productie
OU	Organizational Units in de AD
PII	Personal Identifiable Information
PO	Privacy Officer
SaaS	Software as a Service. Dit zijn veelal applicaties die via een web-oplossing worden geleverd.
SDLC	Software Development Life Cycle
SIEM	Security Information and Event Management
SLA	Service Level Agreement
SMTP	Simple Mail Transfer Protocol
SOC	Security Operating Center
SQL	Structured Query Language. Dit is een programmeertaal voor toegang tot gegevensbestanden.
SSL	Secure Socket Layer. SSL is verouderd. TLS 1.2 of hoger dient te worden gebruikt.
VLAN	Virtual Local Area Network
VPN	Virtual Private Network. Dit is een versleutelde verbinding over internet.
XSS	Cross Site Scripting

Document 9.4

SOC Team
Zwarte Woud 2
3524 SJ Utrecht
Telefoon 030 252 3004
Email [redacted]

INTERN

Procesbeschrijving

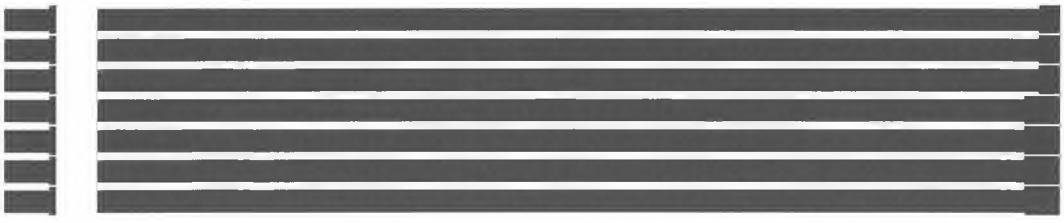
Triage bij CoronIT

Versie: 1.02

Opdrachtgever	[redacted]
Auteur	[redacted]
Kwaliteitszorg	[redacted]
Rapportnummer	A.16.1.3.a
Classificatie	Intern
Status	Definitief
Datum	24 juni 2021
File Naam	Procesbeschrijving Triage CoronIT

Template versie 0.03

Inhoud



Documentbeheer

Versiebeheer

Versie	Datum	Auteur	Omschrijving verandering	Status
0.01	15-03-2021	[redacted]	Initiële opzet	Concept
0.02	15-03-2021	[redacted]	Uitwerking hoofdproces en besluiten	Concept
0.04	22-03-2021	[redacted]	Uitwerking onderzoek en bronnen	Concept
0.05	24-03-2021	[redacted]	Uitwerken delen met Politie	Concept
1.00	24-03-2021	[redacted]	Finaliseren	Definitief
1.01	24-04-2021	[redacted]	Criteria verwijderd	Definitief
1.02	24-06-2021	[redacted]	Uitwerken delen met GGD	Definitief

Gecontroleerd door

Versie	Datum	Naam	Functie
1.01	24-04-2021	[redacted]	[redacted]
1.02	24-06-2021	[redacted]	[redacted]

Geautoriseerd door

Versie	Datum	Naam	Functie
1.01	24-04-2021	[redacted]	[redacted]
1.02	24-06-2021	[redacted]	[redacted]

Gerelateerde documenten

Documenttitel	Omschrijving
Algemene Verordening Gegevensbescherming (AVG)	Europese privacy-verordening
Baseline Informatiebeveiliging Overheid (BIO)	Nederlandse richtlijn, gebaseerd op de internationale standaard ISO/IEC 27001:2013
NEN 7510 – Informatiebeveiliging in de Zorg	Nederlandse richtlijn, gebaseerd op de internationale standaard ISO/IEC 27001:2013 en specifiek voor de zorgsector
Criteria Triage CoronIT	Vertrouwelijk document, versie 1.00, 24 april 2021

Volgende review en/of herziening, plus accordering (tenzij eerdere update)

Datum	Functie
31-12-2021	[redacted]

1. Inleiding

Met deze procesbeschrijving voor het proces Triage wil GGD GHOR NL uniformiteit borgen bij het uitvoeren van onderzoeken naar afwijkend gedrag van medewerkers, via analyses van het gedrag zoals dat is vastgelegd in de logs. Deze activiteit is onderdeel van hoofdstuk A.16 'Beheer van informatiebeveiligingsincidenten' van NEN 7510.

1.1. Scope en doelgroep

Deze procesbeschrijving is van toepassing op de door het SOC uit te voeren onderzoeken naar afwijkend gedrag van medewerkers, die werken met privacygevoelige informatie.

Het doel is te voorkomen dat privacygevoelige informatie door individuele medewerkers voor andere doeleinden wordt gebruikt dan waarvoor deze door de GGD'en is verzameld.

De doelgroep bestaat uit de SOC-analisten bij GGD GHOR NL.

1.2. Rollen en verantwoordelijkheden

De Manager SOC is verantwoordelijk voor de inhoud van het proces Triage.

Het SOC voert de onderzoeken uit, gericht op het borgen van de integriteit en vertrouwelijkheid van de te verwerken privacygevoelige informatie.

De resultaten van onderzoeken door het SOC worden gerapporteerd aan de CIO en de Chief Information Security Officer (CISO) van GGD GHOR NL.

1.3. Doelstelling volgens NEN 7510 norm A.16.1.3

Informatiebeveiligingsincidenten omvatten onder andere corruptie of onbedoelde openbaarmaking van persoonsgegevens en persoonlijke gezondheidsinformatie.

Doelstelling A.16 'Beheer van informatiebeveiligingsincidenten' in NEN 7510 is '*Een consistente en doeltreffende aanpak bewerkstelligen van het beheer van informatiebeveiligingsincidenten, met inbegrip van communicatie over beveiligingsgebeurtenissen en zwakke plekken in de beveiliging*'.

Beheersmaatregel A.16.1.3 'Rapportage van zwakke plekken in de informatiebeveiliging' stelt:

- '*Van medewerkers en contractanten die gebruikmaken van de informatiesystemen en -diensten van de organisatie, moet worden geëist dat zij de in systemen of diensten waargenomen of vermeende zwakke plekken in de informatiebeveiliging registreren en rapporteren*'.

1.4. Onderhoud van de procesbeschrijving

Het SOC onderhoudt de procesbeschrijving en communiceert deze naar de betrokken partners.

Document 9.5

Convenant gegevensuitwisseling gezamenlijk verantwoordelijken

INHOUD

De ondergetekenden:

1) De Stichting Projectenbureau Publieke Gezondheid en Veiligheid Nederland, gevestigd te (3524 SJ) Utrecht aan het adres Zwarte Woud 2, ingeschreven in het handelsregister onder KvK nummer 41184548, hierna eveneens te noemen "**GGD GHOR Nederland**", rechtsgeldig vertegenwoordigd door [redacted];

en

2) De Gemeentelijke Gezondheidsdienst Rotterdam-Rijnmond gevestigd te Rotterdam aan de Schiedamsedijk 95, ingeschreven in het handelsregister onder KvK nummer 24483298, hierna eveneens te noemen "**GGD**", rechtsgeldig vertegenwoordigd door [redacted];

3) De Gemeentelijke Gezondheidsdienst IJsselland, gevestigd te Zwolle aan de Zeven Alleetjes 1, ingeschreven in het handelsregister onder KvK nummer 50594761, hierna eveneens te noemen "**GGD**", rechtsgeldig vertegenwoordigd door [redacted];

4) De Gemeentelijke Gezondheidsdienst Noord- en Oost-Gelderland, gevestigd te Warnsveld aan de Rijksstraatweg 65, ingeschreven in het handelsregister onder KvK nummer 51158957, hierna eveneens te noemen "**GGD**", rechtsgeldig vertegenwoordigd door [redacted];

5) De Gemeentelijke Gezondheidsdienst Haaglanden, gevestigd te Den Haag aan het Westeinde 128, ingeschreven in het handelsregister onder KvK nummer 63629216, hierna eveneens te noemen "**GGD**", rechtsgeldig vertegenwoordigd door [redacted];

6) De Gemeentelijke Gezondheidsdienst Twente, gevestigd te Enschede aan de Nijverheidstraat 30, ingeschreven in het handelsregister onder KvK nummer 8195873, hierna eveneens te noemen "**GGD**", rechtsgeldig vertegenwoordigd door [redacted];

7) De Gemeentelijke Gezondheidsdienst Drenthe, gevestigd te Assen aan de Mien Ruysweg 1, ingeschreven in het handelsregister onder KvK nummer 1139196, hierna eveneens te noemen "**GGD**", rechtsgeldig vertegenwoordigd door [redacted];

8) De Gemeentelijke Gezondheidsdienst Hart voor Brabant, gevestigd te 's-Hertogenbosch aan de Vogelstraat 2, ingeschreven in het handelsregister onder KvK nummer 17247544, hierna eveneens te noemen "**GGD**", rechtsgeldig vertegenwoordigd door [redacted];

9) De Gemeentelijke Gezondheidsdienst Hollands Midden, gevestigd te Leiden aan de Parmentierweg 49, ingeschreven in het handelsregister onder KvK nummer 27365105, hierna eveneens te noemen "**GGD**", rechtsgeldig vertegenwoordigd door [redacted];

10) De Veiligheidsregio Fryslân, gevestigd te Leeuwarden aan de Harlingertrekweg 58, ingeschreven in het handelsregister onder KvK nummer 1175778, hierna eveneens te noemen "**GGD**", rechtsgeldig vertegenwoordigd door [redacted];

11) De Dienst Gezondheid & Jeugd Zuid-Holland Zuid, gevestigd te Dordrecht aan de Karel Lotsyweg 40, ingeschreven in het handelsregister onder KvK nummer 54038111, hierna eveneens te noemen "**GGD**", rechtsgeldig vertegenwoordigd door [redacted];

12) De Gemeentelijke Gezondheidsdienst GGD Brabant-Zuidoost, gevestigd te Eindhoven aan het Clausplein 10, ingeschreven in het handelsregister onder KvK nummer 50451154, hierna eveneens te noemen "**GGD**", rechtsgeldig vertegenwoordigd door [redacted];

13) De Gemeentelijke Gezondheidsdienst Zuid-Limburg, gevestigd te Heerlen aan het Overloon 2, ingeschreven in het handelsregister onder KvK nummer 14131474, hierna eveneens te noemen "**GGD**", rechtsgeldig vertegenwoordigd door de [redacted];

14) De Gemeentelijke Gezondheidsdienst Amsterdam, gevestigd te Amsterdam aan de Nieuwe Achtergracht 100, ingeschreven in het handelsregister onder KvK nummer 70036896 , hierna eveneens te noemen "**GGD**", rechtsgeldig vertegenwoordigd door [redacted];

15) De Gemeentelijke Gezondheidsdienst Zeeland, gevestigd te Goes aan de Westwal 37, ingeschreven in het handelsregister onder KvK nummer 20171605, hierna eveneens te noemen "**GGD**", rechtsgeldig vertegenwoordigd door [redacted];

16) De Gemeentelijke Gezondheidsdienst Hollands Noorden , gevestigd te Alkmaar aan de Hertog Aalbrechtweg 22, ingeschreven in het handelsregister onder KvK nummer 37159559, hierna eveneens te noemen "**GGD**", rechtsgeldig vertegenwoordigd door [redacted];
3

17) De Veiligheids- en gezondheidsregio Gelderland-Midden, gevestigd te Arnhem aan de Eusebiusbuitensingel 43, ingeschreven in het handelsregister onder KvK nummer 9217053, hierna eveneens te noemen "**GGD**", rechtsgeldig vertegenwoordigd door [redacted];

18) De Gemeentelijke Gezondheidsdienst Gelderland-Zuid, gevestigd te Nijmegen aan de Groenewoudseweg 275, ingeschreven in het handelsregister onder KvK nummer 9212724, hierna eveneens te noemen "**GGD**", rechtsgeldig vertegenwoordigd door [redacted];

19) De Gemeentelijke Gezondheidsdienst GGD Groningen, gevestigd te Groningen aan het Hanzeplein 120, ingeschreven in het handelsregister onder KvK nummer 62089781, hierna eveneens te noemen "**GGD**", rechtsgeldig vertegenwoordigd door [redacted];

20) De Gemeentelijke Gezondheidsdienst GGD Regio Utrecht, gevestigd te Zeist aan de Dreef 5, ingeschreven in het handelsregister onder KvK nummer 50909185, hierna eveneens te noemen "**GGD**", rechtsgeldig vertegenwoordigd door [redacted];

21) De Gemeenschappelijke Gezondheidsdienst GGD Zaanstreek-Waterland, gevestigd te Zaandam aan de Vurehout 2, ingeschreven in het handelsregister onder KvK nummer 34370893, hierna eveneens "**GGD**", rechtsgeldig vertegenwoordigd door [redacted];

22) De Gemeentelijke Gezondheidsdienst Gooi & Vechtstreek, gevestigd te Bussum aan de Burgemeester de Bordestraat 80, ingeschreven in het handelsregister onder KvK nummer 32152259, hierna eveneens te noemen "**GGD**", rechtsgeldig vertegenwoordigd door [redacted];

23) De Gemeentelijke Gezondheidsdienst Kennemerland, gevestigd te Haarlem aan de Zijlweg 200, ingeschreven in het handelsregister onder KvK nummer 34377971 , hierna eveneens te noemen "**GGD**", rechtsgeldig vertegenwoordigd door [redacted];

24) De Gemeentelijke Gezondheidsdienst GGD Flevoland, gevestigd te Lelystad aan de Noorderwagenstraat 2, ingeschreven in het handelsregister onder KvK nummer 32170514, hierna eveneens te noemen "**GGD**", rechtsgeldig vertegenwoordigd door [redacted];

25) De Gemeentelijke Gezondheidsdienst GGD Limburg-Noord, gevestigd te Blerick aan de Drie Decembersingel 50, ingeschreven in het handelsregister onder KvK nummer 14110234, hierna eveneens te noemen "**GGD**", rechtsgeldig vertegenwoordigd door [redacted];

26) De Gemeentelijke Gezondheidsdienst GGD West-Brabant, gevestigd te Breda aan de Doornboslaan 225-227, ingeschreven in het handelsregister onder KvK nummer 20164916, hierna eveneens te noemen "**GGD**", rechtsgeldig vertegenwoordigd door [redacted];

De partijen sub 1 t/m 26, hierna *gezamenlijk* te noemen: "**Partijen**", de partijen sub 2 t/m 26 ook "**GGD'en**";

OVERWEGENDE DAT:

- Partijen in een specifieke relatie tot elkaar staan en vanuit hun publiekrechtelijke taken (voortvloeiend uit de Wet publieke gezondheid) dienen te acteren ter bevordering van de publieke gezondheid.
- De hierboven genoemde specifieke relatie tussen Partijen onder meer blijkt uit de vastgestelde Verenigingsgovernance van GGD GHOR Nederland versie 29 juni 2018.
- Partijen in een eerder stadium met elkaar zijn overeengekomen dat GGD GHOR Nederland het opzetten van een landelijk informatiesysteem met daaraan verbonden hard- en softwarekoppelingen ten behoeve van de bestrijding van COVID-19 door de GGD'en ('CoronIT') coördineert en ten behoeve van die bestrijding in Nederland zorg draagt voor de continuïteit van het systeem en de voornoemde bestrijding.
- De ingebruikneming van CoronIT met zich meebrengt dat persoonsgegevens worden verwerkt en daarmee wet- en regelgeving van toepassing is die de bescherming van persoonsgegevens beoogt, waaronder de Algemene Verordening Gegevensbescherming ("**AVG**") en de daarop van toepassing zijnde Uitvoeringswet.
- De verwerking van persoonsgegevens via CoronIT ex artikel 6 lid 1 sub c en e AVG een rechtmatige basis heeft, namelijk artikel 22 e.v. en artikel 29 Wet publieke gezondheid.
- Op basis van de AVG en de wijze waarop CoronIT dataverkeer tussen Partijen mogelijk maakt, het van belang is dat – afhankelijk van de datastroom tussen Partijen – wordt beoordeeld wie (mede)verwerkingsverantwoordelijke of (sub)verwerker is.
- Partijen op basis van jurisprudentie van het Hof van Justitie van de Europese Unie uit 2018 hun rol ten aanzien van de verwerking van persoonsgegevens via CoronIT hebben geanalyseerd. Partijen tot het oordeel zijn gekomen dat zij, ten aanzien van de voornoemde beoordeling, ex artikel 26 AVG *gezamenlijk verwerkingsverantwoordelijken* zijn.
- Artikel 26 lid 1 AVG onder meer bepaalt dat gezamenlijk verwerkingsverantwoordelijken op transparante wijze hun respectieve verantwoordelijkheden voor de nakoming van de verplichtingen uit de AVG vaststellen door middel van een onderlinge regeling.
- Partijen de voornoemde verplichting wensen vast te leggen in dit document (hierna "**Convenant**");
- Het Convenant als zodanig niet een op zichzelf staand document is, maar onderdeel vormt van een eerder (gedocumenteerd) besluitvormingsproces tussen Partijen en daaruit voortvloeiende contractuele afspraken namens Partijen.

KOMEN OVEREEN:

Artikel 1: Definities

1. Aan de hierna genoemde begrippen wordt dezelfde betekenis gegeven als bedoeld in art. 4 AVG: Persoonsgegevens,Verwerking, Verwerkingsverantwoordelijke, Betrokkene, Inbreuk in verband met persoonsgegevens, Toezichthoudende autoriteit.

Artikel 2: Scope

1. Dit Convenant heeft uitsluitend betrekking op de verwerking van persoonsgegevens ter uitvoering van werkzaamheden verbonden aan CoronIT, Partijen genoegzaam bekend.

2. Partijen hebben in Bijlage I de aard, het soort persoonsgegevens en de categorieën van betrokkenen omschreven.

3. Het Convenant is een leidend document tussen Partijen betreffende de verwerking van persoonsgegevens via CoronIT. Partijen sluiten onderling geen andersoortige overeenkomsten betreffende de verwerking van persoonsgegevens via CoronIT. Andersoortige overeenkomsten tussen Partijen betreffende CoronIT kunnen op geen enkele wijze afbreuk doen aan rechten en plichten als vastgelegd in het Convenant noch aan de doelstelling die ten grondslag ligt aan CoronIT en welke – geparafraseerd – inhoudt:
   • CoronIT maakt het mogelijk om de bestrijding van COVID-19 doelmatig en efficiënt in de verschillende regio's van het land te organiseren;

   • CoronIT voorziet in laagdrempelige en veilige toegang tot gegevens van te testen en geteste personen en de daarbij behorende testresultaten;

   • CoronIT wordt ondersteund door een landelijk te gebruiken testplatform.

4. Partijen verplichten zich tegenover elkaar op een zodanig pro-actieve en transparante wijze te handelen dat de doelstelling die ten grondslag ligt aan CoronIT, wordt gerealiseerd.

Artikel 4: Rollen en verhoudingen

1. GGD GHOR Nederland draagt er, met behulp van door haar geselecteerde partijen welke zijn weergegeven in Bijlage 2, zorg voor dat CoronIT operationeel beschikbaar is voor de GGD'en. Daartoe heeft GGD GHOR Nederland namens Partijen ook contractuele afspraken gemaakt met de in Bijlage 2 genoemde partijen, waaronder – indien daartoe een verplichting bestaat - afspraken over de verwerking van persoonsgegevens in verwerkersovereenkomsten.

2. GGD GHOR Nederland fungeert ten opzichte van de in Bijlage 2 genoemde partijen als exclusief aanspreekpunt voor aangelegenheden die CoronIT betreffen. De GGD'en verbinden zich om eventuele kwesties betreffende CoronIT welke gerelateerd zijn aan een of meerdere van de in Bijlage 2 genoemde partijen, te allen tijde eerst voor te leggen aan GGD GHOR Nederland. De laatstgenoemde verplichting geldt niet voor eventuele eerste-lijns-hulp welke ten behoeve van de GGD'en door GGD GHOR Nederland is afgesloten bij een of meerdere van de partijen genoemd in Bijlage 2.

3. Iedere GGD is zelfstandig verantwoordelijk voor het gebruik van CoronIT bij de uitvoering van aan haar toebedeelde taken. Onder gebruik wordt mede verstaan de invoer, verwijdering, aanpassing, beschikbaarstelling, vernietiging van Persoonsgegevens binnen CoronIT. Zonder nadrukkelijke toestemming dan wel wettelijke verplichting, zal GGD GHOR Nederland geen persoonsgegevens van betrokkenen - in de zin van de AVG - binnen CoronIT invoeren, aanpassen, verwijderen en/of vernietigen.

4. Partijen zijn zelfstandig verantwoordelijk voor het nemen van interne technische en organisatorische maatregelen ter voorkoming van ongeautoriseerde toegang en verwerking van Persoonsgegevens binnen CoronIT.

Artikel 5: Gegevensverwerking

1. Ieder van de Partijen is zelfstandig verantwoordelijk voor de verwerking van de Persoonsgegevens in eigen beheer zijnde. Partijen verwerken de Persoonsgegevens alleen op de wijze zoals in dit Convenant is overeengekomen en zullen Persoonsgegevens niet op een andere manier verwerken, tenzij dit gezamenlijk is overeengekomen.

2. Partijen verwerken Persoonsgegevens binnen CoronIT uitsluitend in overeenstemming met geldende wet- en regelgeving, met name de AVG en de Uitvoeringswet AVG.

3. Onverminderd hetgeen is bepaald in artikel 4.4 van het Convenant, komen Partijen overeen dat de in Bijlage 2 opgesomde maatregelen ten tijde van het sluiten van het Convenant de basismaatregelen zijn welke aantoonbaar nageleefd dienen te worden ter uitvoering van de verplichting als opgenomen in artikel 24 en 32 AVG. Partijen zullen – via het alsdan bestaande overlegorgaan – jaarlijks de in Bijlage 2 getroffen maatregelen evalueren en toetsen of deze toereikend zijn in de zin van voornoemde artikelen. Eventuele aanpassingen die voortvloeien uit de evaluatie, worden door Partijen zo spoedig mogelijk ten uitvoer gebracht.

4. Indien een van de Partijen wordt benaderd (bezoek/e-mail/brief/telefoon) door een toezichthoudende autoriteit (waaronder de Autoriteit Persoonsgegevens) of een gerechtelijk bevel ontvangt betreffende een kwestie die op enigerlei wijze gekoppeld is of kan worden gekoppeld aan CoronIT zal zij de andere Partij daarover direct informeren. Daartoe zal de betreffende Partij in ieder geval onmiddellijk en onverwijld GGD GHOR Nederland informeren via de Functionaris Gegevensbescherming van de GGD GHOR Nederland via een e-mail aan het adres fg@ggdghor.nl en [redacted] via [redacted]. De desbetreffende Partij verplicht zich geen inhoudelijk standpunt tegenover de toezichthoudende autoriteit in te nemen voordat afstemming heeft plaatsgevonden met GGD GHOR Nederland.

Artikel 6: Wettelijke grondslag voor de gegevensverwerkingen

1. Partijen verwerken de persoonsgegevens voor de uitvoering van de plichten gesteld in de Wet publieke gezondheid (art. 22 e.v.).

2. Partijen dragen er zorg voor dat aan de AVG en Uitvoeringswet AVG (UAVG) wordt voldaan.

Artikel 7: Rechten van betrokkenen

1. Indien een betrokkene zich wendt tot een GGD, zal de desbetreffende Partij zelfstandig uitvoering geven aan haar verplichtingen die voortvloeien uit de AVG en andere wet- en regelgeving tegenover die betrokkene. Mocht een GGD van oordeel zijn dat een andere GGD uitvoering dient te geven aan verplichtingen tegenover die betrokkene, dan stemmen de GGD'en dit onderling af zonder dat dit rechten van betrokkenen schaadt. Mocht een GGD van mening zijn dat de medewerking van GGD GHOR Nederland noodzakelijk is voor het nakomen van verplichtingen tegenover een betrokkene, dan zal de betreffende GGD dit gemotiveerd verzoeken aan GGD GHOR Nederland.

2. Indien een betrokkene zich rechtstreeks wendt tot GGD GHOR Nederland, dan zal GGD GHOR Nederland zo spoedig mogelijk contact opnemen met de GGD die als laatste verbonden is aan deze betrokkene, waarna die GGD uitvoering geeft aan haar verplichtingen als omschreven in artikel 7.1.

3. Iedere GGD is tegenover een betrokkene, waarvan zij Persoonsgegevens verwerkt, zelfstandig verplicht om uitvoering te geven aan de informatieverplichtingen als genoemd in artikel 13 en 14 AVG.

Artikel 8: Inbreuk in verband met persoonsgegevens

1. Indien zich een Inbreuk in verband met persoonsgegevens bij één van de Partijen voordoet, handelt iedere Partij deze volledig in eigen verantwoordelijkheid en conform de vereisten van de AVG af.

2. Ieder der Partijen is zelfstandig gehouden tot een afweging van eventuele maatregelen – en zo nodig het treffen van maatregelen – indien zij bekend raakt met een inbreuk in verband met persoonsgegevens in de zin van artikel 33 AVG. Alvorens een van de Partijen op basis van een afweging als bedoeld in het voorgaande lid besluit tot een melding aan de bevoegde toezichthoudende autoriteit, zal zij daarover voorafgaand afstemming hebben met de andere Partij.

Artikel 10: Geheimhouding

1. Partijen en alle personen die voor of namens Partijen werkzaamheden uitvoeren, zijn verplicht tot geheimhouding met betrekking tot de Persoonsgegevens waarvan zij kennis kunnen nemen, met uitzondering van de wettelijke voorschriften die de verstrekking verplichten.

2. Partijen zorgen ervoor dat de geheimhoudingsverplichting van de in lid 1 genoemde personen bij een verklaring is ondertekend ofwel onderdeel uitmaakt van de ondertekende arbeidsovereenkomst.

3. Na het beëindigen van dit Convenant, blijft de geheimhoudingsplicht van kracht.

Artikel 11: Aansprakelijkheid

1. Schade welke voortvloeit uit het niet nakomen van verplichtingen uit het Convenant, komt voor rekening van de partij(en) die toerekenbaar is tekort geschoten. Ingeval schade ontstaat op grond van dit Convenant zullen Partijen met elkaar in overleg treden.

2. Partijen verplichten zich jegens elkaar om bij constatering van fouten in de gegevensuitwisseling, zoals bedoeld in dit Convenant, elkaar daarvan zo spoedig mogelijk op de hoogte te stellen. Bij constatering van fouten zetten Partijen zich maximaal in om de ontstane fout te herstellen en gegevens op correcte wijze uit te wisselen. Een en ander conform de vastgestelde normen die daarvoor zijn beschreven.

3. Ieder van de Partijen is verantwoordelijk voor de schade ontstaan uit de onrechtmatige verwerkingen van persoonsgegevens die onder eigen verantwoordelijkheid conform dit Convenant zijn verwerkt en eventueel de daarvoor opgelegde sancties door de Autoriteit Persoonsgegevens en de schadevorderingen vanuit de betrokkenen.

Artikel 12: Tussentijde wijzigingen van het convenant en evaluatie

1. Partijen verbinden zich om minimaal een keer per jaar het Convenant en de daaruit voortvloeiende verplichtingen en werkzaamheden te evalueren. Daarbij verklaren Partijen zich bereid om het Convenant aan te passen indien een evaluatie, inbreuk in verband met persoonsgegevens, gewijzigde wet- en regelgeving, beleid van toezichthoudende instanties dan wel de stand der techniek dit vereist.

Uitgangspunt daarbij is dat het Convenant te allen tijde ten minste aan de wettelijke vereisten ter zake de bescherming van Persoonsgegevens dient te voldoen.

2. GGD GHOR Nederland is penvoerder met betrekking tot het Convenant. Eventuele wijzigingen ten aanzien van Bijlage 4 worden door Partijen gecommuniceerd via het mailadres fg@ggdghor.nl en zullen door GGD GHOR Nederland zo spoedig mogelijk met Partijen worden gedeeld.

2. Aanpassingen van het Convenant en/of de overige Bijlagen kan alleen plaatsvinden nadat daarover besluitvorming tot stand is gekomen via het Directieteam op advies van de FG.

.

Artikel 13: Toepasselijk recht en geschillenbeslechting

1. Op dit Convenant en op alle geschillen, die daaruit voortvloeien of daarmee samenhangen, is in Nederland van toepassing zijnde recht van toepassing.

2. Alle geschillen die tussen de Partijen ontstaan in verband met dit Convenant worden voorgelegd aan de bevoegde rechter van de rechtbank Midden-Nederland locatie Utrecht.

Artikel 14: Contactpersonen

1. In Bijlage 4 bij het Convenant is een lijst met contactpersonen opgenomen waarin ieder der Partijen is vertegenwoordigd. Daar waar het Convenant Partijen verplicht elkaar te informeren, zal die informatie gericht dienen te zijn tot de contactpersoon als genoemd is Bijlage 4. Om te voorkomen dat informatie een Partij niet bereikt zal ieder der Partijen ook een algemeen e-mail account opnemen in Bijlage 4 zodat in geval van absentie of wijzigingen van functies dan wel het personeelsbestand, de informatiedeling in dat opzicht is geborgd.

Artikel 15: Overige bepalingen

1. Indien één of meerdere bepalingen van dit Convenant nietig blijken te zijn of door de rechter nietig worden verklaard, behouden de overige bepalingen van dit Convenant hun rechtskracht. Partijen zullen voor (elk van) de nietige of vernietigde bepaling(en) een rechtsgeldige bepaling in de plaats stellen die zoveel mogelijk benaderd wat Partijen beoogden overeen te komen.
2. Indien onduidelijkheid bestaat omtrent de uitleg van één of meerdere bepalingen in onderhavige overeenkomst, dan dient de uitleg plaats te vinden 'naar de geest' van deze bepalingen.
3. Ten tijde van ondertekening behoorden tot onderhavige overeenkomst de volgende Bijlagen:
    a. Bijlage 1: Overzicht met verwerkingen van persoonsgegevens en verwerkingsdoeleinden
    b. Bijlage 2: Overzicht met beveiligingsmaatregelen
    c. Bijlage 3: Verwerkers
    d. Bijlage 4: Contactgegevens

Aldus overeengekomen en ondertekend in ……Utrecht……., op ……30 april…….2020

1. de Stichting Projectenbureau Publieke Gezondheid en Veiligheid Nederland, rechtsgeldig vertegenwoordigd door [redacted];

[redacted]

Aldus overeengekomen en ondertekend in Rotterdam, op 12-06-2020

2. De Gemeentelijke Gezondheidsdienst Rotterdam-Rijnmond gevestigd te Rotterdam aan de Schiedamsedijk 95, ingeschreven in het handelsregister onder KvK nummer 24483298, hierna eveneens te noemen "**GGD**", rechtsgeldig vertegenwoordigd door [redacted]

[redacted]

Aldus overeengekomen en ondertekend in Zwolle op 30 april 2020

3. De Gemeentelijke Gezondheidsdienst IJsselland, gevestigd te Zwolle aan de Zeven Alleetjes 1, ingeschreven in het handelsregister onder KvK nummer 50594761, hierna eveneens te noemen "**GGD**", rechtsgeldig vertegenwoordigd door [redacted];

[redacted]

Aldus overeengekomen en ondertekend in Warnsveld, op 6 mei 2020

4. De Gemeentelijke Gezondheidsdienst Noord- en Oost-Gelderland, gevestigd te Warnsveld aan de Rijksstraatweg 65, ingeschreven in het handelsregister onder KvK nummer 51158957, hierna eveneens te noemen "**GGD**", rechtsgeldig vertegenwoordigd door [redacted];

[redacted]

Aldus overeengekomen en ondertekend in Den Haag, op 1 mei 2020

5. De Gemeentelijke Gezondheidsdienst Haaglanden, gevestigd te Den Haag aan het Westeinde 128, ingeschreven in het handelsregister onder KvK nummer 63629216, hierna eveneens te noemen "**GGD**", rechtsgeldig vertegenwoordigd door [redacted]

[redacted]

Aldus overeengekomen en ondertekend in ..Enschede....., op ..30/4.....2020

6. De Gemeentelijke Gezondheidsdienst Twente, gevestigd te Enschede aan de Nijverheidstraat 30, ingeschreven in het handelsregister onder KvK nummer 8195873, hierna eveneens te noemen "**GGD**", rechtsgeldig vertegenwoordigd door [redacted]

.....

[redacted]

ekomen en ondertekend in Assen, op 4 mei 2020

7 [redacted] ke Gezondheidsdienst Drenthe, gevestigd te Assen aan de Mien Ruysweg 1, het handelsregister onder KvK nummer 1139196, hierna eveneens te , rechtsgeldig vertegenwoordigd door [redacted]

.....

Aldus overeengekomen en ondertekend in s'-Hertogenbosch, op 4 mei 2020

8. De Gemeentelijke Gezondheidsdienst Hart voor Brabant, gevestigd te 's-Hertogenbosch aan de Vogelstraat 2, ingeschreven in het handelsregister onder KvK nummer 17247544, hierna eveneens te noemen "**GGD**", rechtsgeldig vertegenwoordigd door [redacted];

[redacted]

Aldus overeengekomen en ondertekend in Leiden op 29 april 2020

9. De Gemeentelijke Gezondheidsdienst Hollands Midden, gevestigd te Leiden aan de Parmentierweg 49, ingeschreven in het handelsregister onder KvK nummer 27365105, hierna eveneens te noemen "**GGD**", rechtsgeldig vertegenwoordigd door [redacted];

Aldus overeengekomen en ondertekend in Leeuwarden, op 1 mei 2020

10. De Veiligheidsregio Fryslân, gevestigd te Leeuwarden aan de Harlingertrekweg 58, ingeschreven in het handelsregister onder KvK nummer 1175778, hierna eveneens te noemen "**GGD**", rechtsgeldig vertegenwoordigd door [redacted];

[redacted]

Aldus overeengekomen en ondertekend in Dordrecht, op 30 april 2020

11. De Dienst Gezondheid & Jeugd Zuid-Holland Zuid, gevestigd te Dordrecht aan de Karel Lotsyweg 40, ingeschreven in het handelsregister onder KvK nummer 54038111, hierna eveneens te noemen "**GGD**", rechtsgeldig vertegenwoordigd door de [redacted];

[redacted]

Aldus overeengekomen en ondertekend in Eindhoven op 6 mei 2020

12. De Gemeentelijke Gezondheidsdienst GGD Brabant-Zuidoost, gevestigd te Eindhoven aan het Cla[redacted]het handelsregister onder KvK nummer 50451154, hierna eve[redacted]chtsgeldig vertegenwoordigd door[redacted];

.....[redacted].....

Aldus overeengekomen en ondertekend in Heerlen, op 13-5-2020

13. De Gemeentelijke Gezondheidsdienst Zuid-Limburg, gevestigd te Heerlen aan het Overloon 2, ingeschreven in het handelsregister onder KvK nummer 14131474, hierna eveneens te noemen "**GGD**", rechtsgeldig vertegenwoordigd d[redacted]

Aldus overeengekomen en ondertekend in ...Amsterdam....., op ....30 april....2020

14. De Gemeentelijke Gezondheidsdienst Amsterdam, gevestigd te Amsterdam aan de Nieuwe Achtergracht 100, ingeschreven in het handelsregister onder KvK nummer 70036896 , hierna eveneens te noemen "**GGD**", rechtsgeldig vertegenwoordigd door [redacted]

.....

Aldus overeengekomen en ondertekend in Goes, op 30-4-2020

15. De Gemeentelijke Gezondheidsdienst Zeeland, gevestigd te Goes aan de Westwal 37, ingeschreven in het handelsregister onder KvK nummer 20171605, hierna eveneens te noemen "GGD", rechtsgeldig vertegenwoordigd door [redacted];

[redacted]

.....

Ggd Gemeenschappelijke Gezondheidsdienst Zeeland

Aldus overeengekomen en ondertekend in Alkmaar, op 30/4/2020

16. De Gemeentelijke Gezondheidsdienst Hollands Noorden , gevestigd te Alkmaar aan de Hertog Aalbrechtweg 22, ingeschreven in het handelsregister onder KvK nummer 37159559, hierna eveneens te noemen "GGD", rechtsgeldig vertegenwoordigd door [redacted]

[redacted]

.....

Aldus overeengekomen en ondertekend in Arnhem, op 1 mei 2020

17. De Veiligheids- en gezondheidsregio Gelderland-Midden, gevestigd te Arnhem aan de Eusebiusbuitensingel 43, ingeschreven in het handelsregister onder KvK nummer 9217053, hierna eveneens te noemen "**GGD**", rechtsgeldig vertegenwoordigd door [redacted];

.....

Aldus overeengekomen en ondertekend in ..... Nijmegen ....., op 6 mei 2020

18. De Gemeentelijke Gezondheidsdienst Gelderland-Zuid, gevestigd te Nijmegen aan de Groenewoudseweg 275, ingeschreven in het handelsregister onder KvK nummer 9212724, hierna overeenns te noemen "GGD", rechtsgeldig vertegenwoordigd door [redacted]

[redacted]

.....

Aldus overeengekomen en ondertekend in Gronignen, op 1 mei 2020

19. De Gemeentelijke Gezondheidsdienst GGD Groningen, gevestigd te Groningen aan het Hanzeplein 120, ingeschreven in het handelsregister onder KvK nummer 62089781, hierna eveneens te noemen "**GGD**", rechtsgeldig vertegenwoordigd door [redacted];

[redacted]

Aldus overeengekomen en ondertekend in Zeist , op 30 april .2020

20. De Gemeentelijke Gezondheidsdienst GGD Regio Utrecht, gevestigd te Zeist aan de Dreef 5, ingeschreven in het handelsregister onder KvK nummer 50909185, hierna eveneens te noemen "**GGD**", rechtsgeldig vertegenwoordigd door [redacted]

[redacted]

Aldus overeengekomen en ondertekend in Zaanstad, op 6/5/2020

21. De Gemeenschappelijke Gezondheidsdienst GGD Zaanstreek-Waterland, gevestigd te Zaandam aan de Vurehout 2, ingeschreven in het handelsregister onder KvK nummer 34370893, hierna eveneens "**GGD**", rechtsgeldig vertegenwoordigd door [redacted]

[redacted]

.....

Aldus overeengekomen en ondertekend in Bussum, op 30 april.2020

22. De Gemeentelijke Gezondheidsdienst Gooi & Vechtstreek, gevestigd te Bussum aan de Burgemeester de Bordesstraat 80, ingeschreven in het handelsregister onder KvK nummer 32152259, hierna eveneens te noemen "**GGD**", rechtsgeldig vertegenwoordigd door [redacted]

[redacted]

Aldus overeengekomen en ondertekend in Haarlem op 20 mei 2020

23. De Gemeentelijke Gezondheidsdienst Kennemerland, gevestigd te Haarlem aan de Zijlweg 200, ingeschreven in het handelsregister onder KvK nummer 34377971 , hierna eveneens te noemen "**GGD**", rechtsgeldig vertegenwoordigd door [redacted];

.....

Aldus overeengekomen en ondertekend in Lelystad, op 30 april 2020

24. De Gemeentelijke Gezondheidsdienst GGD Flevoland, gevestigd te Lelystad aan de Noorderwagenstraat 2, ingeschreven in het handelsregister onder KvK nummer 32170514, hierna eveneens te noemen "**GGD**", rechtsgeldig vertegenwoordigd door [redacted];

[redacted]

drs. [redacted]
directeur Publieke Gezondheid

Aldus overeengekomen en ondertekend in ....Venlo...., op 11 juni 2020

25. De Gemeentelijke Gezondheidsdienst GGD Limburg-Noord, gevestigd te Blerick aan de Drie Decembersingel 50, ingeschreven in het handelsregister onder KvK nummer 14110234, hierna eveneens te noemen "**GGD**", rechtsgeldig vertegenwoordigd door [redacted]

[redacted]

Aldus overeengekomen en ondertekend in . , op 2020

26. De Gemeentelijke Gezondheidsdienst GGD West-Brabant, gevestigd te Breda aan de Doornboslaan 225-227, ingeschreven in het handelsregister onder KvK nummer
hierna eveneens te noemen "**GGD**", rechtsgeldig vertegenwoordigd door

Bijlage 1: Overzicht met verwerkingen van persoonsgegevens

Het onderwerp/aard en doel van de Verwerking: Functioneel beheer van de CoronIT applicatie, via welke een test kan worden aangevraagd, de geteste persoon kan worden geregistreerd en gekoppeld aan een barcode, de testresultaten kunnen worden geregistreerd en de uitslag kan worden gecommuniceerd naar de aanvrager en de betrokkene. Bestrijding van COVID-19 kan zo landelijk worden gecoördineerd op basis van de Wet publieke gezondheid. Coronavirussen behoren tot infectiegroep A en de registratie ervan is verplichting op grond van artikel 29 Wet publieke gezondheid .

Het soort Persoonsgegevens: Er worden hoofdzakelijk gegevens verwerkt over de gezondheid, dus bijzondere persoonsgegevens zoals bedoeld in artikel 9 van de AVG waardoor de verwerking in de risicoklasse 'hoog' valt.

Beschrijving categorieën Persoonsgegevens: Er worden 3 categorieën gegevens verwerkt. Deze zijn:

- Contactgegevens en BSN van de geteste persoon;
- Gegevens over de gezondheid van de geteste persoon (anamnese, uitslag test);
- Contactgegevens van de aanvrager (voor het terugkoppelen van het testresultaat).

Beschrijving categorieën Betrokkenen: Iedereen in Nederland die vermoedelijk geïnfecteerd is met het virus en aangemeld is voor een test voor COVID-19. In eerste instantie gaat het om een groep van zorgmedewerkers die getest moet worden, waarna de groep geleidelijk zal worden uitgebreid tot iedereen die vermoedelijk geïnfecteerd is.

Beschrijving categorieën ontvangers van Persoonsgegevens:

- Aanvrager van de test;
- Laboratoria;
- GGD;
- RIVM.

Bewaartermijn: 5 jaar (art. 29 Wet publieke gezondheid)

Bijlage 2: Beveiligingsmaatregelen

Partijen werken aantoonbaar in overeenstemming met IS027001 en NEN 7510. Indien een of meerdere van de hierboven genoemde normen wijziging ondergaat of wordt vervangen door een nieuwe norm, zullen Partijen vanaf het bekend worden van die nieuwe normering binnen redelijke termijn, de beveiliging van de Persoonsgegevens uitvoeren conform de nieuwe normering.

Partijen voldoen aantoonbaar aan de veiligheidseisen voor netwerkverbindingen op basis van NEN7512.

Partijen voldoen aantoonbaar aan de eisen ten aanzien van logging op basis van NEN7513.

Bijlage 3: Verwerkers

1) Topicus Healthcare B.V. gevestigd te 7411HW, Deventer aan de Singel 25 ingeschreven zijnde in het register van de Kamer van Koophandel onder het nummer 64768147.

Contactpersoon Verwerker:	Naam: [redacted] Contactgegevens: [redacted]
FG Verwerker:	Naam: [redacted] Contactgegevens: [redacted]

Document 9.6

Richtlijn afhandeling verwijderingsverzoek Covid-19 (CoronIT & HPZone)

In het kader van de bestrijding van Covid-19 worden bij GGD'en en bij GGD GHOR Nederland persoonsgegevens verwerkt. Er worden persoonsgegevens verwerkt als mensen (betrokkenen) zich laten testen voor Covid-19 (CoronIT) en als de GGD bron- en contactopsporing uitvoert (HPZone). Het kan voorkomen dat betrokkenen deze persoonsgegevens willen laten verwijderen. Dit kunnen zij doen door een verzoek bij de plaatselijke GGD in te dienen. Omdat ten aanzien van de bestrijding van Covid-19 een en ander vanuit GGD GHOR Nederland wordt georganiseerd (zo ook opzet en beheer van CoronIT en koppelingen met HPZone) wordt vanuit GGD GHOR Nederland in deze richtlijn uiteengezet over hoe om te gaan met verwijderingsverzoeken betreffende de gegevensverwerkingen in CoronIT en HPZone, ofwel de verwerkingen aangaande de bestrijding Covid-19.

Deze richtlijn is bedoeld voor medewerkers die bevoegd zijn om verwijderingsverzoeken in het kader van CoronIT en HPZone in behandeling nemen en af te handelen. Hier kan gedacht worden aan de privacy organisatie of een bevoegd persoon binnen het GGD Coronateam. Dit kan per GGD afhangen. Het doel van deze richtlijn is om de verwijderingsverzoeken landelijk zo uniform mogelijk af te handelen.

Ongeacht de richtlijn voor het verwijderen van persoonsgegevens, is het belangrijk dat GGD'en en GGD GHOR Nederland, de verzoeken die op dit moment worden ontvangen als gevolg van de recent bekend geworden datadiefstal, niet alleen procedureel benaderen. Wij als GGD GHOR en de GGD'en begrijpen en voelen heel goed dat de datadiefstal het vertrouwen van mensen kan hebben geschaad en willen hen dus ook zo goed en snel mogelijk helpen bij hun verzoek.

1. Waar heeft de betrokkene recht op?

De betrokkene heeft het recht op vergetelheid.[1] Dit betekent dat in een aantal gevallen de betrokkene de GGD kan vragen om zijn of haar persoonsgegevens te verwijderen. In bepaalde gevallen moet gehoor worden gegeven aan het verzoek van de betrokkene. Er zijn ook een aantal situaties waarin het recht op verwijdering van de persoonsgegevens niet geldt of soms gelden er beperkingen. Deze uitzonderingen, die met name gelden in het kader van infectieziektebestrijding, worden onder paragraaf 3 uiteengezet.

2. Waar moet het verzoek aan voldoen?

Het is van belang dat het verzoek specifiek is. Dat wil zeggen dat verzoek duidelijk moet zijn omschreven. Het ontbreken van een reden mag geen aanleiding vormen om het verzoek te

[1] Artikel 17 AVG.

weigeren. Is het verzoek gebaseerd op emoties of is het verzoek niet helder geformuleerd en laat ruimte voor invulling, vraag de betrokkene het verzoek nader te specificeren.

a) Waar (op welke verwerking) binnen de GGD'en heeft het verzoek specifiek betrekking op?
b) Welke persoonsgegevens wil de betrokkene laten verwijderen?
c) Is het verzoek niet duidelijk, neem contact op met de betrokkene en vraag na wat het verzoek inhoudt. Wil de betrokkene gegevens inzien, laten verwijderen of een klacht indienen? Misschien wel alle drie?
d) Heeft de betrokkene (ook) een inzageverzoek ingediend? Zie hiervoor in dat geval de Richtlijn afhandeling inzageverzoeken covid-19 (CoronIT & HPZone). Handel in dit geval eerst het inzageverzoek af.
e) Een verzoek moet schriftelijk worden ingediend.

3. Wanneer mag het verzoek worden geweigerd?

In onderstaande situatie mag het verwijderingsverzoek worden geweigerd:

a) De betrokkene dient een verzoek tot verwijdering in voor persoonsgegevens van of namens een andere betrokkene.
b) Wanneer bron- en contactopsporing (BCO) wordt uitgevoerd, zal moeten worden afgewogen of het verwijderen van het dossier geen nadelige gevolgen heeft voor de voortzetting van BCO. Dit is omdat in HPZone ook persoonsgegevens van contacten worden opgenomen. Zolang het BCO loopt, moet worden afgewogen of het verwijderen van het dossier van de index en het contact geen nadelige gevolgen heeft voor de uitvoering van BCO. Zijn er geen nadelige gevolgen dan kan het dossier worden verwijderd (inclusief door de index opgegeven contacten in dat dossier). Zijn er wel nadelige gevolgen, dan kan het dossier tijdens de uitvoering van BCO niet worden verwijderd.
c) Het verzoek wordt ten aanzien van CoronIT ná testafname of vóór testuitslag ingediend. Wordt het verzoek tot verwijdering vóór testuitslag ingediend? Laat de betrokkene weten dat hij of zij zich dan niet meer kan laten testen. Heeft de betrokkene de intentie om zich wel te laten testen, dan kan het verzoek niet worden ingewilligd.
d) Is een betrokkene positief getest maar zijn de bij de wet verplichte persoonsgegevens nog niet aan het RIVM verstrekt, dan zal het verzoek nog niet mogen worden ingewilligd.[2] Dit zal pas kunnen plaatsvinden als de persoonsgegevens aan het RIVM zijn verstrekt. **N.B.** Deze situatie is van korte duur nu de verstrekking binnen een termijn van 24 uur moet plaatsvinden. Let om die reden goed op bij deze weigeringsgrond.
e) Als het afwijzen van het verzoek een noodzakelijke evenredige maatregel is ter waarborging van:
    - Nationale veiligheid;
    - Landsverdediging;

[2] Zie artikel 28 lid 1 Wpg en artikel lid 3 Wpg.

- Openbare veiligheid;
- Strafrechtelijke processen;
- Belangrijke doelstellingen van algemeen belang van de EU of Nederland;
- Beroepscodes voor beschermde beroepen;
- Taken op toezicht, inspectie of regelgeving op de bovenstaande punten;
- Onafhankelijkheid van rechters en gerechtelijke procedures;
- Inning van civielrechtelijke vorderingen.[3]

Deze beperkingen lijken in eerste instantie niet van toepassing te zijn op de verwerkingen in CoronIT of HPZone. Het is echter goed om na nadrukkelijk te gaan of deze beperkingen binnen jouw GGD van toepassing zijn, voordat de afweging wordt gemaakt om het verzoek af te wijzen.[4]

4. Wanneer mag je het verzoek niet weigeren?

De volgende gronden mogen geen reden zijn voor afwijzing van het verzoek en/of weigering om bepaalde persoonsgegevens te verwijderen:

a) Het tegemoetkomen aan het verzoek levert administratieve lasten op.
b) Het verzoek is niet beargumenteerd of niet voorzien van een reden.
c) Wanneer er geen weigeringsgronden zijn om het verzoek af te wijzen.
d) Het verzoek met betrekking tot CoronIT wordt ingediend vóór de testafname.
e) Wanneer de betrokkene ná de testuitslag een negatieve testuitslag blijkt te hebben.
f) Nadat de GGD de bij de wet verplichte persoonsgegevens aan het RIVM heeft verstrekt en er geen andere wettelijke plicht of belemmering voor de uitvoering van de wettelijke taak aanwezig is.
g) Als er nog (wetenschappelijk) onderzoek wordt uitgevoerd, althans verwacht te worden uitgevoerd.

5. Waar moet je opletten bij het in behandeling nemen en afhandelen van het verwijderingsverzoek?

a) Zorg ervoor dat voordat het verzoek in behandeling wordt genomen, de identiteit van de betrokkene vooraf wordt vastgesteld. Volg hierbij de interne GGD – procedure.
b) Is het verwijderingsverzoek voor/namens iemand anders ingediend, let erop of deze persoon gemachtigd of bevoegd is en volg hierbij de interne GGD-procedure.
c) Houd tijdens het proces rekening met de behandelingstermijn van één maand en voorkom dat deze wordt overschreden. Als deze toch dreigt te worden overschreden omdat het verzoek complex is of als je veel verzoeken hebt ontvangen, zorg dan dat binnen de eerste maand de betrokkene op de hoogte wordt gebracht van de verlenging van de behandelingstermijn met twee maanden.

---

[3] Artikel 23 AVG.
[4] Artikel 41 UAVG.

d) Wordt het verwijderingsverzoek toegewezen? Bevestig schriftelijk aan het einde van de rit aan de betrokkene dat de persoonsgegevens conform het besluit zijn verwijderd.
e) Let erop dat het besluit om het verzoek toe of af te wijzen een besluit is in de zin van de Awb, omdat de GGD een bestuursorgaan is. Dit betekent dat het besluit aan de vereisten van de Awb moet voldoen.

BIJLAGE 1: STAPPENPLAN

1. Neem het verzoek in behandeling. Registreer de ontvangstdatum. Dit is van belang in verband met de termijnen waar een organisatie zich aan moet houden. De betrokkene moet binnen één maand een reactie ontvangen over het inzageverzoek. Stuur een ontvangstbevestiging naar de betrokkene.
2. Stel vast of het verwijderingsverzoek ziet op verwijdering van persoonsgegevens. Is dit niet het geval? Dan betreft dit geen verwijderingsverzoek in de zin van de AVG en kan er geen beroep worden gedaan op artikel 17 AVG. Verklaar het verzoek niet-ontvankelijk.
3. Controleer de identiteit van verzoeker. Hierbij is het van belang om na te gaan of de identiteit van verzoeker overeenkomt met de identiteit van de persoon zoals opgenomen in het dossier. Komt de identiteit niet overeen? Wijs het verzoek af, tenzij kan worden vastgesteld dat het verzoek namens iemand anders wordt ingediend (zie paragraaf 5).[5]
4. Ga in de tussentijd na of de behandeltermijn van één maand haalbaar is. Is dit niet het geval? Zorg er dan voor dat binnen de eerste maand na ontvangst van het verzoek de behandelingstermijn met maximaal twee maanden wordt verlengd.
5. Zorg ervoor dat de verlening van de termijn gemotiveerd wordt. Indien de GGD op dit moment veel verzoeken tot inzage of verwijdering heeft ontvangen en daarmee niet de capaciteit heeft om het aantal verzoeken deugdelijk binnen één maand af te handelen, dan kan dit een reden zijn de behandelingstermijn van de verzoeken te verlengen op grond van artikel 12 lid 3 AVG.
6. Ga na of het verzoek voldoende is gespecificeerd. Dus ten aanzien van welk proces/welke verwerking en welke persoonsgegevens geldt het verwijderingsverzoek.
7. Is het verzoek niet voldoende gespecificeerd? Neem contact op met de betrokkene om het verzoek verder te specificeren. Met name wanneer het verzoek zeer algemeen is geformuleerd, is het van belang om het verzoek te specificeren tot een bepaald proces of verwerking. Een voorbeeld van een zeer algemeen verzoek is 'ik wil dat al mijn gegevens bij de GGD worden verwijderd'.
8. Ga na of de organisatie persoonsgegevens verwerkt van de betrokkene.
9. Ga na of er weigeringsgronden van toepassing zijn (bepaal welke gegevens niet mogen worden gewist).
10. Neem een besluit over het toewijzen of afwijzen van het verwijderingsverzoek. Neem in het besluit op welke persoonsgegevens zullen worden verwijderd en, indien van toepassing, welke gegevens niet zullen worden verwijderd. Zorg ervoor dat ingeval de verwijdering wordt afgewezen de reden hiervan wordt vermeld met eveneens de vermelding per wanneer de persoonsgegevens wel zullen worden verwijderd.
11. Handel het verzoek af en sluit de registratie van het verzoek.
12. In geval van toewijzing van een verwijderingsverzoek ter zake CoronIT, benader GGD GHOR Nederland met het verzoek om over te gaan tot verwijdering (anonimisering) van

---

[5] 'Hoe kan ik de identiteit vaststellen wanneer iemand zijn/haar privacyrechten uitoefent?, 'https://autoriteitpersoonsgegevens.nl/nl/onderwerpen/algemene-informatie-avg/rechten-van-betrokkenen#hoe-kan-ik-de-identiteit-vaststellen-wanneer-iemand-zijn-haar-privacyrechten-uitoefent-7212'.

de persoonsgegevens van betrokkene conform het besluit van de GGD. Vraag om een bevestiging van de verwijdering (anonimisering).

13. Heeft u het verzoek tot verwijdering toegewezen? Ga na of deze persoonsgegevens in het kader van CoronIT en/of HPZone door een verwerker worden verwerkt. Benader de verwerker met de instructie om over te gaan tot verwijdering. Vraag om een bevestiging van de verwijdering.
14. Geef de betrokkene een schriftelijke (waaronder e-mail) terugkoppeling dat de in het besluit opgesomde persoonsgegevens zijn verwijderd.

BIJLAGE 2: CHECKLIST

	Het verzoek is voldoende specifiek.
	De identiteit van de verzoeker in de systemen komt overeen met de identiteit van de persoon die het verwijderingsverzoek indient.
	In de verwijdering van de gegevens komen geen persoonsgegevens van andere betrokkenen voor dan de verzoekende betrokkene zelf.
	Bij de tegemoetkoming of afwijzing van het verzoek wordt de betrokkene erop gewezen dat de betrokkene het recht heeft om een klacht in te dienen bij de AP.
	Het besluit voldoet aan de vereisten van de Awb.

BIJLAGE 3: PERSOONSGEGEVENS ARTIKEL 28 LID 3 WPG

	Persoonsgegevens zoals opgesomd in artikel 28 lid 3 Wpg
	De infectieziekte dan wel een beschrijving van het ziektebeeld
	De eerste ziektedag
	De vaccinatietoestand
	Het gebruik van chemoprofylaxe
	Eventuele ziekenhuisopname
	De vermoedelijke infectiebron, zonodig met inbegrip van de daaruit voortkomende gevallen
	De datum van vermoeden of vaststelling van infectie
	Het geslacht
	De geboortemaand en het geboortejaar van de betrokken persoon
	Eerste drie cijfers van de postcode
	Uitslag van het nader onderzoek

Document 9.7

Richtlijn afhandeling inzageverzoeken Covid-19 (CoronIT & HPZone)

In het kader van de bestrijding van Covid-19 worden bij GGD'en en bij GGD GHOR Nederland persoonsgegevens verwerkt. Er worden persoonsgegevens verwerkt als mensen (betrokkenen) zich laten testen voor Covid-19 (CoronIT) en als de GGD bron- en contactopsporing uitvoert (HPZone). Het kan voorkomen dat betrokkenen een verzoek om inzage in deze persoonsgegevens indienen bij de plaatselijke GGD. Omdat ten aanzien van de bestrijding van Covid-19 een en ander vanuit GGD GHOR Nederland wordt georganiseerd (zo ook opzet en beheer van CoronIT en koppelingen met HPZone) volgen hieronder richtlijnen vanuit GGD GHOR Nederland over hoe om te gaan met inzageverzoeken betreffende de gegevensverwerkingen in CoronIT en HPZone, ofwel de verwerkingen aangaande de bestrijding Covid-19.

Deze richtlijn is bedoeld voor medewerkers die bevoegd zijn om inzageverzoeken in het kader van CoronIT en HPZone in behandeling nemen en af te handelen. Hier kan gedacht worden aan de privacy organisatie van de GGD of een bevoegd persoon binnen het GGD Coronateam. Dit kan per GGD verschillen. Het doel van deze richtlijn is om de inzageverzoeken landelijk zo uniform mogelijk af te handelen.

Ongeacht de richtlijn voor het verwijderen van persoonsgegevens, is het belangrijk dat GGD'en en GGD GHOR Nederland, de verzoeken die op dit moment worden ontvangen als gevolg van de recent bekend geworden datadiefstal, niet alleen procedureel benaderen. Wij als GGD GHOR en de GGD'en begrijpen en voelen heel goed dat de datadiefstal het vertrouwen van mensen kan hebben geschaad en willen hen dus ook zo goed en snel mogelijk helpen bij hun verzoek.

1. Waar heeft de betrokkene recht op?

De betrokkenen hebben het recht van inzage in de persoonsgegevens die worden verwerkt.[1] Deze inzage in de persoonsgegevens zal begeleid moeten worden met informatie over de verwerkte persoonsgegevens. Dit recht is een sterk recht maar is niet absoluut, dat wil zeggen dat er beperkingen gelden. Deze beperkingen en met name die gelden voor verwerkingen in het kader van Covid-19, worden onder paragraaf 3 behandeld.

2. Waar moet het verzoek aan voldoen?

Het is van belang dat het verzoek specifiek is. Dat wil zeggen dat het verzoek duidelijk moet zijn omschreven. Het ontbreken van een reden is overigens geen reden om het verzoek te weigeren. Is het verzoek gebaseerd op emoties of is het verzoek niet helder geformuleerd en laat ruimte over voor invulling, vraag de betrokkene het verzoek nader te specificeren. Zorg ervoor dat je antwoord hebt op de volgende vragen.

a) Waar (op welke verwerking) binnen de GGD'en heeft het verzoek betrekking op?
b) Is het verzoek niet duidelijke, neem contact op met de betrokkene en vraag na wat het verzoek inhoudt? Wil de betrokkene gegevens inzien, laten verwijderen of een klacht indienen? Misschien wel alle drie?
c) Blijkt dat de betrokkene een verwijderingsverzoek heeft ingediend? Zie hiervoor in dat geval de Richtlijn afhandeling verwijderingsverzoek Covid-19 (CoronIT & HPzone).

[1] Artikel 15 AVG.

d) Een verzoek moet schriftelijk worden ingediend.

3. Wanneer mag het verzoek worden geweigerd?

In de onderstaande situaties mag het verzoek worden geweigerd:

a) De betrokkene dient een verzoek voor inzage in voor persoonsgegevens van een andere betrokkene.
b) Bij de verstrekking van inzage in de persoonsgegevens is de bescherming van de betrokkene of de bescherming van de rechten en vrijheden van anderen in het gedrang. Dit betekent dat als er loggegevens worden verstrekt van HPZone of CoronIT dat het daarbij enkel functie/rol/afdeling maar geen identificeerbare gegevens van degenen die toegang hebben gehad in het dossier, worden verstrekt.
c) Als het onder het mom van een WOB-verzoek een verzoek omtrent inzage in persoonsgegevens wordt ingediend. De betrokkene mag worden gevraagd het verzoek verder te specificeren.
d) Als het afwijzen van het verzoek een noodzakelijke en evenredige maatregel is ter waarborging van:
    - Nationale veiligheid;
    - Landsverdediging;
    - Openbare veiligheid;
    - Strafrechtelijke processen;
    - Belangrijke doelstellingen van algemeen belang van de EU of Nederland;
    - Beroepscodes voor beschermde beroepen;
    - Taken op toezicht, inspectie of regelgeving op de bovenstaande punten;
    - Onafhankelijkheid van rechters en gerechtelijke procedures;
    - Inning van civielrechtelijke vorderingen;[2]

Deze beperkingen lijken in eerste instantie niet van toepassing op de verwerkingen in CoronIT of HPZone. Het is echter goed om nadrukkelijk na te gaan of deze beperkingen binnen jouw GGD van toepassing zijn, voordat de afweging wordt gemaakt om het verzoek af te wijzen.[3]

4. Wanneer mag je het verzoek niet weigeren?

De volgende redenen mogen geen reden zijn voor verwijdering van het verzoek:

a) Het tegemoetkomen aan het verzoek levert administratieve lasten op.
b) Het verzoek is niet beargumenteerd.
c) De betrokkene is reeds bekend met de inhoud van de verwerking en de persoonsgegevens.
d) Wanneer het verzoek betrekking heeft op de persoonsgegevens van anderen dan de verzoekende betrokkene.
e) Wanneer er geen weigeringsgronden uit paragraaf 3 zijn om het verzoek af te wijzen.

5. Welke informatie moet worden verstrekt met het verstrekken van inzage?

Is het verzoek specifiek dan zal moeten worden beoordeeld of er weigeringsgronden aanwezig zijn om het verzoek af te wijzen. Zie hiervoor paragraaf 3.

---

[2] Artikel 23 AVG.

Wanneer er geen belemmeringen zijn dan zal aan het verzoek tegemoet worden gekomen. Met de beantwoording aan het verzoek zal in ieder geval de volgende informatie zullen moeten worden verstrekt.

I. ***Doel van de verwerkingen in CoronIT en HPzone***

CoronIT: Er worden persoonsgegevens verwerkt in CoronIT om het Covid-19 testproces te centraliseren, automatiseren, versnellen en vergemakkelijken en het geven van inzicht in de ontwikkeling van de pandemie doordat testresultaten in dat systeem worden verwerkt. De verwerking van bepaalde persoonsgegevens in CoronIT is noodzakelijk om te bepalen of iemand klachten heeft en getest moet worden, de test uit te voeren en het resultaat terug te koppelen aan de betrokkene.
HPZone: De GGD'en zijn verplicht om een registratie van positieve testuitslagen van infectieziekten waaronder Covid-19 bij te houden.[3] Deze registratie vindt plaats in HPZone en HPZone Lite. HPZone wordt gebruikt door GGD-medewerkers, HPZone Lite is ingericht voor de landelijke schil, waarbij medewerkers flexibel bij GGD'en worden ingezet. Naast de registratie van positieve uitslagen worden ook gegevens van de contacten van de betrokkene geregistreerd. Het gaat daarbij om persoonsgegevens van degene met wie de positief geteste persoon contact heeft gehad. Deze registratie vindt plaats omdat de GGD'en verplicht zijn om een bron- en contactopsporing uit te voeren.[4] Daarvoor is de verwerking van persoonsgegevens van de contacten van de positief geteste personen noodzakelijk.

II. ***Soorten persoonsgegevens die verwerkt worden***

In CoronIT worden zowel gewone (bijv. NAW, contactgegevens), bijzondere (bijv. klachten (symptomen), testuitslagen) als wettelijk identificerende persoonsgegevens (BSN) verwerkt. In CoronIT worden slechts persoonsgegevens verwerkt die noodzakelijk zijn om te bepalen of iemand klachten heeft en of iemand getest kan worden, de test uit te voeren en het resultaat terug te koppelen.

In HPZone worden zowel gewone (NAW, contactgegevens), bijzondere (klachten testuitslag

III. ***Organisaties die persoonsgegevens ontvangen***

Zie Bijlage 1 voor de organisaties die naast de GGD ook persoonsgegevens die in CoronIT of HPZone voorkomen, verwerken.

IV. **Bewaartermijn persoonsgegevens**

Zowel in HPZone als in CoronIT worden de persoonsgegevens bewaard zolang dat noodzakelijk is voor de bestrijding van de pandemie. Ze worden echter niet langer bewaard dan 5 jaar.[5] Dit is een maximale termijn. In praktijk zullen gegevens dus niet langer worden bewaard dan noodzakelijk is voor het in kaart brengen en bestrijden van de pandemie.

---

[3] Artikel 29 lid 1 Wet publieke gezondheid.
[4] Artikel 6 lid 1 sub c Wet publieke gezondheid.
[5] Artikel 29 lid 2 Wet publieke gezondheid en MvT bij dit artikel.

V. **Dat de betrokkene het recht heeft om een klacht in de dienen bij de AP**
Wijs de betrokkene op het recht om een klacht in te dienen bij de AP.

6. Waar moet je opletten bij het in behandeling nemen en afhandelen van het inzageverzoek?

a) Zorg ervoor dat bij het verstrekken van inzage in de persoonsgegevens in CoronIT of HP Zone geen persoonsgegevens van anderen dan de betrokkene worden verstrekt.
b) Dat er geen persoonsgegevens van degenen die inzage hebben gehad in de gegevens van de betrokkene, worden verstrekt (dit is aan de orde wanneer met bij het verlenen van inzage ook loggegevens worden vrijgegeven). De functie/rol/afdeling van degene die wel inzage heeft gehad mag worden vermeld, maar de specifieke namen van medewerkers of derden mogen niet mee met de inzageverstrekking.
c) Zorg ervoor dat voordat het verzoek in behandeling wordt genomen, de identiteit van de betrokkene vooraf wordt vastgesteld. Volg hierbij de interen GGD-procedure.
d) Is het inzageverzoek voor/namens iemand anders ingediend, let erop of deze persoon gemachtigd of bevoegd is om dit verzoek in te dienen en inzage te verkrijgen en volg hierbij de interne GGD-procedure.
e) Zorg ervoor dat de informatie in een makkelijke, toegankelijke vorm en in duidelijke en eenvoudige taal aangeboden wordt.
f) Zorg ervoor dat de informatie beknopt, transparant en begrijpelijk is.
g) De persoonsgegevens moeten kosteloos en op een makkelijke manier worden verstrekt worden: aangetekend, per beveiligde brief of per beveiligde mail. De betrokkene mag de gegevens natuurlijk ook zelf op komen halen.
h) Houd tijdens het proces rekening met de behandelingstermijn van één maand en voorkom dat deze wordt overschreden. Als deze toch dreigt te worden overschreden omdat het verzoek complex is of omdat je veel verzoeken hebt ontvangen, zorg dan dat binnen de eerste termijn van één maand nadat het verzoek is ingediend de betrokkene op de hoogte wordt gebracht van de verlenging van de behandelingstermijn met twee maanden.
i) De informatie kan slechts mondeling verstrekt worden als de betrokkene hier zelf om vraagt.
j) Let erop dat het besluit om het verzoek toe of af te wijzen een besluit is in de zin van de Awb, omdat de GGD een bestuursorgaan is. Dit betekent dat het besluit aan de vereisten van de Awb moet voldoen.

Zie aanvullend de checklist in Bijlage 3.

BIJLAGE 1: OVERZICHT ORGANISATIES DIE PERSOONSGEGEVENS ONTVANGEN

CoronIT

Betrokken partij	**Doel**
Leveranciers van CoronIT	Uitvoering van technisch beheer doordat de leverancier de applicatie host.
RIVM	Wettelijke plicht om aan RIVM meldingen[6] van infectieziekten in een gepseudonimiseerd bestand door te geven[7] omdat RIVM in opdracht van het ministerie van VWS de taak heeft om werkzaamheden te verrichten bij de bestrijding van infectieziekten.[8]
Externe aanvragers zoals arbo- en instellingsartsen	Degene die de aanmelding doet voor het testen van de betrokkene krijgt een terugkoppeling van de testresultaten.
Labaratoria	Ontvangen BAR-code soms aangevuld met een geboortedatum om monsters te analyseren op besmetting van Covid-19.
TelePerformance	Levert callcentercapaciteit voor de afsprakenlijn voor coronatesten.

HPZone

Betrokken partij	**Doel**
Leveranciers van HPZone en HPZone Lite	Uitvoering van technisch beheer doordat de leverancier de applicatie host.
RIVM	Wettelijke plicht om aan RIVM meldingen[9] van infectieziekten in een gepseudonimiseerd bestand door te geven[10] omdat RIVM in opdracht van het ministerie van VWS de taak heeft om werkzaamheden te verrichten bij de bestrijding van infectieziekten.[11]
Landelijke partners (hulpverleners, namelijk ANWB, SOS International, Yource, Rode Kruis)	Leveren en coördineren de landelijke schil van BCO-medewerkers. Zij zorgen dat medewerkers worden ingezet indien een GGD daar behoefte aan heeft.

[6] Artikel 28 Wet publieke gezondheid.
[7] Artikel 6c lid 3 Wet publieke gezondheid.
[8] Artikel 6c lid 1 Wet publieke gezondheid.
[9] Artikel 28 Wet publieke gezondheid.
[10] Artikel 6c lid 3 Wet publieke gezondheid.
[11] Artikel 6c lid 1 Wet publieke gezondheid.

BIJLAGE 2: STAPPENPLAN

1. Neem het verzoek in behandeling. Registreer de ontvangstdatum. Dit is van belang in verband met de termijnen waar een organisatie zich aan moet houden. De betrokkene moet binnen één maand een reactie ontvangen over het inzageverzoek. Stuur een ontvangstbevestiging naar de betrokkene. De termijn mag worden verlengd met twee maanden als het verzoek complex is, of als de organisatie veel verzoeken heeft ontvangen.
2. Zorg ervoor dat de verlening van de termijn gemotiveerd wordt. Indien de GGD op dit moment veel verzoeken tot inzage of verwijdering heeft ontvangen en daarmee niet de capaciteit heeft om het aantal verzoeken deugdelijk binnen één maand af te handelen, dan kan dit een reden zijn de behandelingstermijn van de verzoeken te verlengen.[12]
3. Stel vast of het inzageverzoek ziet op inzage in persoonsgegevens (het verzoek kan namelijk een klacht of een WOB-verzoek inhouden). Is dit niet het geval? Dan betreft dit geen inzageverzoek in de zin van de AVG en kan er geen beroep worden gedaan op artikel 15 AVG. Verklaar het verzoek niet-ontvankelijk en motiveer.
4. Controleer de identiteit van verzoeker. Hierbij is het van belang om na te gaan of de identiteit van verzoeker overeenkomt met de identiteit van de persoon in wiens persoonsgegevens inzage wordt gevraagd. Komt de identiteit niet overeen? Wijs het verzoek af, tenzij kan worden vastgesteld dat het verzoek namens iemand anders wordt ingediend.[13]
5. Ga na of het verzoek voldoende is gespecificeerd. Zo niet, neem contact op met de betrokkene om het verzoek verder te specificeren. Met name wanneer het verzoek zeer algemeen is geformuleerd, is het van belang om het verzoek te specificeren tot een bepaald proces of verwerking.
6. Controleer of er sprake kan zijn van misbruik van het inzagerecht. De volgende punten leveren een indicatie op van misbruik:
    - Hoge frequentie van het aantal verzoeken van dezelfde verzoeker bij de organisatie;
    - (Recent) afgeronde, lopende of aangekondigde gerechtelijke procedures van dezelfde verzoeker bij de organisatie;
    - Eerdere (veelvuldige) verzoeken op grond van andere wetgeving, zoals de Wob/Wbp/AVG van dezelfde verzoeker bij de organisatie;
    - Eerdere (veelvuldige) klachten en meldingen van dezelfde verzoeker bij de organisatie;
    - Vermoeden van het inzet van verzoek als instrument voor financieel gewin op basis van Wet dwangsom en beroep bij niet tijdig beslissen.
7. Ga na of de organisatie persoonsgegevens verwerkt van de betrokkene.
8. Ga na of er weigeringsgronden van toepassing zijn.
9. Ga na of de betrokkene om een afschrift (kopie) of een overzicht van verwerking vraagt. Zo weet je of je een kopie moet verstrekken van de persoonsgegevens of algemene informatie over de verwerking van de persoonsgegevens van de

---

[12] Artikel 12 lid 3 AVG.

[13] 'Hoe kan ik de identiteit vaststellen wanneer iemand zijn/haar privacyrechten uitoefent?, 'https://autoriteitpersoonsgegevens.nl/nl/onderwerpen/algemene-informatie-avg/rechten-van-betrokkenen#hoe-kan-ik-de-identiteit-vaststellen-wanneer-iemand-zijn-haar-privacyrechten-uitoefent-7212'.

betrokkene. Verstrek dit in een duidelijk overzicht en in een eenvoudige, toegankelijke vorm aan de betrokkene.

10. Handel het verzoek af en sluit de registratie van het verzoek.

BIJLAGE 3: CHECKLIST

	Het verzoek is voldoende specifiek.
	De identiteit van de verzoeker overeenkomt met de identiteit van de persoon in wiens persoonsgegevens inzage wordt gevraagd.
	In de verstrekking van de gegevens komen geen persoonsgegevens van andere betrokkenen voor dan de verzoekende betrokkene zelf.
	Bij de tegemoetkoming van het verzoek wordt de betrokkene erop gewezen dat de betrokkene het recht heeft om een klacht in te dienen bij de AP.
	De informatie wordt in een makkelijke, toegankelijke vorm en in duidelijke en eenvoudige taal aangeboden.
	De informatie is beknopt, transparant en begrijpelijk.
	De betrokkene wordt (eventueel door verwijzing naar het privacybeleid) verwezen naar zijn privacyrechten.
	Informatie over de verwerkingsdoeleinden wordt verstrekt aan de betrokkene.
	Informatie over welke soort persoonsgegevens is verzameld wordt verstrekt.
	Informatie over hoe lang de persoonsgegevens bewaard worden wordt verstrekt.
	Informatie over de verstrekking van persoonsgegevens aan organisaties.
	Het besluit voldoet aan de vereisten van de Awb.

Document 9.8

Governance Proces toegang tot HPZone en HPZone Lite toekennen

04 02 2021 - GGD GHOR Nederland

Partijen:

- **Servicedesk:** verzamelt aanvragen landelijke schil
- **GGD GHOR NL:** voorzitter HPZone gebruikersgroep beoordeelt aanvraag wijzigen rollen
- **GGD GHOR NL:** privacy officer brengt advies uit in aanvraag wijzigen rollen
- **Technisch beheer GGD GHOR NL:** kan landelijk rollen definiëren in HPZone
- **Technisch beheer per GGD-regio:** kent rollen regionaal én landelijk toe in HPZone

Beheer/wijzingen rollen:	
1.	GGD'en en/of landelijke partners doen bij de Servicedesk van GGD GHOR Nederland het verzoek om functies of rechten aan/uit te zetten bij een rol en/of een nieuwe rol te creëren.
2.	Het wijzigen van rollen in HP Zone vindt plaats na goedkeuring van de "voorzitter HP Zone gebruikersgroep" met advies van de privacy officer GGD GHOR NL.
3.	Voorzitter HPZone gebruikersgroep deelt besluit met de Servicedesk.
4.	Bij positief besluit handelt de Servicedesk het verzoek af met inFact.

Toekennen rollen	
1.	Bij indiensttreding op basis van de functie en/of door een aanvrager (leidinggevende van de persoon die de rol ontvangt) wordt rol aangevraagd bij Servicedesk of beheerder van desbetreffende GGD/landelijke partner.
2.	De Servicedesk/beheerder neemt dit in behandeling en laat de lokale proceseigenaar de beoordeling doen.
3.	Het verzoek wordt afgehandeld.

Toekennen toegang GGD voor landelijke partners	
1.	De landelijke medewerker meldt zich bij de identityhub aan.
2.	De beheerders van individuele GGD'en worden benaderd door de coördinator van desbetreffende landelijke partner en op basis hiervan wordt toegang verschaft.

Intrekken toegang GGD voor landelijke partners	
1.	De beheerders van individuele GGD'en trekken de rechten in.

Document 9.9

Controleer verzoek conform stappenplan –
bijlage 1 bij richtlijn verwijderingsverzoek – CoronIT Testen

Test nog niet uitgevoerd of testuitslag nog niet bekend

Het verzoek tot verwijdering kan worden gehonoreerd.

Gevolg: de verzoeker kan zich niet laten testen of de uitslag kan niet worden teruggekoppeld.

Informeer verzoeker dat test niet doorgaat dan wel dat verzoeker testuitslag niet zal ontvangen. Ga na of de verzoeker, ondanks het gevolg, wil doorzetten met de verwijdering.*

Uitzondering:
Persoonsgegevens kunnen niet uit CoronIT worden verwijderd als de verzoeker zich wil vaccineren. Wel kan het testformulier worden verwijderd.

Uitslag is negatief

Het verzoek tot verwijdering kan worden gehonoreerd.

Uitgangspunt: er is geen belang is bij het bewaren van de negatieve testuitslagen met betrekking tot covid-19 in CoronIT.

Gevolg: verwijdering (anonimisering) van de persoonsgegevens kan ertoe leiden dat de betrokkene niet kan worden geïnformeerd of hij of zij een slachtoffer is geweest van de mogelijke datadiefstal.

Informeer verzoeker over het gevolg. Ga na of de verzoeker ondanks het gevolg, wil doorzetten met de verwijdering.

Uitzondering:
Persoonsgegevens kunnen uit CoronIT niet worden verwijderd als de verzoeker zich wil vaccineren. Wel kan het testformulier worden verwijderd.

Uitslag is positief

Het verzoek tot verwijdering kan worden gehonoreerd.

Uitgangspunt: er is weinig tot geen belang is bij het bewaren van de positieve testuitslagen met betrekking tot covid-19 in CoronIT. De positieve uitslagen worden op grond van artikel 24 Wpg doorgemeld naar HPZone, waardoor bewaring van dezelfde persoonsgegevens in CoronIT een onnodig dubbeldossier met zich meeneemt.

Gevolg: verwijdering (anonimisering) van de persoonsgegevens kan ertoe leiden dat de betrokkene niet kan worden geïnformeerd of hij of zij een slachtoffer is geweest van de mogelijk datadiefstal.

Informeer verzoeker over het gevolg. Ga na of de verzoeker ondanks het gevolg, wil doorzetten met de verwijdering.

Uitzondering:
Persoonsgegevens kunnen niet uit CoronIT worden verwijderd als de verzoeker zich wil vaccineren. Wel kan het testformulier worden verwijderd.

* Het gevolg dat door verwijdering de verzoeker niet kan worden geïnformeerd is in dit geval niet van toepassong, omdat het hier gaat om nieuwe afspraken NA het incident.

Controleer verzoek conform stappenplan – bijlage 2 bij richtlijn verwijderingsverzoek – HPZone (lite)

Verzoeker is positief getest (Index) en doorgemeld naar HPZone (meldingsplicht art. 24 Wpg).

Het verzoek tot verwijdering kan in beginsel niet worden gehonoreerd.

Uitgangspunt: op grond van de Wpg *moeten* persoonsgegevens van een positief geteste betrokkene ten aanzien van een infectieziekte (waaronder groep A) worden gemeld aan de GGD. Dit is een meldingsplicht en daarmee een wettelijke verplichting tot verwerking van de gemelde persoonsgegevens door de GGD (art. 24 Wpg). Deze persoonsgegevens mogen maximaal 5 jaar worden bewaard (art. 30 Wpg). In het kader van de coronapandemie is het noodzakelijk dat deze gegevens gedurende de pandemie, maar uiterlijk maximaal 5 jaar, worden bewaard. De bewaring is noodzakelijk om de wettelijke taak van infectieziektebestrijding mogelijk te maken, namelijk het starten van BCO en het mogelijk toepassen van dwingende maatregelen gericht op het individu alsook het toepassen van collectieve maatregelen (MvT Wpg).

Daarnaast is in beginsel het recht op verwijdering niet van toepassing als de gegevens nodig zijn voor het nakomen van een wettelijke verplichting om de gegevens te verwerken, voor het vervullen van een taak van algemeen belang en om redenen van algemeen belang op het gebied van volksgezondheid (art. 17 lid 3, onderdeel b en c AVG).

Verzoeker is niet zelf getest, maar bekend via BCO (het contact) (art. 6 lid 1 sub c Wpg)

Het verzoek tot verwijdering kan in beginsel worden gehonoreerd.

Uitgangspunt: de persoonsgegevens van betrokkene zijn geen verplichte meldingsgegevens en worden alleen verwerkt als het contact wenst mee te werken aan BCO. In de MvT van de Wpg is expliciet bepaald dat in alle gevallen BCO vrijwillig plaatsvindt. Alhoewel de verwerking van persoonsgegevens plaatsvindt onder artikel 6 lid 1 sub c Wpg en daarmee onder het kader van een wettelijke taak van de GGD, kan het onredelijk worden beschouwd dat bij vrijwillige deelname, verwijdering van de persoonsgegevens onmogelijk wordt gemaakt. Daarnaast lijkt de noodzaak om deze gegevens een langere tijd te bewaren niet hoog.

De gegevens kunnen worden geanonimiseerd om de ontwikkeling van de covid-19 in zicht te houden (zoals bijhouden van geaggregeerde data). Dit houdt wel in dat re-identificatie van de persoonsgegevens niet meer tot de mogelijkheid mag behoren. Het resultaat van anonimisering dient even permanent te zijn als uitwissing of vernietiging.

Gevolg: verwijdering (anonimisering) van de persoonsgegevens kan ertoe leiden dat de betrokkene niet kan worden geïnformeerd of hij of zij een slachtoffer is geweest van de mogelijke datadiefstal.

Informeer verzoeker over het gevolg. Ga na of de verzoeker ondanks het gevolg, wil doorzetten met de verwijdering.

Uitzondering in alle drie de gevallen:
Persoonsgegevens kunnen niet uit CoronIT worden verwijderd als de verzoeker zich op het moment van het verwijderingsverzoek wil laten testen. Wel kan het vaccinatieformulier worden verwijderd.

Controleer verzoek conform stappenplan – bijlage 3 bij richtlijn verwijderingsverzoek - CoronIT Vaccinatie

Verwijderingsverzoek in beginsel honoreren, tenzij er sprake is van aanmerkelijk belang om te bewaren, zoals volksgezondheid of de wet zich tegen verwijdering verzet. *(grondslag 7:455 BW)*

Verzoeker heeft afspraak gemaakt, maar nog geen vaccinatie gehad

Het verzoek tot verwijdering kan worden gehonoreerd.

Gevolg: door verwijdering kan vaccinatie geen doorgang vinden.

Informeer verzoeker dat vaccinatie door verwijderingsverzoek geen doorgang kan vinden. Geef verzoeker bedenktermijn. Ga na of de verzoeker, ondanks het gevolg, de verwijdering wil doorzetten.

Verzoeker eerste prik gehad, maar nog niet de tweede

Het verzoek tot verwijdering kan worden gehonoreerd.

Uitgangspunt: alhoewel er een algemeen belang is om dit nieuwe vaccinatieprogramma te evalueren om zo bepalen of de vaccinaties op een effectieve wijze bijdragen aan de bestrijding van de pandemie, ligt de verantwoordelijkheid voor het evalueren van het vaccinatieprogramma niet bij de GGD'en, maar bij het RIVM (art. 6b lid 1 en 2 Wpg). De GGD heeft om die reden geen aanmerkelijk belang (zoals volksgezondheid) om het verzoek tot verwijdering van persoonsgegevens uit het dossier af te wijzen.

Gevolg: door verwijdering kan de tweede vaccinatie geen doorgang vinden, waardoor de verzoeker niet het volledige vaccinatieprogramma doorloopt.

Informeer verzoeker dat vaccinatie door verwijderingsverzoek geen doorgang kan vinden. Geef verzoeker bedenktermijn. Ga na of de verzoeker, ondanks het gevolg, de verwijdering wil doorzetten.

Verzoeker heeft beide prikken gehad

Het verzoek tot verwijdering kan worden gehonoreerd.

Uitgangspunt: alhoewel er een algemeen belang is om dit nieuwe vaccinatieprogramma te evalueren om zo bepalen of de vaccinaties op een effectieve wijze bijdragen aan de bestrijding van de pandemie, ligt de verantwoordelijkheid voor het evalueren van het vaccinatieprogramma niet bij de GGD'en, maar bij het RIVM (art. 6b lid 2 Wpg). De GGD heeft om die reden geen aanmerkelijk belang (zoals volksgezondheid) om het verzoek tot verwijdering van persoonsgegevens uit het dossier af te wijzen.

Gevolg: de verzoeker kan niet meer worden geïnformeerd over bijwerkingen of andere bijzonderheden rondom het vaccinatieprogramma.

Informeer verzoeker dat deze zelf alert dient te zijn op berichten over bijwerkingen en andere bijzonderheden rondom vaccinatieprogramma.

Document 10.12

VOLMACHT AAN GGD GHOR INZAKE MEDEDELING DATALEK AAN BETROKKENEN

25-02-2021

(Partijen 1 t/m 25 hierna gezamenlijk aangeduid als: "**GGD'en**")

1. **GGD Rotterdam-Rijnmond**, alsmede de gemeente Rotterdam als uitvoerende gemeente in het kader van de gemeenschappelijke regeling GGD Rotterdam-Rijnmond, te Rotterdam aan de Schiedamsedijk 95, ingeschreven in het handelsregister onder KvK nummer 24483298, hierna eveneens te noemen "GGD", rechtsgeldig vertegenwoordigd door mevrouw S.V.H. Baas;

2. **De Gemeentelijke Gezondheidsdienst IJsselland**, gevestigd te Zwolle aan de Zeven Alleetjes 1, ingeschreven in het handelsregister onder KvK nummer 50594761, hierna eveneens te noemen "GGD", rechtsgeldig vertegenwoordigd door mevrouw A.M. van den Berg;

3. **De Gemeentelijke Gezondheidsdienst Noord- en Oost-Gelderland**, gevestigd te Warnsveld aan de Rijksstraatweg 65, ingeschreven in het handelsregister onder KvK nummer 51158957, hierna eveneens te noemen "GGD", rechtsgeldig vertegenwoordigd door mevrouw J. Baardman;

4. **De Gemeentelijke Gezondheidsdienst Haaglanden**, gevestigd te Den Haag aan het Westeinde 128, ingeschreven in het handelsregister onder KvK nummer 63629216, hierna eveneens te noemen "GGD", rechtsgeldig vertegenwoordigd door mevrouw A.S. de Boer;

5. **De Gemeentelijke Gezondheidsdienst Twente**, gevestigd te Enschede aan de Nijverheidstraat 30, ingeschreven in het handelsregister onder KvK nummer 8195873, hierna eveneens te noemen "GGD", rechtsgeldig vertegenwoordigd door mevrouw S. Dinsbach;

6. **De Gemeentelijke Gezondheidsdienst Drenthe**, gevestigd te Assen aan de Mien Ruysweg 1, ingeschreven in het handelsregister onder KvK nummer 1139196, hierna eveneens te noemen "GGD", rechtsgeldig vertegenwoordigd door de heer H. Kox;

7. **De Gemeentelijke Gezondheidsdienst Hart voor Brabant**, gevestigd te 's-Hertogenbosch aan de Vogelstraat 2, ingeschreven in het handelsregister onder KvK nummer 17247544, hierna
   eveneens te noemen "GGD", rechtsgeldig vertegenwoordigd door mevrouw T. Claassen;

8. **De Gemeentelijke Gezondheidsdienst Hollands Midden**, gevestigd te Leiden aan de Parmentierweg 49, ingeschreven in het handelsregister onder KvK nummer 27365105, hierna eveneens te **noemen "GGD", rechtsgeldig** vertegenwoordigd door de heer J.M.M. de Gouw;

9. **De Veiligheidsregio Fryslân**, gevestigd te Leeuwarden aan de Harlingertrekweg 58, ingeschreven in het handelsregister onder KvK nummer 1175778, hierna eveneens te noemen "GGD", rechtsgeldig vertegenwoordigd door mevrouw M. de Graaf;

10. **De Dienst Gezondheid & Jeugd Zuid-Holland Zuid**, gevestigd te Dordrecht aan de Karel Lotsyweg 40, ingeschreven in het handelsregister onder KvK nummer 54038111, hierna eveneens te noemen "GGD", rechtsgeldig vertegenwoordigd door de heer C. Vermeer;

11. **De Gemeentelijke Gezondheidsdienst GGD Brabant-Zuidoost**, gevestigd te Eindhoven aan het
    Clausplein 10, ingeschreven in het handelsregister onder KvK nummer 50451154, hierna eveneens te noemen "GGD", rechtsgeldig vertegenwoordigd door mevrouw E. Jeurissen;

12. **De Gemeentelijke Gezondheidsdienst Zuid-Limburg**, gevestigd te Heerlen aan het Overloon 2, ingeschreven in het handelsregister onder KvK nummer 14131474, hierna eveneens te noemen "GGD", rechtsgeldig vertegenwoordigd door de heer F.C.W. Klaassen;

13. **De Gemeentelijke Gezondheidsdienst Amsterdam**, gevestigd te Amsterdam aan de Nieuwe Achtergracht 100, ingeschreven in het handelsregister onder KvK nummer 70036896 , hierna eveneens te noemen "GGD", rechtsgeldig vertegenwoordigd door mevrouw J. Manshanden;

14. **De Gemeentelijke Gezondheidsdienst Zeeland**, gevestigd te Goes aan de Westwal 37, ingeschreven in het handelsregister onder KvK nummer 20171605, hierna eveneens te noemen "GGD", rechtsgeldig vertegenwoordigd door mevrouw J. Gaemers;

15. **De Gemeentelijke Gezondheidsdienst Hollands Noorden**, gevestigd te Alkmaar aan de Hertog Aalbrechtweg 22, ingeschreven in het handelsregister onder KvK nummer 37159559, hierna eveneens te noemen "GGD", rechtsgeldig vertegenwoordigd door de heer E.J. Paulina;

16. **De Veiligheids- en gezondheidsregio Gelderland-Midden**, gevestigd te Arnhem aan de Eusebiusbuitensingel 43, ingeschreven in het handelsregister onder KvK nummer 9217053, hierna eveneens te noemen "GGD", rechtsgeldig vertegenwoordigd door de heer H. Bril;

17. **De Gemeentelijke Gezondheidsdienst Gelderland-Zuid**, gevestigd te Nijmegen aan de Groenewoudseweg 275, ingeschreven in het handelsregister onder KvK nummer 9212724, hierna eveneens te noemen "GGD", rechtsgeldig vertegenwoordigd door mevrouw M. Pieters;

18. **De Gemeentelijke Gezondheidsdienst GGD Groningen**, gevestigd te Groningen aan het Hanzeplein 120, ingeschreven in het handelsregister onder KvK nummer 62089781, hierna eveneens te noemen "GGD", rechtsgeldig vertegenwoordigd door de heer A.A. Rietveld;

19. **De Gemeentelijke Gezondheidsdienst GGD Regio Utrecht**, gevestigd te Zeist aan de Dreef 5, ingeschreven in het handelsregister onder KvK nummer 50909185, hierna eveneens te noemen "GGD", rechtsgeldig vertegenwoordigd door de heer J. Donker;

20. **De Gemeentelijke Gezondheidsdienst GGD Zaanstreek-Waterland**, gevestigd te Zaandam aan de Vurehout 2, ingeschreven in het handelsregister onder KvK nummer 34370893, hierna eveneens "GGD", rechtsgeldig vertegenwoordigd door de heer F.H.J. Strijthagen;

21. **De Gemeentelijke Gezondheidsdienst Gooi & Vechtstreek**, gevestigd te Bussum aan de Burgemeester de Bordestraat 80, ingeschreven in het handelsregister onder KvK nummer 32152259, hierna eveneens te noemen "GGD", rechtsgeldig vertegenwoordigd door de heer A.R.J. Stumpel;

22. **Veiligheidsregio Kennemerland**, gevestigd te Haarlem aan de Zijlweg 200, ingeschreven in het handelsregister onder KvK nummer 34377971 , hierna eveneens te noemen "GGD", rechtsgeldig vertegenwoordigd door de heer A. van de Velden;

23. **De Gemeentelijke Gezondheidsdienst GGD Flevoland**, gevestigd te Lelystad aan de Noorderwagenstraat 2, ingeschreven in het handelsregister onder KvK nummer 32170514, hierna eveneens te noemen "GGD", rechtsgeldig vertegenwoordigd door de heer C. Verdam;

24. **De Gemeentelijke Gezondheidsdienst GGD Limburg-Noord**, gevestigd te Blerick aan de Drie Decembersingel 50, ingeschreven in het handelsregister onder KvK nummer 14110234, hierna eveneens te noemen "GGD", rechtsgeldig vertegenwoordigd door de heer J.J.

Rooijmans;

25. **De Gemeentelijke Gezondheidsdienst GGD West-Brabant**, gevestigd te Breda aan de Doornboslaan 225-227, ingeschreven in het handelsregister onder KvK nummer 20164916, hierna eveneens te noemen "GGD", rechtsgeldig vertegenwoordigd door mevrouw A. van der Zijden;

(Partijen 26 en 27 hierna gezamenlijk aangeduid als: "**GGD GHOR**")

26. **Stichting Projectenbureau Publieke Gezondheid en Veiligheid Nederland**, statutair gevestigd te (3524 SJ) Utrecht, aan het Zwarte Woud 2, ingeschreven in het handelsregister van de Kamer van Koophandel onder nummer 41184548, rechtsgeldig vertegenwoordigd door de heer H.A.M. Backx;

27. **Vereniging met volledige rechtsbevoegdheid GGD GHOR Nederland,** statutair gevestigd te, statutair gevestigd te (3524 SJ) Utrecht, aan het Zwarte Woud 2, ingeschreven in het handelsregister van de Kamer van Koophandel onder nummer 40478156, rechtsgeldig vertegenwoordigd door de heer H.A.M. Backx;

Alle partijen hierna gezamenlijk aan te duiden als "**Partijen**".

KOMEN ALS VOLGT OVEREEN:

1. GGD'en verklaren bij deze volmacht te verlenen aan GGD GHOR en GGD GHOR te machtigen om voor en namens de GGD'en en zichzelf alle handelingen te verrichten die noodzakelijk of wenselijk zijn om te voldoen aan de op de GGD'en en GGD GHOR rustende mededelingsplicht aan de betrokkenen op basis van artikel 34 van de Algemene Verordening Gegevensbescherming (AVG) gerelateerd aan de (vervolg)meldingen door GGD GHOR op 22 en 25 januari 2021 bij de Autoriteit Persoonsgegevens op basis van artikel 33 AVG, alsmede de daarmee verband houdende (vervolg)onderzoeken van de Autoriteit Persoonsgegevens naar ongeautoriseerde toegang tot persoonsgegevens in de relevante systemen CoronIT en HPZone(Lite). De GGD geeft haar volmacht via een los tekenblad (bijlage).

2. GGD GHOR heeft voor de mededeling aan de betrokkenen een concept brief opgesteld. Na vaststelling zal de brief aan de GGD'en verstrekt worden. Deze brief zal daarna door GGD GHOR aan de betrokkenen die (mogelijk) geraakt zijn door het incident, worden gestuurd.

3. Deze volmacht geldt als een aanvulling op het tussen Partijen in april/mei/juni 2020 overeengekomen "Convenant Gegevensuitwisseling Gezamenlijk Verantwoordelijken" om of efficiënter te kunnen voldoen aan de op Partijen rustende mededelingsplichten aan betrokkenen op basis van artikel 34 AVG, en doet geen afbreuk aan de daarin gemaakte afspraken over de verantwoordelijkheden, verplichtingen, en aansprakelijkheden van Partijen.

Aldus overeengekomen op 25-02-2021

Document 10.16

DPG-Raad

d.d.: 22-10-2021	**Agendapunt 04**
Onderwerp:	**Mandaat Security Operation Center**
Strategisch thema:	Informatievoorziening/informatiebeveiliging
Portefeuillehouder:	[redacted]
Opgesteld door:	[redacted]
Overlegd met:	[redacted]
Status:	Ter instemming
	DPG-RAAD
Voorgestelde beslispunten:	- De DPG-Raad wordt gevraagd in te stemmen met de uitbreiding van de opdracht aan het SOC.
Aanleiding:	Na de datadiefstal van eind januari heeft de DPG-raad met een aantal maatregelen ingestemd teneinde de informatiebeveiliging te intensiveren. Eén van die maatregelen vormde de inzet van een Security Operation Center (SOC) dat het gebruik van de systemen CoronIT en HPzone(Lite) screent en de logfiles op afwijkend gedrag controleert. Afwijkingen worden vervolgens onderzocht en indien benodigd worden hierop maatregelen getroffen nadat met de betreffende werkgever (DPG of landelijke partner) in contact is getreden. Inmiddels wordt het SOC ook meer en meer bevraagd en benut in gevallen van (verdenkingen) van fraude zowel door de GGD'en als ook door politie en OM. Dit vraagt om een uitbreiding van de opdracht, en daarmee mandaat van het SOC, teneinde medewerking te geven aan dergelijke verzoeken. De DPG-raad wordt gevraagd om in te stemmen met de uitbreiding van de opdracht aan het SOC en de eigen CISO/informatiemanager evenals FG hierover te informeren.
Beoogd resultaat:	• Effectieve fraudebestrijding • Geformaliseerd mandaat/bevoegdheden SOC • Waarborgen rondom de bejegening en privacy van medewerkers
Argumenten:	Nu in Nederland gewerkt wordt met QR codes om toegang te krijgen tot diverse accommodaties en activiteiten, is het belang om als positief getest en/of gevaccineerd in de systemen te staan toe. Dit leidt ertoe dat mensen ook oneigenlijke wegen bewandelen of medewerkers onder druk zetten om al dan niet tegen betaling valse registraties te doen. In diverse GGD'en speelt dit momenteel en ook de politie krijgt hierover steeds vaker signalen binnen. Deze signalen willen we nader onderzoeken om dergelijke fraude een halt toe te roepen en te voorkomen dat er valse QR-codes in omloop komen. Voor dergelijk onderzoek is toegang tot o.a. onze logfiles, via het SOC benodigd.

	Het SOC dient echter secuur af te wegen of zij wel of niet aan dergelijke verzoeken gehoor kan gegeven, gezien de juridisch context waarbinnen zij dient te acteren. In bijgevoegd stappenplan is zichtbaar gemaakt, hoe de context gewogen dient te worden en wanneer het SOC wel/niet haar medewerking kan geven.
Financiële, personele en juridische consequenties:	• De kosten van het SOC, evenals de uitbreiding als gevolg van de verbreding van haar taak worden volledig gedekt uit de DVO. • Iedere GGD heeft aan haar OR instemming gevraagd voor de werkzaamheden van het SOC. Vervolgens zijn medewerkers zijn geïnformeerd over het bestaan van het SOC en de screening die op hun accounts in de systemen CoronIT en HPzone(Lite) plaatsvindt. • Bijgevoegd stappenplan is bedoeld om inzicht te geven in de zorgvuldige afhandeling van verzoeken door het SOC.
Eerder genomen besluiten:	- Instelling van het SOC - Instemmingsverzoek aan iedere OR rondom SOC
Bijlagen:	- Stappenplan toetsing externe verzoeken