SOLV B.V.
[redacted] en [redacted]
Anne Frankstraat 121
1018 BZ Amsterdam

Kenmerk:	293126616-15154	Datum:	1 juni 2022
Behandeld door:	[redacted]	E-mail:	[redacted]@ggdwestbrabant.nl
Onderwerp:	besluit Wob-verzoek		

Geachte heer [redacted]
Geachte mevrouw [redacted],

In uw brief van 15 februari 2022 verzocht u met een beroep op de Wet openbaarheid van bestuur om – samengevat – informatie en/of documenten over een datalek in de IT-systemen van de GGD'en. Uw verzoek is onderdeel van de bijlage.
De Veiligheidsregio Midden- en West-Brabant stuurde uw (soortgelijk) verzoek aan ons door en liet daarbij weten dat er geen documenten bij haar berusten.

Op 8 april 2022 lieten wij u weten dat wij ernaar streefden om uiterlijk 1 juni een besluit te nemen over uw verzoek. In deze brief staat dat besluit; we maken ook de documenten openbaar, voor zover die bij ons berusten. Het is het resultaat van een zorgvuldige zoektocht. We baseerden ons daarbij op de Wet open overheid (hierna: Woo) en waar nodig maakten we een afweging tussen het algemeen belang van openbaarheid en de door weigeringsgronden te beschermen belangen; zie daarover meer onder het kopje Documenten. Vindt u toch dat er documenten ontbreken, neemt u dan contact met ons op. Een aantal documenten die bij ons berusten heeft de GGD Zeeland intussen openbaar gemaakt. Wij verwijzen u daarvoor naar haar besluit en/of naar de website van de GGD Zeeland.

Zienswijzen
Drie documenten die wij openbaar willen maken gaan over derden die daar mogelijk bezwaar tegen hebben. Wij vragen hen om een zienswijze op ons (voorgenomen) besluit en verdagen voor die documenten ons besluit met vier weken. Daarna nemen wij over deze drie documenten een (deel)besluit. Het besluit in deze brief gaat over de documenten waarover wij geen zienswijze vragen.

Documenten

Van de documenten die u verzocht en die wij hierbij openbaar maken, vindt u een overzicht aan het begin van de bijlage: het is één bestand met alle documenten + de registers daarvan. We ordenden de documenten volgens uw eigen indeling (16 categorieën), met Romeinse cijfers en laten elke categorie voorafgaan door een register met de namen van de documenten.
Bij de documenten zitten ook e-mails die vallen onder de reikwijdte van uw verzoek en de daarbij horende (relevante) bijlagen. Het zijn e-mails over het datalek die wij vonden in de mailboxen van de directeur, de manager van het Programma Corona en de functionaris gegevensbescherming.

In de documenten die wij openbaar maken, maakten wij, met een beroep op artikelen van de Woo, in enkele documenten passages onleesbaar, volgens dit systeem:

- persoonsgegevens (Woo, artikel 5.1, lid 2, onder e.): met zwart;
- persoonlijke beleidsopvattingen (Woo, artikel 5.2, lid 1 en 2): met blauw;
- bedrijfs- en fabricagegegevens (Woo, artikel 5.1, lid 2, onder f.): met rood;
- het goed functioneren van de GGD (Woo, artikel 5.1, lid 2, onder 1.): met groen.

Tevens zijn er enkele documenten waar wij voor u nog naar op zoek zijn. Deze documenten zullen wij daarom conform de eerder genoemde procedure meesturen met het deelbesluit waarin u ook de documenten treft waarover wij een zienswijze hebben gevraagd van derden.

Op grond van de Algemene wet bestuursrecht kunt u tegen dit besluit een bezwaarschrift indienen binnen zes weken na de dag waarop wij het bekendmaakten. Zie daarvoor ons postadres.

Ik vertrouw erop dat ik u hiermee voldoende heb geïnformeerd.

Hoogachtend,
het dagelijks bestuur van de GGD West-Brabant,
namens deze,

Sebastiaan Baan
directeur publieke gezondheid

bijlage: Wob-verzoek ICAM - Documenten GGD West-Brabant
per mail verzonden aan: [redacted]@solv.nl en [redacted]@solv.nl
per brief verzonden aan SOLV B.V.

solv.
Anne Frankstraat 121
1018 BZ Amsterdam
T +31 (0)20 530 01 60
F +31 (0)20 530 01 70
www.solv.nl

16 FEB. 2022

GGD West-Brabant
Postbus 3024
5003 DA Tilburg

Alsmede per e-mail: info@ggdwestbrabant.nl

Datum	15 februari 2022	Van	[redacted], advocaat
Onze ref.	Wob-verzoek GGD-datalek		[redacted]
Uw ref.	-		[redacted]@solv.nl

Betreft: Wob-verzoek GGD-datalek

Geachte heer/mevrouw,

Op 25 januari 2021 werd door berichtgeving van RTL Nieuws bekend dat een grootschalig en ernstig datalek heeft plaatsgevonden in de IT-systemen die door de Gemeentelijke Gezondheidsdiensten ("**GGD'en**") worden gebruikt bij de bestrijding van het coronavirus.[1] Het gaat om de systemen CoronIT (testen en vaccineren), HPZone en HPZone (Lite) (bron- en contactonderzoek).

Namens onze cliënte, de Stichting Initiatieven Collectieve Acties Massaschade ("**ICAM**"), die opkomt voor de belangen van de gedupeerden van dit datalek, verzoeken wij u hierbij op grond van artikel 3 lid 1 van de Wet openbaarheid van bestuur ("**Wob**") de volgende informatie en/of documenten aan ons te verstrekken:

i) Alle offerteaanvragen, programma's van eisen, offertes en overeenkomsten, inclusief bijlagen, met betrekking tot de (door)ontwikkeling, implementatie en uitrol van CoronIT, HPZone en/of HPZone Lite, waaronder in ieder geval:
   a) Offertes GGD GHOR CoronIT d.d. 7 april 2020 en 6 juli 2020;
   b) Plan van aanpak GGD GHOR Fase 1 incl. begroting d.d. 7 april 2020;
   c) Plan van aanpak GGD GHOR Fase 2 incl. begroting d.d. 2 juni 2020 ;
   d) Vervolgaanpak GGD GHOR digitale ondersteuning testprocessen COVID-19 d.d. 27 oktober 2020 incl. bijbehorende offerte;
   e) De ARVODI-2018 ten aanzien van de ontwikkeling en implementatie van CoronIT;

[1] RTL Nieuws, 'Illegale handel in privégegevens miljoenen Nederlanders uit coronasystemen GGD' 25 januari 2021, https://www.rtlnieuws.nl/nieuws/nederland/artikel/5210644/handel-gegevens-nederlanders-ggd-systemen-database-coronit-hpzone.

ii) Alle offerteaanvragen, programma's van eisen, offertes en overeenkomsten, inclusief bijlagen, met betrekking tot de inrichting en instandhouding van een klantcontactcentrum voor test- en vaccinatieafspraken en bron- en contactonderzoek;

iii) Alle offerteaanvragen, programma's van eisen, offertes en overeenkomsten, inclusief bijlagen, met betrekking tot de uitbesteding aan derde partijen van klantcontact- en/of callcenterwerkzaamheden;

iv) Audits, rapportages, analyses en onderzoeken (intern of door derde partijen) met betrekking tot privacy(risico's) en beveiliging(srisico's) in verband met CoronIT, HPZone en HPZone Lite, waaronder in ieder geval:

a) Risicoanalyse uitgevoerd over de test- en traceerketen d.d. 22 december 2020;[2]

b) Analyse KPMG interne systemen d.d. 20 januari 2020; [3]

c) IT-assessment op het IT landschap van de COVID-19 bestrijding door GGD GHOR Nederland van december 2020;[4]

d) IT-audit KPMG d.d. 18 december 2020;[5]

v) Audits, rapportages, analyses en/of onderzoeken (intern of door derde partijen) ten aanzien van de effectiviteit van (beveiligings)maatregelen doorgevoerd na publiek bekend worden van het datalek, waaronder in ieder geval:

e) Rapportage functionele beveiligingstest uitgevoerd door Fox-IT; [6]

f) Extern onderzoek naar de kwaliteit van de software en de kwaliteit van de dienstverlening van de softwareleverancier van HPZone;[7]

g) Gateway reflectie en Gateway Review op verbeterplannen; [8]

h) Externe (technische en cutuur) audits genoemd in Kamerbrief d.d. 23 maart 2021;[9]

vi) Verslagen en notulen Regiegroep DOTT en Landelijke Coördinatiestructuur Testcapaciteit (LCT) met betrekking tot CoronIT en HPZone (Lite);

vii) Informatie over de verschillen in beveiliging tussen het reeds voor de coronacrisis bestaande systeem HPZone en het later ontwikkelde HPZone Lite;

viii) Data Protection Impact Assessments (DPIA) ten aanzien van CoronIT, HPZone en HPZone Lite;

ix) Het gehanteerde beveiligings- of privacybeleid omtrent het omgaan met persoonsgegevens en datalekken in verband met testen, vaccineren en bron- en contractonderzoek, waaronder het beleid ten aanzien van toegangsrechten en autorisatiebeheer en logging en monitoring;

---

2 *Kamerstukken II* 2020-2021, 27 529, nr. 252.
3 *Kamerstukken II* 2020-2021, 27 529, nr. 235, p. 9.
4 *Kamerstukken II* 2020-2021, 27 529, nr. 234, vraag 51.
5 Feitenrelaas inzake gebeurtenissen omtrent coronatest-IT-systeem van de GGD, p. 6.
6 Door de Tweede Kamer ontvangen op 28 april 2021, zoals blijkt uit *Kamerstukken II* 2020-2021, 25295, nr. 1179, p. 41.
7 Stand van zakenbrief digitale ondersteuning pandemiebestrijding d.d. 12 februari 2021.
8 *Kamerstukken II* 2020-2021, 25 295, nr. 995, p. 38-39.
9 *Kamerstukken II* 2020-2021, 25 295, nr. 1063, p. 33.

x) Informatie over signaleringen van gebreken of kwetsbaarheden in de (informatie)beveiliging in het kader van het testen, vaccineren en bron- en contactonderzoek, en de wijze waarop daarop is gereageerd en welke maatregelen daarop zijn genomen, waaronder signaleringen van (externe) GGD-medewerkers en van medewerkers van VWS;

xi) Informatie over de overname van het beheer van HPZone (Lite) door GGD GHOR;

xii) Informatie over de uitfasering van HPZone (Lite) en de vervanging van HPZone (Lite) door GGD Contact, waaronder in ieder geval:
   i) DPIA GGD Contact;
   j) Verwerkingsovereenkomst voor landelijke partner GGD Contact;
   k) Inbeheername GGD Contact door GGD GHOR en DICTUR;
   l) Autorisaties medewerkers GGD'en binnen GGD Contact;
   m) Werkinstructie GGD Contact;[10]

xiii) Overeenkomsten met GGD medewerkers en externen die gebruik maken en hebben gemaakt van CoronIT, HPZone en/of HPZone Lite, waaronder maar niet beperkt tot arbeidsovereenkomsten, opdrachtovereenkomst en/of geheimhoudingsovereenkomsten;

xiv) Informatie en documenten met betrekking tot de training van (externe) medewerkers ten aanzien van het gebruik van CoronIT en HPZone (Lite) en de omgang met persoonsgegevens, waaronder beleid, protocollen, instructies en presentaties;

xv) Informatie die in het kader van de melding van het datalek bij de Autoriteit Persoonsgegevens over en weer is gedeeld, alsmede informatie die over en weer is verstrekt ten behoeve van het onderzoek door de Autoriteit Persoonsgegevens naar aanleiding van het datalek;

xvi) Informatie en documenten over het onderzoek dat heeft plaatsgevonden naar de omvang van de groep gedupeerden en de potentiële schadelijke gevolgen van het datalek.

De bestuurlijke aangelegenheid die dit betreft moet ruim worden opgevat. Het betreft zowel de keuze voor en de ingebruikname en beveiliging van de genoemde IT-systemen en eventuele gerelateerde systemen of diensten, de keuze voor en afspraken met derde partijen, informatiebeveiligingsbeleid en beveiligingsmaatregelen en -procedures, incidenten of signaleringen in verband met de veiligheid van de genoemde systemen, als de wijze waarop de overheid heeft gereageerd op het GGD-datalek.

Uitdrukkelijk merken wij op dat bovengenoemde opsomming niet limitatief is. Cliënte wenst alle informatie te ontvangen die haar in staat stelt om in het kader van het datalek (i) de betrokkenheid, rol en verantwoordelijkheid van de verschillende partijen vast te stellen, (ii) de omvang van het datalek en de schade die de gedupeerden ten gevolg daarvan hebben geleden, te kunnen bepalen en (iii) ten aanzien van de IT-systemen vast te stellen welke eisen voorafgaand aan en na het publiekelijk bekend worden van het datalek zijn gesteld en welke organisatorische en technische beveiligingsmaatregelen zijn getroffen.

[10] Documenten zoals genoemd in: Ministerie VWS, 'Lancering GGD Contact', 24 november 2020.

Buiten klassieke gegevensdragers vallen ook documenten op beeld- en geluidsdragers en digital bestanden onder dit verzoek. Te denken valt aan gespreksverslagen, memo's, nota's, studies, onderzoeken, notulen, voortgangsrapportages en afsprakenlijsten, en tevens aan brieven, faxen, e-mails, werkopdrachten, enzovoorts.

Wij verzoeken u de informatie en documenten zoveel mogelijk te verstrekken door daarvan kopieën te geven of de letterlijke inhoud in andere vorm te verstrekken. Uitsluitend voor zover dat redelijkerwijs niet gevergd kan worden, verzoeken wij u de informatie te verstrekken door kennisneming van de inhoud toe te staan, een uittreksel of een samenvatting van de inhoud te geven, of inlichtingen daaruit te verschaffen.

Wij verzoeken u de verzochte informatie en documenten digitaal toe te sturen aan [redacted]@solv.nl en [redacted]@solv.nl.

Met verwijzing naar de termijn die is genoemd in artikel 6 lid 1 Wob verzoeken wij u om de gevraagde informatie en documenten uiterlijk op **16 maart 2022** toe te sturen.

De uitzonderingsgronden genoemd in artikel 10 en 11 Wob zijn naar het oordeel van cliënte in het onderhavige geval niet van toepassing. Voor zover de in deze bepalingen genoemde belangen aan de orde zouden zijn, dient het belang van de gedupeerden van het GGD-datalek en van Stichting ICAM om inzicht te verkrijgen in de ernst en omvang van het GGD-datalek zwaarder te wegen.

Indien u zich genoodzaakt ziet dit verzoek geheel of gedeeltelijk te weigeren verzoeken wij subsidiair om een ambtelijk beperkte versie en meer subsidiair om een samenvatting. Daarbij verzoeken wij u iedere weigering per document te motiveren.

Daar waar documenten zich niet bij of onder u bevinden, verzoeken wij om doorgeleiding van dit verzoek waar dit een bestuursorgaan betreft. Voor het geval documenten zich bevinden bij niet-bestuursorganen verzoeken wij u de documenten bij u te laten bezorgen en hier een beslissing over te nemen.

Graag ontvangen wij een ontvangstbevestiging van dit verzoek, alsmede de contactgegevens van de persoon tot wie wij ons kunnen wenden voor de opvolging van dit verzoek.

Wij zijn graag beschikbaar voor overleg over dit verzoek.

Hoogachtend,

SOLV Advocaten
mr. [redacted]
mr. [redacted]

Bijlage 1: Wob-verzoek ICAM - Documenten GGD West-Brabant

- 1 Documenten over coronit, HPZone en HPzone Lite
- 2 Documenten m.b.t. KKC voor test, vaccinatie en BCO
- 3 Documenten m.b.t. uitbestedingen aan derden van KCC
- 4 Documenten m.b.t. privacy en beveiliging i.v.m. systemen
- 5 Documenten m.b.t. maatregelen na datalek
- 6 Documenten DOTT en LTC m.b.t. CoronIT en HPZone(lite)
- 7 Documenten m.b.t. verschillen systemen HPZone en Lite
- 8 DPIA t.a.v. systemen
- 9 Beveiliging- en privacy beleid omtrent persoonsgegevens
- 10 Documenten over gebreken van informatiebeveiliging
- 11 Documenten over overname van HPZone door GGD GHOR
- 12 Documenten over uitfasering HPZone(lite) en vervanging door GGD contact
- 13 Opdracht- en geheimhoudingsovereenkomst medewerkers
- 14 Documenten m.b.t. training medewerkers over omgang persoonsgegevens
- 15 Documenten m.b.t. de melding van datalek bij AP
- 16 Documenten over onderzoek van gedupeerden en gevolgen hiervan

Wob-verzoek SOLV/ICAM datalek 2021 coronasysteem

1.0 Tekst Wob-verzoek en register documenten

Tekst verzoek (i)

Alle offerteaanvragen, programma's van eisen, offertes en overeenkomsten, inclusief bijlagen, met betrekking tot de (door)-ontwikkeling, implementatie en uitrol van CoronIT, HPZone en/of HPZone Lite, waaronder in ieder geval:

a) Offertes GGD GHOR CoronIT d.d. 7 april 2020 en 6 juli 2020;

b) Plan van aanpak GGD GHOR Fase 1 incl. begroting d.d. 7 april 2020;

c) Plan van aanpak GGD GHOR Fase 2 incl. begroting d.d. 2 juni 2020;

d) Vervolgaanpak GGD GHOR digitale ondersteuning testprocessen COVID 19 d.d. 27 oktober2020 incl. bijbehorende offerte;

e) De ARVODI-2018 ten aanzien van de ontwikkeling en implementatie van CoronIT

Register

Een screenshot van de verkennerpagina van map 1:

Brabant-Zuidoost

Betreft: [redacted]
Datum: 19 oktober 2020

Dag [redacted]

Graag licht ik mijn standpunt toe ter zake waarom de gegevens in CoronIT onder andere onder de Wpg worden verzameld en daarmee toestemming van de betrokkene niet vereist is voor wat betreft het verdere gebruik van deze gegevens voor het dashboard en mogelijke andere statistische- of onderzoekdoeleinden.

Ik ben het eens met [redacted] dat het testen van mensen op COVID-19 op de teststraten geen Wpg-taak is. Hier komt de WGBO om de hoek heen kijken. Echter, is het belangrijk om een goed onderscheid te blijven maken tussen gegevens die verkregen zijn op grond van de Wpg en de WGBO, ondanks de vermening van Wpg en WGBO. Dit geldt zowel voor CoronIT en HPZone. Daarnaast worden de gegevens in CoronIT niet zonder meer enkel verkregen op basis van de uitgevoerde coronatesten op de teststraat. Alle gegevens (met uitzondering van de monsters, registratie daarvan en adviezen) van de betrokkene worden verkregen door het callcenter en/of burgerportaal en de labs.

Wet publieke gezondheid (Wpg)

I. CoronIT bestaat uit Wpg en voor een bepaald gedeelte uit WGBO (ten minste voor wat betreft de afgenomen monsters, registratie daarvan en adviezen). Vanuit Wpg kunnen gegevens verder worden verwerkt voor statistische of onderzoeksdoeleinden (zolang die in het kader van de Wpg zijn aangeleverd en er natuurlijk wordt voldaan aan andere eisen van de AVG). Normaliter krijgt de GGD op grond van artikel 21 en 24 Wpg meerdere gegevens aangeleverd in het kader van infectieziektebestrijding. Het gaat om de volgende gegevens:

> ***a****. de naam, het adres, het geslacht, de geboortedatum, het burgerservicenummer en de verblijfplaats van de betrokken persoon,*
>
> ***b.*** *de infectieziekte dan wel een beschrijving van het ziektebeeld, de eerste ziektedag, de vaccinatietoestand, het gebruik van chemoprofylaxe, de vermoedelijke infectiebron, de datum van vermoeden of vaststelling van infectie, de wijze van vaststelling van die infectieziekte, en*
>
> ***c.*** *indien nodig, of de betrokken persoon dan wel een persoon in zijn directe omgeving beroeps- of bedrijfsmatig betrokken is bij de behandeling van eet- of drinkwaren of bij de behandeling, verpleging of verzorging van andere personen.*

Deze pandemie heeft ervoor gezorgd dat de werkwijze heeft moeten afwijken van de standaard. Het zijn niet meer de artsen die bovenstaande gegevens aanleveren, maar dit gebeurt vanuit CoronIT (het callcenter), nu het niet mogelijk was om artsen hiervoor te gaan inzetten. Alhoewel in het kader hiervan vaak geen sprake is van een arts zoals bedoeld in de Wpg (door de bijzondere inrichting van het callcenter en de teststraten en coronIT), wordt de Wpg naar analogie gebruikt. Dit gebeurt op grond van artikel 6 Wpg. Dit is in overleg met het VWS bepaald. Dit betekent dat wij op grond van artikel 6 Wpg (naar analogie van

artikel 21 en 24 Wpg) recht hebben op bovenstaande gegevens. Onze grondslag om deze gegevens in CoronIT (en deels HPZone) te verwerken is om die reden op grond van de Wpg. Wij hebben recht op bovenstaande gegevens en kunnen deze gebruiken om in het kader van volksgezondheid een beeld te krijgen op de ontwikkeling van de verspreiding van het virus (los van het BSN uiteraard). Er zit een noodzaak aan vast. Uiteraard moeten wij dit goed verantwoorden, maar toestemming als grondslag voor verwerking is dan niet nodig. Immers, op grond van de AVG is verdere verwerking op grond van statistische- of onderzoeksdoeleinden verenigbaar met het doel waarvoor de gegevens in beginsel zijn verwerkt (Wpg). Dit betekent dat de Wpg als grondslag voor de verdere verwerking dient.

II. Ook krijgen wij op grond van artikel 25 lid 2 en 3 Wpg gegevens van het laboratorium. Het betreft dan:

> ***2*** *Onverminderd artikel 22 meldt het hoofd van het laboratorium de vaststelling van een verwekker van een infectieziekte behorend tot groep A, B1, B2 of C aan de gemeentelijke gezondheidsdienst van de gemeente waarin de arts die het onderzoek bij het laboratorium heeft aangevraagd zijn praktijk heeft.*
>
> ***3*** *De melding bevat de volgende gegevens: de naam van de arts, de naam, de geboortedatum en het burgerservicenummer van de betrokken persoon.*

Ook deze gegevens verwerkt de GGD op grond de Wpg. Indien de GGD deze gegevens verder verwerkt voor statistische- of onderzoekdoeleinden, om zo een beeld te krijgen op de ontwikkeling van de verspreiding van de ziekte, is de toestemming van de betrokkene niet nodig. Immers, ook hier is de verwerking verenigbaar met het doel waarvoor de persoonsgegevens in beginsel worden verwerkt.

III. Indien de arts (deze is nu niet van toepassing, maar het idee is niet anders) andere gegevens dan zoals boven genoemd aan de GGD wil strekken (dus eigenlijk als wij in het dasboard andere gegevens meenemen dan zoals hierboven vermeld), dan moet aan de betrokkene wel om toestemming worden vragen. Denk aan telefoonnummer en e-mailadres die in CoronIT worden verwerkt. Immers, deze 'extra' gegevens zijn niet verkregen op grond van de Wpg -> art. 24 lid 4 Wpg vermeldt:

> *De arts verstrekt aan de gemeentelijke gezondheidsdienst uitsluitend andere medische gegevens over de betrokken persoon indien:*
>
> ***b.*** *de betrokken persoon daarvoor toestemming geeft.*

WGBO

Het benoemen van onderzoek in het kader van WGBO is begrijpelijk, doch lijkt in beginsel dat GGD geen onderzoeken uitvoert als bedoeld in de WGBO. Denk aan onderzoek waarbij de monster worden geanalyseerd om de werking van het virus te begrijpen. Het doel van de GGD is de focus op de ontwikkeling van de verspreiding van het virus in het kader van volksgezondheid. Indien en voor zover de GGD'en ook onderzoek in het kader van de WGBO uitvoeren, dan geldt het volgende vanuit de WGBO. De gegevens van de 'patiënt' van het medische dossier kan aan een ander worden verstrekt in het kader van statistische doeleinden. Dit zou dus in basis de monsters betreffen. Het klopt dat toestemming niet nodig is als het vragen van die toestemming onmogelijk is.

Echter, is dit 1 van de 2 uitzondering. De tweede uitzondering wordt niet benoemd. De tweede uitzondering is;

'het vragen van toestemming, gelet op de aard en het doel van het onderzoek, in redelijkheid niet kan worden verlangd en de hulpverlener zorg heeft gedragen dat de gegevens in zodanige vorm worden verstrekt dat herleiding tot individuele natuurlijke personen redelijkerwijs wordt voorkomen.'

De wet legt de tweede uitzondering als volg uit: *'Met de woorden 'in redelijkheid niet te verlangen' heeft de wetgever speciaal gedacht aan onderzoeken waarbij zo grote aantallen patiënten zijn betrokken dat redelijkerwijs niet kan worden gevergd dat inspanningen worden gedaan om hen allen te bereiken, dan wel, in uitzonderlijke omstandigheden, aan onderzoeken van zodanige aard dat het vragen van toestemming zou leiden tot een selectieve respons en daarvan een vertekend beeld van het onderzoeksresultaat als reëel gevolg moet worden gevreesd (NvW 4, Kamerstukken II, 21561, 20, p. 3)'*

Op grond van bovenstaande zou gesteld kunnen worden, indien en voor zover de analyses van de GGD'en kunnen worden gezien als onderzoeken in het kader van de WGBO (wat te betwijfelen valt), op grond van de tweede uitzondering een mogelijkheid bestaat om de toestemming van de betrokkene te 'passeren'. Uiteraard moet er dan voor gezorgd worden, zoals de tweede uitzondering stelt, dat herleiding tot individuele natuurlijke personen redelijkerwijs wordt voorkomen. Dit zal voor ons tijdens de verwerking lastiger zijn, nu wij natuurlijk ook de herleidbare gegevens hebben, maar uiteraard moeten de gegevens in het onderzoek zelf zodanig worden uitgezet, dat uit een analyse of onderzoek zelf de betrokkene rederlijkwijs niet herleidbaar is.

Conclusie

Zoals hierboven vermeld is de toestemming van betrokkene niet nodig indien de gegevens op grond van de Wpg worden verzameld, hetgeen in verre weg de meeste gevallen het geval is. Indien er sprake zou zijn van de WGBO, kan gebruik worden gemaakt van de tweede uitzondering voor wat betreft het niet hoeven vragen om toestemming. Let wel dat te allen tijde goed moeten worden gemotiveerd waarom geen toestemming wordt gevraagd. Enige uitzondering waarvoor wel toestemming moet worden gevraagd, betreft die gegevens zoals vermeld in artikel 24 lid 4 Wpg, namelijk gegevens die zowel niet zijn verzameld op grond van de Wpg als niet op grond van de WGBO.

Hopende jullie hier van voldoende informatie te hebben voorzien.

Met vriendelijke groeten,

[redacted]

Wat is CoronIT?

CoronIT is een digitaal landelijk systeem dat het uitvoeren van de COVID-19 testprocessen bij GGD'en en laboratoria efficiënt kan ondersteunen bij:

- triage en aanmelden;
- inplannen;
- afname en registratie;
- het vastleggen van de resultaten;
- het doorgeven van resultaten.

Doordat gegevens digitaal bij de bron worden vastgelegd kunnen GGD'en en laboratoria efficiënter en met meer kwaliteit werken.

Van wie is CoronIT?

De realisatie van CoronIT gebeurt in een samenwerkingsverband van GGD GHOR Nederland, de FSB (Facilitaire Samenwerking Bevolkingsonderzoeken), het RIVM, Topicus en Roche. GGD GHOR Nederland treedt daarbij op als projectleider. De kosten van het project worden vergoed door VWS.

Waar kan CoronIT bij helpen?

Bij de testprocessen rond COVID-19 zijn diverse partijen betrokken: artsen, GGD'en, de reguliere laboratoria waar de GGD'en mee samenwerken, extra laboratoria en in de nabije toekomst mogelijk ook de organisaties voor bevolkingsonderzoeken en anderen die GGD'en helpen met extra testfaciliteiten. Een deel van genoemde partijen heeft niet eerder samengewerkt en zal dat in deze combinatie, naar verwachting, ook in de toekomst niet meer doen.

Door betrokken partijen op één digitaal systeem aan te sluiten (CoronIT) is het beter mogelijk om landelijk overzicht te bewaren en alle beschikbare capaciteit goed te gebruiken. Bovendien kan veel tijd worden bespaard, doordat in het CoronIT systeem gegevens maar één keer hoeven te worden ingevoerd.

CoronIT is één (tijdelijk te gebruiken) systeem dat de testprocessen zo goed mogelijk ondersteunt doordat:

- De triage wordt uitgevoerd door de triage-arts (voor werknemers bij voorkeur de bedrijfsarts, anders behandelend arts, huisarts of instellingsarts) en niet hoeft te worden overgedaan door de GGD tenzij er nog geen triage heeft plaatsgevonden (vangnetfunctie).
- De afspraak desgewenst ook tijdens het contact van de medewerker met de triage-arts kan worden gemaakt. Als alle beschikbare testfaciliteiten op CoronIT zijn aangesloten, is voor alle triage-artsen en GGD'en zichtbaar bij welke testfaciliteit en op welk tijdstip er plaats is voor een testafname en kan de beschikbare capaciteit optimaal worden benut. Dit leidt tot een kortere doorlooptijd. Ook andere varianten, zoals in het geval dat de GGD de afspraak zelf maakt omdat er met een centraal afsprakencentrum wordt gewerkt, zijn eenvoudig aan te sluiten op dit systeem.

- Testresultaten automatisch worden vastgelegd in het CoronIT systeem en daarmee direct beschikbaar zijn voor de GGD en aanvrager, en niet meer (zoals nu) via (zorg)mail door het laboratorium aan de GGD doorgegeven en daarna handmatig overgenomen.
- De capaciteit optimaal kan worden benut omdat alle testfaciliteiten en alle laboratoria op het CoronIT systeem zijn aangesloten. Daardoor kan een GGD, indien nodig, eenvoudig (tijdelijk) monsters naar een ander lab versturen.
- Er controle is op de testketen, doordat de aankomst van een monster in een lab door het lab in het systeem bevestigd wordt.
- Aanvragers direct na binnenkomst van het resultaat geautomatiseerd kunnen worden ingelicht over de uitslag.
- Om vertraging te voorkomen de testuitslag van zorgmedewerkers evt. direct toegestuurd kan worden.
- Landelijke en regionale overzichten van het aantal afgenomen testen en resultaten, inclusief trends, dagelijks automatisch worden aangeleverd aan GGD'en, RIVM en andere gerechtigden.
- Het landelijk inzicht behouden blijft en GGD'en blijven positieve resultaten automatisch ontvangen, ook als in een opgeschaalde situatie testen door andere partijen zijn afgenomen.

Wat kan CoronIT op dit moment?

Versie 1.0 van CoronIT is gereed voor uitrol en gebruik. Deze versie bevat de volgende functionaliteiten:

- door de GGD-plannen van het testproces;
- geautomatiseerd (per e-mail en SMS) bevestigen van afspraken van te testen personen in de testfaciliteit;
- registratie bemonstering;
- geautomatiseerd vastleggen labuitslagen.

Welke functionaliteiten komen daar nog bij?

CoronIT wordt doorontwikkeld en wordt steeds aangepast aan de veranderende situatie. De volgende functionaliteiten worden de komende dagen/weken in ieder geval uitgewerkt:

- Vastleggen aanvraag test.
- Onderzoek (en zo mogelijk realisatie) aansluiten bedrijfsartsen/instellingsartsen.
- Vastleggen aanvraag test en inplannen afspraken door arts.
- Desgewenst: uitbreiden inrichting voor testen patiënten in GGD-testfaciliteiten, incl. onderzoek naar aansluiten huisartsen.
- Desgewenst: uitbreiden inrichting voor inplannen huisbezoek voor afname test.
- Geautomatiseerd (per e-mail) delen van uitslagen met betrokkenen.
- Bij positieve test: gegevens doorsturen naar IZB-systemen van de GGD'en (HPZone e.a.).
- Dagelijks geautomatiseerd aanleveren van rapportages aan alle betrokkenen.

De komende dagen (vandaag en wellicht ook morgen) wordt een planning opgesteld voor de ontwikkeling van hierboven genoemde functionaliteiten. Zodra deze bekend is zullen we die

communiceren via de bij GGD GHOR Nederland bekende contactpersonen voor de COVID-testfaciliteit.

Wie zijn (en/of worden binnenkort) aangesloten?

Al in de beginfase van het project is op verzoek van VWS afgesproken, dat de BVO HPV-laboratoria, het lab van Sanquin en de twee diergeneeskundige laboratoria als eerste op het systeem worden aangesloten zodat de extra testcapaciteit van deze labs zo snel mogelijk voor het hele land beschikbaar is. Dit proces is in volle gang: vandaag vinden de eerste systeemtesten plaats. Als die succesvol zijn, kan deze fase snel worden afgerond.

Ook starten we deze week met het aansluiten van de IZB-afdeling en het laboratorium van de GGD Amsterdam. Deze implementatie wordt gebruikt om de implementatiedraaiboeken en de handleidingen en die ontwikkeld zijn te testen en waar nodig bij te stellen. Kort daarna volgt de landelijke implementatie, waarbij alle GGD'en en alle Medisch Microbiologisch laboratoria worden aangesloten. Het aansluiten van laboratoria vraagt geen actie van de GGD.

Hoe gaat het dan (praktisch) werken?

Op dit moment is een implementatieteam aan het werk om de uitrol bij de GGD'en en bij de verschillende laboratoria voor te bereiden en uit te voeren. Werkinstructies, procesbeschrijvingen en opleidingsmateriaal afgestemd op de verschillende gebruikersgroepen worden voorbereid. Ook wordt nagedacht over de wijze waarop we grote groepen (toekomstige) gebruikers kunnen gaan opleiden. Denk bijvoorbeeld aan instructie-video's, webinars, etc. Het uitroldraaiboek wordt met iedere GGD en laboratorium afgestemd. De komende week neemt het implementatieteam contact op met alle GGD'en om de implementatie verder voor te bereiden.

Wat gaat er in de praktijk veranderen als ik met CoronIT werk?

De wijzigingen die nodig zijn kunnen per GGD verschillen. Het landelijke implementatieteam helpt om de nieuwe werkwijze zo goed mogelijk aan de specifieke situatie aan te passen. Over de details van het werken met CoronIT nemen we nog contact op via de bij GGD GHOR Nederland bekende contactpersonen voor de COVID-testfaciliteit.

Werken met CoronIT betekent in ieder geval dat:

- Veel werk dat nu (handmatig) door de GGD wordt gedaan niet meer nodig is.
- Formulieren en teksten van mails en SMS-jes in het hele land hetzelfde zijn (uiteraard met uitzondering van bijvoorbeeld datum, tijd en locatie van de test).
- GGD-medewerkers om veilig (met multifactor authenticatie) in te kunnen loggen moeten beschikken over een mobiele telefoon. Als dit onmogelijk is kunnen er tokens verstrekt worden.
- In overleg met de betrokken laboratoria overgestapt wordt op het gebruik van monsterbuizen die vooraf van een barcodesticker voorzien worden. Iedere monsterbuis is daarmee voorzien van een uniek nummer.

- Op de afnameplek (teststraat etc.) een laptop met internet en een barcodescanner aanwezig moet zijn, zodat de monsterbuis aan de client kan worden gekoppeld.

Wie zitten er in het CoronIT implementatieteam?

Aan de realisatie en implementatie van CoronIT wordt gewerkt door een groot team van medewerkers. Het kernteam bestaat uit:

- [redacted] (M&I): Projectleiding
- [redacted] (GGD GHOR Nederland): Informatiemanager
- [redacted] (FSB): Opdrachtgever Topicus en aansluiting 8 extra laboratoria
- [redacted] (RIVM): Aansluiting Medisch Microbiologische laboratoria
- [redacted] (M&I): Training en implementatie
- [redacted] (GGD GHOR Nederland): Organisatie Servicedesk
- [redacted] (Cuccibu): Functionaris Gegevensbescherming
- [redacted] (Significant): Manager contracten
- [redacted] (GGD GHOR Nederland): Communicatie
- [redacted] (Topicus): Vertegenwoordiging ontwikkelteam Topicus

Wat als ik meer wil weten?

We realiseren ons, dat nog niet alle informatie bekend is. Daarom zullen we de komende dagen regelmatig updates versturen. Mocht je nu al dringende vragen hebben, dan kan je die stellen via coronit@ggdghor.nl

Beste [redacted]

Hierbij willen wij je informeren over het landelijke, digitale registratiesysteem CoronIT. CoronIT is een systeem dat het uitvoeren van de COVID-19 testprocessen bij GGD'en en laboratoria efficiënt kan ondersteunen. Deze webapplicatie wordt vergoed door het ministerie van VWS en gaat op zeer korte termijn live bij alle GGD'en. Het is de bedoeling dat GGD'en uiterlijk op 8 mei werken met CoronIT of bezig zijn met de implementatie daarvan. Het projectleiderschap van CoronIT is in handen van GGD GHOR Nederland.

Registratiesysteem CoronIT

Het doel van de CoronIT is het automatiseren, vergemakkelijken, versnellen en zoveel mogelijk centraliseren van de administratie behorende bij het testproces op COVID-19. CoronIT maakt het mogelijk om het proces van triage, aanvraag tot het terugkoppelen en het delen van een testuitslag te vereenvoudigen en te versnellen. Hierdoor wordt het mogelijk om de opgeschaalde testcapaciteit van de laboratoria gericht en efficiënt in te zetten. Met behulp van het registratiesysteem kunnen GGD'en en externe aanvragers bij vermoeden van besmetting, personen snel en efficiënt laten testen op COVID-19.

Informatie met betrekking tot CoronIT

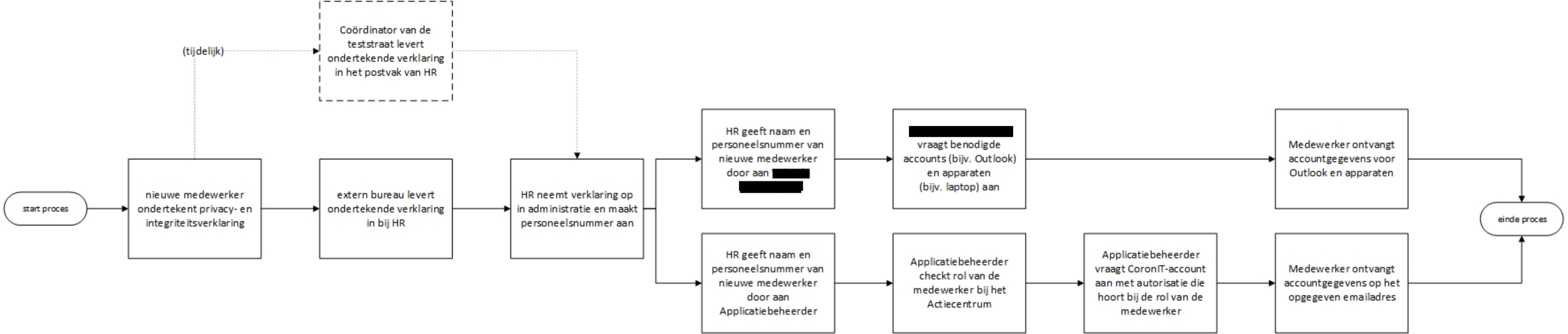
In het project is een FG betrokken, die risico's in kaart brengt en adviezen geeft over adequate bescherming van persoonsgegevens. Wij gaan alle relevante informatie met u te delen, maar zijn op dit moment nog zoekende naar de meest optimale manier daarvoor. Zodra dit bekend is, stellen wij u op de hoogte en krijgt u toegang tot de informatie. Op dit moment werken wij nog aan de DPIA op de webapplicatie. Wij houden u op de hoogte van relevante ontwikkelingen.

Vragen

Wellicht was u nog niet op de hoogte van de implementatie van het registratiesysteem CoronIT. In eerste instantie zijn de bij ons bekende contactpersonen van de teststraten van de GGD'en geïnformeerd. Hebt u vragen naar aanleiding van dit bericht, de webapplicatie of specifieke vragen over de privacy en security aspecten van CoronIT, dan kunt u per mail contact opnemen met het projectteam implementatie via coronit@ggdghor.nl.

Wij hopen u hiermee vooralsnog voldoende te hebben geïnformeerd.

Met vriendelijke groet,
Namens het projectteam implementatie CoronIT


(tijdelijk)
Coördinator van de teststraat levert ondertekende verklaring in het postvak van HR
start proces
nieuwe medewerker ondertekent privacy- en integriteitsverklaring
extern bureau levert ondertekende verklaring in bij HR
HR neemt verklaring op in administratie en maakt personeelsnummer aan
HR geeft naam en personeelsnummer van nieuwe medewerker door aan [redacted]
[redacted] vraagt benodigde accounts (bijv. Outlook) en apparaten (bijv. laptop) aan
Medewerker ontvangt accountgegevens voor Outlook en apparaten
HR geeft naam en personeelsnummer van nieuwe medewerker door aan Applicatiebeheerder
Applicatiebeheerder checkt rol van de medewerker bij het Actiecentrum
Applicatiebeheerder vraagt CoronIT-account aan met autorisatie die hoort bij de rol van de medewerker
Medewerker ontvangt accountgegevens op het opgegeven emailadres
einde proces

Agenda

Aan: [redacted]

Van: [redacted]

Betreft: Actiepunten 19/8/2020 Informatie beveiligingsmanagement forum GGD WB
Verzet naar 14/9/2020

Locatie: **MS Teams (zie outlook uitnodiging)**

1. In-, door- en uitstroom Beaufort, AD (en Coron IT/ HPZone)

- Zorgen over beperkt zicht uit uitgifte van druppels en ICT materialen (laptops) aan nieuwe (tijdelijke) medewerkers ivm Corona.
- Zorgen over ondertekening van integriteits- en geheimhoudingsverklaringen en (geldige) VOG's voor nieuwe (tijdelijke) medewerkers op de teststraat en tbv BCO

Actiepunten:

1. [redacted] maakt een legenda op basis waarvan de concreet te nemen acties adhv de lijst verklaard worden
2. [redacted] neemt contact op met HR om de lijst samen door te spreken
3. [redacted] plant overleg in tussen [redacted] over de (eventueel) te nemen acties t.a.v. de risico's die gepaard gaan met verstrekking van druppels, laptops en het niet ondertekenen of administreren van een contractuele verplichting tot geheimhouding van nieuw personeel.

2. Rapportage Inzigt – meldingen Topdesk

Actiepunten:

4. [redacted] maakt een bericht met een trendanalyse. Wie meldt er, waarover, hoev aak, toe- of afnames, duiding en verklaringen.

3. Incidenten en datalekken

4. Stand van zaken GAP analyse informatiebeveiliging en implementatie risicomanagement informatiebeveiliging / implementatie NEN7510/BIO

Zie bijlage 'IB risicoregister'

5. [redacted] plant aparte afspraak in over IB risicomanagement bij GGD WB met [redacted]. Hierbij wordt zowel inhoudelijk als procesmatig de actuele stand van zaken beoordeeld.

5. Reacties uit het veld mbt veilig mailen via Microsoft

6. Informeren bestuur over stand van zaken informatieveiligheid

7. Nieuwe ontwikkelingen

- CIIO

Agenda

- CoronaMelderApp
- Datawarehouse: verwerking persoonsgegevens GGD BZO
- Corona uitslagen via portaal
- Corona ChatBot
- ISO 9001 CIIO

7. Wvttk

6. [redacted] stuurt DPIA's over nieuwe verwerkingen zo veel mogelijk door aan [redacted]

Datum: 2 december 2020

Betreft: **Onderlegger voor gesprek DPG en IZB-team over HP Zone**

Beste collega,

Afgelopen woensdag is de notitie 'Samen naar een betere digitale ondersteuning van infectieziektebestrijding' besproken in de DPG Raad.

Ik heb toegezegd in aansluiting daarop een notitie op te stellen die als onderlegger kan dienen voor het door elk van jullie te voeren gesprek in je eigen GGD; met de eigen IZB-professionals van je GGD. Hierbij los ik deze toezegging in.

Kern van de notitie zoals besproken op woensdag 25 november jl is dat het na negen maanden pandemiebestrijding tijd is om de kwetsbaarheden op het gebied van ICT binnen de IZB-keten aan te pakken. Optimale IZB en optimale ICT gaan hand in hand. Sinds februari wordt er door een grote groep IZB-professionals keihard gewerkt om het coronavirus in te dammen. De opgave is enorm. De geleverde prestaties ook. Steeds meer is de samenwerking met collega's elders in het land gezocht en gevonden. En dat was nodig. We hebben geleerd dat corona zich niks aantrekt van grenzen. Dit ene virus kunnen we alleen bestrijden door over onze eigen grenzen heen te stappen. Het is nu het moment om hierin verdere stappen te zetten. Samen. Ik zet hier even op een rijtje wat er de komende tijd allemaal staat te gebeuren.

HP Zone

Op korte termijn neemt GGD GHOR Nederland HP Zone in beheer. Bij het verenigingsbureau zal daarvoor een team functioneel beheer en een helpdesk worden ingericht. GGD GHOR Nederland zal overzicht houden over de te ontwikkelen functionaliteit en de prioritering bespreken met de leverancier, Infact. De helpdesk zal vragen en problemen bij het gebruik van HP Zone oppakken en zo nodig contact leggen met de leverancier.

HP Zone is natuurlijk de software van de infectieziekteprofessionals van de regionale GGD'en. Zonder hen was HP-zone er nooit geweest. Er zit veel tijd en inzet van hen in HP-zone. Het is dan ook van belang dat de IZ-professionals nauw betrokken blijven bij beheer en de ontwikkeling. De HP Zone-gebruikersgroep heeft, ook toen de infectieziektebestrijding minder bestuurlijke en politieke aandacht kreeg, met hart en ziel de applicatie ontwikkeld en onderhouden. Dat verdient onze waardering. Belangrijk aandachtspunt voor GGD GHOR is het versterken van de regie op de beheer- en ontwikkelprocessen van de leverancier namens de GGD-en. Dat borgt dat de werkprocessen in HPZone en de ondersteunende ICT steeds blijven aansluiten bij de praktijk van alle dag.

De gebruikersgroep krijgt daarom ook in de nieuwe governance van HP Zone een centrale plek. De gebruikersgroep zal als product owner gedelegeerd opdrachtgever zijn richting de beheerorganisatie bij

GGD GHOR Nederland en de prioriteiten stellen voor de ontwikkeling van HP Zone. De product owner zal in de nieuwe beheerorganisatie ondersteund worden voor wat betreft ICT aspecten van bijvoorbeeld verbeteringsvoorstellen (RFC's). De vereniging GGDGHOR NL heeft voor de inbeheername een programmamanager aangesteld, [redacted]

Toekomstige ontwikkelingen

De COVID-19-epidemie stelt de infectieziektebestrijding en de ondersteunende ICT-infrastructuur voor grote uitdagingen. HP Zone is een onderdeel van een veel breder ICT-landschap dat de hele test- en traceerketen ondersteunt. Gegevens worden uitgewisseld met RIVM (Osiris, contactdata), VWS en CBS. De huidige inrichting van het ICT-landschap is niet optimaal. De uitwisseling van gegevens is regelmatig beperkt of helemaal niet geautomatiseerd. Cruciale applicaties en koppelingen zijn niet altijd betrouwbaar en mogelijkheden van moderne technologie worden onvoldoende benut. Diverse ICT-oplossingen worden regionaal uitgedacht en geïmplementeerd; n komen niet tot breder gebruik terwijl ze dat wel zouden verdienen.

Er is een breed besef, niet alleen bij GGD GHOR Nederland, maar ook bij VWS, dat de ICT infrastructuur infectieziektebestrijding robuuster kan en moet zijn. GGD GHOR Nederland gaat daarom een verkenning doen van de toekomstbestendigheid van HP Zone en eisen en wensen voor de digitale ondersteuning van IZB (in de volle breedte). De verkenning zal in samenwerking met VWS en het RIVM worden uitgevoerd. [redacted], programmamanager digitalisering van GGD GHOR Nederland, is aangesteld om deze verkenning te leiden.

Hoe worden IZ-professionals betrokken bij de nieuwe ontwikkelingen?

Als [redacted] van de Corona Programma Organisatie van GGD GHOR Nederland heb ik bovenstaande plannen en ontwikkelingen deze week op hoofdlijn besproken met [redacted] (voorzitter HP Zone gebruikersgroep), [redacted], [redacted] (coördinator RAC), [redacted] (voorzitter LOI) en [redacted] (voorzitter NVIB). Met name over achtergrond van de beweging die we willen maken en over het belang van het betrekken van de professionals bij deze ontwikkelingen.
De programmamanagers inbeheername HP Zone en digitalisering van GGD GHOR Nederland zullen regelmatig overleg hebben met [redacted] voorzitter HP Zone gebruikersgroep. [redacted] zal binnenkort de HP Zone-gebruikersgroep bijpraten over de inbeheername van HP Zone.
Belangrijke ontwikkelingen zullen worden gepresenteerd in het Landelijk Overleg Infectieziekten.
Komend Landelijk Overleg Infectieziektebestrijding, 8 december, zal [redacted] de inbeheername HP Zone en toekomstige ontwikkelingen presenteren.

Met vriendelijke groet,

[redacted]
Directeur Covid-19 Programmaorganisatie GGD GHOR Nederland

Wob-verzoek SOLV/ICAM datalek 2021 coronasysteem

3.0 Tekst Wob-verzoek en register documenten

Tekst verzoek (i)

Alle offerteaanvragen, programma's van eisen, offertes en overeenkomsten, inclusief bijlagen, met betrekking tot de uitbesteding aan derde partijen van klantcontact- en/of callcenterwerkzaamheden.

Register

Een screenshot van de verkennerpagina van map 3:

PELS RIJCKEN

Per e-mail: [redacted]
GGD West-Brabant
[redacted]
Postbus 3024
5003 DA Tilburg

onze ref. TG/TG/-
uw ref. -
inzake Kosteninschatting advies uitbesteding bron- en contactonderzoek GGD

[redacted]
advocaat
t [redacted]
f [redacted]
[redacted]

17 juni 2020

Geachte [redacted],

De gemeentelijke gezondheidsdienst West-Brabant ('GGD') is voornemens om het bron- en contactonderzoek en de daarmee gepaarde verwerkingsactiviteiten (gedeeltelijk) uit te besteden aan diverse private partijen. Aangezien deze partijen in het kader van het verrichten van het bron- en contactonderzoek gevoelige persoonsgegevens (gezondheidsgegevens) zullen verwerken, is het van belang dat de GGD passende en zorgvuldige afspraken maakt over de wijze waarop de verwerking van deze persoonsgegevens plaats zal vinden. De GGD heeft daartoe enkele (concept)verwerkersovereenkomsten opgesteld. U heeft ons gevraagd om een juridische check te verrichten van de door de GGD opgestelde verwerkersovereenkomsten. Uiteraard zijn wij daar graag toe bereid. Zoals verzocht, treft u hieronder een beknopte kosteninschatting aan.

Ons voorstel is dat dit advies in behandeling zal worden genomen door mijn collega's [redacted] zijn beiden werkzaam bij de sectie Innovatie, Privacy & Technologie van Pels Rijcken en zijn gespecialiseerd in het IT-contractenrecht. Zij hebben ruime ervaring met het opstellen van verwerkersovereenkomsten en zijn goed

op de hoogte van de huidige ontwikkelingen met betrekking tot het bron- en contactonderzoek en de ontwikkeling van de Corona-app. Zij kunnen de GGD daardoor goed adviseren over de contractuele afspraken die de GGD dient te hanteren om een zorgvuldige gegevensverwerking te borgen. Voor zover noodzakelijk zal ik vanuit mijn expertise van het privacyrecht en mijn betrokkenheid bij de ontwikkeling van de Corona-app meeschrijven met het advies.

Hoewel de vraag van de GGD zich uitsluitend richt op de inhoud van de (concept)overeenkomsten, merken wij op voorhand op dat voor de correcte advisering van de GGD enkele voorvragen van belang zijn:

- Mag de GGD het verrichten van bron- en contactonderzoek uitbesteden aan private partijen?
- Treden de private partijen in een dergelijk geval op als verwerkingsverantwoordelijke of verwerkers?

Bovengenoemde vragen zijn bepalend voor de aanwezigheid van wettelijke grondslag voor de verwerking van gezondheidsgegevens, alsmede de vorm van de contractuele afspraken (een verwerkersovereenkomst of een zogenoemde 'overeenkomst zorgvuldige verwerking'). Gezien het belang van de hiervoor beschreven voorvragen, hebben wij de tijd die naar verwachting gemoeid is met het beantwoorden van deze voorvragen, meegenomen in deze kosteninschatting.

In aanvulling op een juridische check op de verwerkersovereenkomsten, achten wij het bovendien verstandig dat de GGD vertrouwelijkheidsverklaringen opstelt en bovendien afspraken maakt over het gebruik van haar informatiesysteem.

Gelet op het voorgaande schat ik in dat met de behandeling van dit advies 23 uren gemoeid zullen zijn, waarvan naar verwachting 8 uren van J[redacted] en 12 uren van [redacted]. Daarnaast heb ik zekerheidshalve 3 uren voor mijzelf begroot voor het meedenken en meeschrijven met het advies. Op basis van het uurtarief van [redacted] van [redacted], het uurtarief van [redacted] van [redacted] en mijn uurtarief van [redacted] komt onze kosteninschatting voor dit advies uit op een bedrag van circa [redacted] exclusief BTW en exclusief kantoorkosten.

Voor alle duidelijkheid: het betreft geen vaste prijs of maximum. Met eventuele complicaties is bij het uitbrengen van deze feequote geen rekening gehouden. Onze werkzaamheden worden maandelijks op uurbasis gedeclareerd tegen een toepasselijk uurtarief. We zullen u een alert sturen zodra 80% van het genoemde budget is bereikt.

Op onze werkzaamheden zijn onze algemene voorwaarden van toepassing, die ik als bijlage bij deze brief voeg.

Ik hoop u hiermee voldoende te hebben geïnformeerd. Vanzelfsprekend ben ik graag bereid om deze kosteninschatting nader toe te lichten, dan wel hierover met u in overleg te treden.

Met vriendelijke groet,
Pels Rijcken & Droogleever Fortuijn N.V.

[redacted]

Advies in verband met de inhuur van externe medewerkers voor de uitvoering van Bron- en contactonderzoeken in relatie tot gegevensbescherming

Inleiding

Onderstaand advies is opgesteld in verband met de naleving van privacywetgeving in verband met de uitvoering van Bron- en contactonderzoeken (Bco) door de GGD'en. Uitgangspunt daarbij is dat er sprake is van inhuur van externe medewerkers en dat het reguliere proces van Bco niet wijzigt als gevolg van de inhuur. Daarmee wordt ervan uitgegaan dat de bestaande processen voldoen aan de daaraan te stellen eisen vanuit de Algemene Verordening Gegevensbescherming (AVG) en de Wet publieke gezondheid. Onderstaand advies is gebaseerd op informatie uit telefonische gesprekken. Het richt zich op de aspecten waarbij rekening gehouden moet gehouden bij de externe inhuur van medewerkers in het licht van gegevensbescherming. Daarnaast wordt op hoofdlijnen toegelicht welke aandachtspunten er zijn, indien (onderdelen van) het Bco worden uitbesteed aan een derde partij.

Aandachtspunten voor ingehuurde medewerkers

1.1 Aanstellingsvoorwaarden

Voor het inhuren van externe medewerkers gelden in principe dezelfde functie- eisen en voorwaarden die gesteld worden bij kleinschalige inhuur. Hierbij kan worden aangesloten bij bestaande werkprocessen vanuit P&O. Vanuit het oogpunt van gegevensbescherming verdient daarbij extra aandacht het vragen naar een verklaring omtrent het gedrag (VOG) en de ondertekening van een geheimhoudingsverklaring.

1.2 Opleiding ingehuurde medewerkers

Het uitvoeren van een Bco brengt met zich mee dat de ingehuurde medewerkers te maken krijgen met vertrouwelijke gegevens, waaronder gezondheidsgegevens. Belangrijk is dat medewerkers worden opgeleid om hier op een zorgvuldige wijze mee om te gaan.
Dit kan door het (intern) verzorgen van opleidingen waarmee ze vertrouwd worden gemaakt met systemen en werkwijzen binnen de GGD en het Bco-onderzoek.

Binnen deze opleiding dient ook aandacht te worden besteed aan de vertrouwelijkheid van de informatie waarmee ze te maken krijgen, het herkennen en melden van datalekken en de rechten van betrokkenen. Onderdeel van de vertrouwelijkheid is ook afspraken over situaties waarin de Bco- uitvoerder bekend is met betrokkene(n).

In het kader van verantwoording is het van belang dat wordt vastgelegd dat een ingehuurde medewerker de (interne) opleiding heeft gevolgd en dat ook vastligt uit welke onderdelen de opleiding bestaat.

1.3 Opname van gesprekken voor trainingsdoeleinden

Voor het opleiden van medewerkers kan het behulpzaam zijn ze te laten meeluisteren met opgenomen gesprekken. Voorwaarden voor het opnemen van gesprekken is in de eerste plaats dat er een gerechtvaardigd belang is voor de organisatie, in dit geval de GGD. Dit gerechtvaardigd belang kan liggen in de bedrijfsvoering of het dagelijks beheer van de organisatie. Een van de door de toezichthouder (Autoriteit Persoonsgegevens (AP)) genoemde voorbeelden is om de telefonische dienstverlening door de werknemers van de organisatie (bijvoorbeeld van een callcenter) te verbeteren. Het opleiden van medewerkers wordt niet expliciet genoemd als voorbeeld. Wel wordt het opleiden van medewerkers genoemd in het kader van de informatieplicht. Verder is het opnemen van telefoongesprekken voor trainingsdoelen gebruikelijk binnen verschillende branches, waaronder callcenters. Daarmee kan voldoende aannemelijk worden beargumenteerd dat het voor trainingsdoeleinden opnemen van gesprekken mogelijk is. Daarbij wordt wel de voorwaarde gesteld dat een een afweging moet worden gemaakt tussen het organisatiebelang en de belangen en rechten van betrokkenen. Het organisatiebelang is gelegen in het op korte termijn opleiden van medewerkers om uitvoering te kunnen geven aan de opdracht tot het uitvoeren van een Bco ter bestrijding van een pandemie. Afwegingen die daarbij te maken zijn, zijn onder andere de bewaartermijn van de opnamen en de omvang van de opnamen (alle gesprekken of steekproefsgewijs) en de impact voor betrokkenen. Bij dat laatste kan met name worden gedacht aan het voorkomen dat de personen van wie gesprekken zijn opgenomen bekenden zijn van diegenen die worden opgeleid.

Voorwaarden zijn dat bij inboundgesprekken er een bandje wordt afgespeeld waarin wordt toegelicht dat het gesprek kan worden opgenomen voor trainingsdoeleinden en welke rechten betrokkene heeft. Bij outboundgesprekken geldt hetzelfde; ook kan ervoor worden gekozen om een belscript voor te lezen. Aandachtspunt vormt verder het betrekken van de OR omdat ook de medewerkers worden vastgelegd.

1.4 Thuiswerkafspraken

In verband met COVID-19 is de realiteit dat veel medewerkers thuiswerken. Voor de beveiliging van persoonsgegevens geeft dit specifieke aandachtspunten. Voor de hand liggende afspraken over het afsluiten van de mogelijkheid om thuis te printen of documenten te downloaden op eigen apparatuur, het verbod op het gebruik van mobiele gegevensdragers, tenzij voorzien van afdoende encryptie, het niet onbeheerd achterlaten van de laptop en het voorkomen dat huisgenoten kennis kunnen nemen van vertrouwelijke gegevens.

2. Aandachtspunten voor het inhuren van externe partijen

2.1 Inleiding

Indien van een derde partij medewerkers worden ingehuurd, dan gelden de onder 1 genoemde aandachtspunten voor de ingehuurde medewerkers. Indien daarnaast of los daarvan ook een beroep wordt gedaan op dienstverlening voor de uitvoering van het Bco waarbij persoonsgegevens worden verwerkt, dan gelden aanvullende eisen. Deze worden onderstaand toegelicht.

2.2 Verwerkersovereenkomst

Indien voor taken in het kader van het Bco door een derde partij persoonsgegevens worden verwerkt in opdracht van de GGD, dan is daarvoor een overeenkomst nodig. Naast de dienstverleningsovereenkomst is dan een aparte overeenkomst nodig waarin afspraken staan over het verwerken van persoonsgegevens. Dit heet een verwerkersovereenkomst. In deze verwerkersovereenkomst worden onder andere afspraken gemaakt over de beveiliging van de gegevens, de teruggave of vernietiging van de gegevens na afloop van de overeenkomst en op welke wijze gebruikgemaakt mag worden van de gegevens[1]. Hiervoor kan een standaard verwerkersovereenkomst worden gebruikt die binnen de GGD gebruikelijk is, aangevuld met specifieke afspraken die betrekking hebben op het Bco. Indien gewenst kunnen conceptverwerkersovereenkomsten door ons worden getoetst.

2.3 Beveiligingseisen

Op grond van de Algemene Verordening Gegevensbescherming is het verplicht passende maatregelen te treffen ter beveiliging van persoonsgegevens. Ook binnen de GGD gelden eisen voor de beveiliging van systemen en persoonsgegevens. Over het algemeen zijn deze afgeleid van internationaal of binnen een sector gebruikelijke en erkende normen. Dit zijn bijvoorbeeld de NEN 7510, ISO 27001 of de Baseline Informatiebeveiliging overheid (BIO).
Voor het inhuren van een derde partij gelden dezelfde beveiligingseisen als voor de GGD zelf. Deze eisen worden in de verwerkersovereenkomst expliciet vastgelegd. Daarbij is niet noodzakelijk dat exact dezelfde norm wordt toegepast, wel vergelijkbare normen die hetzelfde effect sorteren.

2.4 Autorisaties, logging en controle van logging

Bij het inhuren van grote(re) groepen nieuwe medewerkers is het belangrijk aandacht te besteden aan het toekennen van autorisaties. De toegekende autorisaties moeten zijn toegekend op basis van een functieprofiel, passend bij de uitvoering van de taken.

Daarnaast is het beheer van de autorisaties van belang en wanneer er sprake is van tijdelijke inhuur waarbij de mogelijkheid aanwezig is dat ingehuurde medewerkers achtereenvolgens voor verschillende GGD'en werkzaam zijn. Dat maakt dat zorgvuldig moet worden omgegaan met het beheer van autorisaties en met name een tijdige beëindiging van autorisaties.

[1] Voor een volledig overzicht: artikel 28 lid 3 AVG

Zodra de inzet voor een GGD eindigt, moet ook de autorisatie daarvoor worden beëindigd. Naast een zorgvuldige omgang met autorisaties, dient ook logging worden toegepast en gecontroleerd volgens het daarvoor geldende beleid. De AP heeft meermaals aangegeven dat logging en controle daarop een onderdeel is van het beveiligingsbeleid en voor het nalaten daarvan een boete oplegt.

2.5 Datalekken en beveiligingsincidenten

Ondanks de aandacht voor beveiliging, kunnen zich er incidenten voordoen waarbij sprake is van een inbreuk in verband met persoonsgegevens. Afhankelijk van de aard en ernst kan sprake zijn van:

- een beveiligingsincident;
- een datalek dat wel geregistreerd moet worden door de verwerker, maar niet gemeld hoeft te worden bij de AP;
- een datalek dat gemeld moet worden bij de AP;
- een datalek dat gemeld moet worden bij de AP en de betrokkene(n).

Binnen de GGD gelden voor het melden en beoordelen afspraken en werkwijzen. Het is van belang dat ook met een ingeschakelde derde (verwerker) afspraken worden gemaakt over de omgang met datalekken en beveiligingsincidenten. Deze afspraken zien met name toe op het tijdig bekendmaken aan de betreffende GGD, procedures en bereikbaarheid. Gelet op de aandacht voor het onderwerp COVID-19 en het onderwerp datalekken, is het van belang hier duidelijke afspraken over te maken tussen de GGD en de verwerker, ook in relatie tot de communicatie hierover. Eerder is al genoemd dat het daarbij ook van belang is dat de betreffende medewerkers voldoende zijn opgeleid in het herkennen van datalekken of beveiligingsincidenten. Daarnaast is het van belang dat zij bekend zijn met de procedures voor het melden daarvan, ook buiten kantoortijden.

2.5 Gebruik van e-mail door verwerker

Als de ingehuurde organisatie (verwerker) gebruikmaakt van eigen e-mailadressen, is het van belang afspraken te maken over transparantie naar betrokkenen en het beheer van de e-mails. Wat betreft de transparantie is het van belang dat een betrokkene vooraf weet dat hij een e-mail ontvangt van een derde partij, maar dat dit namens een GGD is. Dit voorkomt verwarring over de rol van de verwerker. Wat betreft het beheer van de e-mails is het van belang dat afspraken worden gemaakt over de bewaartermijnen daarvan. Voor het bepalen daarvan dient aansluiting te worden gezocht bij de reguliere bewaartermijn van gegevens binnen het Bco-proces van de GGD.

3. Aandachtspunten uitvoeren Bco

3.1 Transparantie naar inwoners

Voor het uitvoeren van een Bco worden van verschillende personen gegevens vastgelegd, bijvoorbeeld gezondheidsgegevens. Belangrijk daarbij is dat transparant is voor betrokkenen hoe wordt omgegaan met deze gegevens wat betreft gebruik, verstrekking, vertrouwelijkheid verwijdering en welke rechten zij hierin hebben. Hierbij kan gebruikgemaakt worden van bestaande folders, brieven en informatie op websites.

3.2 Betrekken van Functionaris Gegevensbescherming

Iedere GGD heeft op grond van de AVG een eigen, interne privacytoezichthouder; de [redacted] De [redacted] heeft onder andere als taak om toezicht te houden op de verwerking van persoonsgegevens binnen de organisatie en te informeren en te adviseren daarover waar nodig. Gelet op de rol van de [redacted] en zijn expertise op grond van gegevensbescherming, is het van belang deze te betrekken bij de vraagstukken die spelen bij de inhuur van externe medewerkers voor de uitvoering van een Bco. Aandachtspunten van de [redacted] kunnen zo worden betrokken bij de inrichting van nieuwe werkwijzen en processen. Niet alleen wordt daarmee gebruik- gemaakt van de expertise van de [redacted] ook wordt de [redacted] niet verrast in zijn toezichthoudende rol.

3.3 Uitvoering Data Protection Impact Assessment

De AVG verplicht in een aantal situaties tot het uitvoeren van een Data Protection Impact Assessment (DPIA). Een DPIA is bedoeld om voorafgaand aan de verwerking van persoonsgegevens risico's te inventariseren en hier vervolgens maatregelen op uit te voeren. Een voorbeeld van een situatie waarin de uitvoering van de DPIA verplicht is, betreft de grootschalige verwerking van bijzondere gegevens. Hieronder wordt onder andere verstaan gezondheidsgegevens. De uitvoering van Bco's door GGD'en kwalificeert zich daarmee als een verwerking waarvoor de uitvoering van een DPIA verplicht is. In de situatie dat extra personeel wordt ingehuurd en bestaande werkprocessen in het kader van het Bco niet wijzigen, is er geen aanleiding voor het uitvoeren van een DPIA. Indien bestaande werkprocessen substantieel wijzigen en daarmee risico's voor de verwerking van gegevensverwerking wijzigen, dient de uitvoering van een DPIA te worden beoordeeld. In de bijlage is de vragenlijst toegevoegd die door ons wordt gebruikt bij de uitvoering van een DPIA.

3.4 Toestemming indexpatiënt

Door de medewerker die telefonisch het Bco-gesprek voert wordt toestemming gevraagd aan de indexpatiënt om zijn/haar naam te noemen aan de contactpersonen. Belangrijk daarbij is wel de notie dat toestemming vragen ook betekent dat die geweigerd kan worden en voor betrokkene geen nadelige gevolgen heeft. Belangrijk is om deze toestemming te documenteren. Dit kan bijvoorbeeld door het vragen van toestemming op te nemen in de vragenlijst en dat dit in HPZone wordt aangevinkt. Dit om (het vragen van) de toestemming aantoonbaar te maken.

4. Overzicht aandachtspunten

Uitvoering Bco	Inhuur externe partij	Inhuur externe medewerkers
Betrek de [redacted] bij aangelegenheden die betrekking hebben op de verwerking van persoonsgegevens in het kader van de uitbesteding van taken in het Bco.	Er is een verwerkersovereenkomst afgesloten. Daarbij is gebruik-gemaakt van het model dat door de GGD wordt gebruikt.	Geheimhoudingsverklaring is getekend.
Zorg voor transparantie naar inwoners over de verwerking van persoonsgegevens in het Bco-proces.	Er zijn afspraken gemaakt over de beveiliging van gegevens die zijn vastgelegd in de verwerkersovereenkomst.	Verklaring Omtrent Gedrag is ontvangen.
Beoordeel bij veranderingen van werkprocessen of een DPIA moet worden uitgevoerd.	Onderdeel van de beveiligingsafspraken zijn afspraken over het toekennen en beheer van autorisaties, logging en controle van logging.	Voldoet aan opleidings- en ervaringseisen.
Zorg bij het opnemen van telefoongesprekken voor een transparante afweging tussen het belang van de organisatie en de betrokkene. Informeer bij zowel in- als outboundgesprekken de betrokkene vooraf, stel vast hoeveel (alle of steekproefsgewijs) gesprekken worden vastgelegd, stel vast hoe lang gesprekken worden bewaard. Betrek de OR.	In de verwerkersovereenkomst zijn afspraken gemaakt over het registreren en melden van inbreuken op de beveiliging en datalekken.	Heeft interne opleiding gevolgd voor Bco met aandacht voor aspecten gegevensverwerking (datalekken, rechten van betrokkenen en wijze waarop wordt omgegaan met bekenden van de medewerker bij uitvoering Bco-onderzoek).
Zorg dat het vragen van toestemming aan de indexpatiënt is gedocumenteerd en is opgenomen in het werkproces/ vragenlijst.	In de verwerkersovereenkomst zijn afspraken gemaakt over het gebruik van eigen e-mailadressen door de verwerker en het beheer van die e-mails.	In het dossier van de ingehuurde medewerkers wordt vastgelegd dat zij de training hebben gevolgd en uit welke onderdelen de training bestaat.
		Informatie over het herkennen en melden van beveiligingsincidenten en datalekken is aan betrokkene toegelicht. De medewerker is geïnformeerd over waar hij deze informatie terug kan vinden.
		De medewerker is geïnformeerd over het logging van handelingen binnen de applicatie en indien van toepassing over het opnemen van gesprekken.
		Er zijn afspraken gemaakt over thuiswerken en de zorgvuldige omgang met persoonsgegevens daarbij. Deze afspraken liggen vast.
		Alle reguliere werkprocessen en afspraken in het kader van P&O zijn gevolgd.

BIJLAGE DPIA-vragenlijst

Onderwerp:

Ingevuld door:

Datum:

Nr.	Vraag	Ref.	Antwoord?
	Informatie over de verwerking		
1.	Wat zijn de verwerkingsdoeleinden? Waarom is de verwerking nodig?	AVG 5.1b AVG 30b	
2.	Welke organisatie is de verantwoordelijke in de zin van de AVG?	AVG 30.1a	
3.	Welke stappen heeft het proces en wie voert deze uit? Voeg een proces- of procedurebeschrijving bij, bijvoorbeeld een flowchart en/of een zwembanendiagram		
4. *	Welke interne afdelingen zijn betrokken bij de verwerking?		
5. *	Welke andere organisaties verwerken de gegevens in opdracht van de verantwoordelijke? (welke organisaties zijn verwerkers in de zin van de AVG?)	AVG 30.2	
6.	Wat is de grondslag voor rechtmatigheid van de verwerking? (a) toestemming, b) uitvoering contract, c) wettelijke verplichting, d) vitaal belang, e) algemeen belang/openbaar gezag, f) gerechtvaardigd belang) Neem een toelichting op.	AVG 5.1a, 6	
7.	Wat is de herkomst van de gegevens? (van wie en op welke manier verzameld?)	AVG 5.1b	
8.	Met welk doel zijn/worden de gegevens verzameld? (indien anders dan 1)	AVG 5.1b	
9.	Wie zijn de betrokkenen in de zin van de AVG?	AVG 30.1 c	
10.	Om hoeveel betrokkenen gaat het?		

11.	Om welke persoonsgegevens gaat het? (per groep betrokkenen alle velden benoemen)	AVG 30.1c	
12. *	Welke van de volgende gegevens worden verwerkt? - Bijzondere: religie, ras, politieke opvattingen, gezondheid, genetische/biometrische gegevens, seksueel gedrag/geaardheid, lidmaatschap van vakbonden, - strafrechtelijke gegevens - BSN - Communicatiegegevens - Locatiegegevens - Financiële/fiscale gegevens	AVG 9, 10, 30.1c AVG 87	
13.	Waarom is de verwerking van elk van de gegevens noodzakelijk voor het doel (proportionaliteit)?		
14.	Hoe zou het doel bereikt kunnen worden zonder verwerking van de gegevens, met minder gegevens of met geanonimiseerde/gepseudonimiseerde gegevens (subsidiariteit)?		
15. *	Wordt de betrokkene geïdentificeerd? - Feitelijk (bijvoorbeeld met ID) - In de registratie (bijvoorbeeld met naam, klantnr., etc.) Indien ja, hoe en waarom is dit noodzakelijk voor het doel?	AVG 11	
16.	Hoe worden de betrokkenen geïnformeerd over het doel van de verwerking, de identiteit en contactgegevens van de verantwoordelijke en de [redacted] verstrekkingen aan derden, gerechtvaardigd belang, doorgifte buiten de EU (bijvoorbeeld door een privacyreglement/-statement)	AVG 5.1a, 12.1, 13, 14	
17.	Hoe wordt de betrokkene geïnformeerd bij verkrijging van gegevens van de betrokkene zelf? (te verstrekken informatie, zie AVG 13.1) opslagperiode, rechten van de betrokkene, incl. intrekken van toestemming indien van toepassing en het recht om een	AVG 13	

	klacht in te dienen, of het er een wettelijke of contractuele verplichting is, wat de gevolgen van niet verstrekking zijn, eventuele geautomatiseerde besluitvorming?		
18.	Hoe wordt de betrokkene geïnformeerd bij verkrijging van gegevens van anderen dan de betrokkene zelf? (te verstrekken informatie, zie AVG 14)	AVG 14	
19.	Hoe kan de betrokkene verzoeken ten aanzien van zijn rechten indienen? Hoe worden deze afgehandeld? (procesbeschrijving)		
20.	Met behulp van welke systemen/applicaties worden de gegevens verwerkt? Geef een overzicht van de gehele keten van systemen en netwerken incl. gegevensuitwisselingen en werkstations (incl. toegang van buiten de organisatie/telewerken)	AVG 5.1f	
21.	Welke andere hulpmiddelen worden gebruikt?		
22. *	Aan welke ontvangers (anders dan verwerkers) kunnen de gegevens worden verstrekt en welke gegevens?	AVG 30.1d	
23.	Rechtmatige grondslag voor verstrekking van de gegevens	Zie ontvangers	
24. *	Welke gegevens worden doorgegeven naar ontvangers of worden verwerkt buiten de EU	AVG 30.1e	
25.	Basis voor de rechtmatigheid van doorgifte naar ontvangers/verwerking buiten de EU	AVG 44-49	
26.	Minimale bewaartermijn van de gegevens en de grondslag daarvoor		
27.	Maximale bewaartermijn van de gegevens (waarna deze moeten worden vernietigd) en de grondslag daarvoor	AVG 30.1f	
28.	Op welke wijze wordt de daadwerkelijke wissen van gegevens na de bewaartermijn geregeld en gewaarborgd?		
29.	Vertrouwelijkheidsclassificatie (openbaar, bedrijfsvertrouwelijk, vertrouwelijk, geheim)		
30. *	Welke (sectorale) wet- en regelgeving anders dan WBP/AVG,		

	is van toepassing? Zoals beleidsregels van de AP, gedragscodes al dan niet goedgekeurd door de AP, WBGO, Wmo, Jeugdwet, Wlz, etc.		
	Stakeholders		
31.	Wie zijn betrokken bij het project of op een andere manier belanghebbenden/stakeholders of hun vertegenwoordigers? - Betrokkenen (OR, Cliëntenraad, ouderraad, etc.) - Toezichthouders, zoals [redacted] - Verwerkers - Brancheorganisaties en/of geschillencommissies - …		
32.	Welke van deze belanghebbenden moet om advies worden gevraagd? - [redacted] en betrokkenen (NB Instemmingsrecht OR in de WOR, mogelijk adviesrecht o.b.v. andere wet- en regelgeving (cliëntenraden, etc.))	WOR Art.27	
33. *	Welke maatschappelijke belanghebbenden zijn er, zoals belangenorganisaties, actiegroepen?		
	Risicoprofiel		
34.	Welke van de volgende situaties is van toepassing? a. Beoordelen van mensen op basis van persoonskenmerken (profilering en het maken van prognoses, bijv. kredietbeoordeling) b. Geautomatiseerde beslissingen met rechtsgevolgen of andere wezenlijke gevolgen c. Stelselmatige en grootschalige monitoring openbaar toegankelijke ruimten, bijvoorbeeld cameratoezicht of wifi tracking d. Gevoelige gegevens (bijzondere, strafrechtelijke, communicatie, locatie, financieel) (zie vraag 11) e. Grootschalige gegevensverwerkingen (op basis van hoeveelheid mensen	AVG 35.1, .3 a, b WBP 42 AVG 22 g AVG 88, WOR	

	(grote delen van de bevolking), hoeveelheid/verscheidenheid gegevens, tijdsduur, geografische reikwijdte) f. Gekoppelde databases, koppeling van gegevens g. Gegevens over kwetsbare personen/personen met een ongelijke machtsverhouding met de verantwoordelijke (bijv. werknemers, kinderen, patiënten, verstandelijk gehandicapten, etc.) h. Gebruik van nieuwe technologieën (IoT, etc.) i. Doorgifte van persoonsgegevens buiten de EU j. Blokkering van een recht, dienst of contract (bijv. zwarte lijsten, beoordeling kredietwaardigheid, etc.) NB Een PIA en eventueel een voorafgaande raadpleging bij een hoog restrisico na het nemen van maatregelen is verplicht: - bij een hoog risico (AVG 35.1) - bij de criteria a+b, c, d+e of h (AVG 35). - bij 2 of meer criteria (AP en WP29 Guidelines)		
35.	Staat de verwerking op de door de AP uitgegeven lijst van verwerkingen waarvoor een PIA vereist is?		
36.	Welke andere risicofactoren zijn er? (* in bovengenoemde vragen, soms afhankelijk van de omvang) - Veel interne partijen - Veel externe partijen - Heimelijke waarneming (camera's, wifi tracking) - Verkoop van gegevens - …		
37.	Wanneer heeft de laatste PIA of andere analyse t.a.v. privacy plaatsgevonden?		
38.	Welke aanzienlijke veranderingen van de verwerking, risico's en		

	omgeving hebben sindsdien plaatsgevonden?		
	Risico's en Maatregelen		
39.	Welke risico's, bedreigingen en mogelijke gevolgen zijn er voor de privacy? - Onrechtmatige toegang - Ongewenste wijziging - Vernietiging		
40.	Welke maatregelen zijn voorzien om risico's te beperken?		
41.	<u>Welke beveiligingsmaatregelen worden/zijn er getroffen?</u> - In algemene zin - Autorisatie en authenticatie wordt daarbij gebruik gemaakt van DigID of andere authenticatiediensten? - Specifiek voor de te onderzoeken verwerking	AVG 30.1g	
42.	Wie is verantwoordelijk voor het in stand houden en evalueren van de getroffen maatregelen?		
43.	Hoe wordt aangetoond dat aan de AVG wordt voldaan?		
	Beveiligingsmaatregelen t.a.v. applicaties (marginale, geen volledige toets. Vraag ook naar de mate van, implementatie van BIO, NEN7510 ISO27001 of vergelijkbaar)		
	Gegevensbeheer		
44.	Gegevens worden geanonimiseerd wanneer identificatie voor het doel niet (meer) nodig is, of gepseudonimiseerd om risico's te beperken.		
45.	Ondersteunt de applicatie het verwijderen van gegevens na het verstrijken van de bewaartermijn?		
	Authenticatie en autorisatie		
46.	Hoe loopt het aanvragen/verkrijgen van een account?		
47.	Wat is het wachtwoordbeleid en wordt dit door de applicatie afgedwongen? (lengte en complexiteit, geldigheidsduur, aantal pogingen, etc.)		

48.	Hoe worden initiële wachtwoorden aan gebruikers verstrekt en hoe verloopt het resetten van een wachtwoord?		
49.	Is de applicatie toegankelijk via onvertrouwde netwerken, zoals het internet en wordt in die gevallen twee-factor-authenticatie ingezet?		
50.	Hebben beheerders separate accounts voor beheerwerkzaamheden (naast hun gebruikersaccount)?		
51.	Worden wachtwoorden in de applicatie opgeslagen als salted hashes?		
52.	Worden autorisaties op basis van rolprofielen toegekend?		
53.	Hebben medewerkers toegang tot meer informatie/dossiers dan nodig voor hun werk?		
54.	Wordt het scherm na 15 minuten automatisch geblokkeerd?		
55.	Welke gebeurtenissen worden gelogd?		
56.	Hoe worden de logs geanalyseerd en door wie?		
	Opslag van gegevens		
57.	Op welke locatie worden de gegevens opgeslagen?		
58.	Zijn de gegevens versleuteld opgeslagen en op welke manier?		
59.	Hoeveel dataverlies kan er bij het herstellen van een backup optreden (tijd tussen twee backups)?		
60.	Hoe vaak wordt een complete restore van het systeem getest?		
61.	Welke gegevens kunnen op het eindapparaat worden opgeslagen of achterblijven (bijv. in de browsercache of in de downloadmap)?		
	Webapplicaties		
62.	Hoe is de verbinding tussen gebruiker en server versleuteld? (TLS vx.x. evt. checken met www.ssllabs.com/ssltest/)		
63.	Welke third party cookies en andere trackers worden gebruikt?		
64.	Welke IP-poorten op de server zijn toegankelijk vanaf het internet?		
65.	Op welke punten voldoet de inrichting niet aan de NCSC ICT		

	beveiligingsrichtlijnen voor webapplicaties?		
	Ontwikkeling en onderhoud		
66.	Welke gescheiden omgevingen zijn er voor ontwikkeling, test, acceptatie, opleiding en productie?		
67.	Hoe worden testgegevens gegenereerd voor de ontwikkel- en testomgevingen?		
68.	Welke afspraken zijn er met leveranciers over beveiligingsupdates?		
69.	Hoe wordt de beveiliging getest? (vgl. OWASP testing guide)		
	Bij eigen ontwikkeling: in hoeverre wordt de OWASP secure coding richtlijn gevolgd?		
70.	Welke penetratietests en/of vulnerability scans zijn/worden er gedaan voor ingebruikname?		
	Bij beheer door een leverancier/Cloud		
71.	Is de leverancier ISO27001-gecertificeerd?		
72.	Kan de leverancier een SOC2 of ISAE 3402 type 2-verklaring overleggen?		

Archived: donderdag 12 mei 2022 11:41:21
From: [redacted]
Mail received time: Tue, 23 Jun 2020 12:51:18
Sent: dinsdag 23 juni 2020 14:51:19
To: [redacted]
Cc: [redacted]
Subject: CONCEPT Advies GGD WB en Hart van Brabant (incl. tekstvoorstellen documenten Yource) [PRDF-11014083]
Importance: Normal
Sensitivity: None
Attachments:
20200623_Notitie GGD inzake uitbesteding bron- en contactonderzoek (v4.0).docx; 200621 OVK GGDHvB-Yource-Bijlage02-Verwerkers-PRDFreview [PRDF-3560642].docx; 200622 OVK GGDWB-Yource-Bijlage01-Dienst-PRDFreview.docx; 20200621 OVK GGDHvB-Yource-AlgRaam-PRDFreview [PRDF-3560620].docx; 20200621 OVK GGDHvB-Yource-AlgRaam-PRDFreview.docx;

Beste [redacted],

Zoals besproken, stuur ik jullie hierbij onze bevindingen toe inzake de uitbesteding van het bron- en contactonderzoek aan Yource.

In de bijlagen bij deze e-mail treffen jullie allereerst een notitie aan waarin ik toelicht of de GGD het verrichten van bron- en contactonderzoek mag uitbesteden aan private partijen zoals Yource. In dezelfde notitie analyseer ik of Yource in dit concrete geval kwalificeert als verwerker van de GGD.

Mijn conclusie is kortgezegd dat de uitbesteding doorgang kan vinden indien de opdracht beperkt blijft tot 'verwerkingsactiviteiten' en de GGD voldoende regie behoudt over de wijze waarop Yource zijn werkzaamheden verricht. Ik heb de huidige overeenkomsten en werkafspraken geanalyseerd om vast te stellen of deze regierol momenteel voldoende is geborgd. Voor zover ik op basis van de documentatie kan vaststellen, heeft GGD door middel van werkafspraken, protocollen en invulformats in voldoende mate geregeld op welke wijze Yource de werkzaamheden moet verrichten. Gezien deze gezagsrelatie is aldus géén sprake van een onrechtmatige uitbesteding van kerntaken van de GGD. Naar mijn inschatting handelt Yource bij de uitvoering van de werkzaamheden als verwerker van de GGD.

Mijn collega's [redacted] zijn door de contractstukken heen gegaan. Zij hebben in de kantlijn opmerkingen gemaakt en waar mogelijk tekstvoorstellen gedaan met track changes. Hun algemene indruk is wel dat de kwaliteit van de documenten te wensen overlaat. Met de door hen gedane tekstvoorstellen en opmerkingen kan die kwaliteit op belangrijke punten worden verbeterd. Een perfect stuk zal het daarmee echter niet worden. Hun voorstel is daarom om de stukken samen met jullie telefonisch door te spreken, om zo te controleren of in ieder geval de belangrijkste risico's nu in de stukken worden geadresseerd.

Onze secretaresse neemt vanmiddag contact met jullie op om (zo spoedig mogelijk) een telefonische bespreking met jullie in te plannen. Wij lichten onze bevindingen dan graag toe.

Vriendelijke groeten, mede namens [redacted]

[redacted] | advocaat | Pels Rijcken & Droogleever Fortuijn N.V. | Bezuidenhoutseweg 57 | Postbus 11756, 2502 AT Den Haag | [redacted] | [redacted] | www.pelsrijcken.nl |

Archived: donderdag 12 mei 2022 11:41:17
From: [redacted]
Mail received time: Wed, 24 Jun 2020 08:02:33
Sent: Wed, 24 Jun 2020 08:00:27
To: [redacted]
Cc: [redacted]
Subject: RE: CONCEPT Advies GGD WB en Hart van Brabant (incl. tekstvoorstellen documenten Yource) [PRDF-11014083]
Importance: Normal
Sensitivity: None
Attachments:
20200624_Notitie GGD inzake uitbesteding bron- en contactonderzoek aangepast PRDF-3566115 [PRDF-3566780].docx;

Beste [redacted]

Vanochtend stuitte ik tijdens een aanvullend onderzoek op een onderzoek van de Autoriteit Persoonsgegevens naar aanleiding van een klacht over het UWV. Het betrof een (met de GGD) enigszins vergelijkbare situatie waarbij UWV een private partij had ingeschakeld om kortgezegd medische keuringen te verrichten vanaf een externe locatie. In het onderzoek ging het kortgezegd om de vraag of de externe partij was aan te merken als een 'verwerker' of 'intern beheer'. Hoewel de AP het uiteindelijke oordeel in het midden laat, stelt zij in het onderzoeksrapport dat in ieder geval sprake is van een gezagsverhouding (ondanks de omstandigheid dat het ging om een externe partij). De AP achtte het gerechtvaardigd dat UWV door middel van een verwerkersovereenkomst afspraken had gemaakt met de externe partij.

Ik heb in het licht van het bovenstaande mijn notitie nog op enkele aspecten aangevuld. De conclusie van het advies blijft hetzelfde. Het lijkt goed te verdedigen dat Yource handelt handelen als 'verwerker', zeker nu sprake is van een externe relatie. Ik stuur jullie de nieuwe versie van het advies alvast toe.

Met vriendelijke groet,
[redacted]

[redacted] | advocaat | Pels Rijcken & Droogleever Fortuijn N.V. | Bezuidenhoutseweg 57 | Postbus 11756, 2502 AT Den Haag | [redacted] | [redacted] | www.pelsrijcken.nl |

Van: [redacted]
Verzonden: dinsdag 23 juni 2020 14:48
Aan: [redacted]
CC: [redacted]
Onderwerp: CONCEPT Advies GGD WB en Hart van Brabant (incl. tekstvoorstellen documenten Yource) [PRDF-11014083]

Beste [redacted],

Zoals besproken, stuur ik jullie hierbij onze bevindingen toe inzake de uitbesteding van het bron- en contactonderzoek aan Yource.

In de bijlagen bij deze e-mail treffen jullie allereerst een notitie aan waarin ik toelicht of de GGD het verrichten van

bron- en contactonderzoek mag uitbesteden aan private partijen zoals Yource. In dezelfde notitie analyseer ik of Yource in dit concrete geval kwalificeert als verwerker van de GGD.

Mijn conclusie is kortgezegd dat de uitbesteding doorgang kan vinden indien de opdracht beperkt blijft tot 'verwerkingsactiviteiten' en de GGD voldoende regie behoudt over de wijze waarop Yource zijn werkzaamheden verricht. Ik heb de huidige overeenkomsten en werkafspraken geanalyseerd om vast te stellen of deze regierol momenteel voldoende is geborgd. Voor zover ik op basis van de documentatie kan vaststellen, heeft GGD door middel van werkafspraken, protocollen en invulformats in voldoende mate geregeld op welke wijze Yource de werkzaamheden moet verrichten. Gezien deze gezagsrelatie is aldus géén sprake van een onrechtmatige uitbesteding van kerntaken van de GGD. Naar mijn inschatting handelt Yource bij de uitvoering van de werkzaamheden als verwerker van de GGD.

Mijn collega's [redacted] zijn door de contractstukken heen gegaan. Zij hebben in de kantlijn opmerkingen gemaakt en waar mogelijk tekstvoorstellen gedaan met track changes. Hun algemene indruk is wel dat de kwaliteit van de documenten te wensen overlaat. Met de door hen gedane tekstvoorstellen en opmerkingen kan die kwaliteit op belangrijke punten worden verbeterd. Een perfect stuk zal het daarmee echter niet worden. Hun voorstel is daarom om de stukken samen met jullie telefonisch door te spreken, om zo te controleren of in ieder geval de belangrijkste risico's nu in de stukken worden geadresseerd.

Onze secretaresse neemt vanmiddag contact met jullie op om (zo spoedig mogelijk) een telefonische bespreking met jullie in te plannen. Wij lichten onze bevindingen dan graag toe.

Vriendelijke groeten, mede namens [redacted],
[redacted]

[redacted] | advocaat | Pels Rijcken & Droogleever Fortuijn N.V. | Bezuidenhoutseweg 57 | Postbus 11756, 2502 AT Den Haag | [redacted] | [redacted] | www.pelsrijcken.nl |
Printen, echt nodig?

Wob-verzoek SOLV/ICAM datalek 2021 coronasysteem

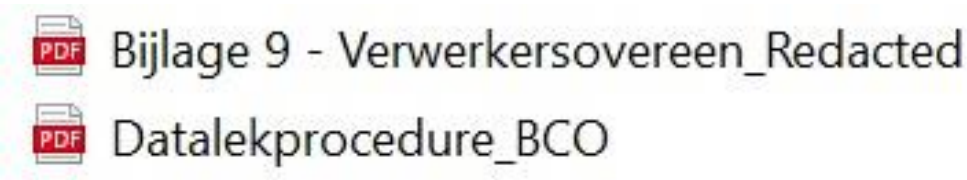
2.0 Tekst Wob-verzoek en register documenten

Tekst verzoek (ii)

Alle offerteaanvragen, programma's van eisen, offertes en overeenkomsten, inclusief bijlagen, met betrekking tot de inrichting en instandhouding van een klantcontact-centrum voor test- en vaccinatieafspraken en bron- en contactonderzoek

Register

Een screenshot van de verkennerpagina van map 2:



Model Verwerkersovereenkomst Brancheorganisaties Zorg

verenigd in

12 december 2017

VERWERKERSOVEREENKOMST

DE ONDERGETEKENDEN:

1. GGD West-Brabant, statutair gevestigd te Breda, te dezen rechtsgeldig vertegenwoordigd door [redacted], Directeur Publieke Gezondheid (hierna: "**Verwerkingsverantwoordelijke**"); en

2. Yource Operations B.V. (Cendris Customer Contact B.V.), statutair gevestigd te Leeuwarden, te dezen rechtsgeldig vertegenwoordigd door [redacted], Country Director (hierna "**Verwerker**").

hierna gezamenlijk ook aan te duiden als: "Partijen" en afzonderlijk als "Partij".

OVERWEGENDE DAT:

(a) Verwerker diensten verricht ten behoeve van Verwerkingsverantwoordelijke, zoals beschreven in de in Bijlage 1 omschreven overeenkomsten.
(b) De diensten meebrengen dat Persoonsgegevens worden verwerkt, waaronder gegevens betreffende de gezondheid.
(c) Verwerker de betreffende gegevens louter in opdracht van Verwerkingsverantwoordelijke verwerkt en niet voor eigen doeleinden.
(d) Per 25 mei 2018 van toepassing zal zijn Verordening (EU) 2016/679 van het Europees Parlement en de Raad van 27 april 2016 (Algemene verordening gegevensbescherming).
(e) Partijen in deze Verwerkersovereenkomst de afspraken met betrekking tot de verwerking van Persoonsgegevens in het kader van de diensten wensen vast te leggen.
(f) Deze Verwerkersovereenkomst, indien van toepassing, alle eerdere Overeenkomst(en) van gelijke strekking tussen Partijen vervangt.

VERKLAREN TE ZIJN OVEREENGEKOMEN ALS VOLGT:

Artikel 1. Definities

1.1. In deze Verwerkersovereenkomst wordt onder de volgende met een hoofdletter aangeduide begrippen het volgende verstaan:

a)	Algemene Verordening Gegevens Bescherming of AVG	Verordening (EU) 2016/679 van het Europees Parlement en de Raad van 27 april 2016 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens en tot intrekking van Richtlijn 95/46/EG.

b)	Betrokkene	een geïdentificeerde of identificeerbare natuurlijke persoon (artikel 4 sub 1 AVG).
c)	Derde	een derde als bedoeld in artikel 4 sub 10 AVG.
d)	Functionaris voor de Gegevensbescherming	een functionaris als bedoeld in artikel 37 e.v. AVG.
e)	Incident	i een klacht of (informatie)verzoek van een Betrokkene met betrekking tot de verwerking van Persoonsgegevens door Verwerker; ii een onderzoek naar of beslaglegging door overheidsfunctionarissen op de Persoonsgegevens of een vermoeden dat dit gaat plaatsvinden; iii een inbreuk in verband met Persoonsgegevens als bedoeld in artikel 4 onder 12 AVG; iv iedere ongeautoriseerde toegang, verwijdering, verminking, verlies of enige andere vorm van onrechtmatige verwerking van de Persoonsgegevens.
f)	Medewerker	de door Partijen voor de uitvoering van deze Verwerkersovereenkomst betrokken natuurlijke persoon die werkzaam is bij of voor een van de Partijen.
g)	Overeenkomst(en)	de in Bijlage 1 vermelde overeenkomst(en) betreffende de levering van producten en/of diensten.
h)	Partij	Verwerkingsverantwoordelijke of Verwerker.
i)	Partijen	Verwerkingsverantwoordelijke en Verwerker.
j)	Persoonsgegeven	alle informatie over een geïdentificeerde of identificeerbare natuurlijke persoon in de zin van artikel 4 onder 1 AVG.
k)	Subverwerker	iedere niet-ondergeschikte derde partij die door Verwerker is betrokken bij de verwerking van Persoonsgegevens in het kader van de Overeenkomst, niet zijnde Medewerkers.
l)	Verwerker	de verwerker als bedoeld in artikel 4 sub 8 AVG
m)	Verwerkersovereenkomst	de onderhavige overeenkomst.
n)	Verwerkingsverantwoordelijke	de verwerkingsverantwoordelijke als bedoeld in artikel 4 sub 7 AVG
o)	Wet bescherming persoonsgegevens of	Wet van 6 juli 2000, houdende regels inzake

Wbp	de bescherming van persoonsgegevens (Wet bescherming persoonsgegevens), inclusief latere wijzigingen.

1.2. Voornoemde en overige begrippen worden geïnterpreteerd overeenkomstig de AVG. Tot aan 25 mei 2018 worden begrippen geïnterpreteerd overeenkomstig de vergelijkbare bepaling uit de Wbp.

1.3. Waar in deze Verwerkersovereenkomst naar bepaalde normen wordt verwezen (zoals NEN7510) wordt daarmee steeds gedoeld op de meest actuele versie daarvan. Voor zover de betreffende norm niet meer wordt onderhouden, dient in de plaats daarvan de meest actuele versie van de logische opvolger van de betreffende norm gelezen te worden.

1.4. Eventuele afwijkingen op de tekst zijn alleen geldig voor zover deze zijn gespecificeerd in bijlage 4. Het bepaalde in bijlage 4 prevaleert op het overigens bepaalde in deze verwerkersovereenkomst.

Artikel 2. Onderwerp van deze Verwerkersovereenkomst

2.1. Deze Verwerkersovereenkomst heeft betrekking op de verwerking van Persoonsgegevens door Verwerker in opdracht van de Verwerkingsverantwoordelijke in het kader van de uitvoering van de Overeenkomst(en).

2.2. Partijen sluiten de Overeenkomst(en) om de expertise die Verwerker heeft als het gaat om het verwerken en beveiligen van Persoonsgegevens te gebruiken voor de uit de Overeenkomst(en) voortvloeiende en in deze Verwerkersovereenkomst nader beschreven doeleinden. Verwerker staat er voor in dat hij hiertoe gekwalificeerd is.

2.3. Deze Verwerkersovereenkomst maakt onverbrekelijk deel uit van de Overeenkomst(en). Voor zover het bepaalde in de Verwerkersovereenkomst strijdig is met het bepaalde in de Overeenkomst(en), prevaleert het bepaalde in de Verwerkersovereenkomst.

Artikel 3. Uitvoering verwerking

3.1. Verwerker garandeert dat hij ten behoeve van Verwerkingsverantwoordelijke uitsluitend Persoonsgegevens zal verwerken voor zover:

a.) dit noodzakelijk is voor de uitvoering van de Overeenkomst (binnen de kaders als gespecificeerd in Bijlage 1); of

b.) Verwerkingsverantwoordelijke daartoe nadere schriftelijke instructies heeft gegeven;

3.2. In het kader van het bepaalde in het eerste lid van artikel 3 onder a) zal Verwerker uitsluitend de in Bijlage 1 gespecificeerde Persoonsgegevens verwerken in het kader van de in die bijlage beschreven aard en doeleinden van de verwerking.

3.3. Verwerker zal alle redelijke instructies van Verwerkingsverantwoordelijke in verband met de verwerking van de Persoonsgegevens opvolgen. Verwerker stelt Verwerkingsverantwoordelijke onmiddellijk op de hoogte indien naar zijn oordeel instructies in strijd zijn met de toepasselijke wetgeving met betrekking tot de verwerking van Persoonsgegevens.

3.4. Onverminderd het bepaalde in het eerste lid van dit artikel 3, is het Verwerker toegestaan om Persoonsgegevens te verwerken indien een wettelijk voorschrift (waaronder begrepen daarop

gebaseerde rechterlijke of bestuurlijke bevelen) hem tot een verwerking verplicht. In dat geval stelt de Verwerker voorafgaand aan de verwerking Verwerkingsverantwoordelijke in kennis van de beoogde verwerking en het wettelijk voorschrift, tenzij die wetgeving deze kennisgeving om gewichtige redenen van algemeen belang verbiedt. Verwerker zal Verwerkingsverantwoordelijke, waar mogelijk, in staat stellen zich te verweren tegen deze verplichte verwerking en ook overigens de verplichte verwerking beperken tot het strikt noodzakelijke.

3.5. Verwerker zal de Persoonsgegevens aantoonbaar, op behoorlijke en zorgvuldige wijze verwerken en in overeenstemming met de op hem als Verwerker rustende verplichtingen op grond van de AVG, voor zover nog van toepassing de Wbp, en overige wet- en regelgeving. Verwerker zal in dat kader ten minste een register van verwerkingen aanleggen als bedoeld in artikel 30 AVG en Verwerkingsverantwoordelijke op eerste verzoek een kopie verstrekken van het onderdeel van het register dat ziet op de verwerking van persoonsgegevens in het kader van onderhavige dienstverlening. Na verwerking en overdracht aan Verwerkingsverantwoordelijke dienen de gegevens te worden verwijderd.

3.6. Indien de dienstverlening door Verwerker de verwerking van gezondheidsgegevens of andere bijzondere Persoonsgegevens impliceert, garandeert Verwerker dat hij niet in strijd met gezondheidswetgeving zal handelen. Verwerker handelt hierin conform de expliciete instructie van Verwerkingsverantwoordelijke.

3.7. Verwerker zal, tenzij hij hiervoor uitdrukkelijke voorafgaande schriftelijke toestemming heeft verkregen van Verwerkingsverantwoordelijke, geen Persoonsgegevens verwerken of laten verwerken door hemzelf of door derden in landen buiten de Europese Economische Ruimte (“EER”).

3.8. Verwerker waarborgt dat betrokken Medewerkers een geheimhoudingsovereenkomst hebben getekend en geeft Verwerkingsverantwoordelijke op verzoek inzage in deze geheimhoudingsovereenkomst.

Artikel 4. Beveiliging Persoonsgegevens en controle

4.1. Verwerker zal aantoonbaar, passende en doeltreffende technische en organisatorische beveiligingsmaatregelen nemen, die gezien de huidige stand der techniek en de daarmee gemoeide kosten overeenstemmen met de (in Bijlage 1 gespecificeerde) aard van de te verwerken Persoonsgegevens, ter bescherming van de Persoonsgegevens tegen verlies, onbevoegde kennisname, verminking of enige vorm van onrechtmatige verwerking, alsmede om de (tijdige) beschikbaarheid van de gegevens te garanderen. In deze beveiligings-maatregelen zijn de mogelijk in de Overeenkomst reeds bepaalde maatregelen begrepen. De maatregelen omvatten in ieder geval:

a.) maatregelen om te waarborgen dat enkel bevoegde Medewerkers toegang hebben tot de Persoonsgegevens voor de doeleinden die zijn uiteengezet;

b.) maatregelen waarbij de Verwerker zijn Medewerkers en Subverwerkers uitsluitend toegang geeft tot Persoonsgegevens via op naam gestelde accounts, waarbij het gebruik van die accounts adequaat gelogd wordt en waarbij de betreffende accounts alleen toegang geven tot die Persoonsgegevens waartoe de toegang voor de betreffende (rechts)persoon noodzakelijk is;

c.) maatregelen om de Persoonsgegevens te beschermen tegen onopzettelijke of onrechtmatige vernietiging, onopzettelijk verlies of wijziging, onbevoegde of onrechtmatige opslag, verwerking, toegang of openbaarmaking;
d.) maatregelen om zwakke plekken te identificeren ten aanzien van de verwerking van Persoonsgegevens in de systemen die worden ingezet voor het verlenen van diensten aan Verwerkingsverantwoordelijke;
e.) maatregelen om de tijdige beschikbaarheid van de Persoonsgegevens te garanderen;
f.) maatregelen om te waarborgen dat Persoonsgegevens logisch gescheiden worden verwerkt van de Persoonsgegevens die hij voor zichzelf of namens derde partijen verwerkt;
g.) de overige maatregelen die Partijen zijn overeengekomen zoals vastgelegd in Bijlage 2.

4.2. Verwerker werkt aantoonbaar in overeenstemming met ISO27001 en/of NEN 7510 en heeft een passend, geschreven beveiligingsbeleid geïmplementeerd voor de verwerking van Persoonsgegevens, waarin in ieder geval de in het eerste lid van dit artikel 4 genoemde maatregelen uiteen zijn gezet.

4.3. Verwerker voldoet aantoonbaar aan de veiligheidseisen voor netwerkverbindingen zoals beschreven in NEN7512.

4.4. Verwerker voldoet aantoonbaar aan de eisen ten aanzien van logging zoals beschreven in NEN7513.

4.5. Verwerker voldoet aantoonbaar aan de eisen van andere NEN-normen voor zover die voor de gezondheidszorg van toepassing zijn verklaard.

4.6. Verwerker zal op eerste verzoek van Verwerkingsverantwoordelijke een door een onafhankelijke en ter zake deskundige derde afgegeven geldig certificaat overleggen, indien deze daarover beschikt, waaruit volgt dat Verwerker de verplichtingen uit dit artikel naleeft.

4.7. Verwerkingsverantwoordelijke heeft het recht toe te (laten) zien op de naleving van de hiervoor onder artikel 4.1 tot en met 4.4 genoemde maatregelen. Verwerker stelt Verwerkingsverantwoordelijke, indien Verwerkingsverantwoordelijke daarom verzoekt, hiertoe in elk geval eenmaal per jaar in de gelegenheid op een door Partijen in gezamenlijk overleg nader te bepalen tijdstip en verder indien Verwerkingsverantwoordelijke daar aanleiding toe ziet naar aanleiding van (vermoeden van) informatie- of privacy-incidenten, dat te (laten) controleren. Verwerker zal in alle redelijkheid haar medewerking verlenen aan een dergelijk onderzoek. Verwerker zal eventuele door Verwerkingsverantwoordelijke naar aanleiding van een dergelijk onderzoek in redelijkheid gegeven instructies tot aanpassing van het beveiligingsbeleid binnen een redelijke termijn opvolgen. De kosten van onderzoeken die in opdracht van Verwerkingsverantwoordelijke worden uitgevoerd worden door Verwerkingsverantwoordelijke gedragen. Onderzoeken dienen te worden uitgevoerd door een onafhankelijke derde.

4.8. Partijen erkennen dat beveiligingseisen voortdurend veranderen en dat een effectieve beveiliging frequente evaluatie en regelmatige verbetering van verouderde beveiligingsmaatregelen vereist. Verwerker zal daarom de maatregelen zoals geïmplementeerd op basis van dit artikel 4 periodiek evalueren en, waar nodig, de maatregelen verbeteren om te blijven voldoen aan de verplichtingen onder dit artikel 4. Het voorgaande laat de instructiebevoegdheid van Verwerkingsverantwoordelijke om zo nodig aanvullende maatregelen te (doen) treffen onverlet.

Artikel 5. Monitoring, informatieplichten en incidentenmanagement

5.1. Verwerker zal actief monitoren op inbreuken op de beveiligingsmaatregelen en over de resultaten van de monitoring in overeenstemming met dit artikel 5 rapporteren aan Verwerkingsverantwoordelijke.

5.2. Zodra zich een Incident voordoet, heeft voorgedaan of zou kunnen voordoen, is Verwerker verplicht Verwerkingsverantwoordelijke daarvan onmiddellijk in kennis te stellen en daarbij alle relevante informatie te verstrekken over:

1) de aard van het Incident;
2) de (mogelijk) getroffen Persoonsgegevens;
3) de geconstateerde en de vermoedelijke gevolgen van het Incident; en
4) de maatregelen die getroffen zijn of zullen worden om het Incident op te lossen dan wel de gevolgen/schade zoveel mogelijk te beperken.

5.3. Verwerker is, onverminderd de overige verplichtingen uit dit artikel, verplicht om maatregelen te treffen die redelijkerwijs van hem kunnen worden verwacht om het Incident zo snel mogelijk te herstellen dan wel de verdere gevolgen zoveel mogelijk te beperken. Verwerker treedt zonder uitstel in overleg met Verwerkingsverantwoordelijke teneinde hierover nadere afspraken te maken.

5.4. Verwerker zal Verwerkingsverantwoordelijke te allen tijde zijn medewerking verlenen en zal de instructies van Verwerkingsverantwoordelijke opvolgen en stelt Verwerkingsverantwoordelijke in staat een deugdelijk onderzoek te verrichten naar het Incident, een correcte respons te formuleren en passende vervolgstappen te nemen ten aanzien van het Incident, waaronder begrepen het informeren van de Autoriteit Persoonsgegevens (AP) en/of de Betrokkene zoals bepaald in artikel 5.8.

5.5. Verwerker zal te allen tijde geschreven procedures voorhanden hebben die hem in staat stellen om Verwerkingsverantwoordelijke van een onmiddellijke reactie over een Incident te voorzien, en om effectief samen te werken met Verwerkingsverantwoordelijke om het Incident af te handelen. Verwerker zal Verwerkingsverantwoordelijke voorzien van een afschrift van dergelijke procedures indien Verwerkingsverantwoordelijke daarom verzoekt.

5.6. Meldingen die worden gedaan op grond van artikel 5.2 worden ogenblikkelijk gericht aan Verwerkingsverantwoordelijke of, indien relevant, aan een door Verwerkingsverantwoordelijke tijdens de duur van deze Verwerkersovereenkomst schriftelijk bekendgemaakte Medewerkers van Verwerkingsverantwoordelijke. Indien Verwerkingsverantwoordelijke een [redacted] heeft aangesteld, worden de meldingen gericht aan deze [redacted].

5.7. Het is Verwerker niet toegestaan informatie te verstrekken over Incidenten aan betrokkenen of andere derde partijen, behoudens voor zover Verwerker daartoe wettelijk verplicht is of Partijen anderszins zijn overeengekomen.

5.8. Indien en voor zover Partijen zijn overeengekomen dat Verwerker in relatie tot een Incident rechtstreeks contact onderhoudt met autoriteiten of andere derde partijen, dan houdt de Verwerker de Verwerkingsverantwoordelijke daarvan voortdurend op te hoogte.

Artikel 6. Medewerkingsverplichtingen

6.1. De AVG en overige (privacy)wetgeving kent aan de Betrokkene bepaalde rechten toe. Verwerker zal zijn volledige en tijdige medewerking verlenen aan

Verwerkingsverantwoordelijke bij de nakoming van de op Verwerkingsverantwoordelijke rustende verplichtingen voortvloeiend uit deze rechten.

6.2. Een door Verwerker ontvangen klacht of een verzoek van een Betrokkene met betrekking tot verwerking van Persoonsgegevens wordt door Verwerker zonder uitstel doorgestuurd naar Verwerkingsverantwoordelijke.

6.3. Op het eerste daartoe strekkende verzoek van Verwerkingsverantwoordelijke zal Verwerker aan Verwerkingsverantwoordelijke alle relevante informatie verstrekken betreffende de aspecten van de door hem verrichte verwerking van Persoonsgegevens zodat Verwerkingsverantwoordelijke, mede aan de hand van die informatie, aan kan tonen dat zij de toepasselijke (privacy) wetgeving naleeft.

6.4. Verwerker zal voorts op eerste verzoek van Verwerkingsverantwoordelijke alle noodzakelijke bijstand verlenen bij de nakoming van de op grond van de toepasselijke privacywetgeving op Verwerkingsverantwoordelijke rustende wettelijke verplichtingen (zoals het uitvoeren van een privacy impact assessment).

Artikel 7. Inschakeling subverwerkers

7.1. Verwerker zal zijn activiteiten die bestaan uit het verwerken van Persoonsgegevens of vereisen dat Persoonsgegevens verwerkt worden, niet uitbesteden aan een Subverwerker zonder voorafgaande schriftelijke toestemming van Verwerkingsverantwoordelijke. Het voorgaande is niet van toepassing op de in Bijlage 1 vermelde Subverwerkers.

7.2. Voor zover Verwerkingsverantwoordelijke instemt met de inschakeling van een Subverwerker, zal Verwerker aan deze Subverwerker dezelfde of strengere verplichtingen opleggen als voor hemzelf uit deze Verwerkersovereenkomst en de wet voortvloeien. Verwerker zal deze afspraken schriftelijk vastleggen en zal toezien op de naleving daarvan door de Subverwerker. Verwerker zal Verwerkingsverantwoordelijke op verzoek afschrift verstrekken van de met de Subverwerker gesloten overeenkomst(en).

7.3. Niettegenstaande de toestemming van Verwerkingsverantwoordelijke voor het inschakelen van een Subverwerker die in opdracht van de Verwerker (gedeeltelijk) gegevens verwerkt, blijft Verwerker volledig aansprakelijk jegens Verwerkingsverantwoordelijke voor de gevolgen van het uitbesteden van werkzaamheden aan een Subverwerker De toestemming van Verwerkingsverantwoordelijke voor het uitbesteden van werkzaamheden aan een Subverwerker laat onverlet dat voor de inzet van Subverwerkers in een land buiten de Europese Economische Ruimte toestemming vereist is in overeenstemming met artikel 3.7 van deze Verwerkersovereenkomst.

Artikel 8. Aansprakelijkheid

8.1. Partijen zijn ieder verantwoordelijk en aansprakelijk voor hun eigen handelen.

8.2. Enige beperking van de aansprakelijkheid in de Overeenkomst is *mutatis mutandis* ook van toepassing op deze Verwerkersovereenkomst, met dien verstande dat:

a.) eventuele (impliciete of expliciete) uitsluitingen van aansprakelijkheid voor verlies en/of verminking van Persoonsgegevens zijn uitgesloten;

b.) eventuele (impliciete of expliciete) uitsluitingen van aansprakelijkheid voor boetes die door de Autoriteit Persoonsgegevens of een andere toezichthouder worden opgelegd die

rechtstreeks verband houden met een toerekenbare tekortkoming van Verwerker, of een aan Verwerker toerekenbaar gedraging of nalaten, zijn uitgesloten.

8.3. Verwerker vrijwaart Verwerkingsverantwoordelijke en stelt de Verwerkingsverantwoordelijke schadeloos voor alle claims, acties, aanspraken van derden, alsmede boetes van de Autoriteit Persoonsgegevens, die rechtstreeks voortvloeien uit een toerekenbare tekortkoming door Verwerker en/of diens onderaannemers/Subverwerkers in de nakoming van zijn verplichtingen onder deze Verwerkersovereenkomst en/of enige schending door Verwerker en/of diens onderaannemers/Subverwerkers van de van toepassing zijnde wetgeving op het gebied van verwerking van Persoonsgegevens.

8.4. Voor zover Partijen hoofdelijk aansprakelijk zijn jegens derden, waaronder begrepen de betrokkene, of gezamenlijk een boete opgelegd krijgen door de Autoriteit Persoonsgegevens, zijn zij jegens elkaar, ieder voor het gedeelte van de schuld dat hem in hun onderlinge verhouding aangaat, verplicht overeenkomstig het bepaalde in Boek 6, Titel 1, Afdeling 2 van het Burgerlijk Wetboek in de schuld en kosten bij te dragen, tenzij de AVG anders bepaalt in welk geval de AVG voorgaat.

8.5. Voor zover in de Overeenkomst geen beperking van aansprakelijkheid voor Verwerkingsverantwoordelijke is opgenomen, geldt de in lid 2 opgenomen beperking voor Verwerker eveneens voor de Verwerkingsverantwoordelijke.

8.6. Iedere beperking van aansprakelijkheid komt voorts voor de betreffende Partij te vervallen in geval van opzet of grove schuld aan de zijde van de betreffende Partij.

8.7. Partijen dragen zorg voor afdoende dekking van de aansprakelijkheid.

8.8. Verwerkingsverantwoordelijke garandeert dat de verwerking van de Persoonsgegevens in overeenstemming met de wet plaatsvindt. Dit betekent in ieder geval dat Verwerkingsverantwoordelijke garandeert dat hij het recht heeft om de Persoonsgegevens te (laten) verzamelen en hij gerechtigd is tot het (laten) verwerken van deze gegevens.

Artikel 9. Kosten

9.1. De kosten voor de verwerking van gegevens die inherent zijn aan de normale uitvoering van de Overeenkomst, worden geacht besloten te liggen in de op grond van de Overeenkomst reeds verschuldigde vergoedingen.

9.2. Enige ondersteuning of enige andere aanvullende dienstverlening die Verwerker op grond van deze Verwerkersovereenkomst dient te verlenen, of die wordt verzocht door Verwerkingsverantwoordelijke, inclusief alle verzoeken tot aanvullende informatie en/of aanpassingen in werkwijze/beleid, zullen in rekening worden gebracht bij Verwerkingsverantwoordelijke overeenkomstig de in Bijlage 3 gespecificeerde tarieven.

9.3. De voorgaande bepaling is niet van toepassing indien de werkzaamheden verband houden met een toerekenbare tekortkoming van Verwerker onder deze Verwerkersovereenkomst. De werkzaamheden zullen in dat geval kosteloos worden verricht (onverminderd het recht van Verwerkingsverantwoordelijke de daadwerkelijk geleden schade op Verwerker te verhalen).

Artikel 10. Duur en beëindiging

10.1. Deze Verwerkersovereenkomst gaat in op de datum van ondertekening en de duur van deze Verwerkersovereenkomst is gelijk aan de duur van de in Bijlage 1 genoemde Overeenkomst(en), inclusief eventuele verlengingen daarvan.

10.2. De Verwerkersovereenkomst maakt na ondertekening ervan door beide Partijen integraal en onlosmakelijk deel uit van de Overeenkomst(en). Beëindiging van de Overeenkomst(en), op welke grond dan ook (opzegging/ontbinding), heeft tot gevolg dat de Verwerkersovereenkomst eveneens op dezelfde grond beëindigd wordt (en vice versa), tenzij Partijen in voorkomend geval anders overeenkomen.

10.3. Verplichtingen welke naar hun aard bestemd zijn om ook na beëindiging van deze Verwerkersovereenkomst voort te duren, blijven na beëindiging van deze Verwerkersovereenkomst gelden. Tot deze bepalingen behoren bijvoorbeeld die welke voortvloeien uit de bepalingen betreffende geheimhouding, aansprakelijkheid, geschillenbeslechting en toepasselijk recht.

10.4. Ieder der Partijen is gerechtigd, onverminderd hetgeen daartoe bepaald is in de Overeenkomst, de uitvoering van deze Verwerkersovereenkomst en de daarmee samenhangende Overeenkomst op te schorten, dan wel zonder rechterlijke tussenkomst met onmiddellijke ingang te ontbinden, indien:

a.) de andere Partij wordt ontbonden of anderszins ophoudt te bestaan;
b.) de andere Partij aantoonbaar [ernstig] tekortschiet in de nakoming van de verplichtingen die voortvloeien uit deze Verwerkersovereenkomst en die toerekenbare tekortkoming niet binnen 30 dagen is hersteld na een daartoe strekkende schriftelijke ingebrekestelling;
c.) een Partij in staat van faillissement wordt verklaard of surséance van betaling aanvraagt.

10.5. Gelet op de grote afhankelijkheid van Verwerkingsverantwoordelijke van Verwerker alsmede het continuïteitsrisico bij incidenten en calamiteiten (zoals faillissement), verklaart Verwerker zich reeds nu voor alsdan bereid op eerste verzoek van Verwerkingsverantwoordelijke aanvullende afspraken met Verwerkingsverantwoordelijke te maken teneinde voornoemde risico's te verkleinen. Deze aanvullende afspraken kunnen onder meer bestaan uit:

a.) het maken van afspraken over het periodiek terug of aan een derde partij leveren van de door Verwerker verwerkte gegevens; en/of
b.) het met een derde partij sluiten van een overeenkomst die ertoe strekt dat de betreffende derde partij zich hoofdelijk verbindt tot of borg staat voor de nakoming van de Overeenkomst; en/of
c.) het met een derde partij sluiten van een (tri-partite) overeenkomst die ertoe strekt dat de betreffende derde partij (voortdurend) over alle benodigde gegevens komt te beschikken om in voorkomend geval (een deel van) de op grond van de Overeenkomst te verrichten prestaties – al dan niet op basis van een nieuwe overeenkomst – in plaats van of parallel aan Verwerker te kunnen (gaan) verrichten.

10.6. Verwerker heeft een exit-plan voor het nakomen van alle verplichtingen uit deze Verwerkersovereenkomst, ingeval de Overeenkomst of de Verwerkersovereenkomst (tussentijds) beëindigd wordt. Verwerker geeft op eerste verzoek van Verwerkingsverantwoordelijke afschrift van dit plan.

10.7. Verwerkingsverantwoordelijke is gerechtigd deze Verwerkersovereenkomst en de Overeenkomst per direct te ontbinden indien Verwerker te kennen geeft niet (langer) te kunnen voldoen aan de betrouwbaarheidseisen die op grond van ontwikkelingen in de wet en/of de rechtspraak aan de verwerking van de Persoonsgegevens worden gesteld.

10.8. Verwerker dient Verwerkingsverantwoordelijke voorafgaand en tijdig te informeren over een voorgenomen overname of eigendomsoverdracht.
10.9. Het is Verwerker niet toegestaan om zonder uitdrukkelijke en schriftelijke toestemming van Verwerkingsverantwoordelijke deze Verwerkersovereenkomst en de rechten en plichten die samenhangen met deze Verwerkersovereenkomst over te dragen aan een derde partij.

Artikel 11. Bewaartermijnen, teruggave en vernietiging van Persoonsgegevens

11.1. Verwerker bewaart de Persoonsgegevens niet langer dan strikt noodzakelijk, waaronder begrepen de wettelijke bewaartermijnen of een eventueel tussen Partijen gemaakte afspraak over bewaartermijnen zoals vastgelegd in Bijlage 1. In geen geval bewaart Verwerker de Persoonsgegevens langer dan tot het einde van deze Verwerkersovereenkomst. Verwerkingsverantwoordelijke bepaalt of en zo ja hoe lang gegevens bewaard moeten blijven.
11.2. Bij beëindiging van de Verwerkersovereenkomst, of indien van toepassing aan het einde van de overeengekomen bewaartermijnen, of op schriftelijk verzoek van Verwerkingsverantwoordelijke zal Verwerker, tegen redelijke kosten, naar keuze van Verwerkingsverantwoordelijke, de Persoonsgegevens onherroepelijk (doen) vernietigen of teruggeven aan Verwerkingsverantwoordelijke. Op verzoek van Verwerkingsverantwoordelijke verstrekt Verwerker bewijs van het feit dat de gegevens onherroepelijk zijn vernietigd of verwijderd. Eventuele teruggave van de gegevens zal in een algemeen gangbaar, gestructureerd en gedocumenteerd gegevensformaat langs elektronische weg plaatsvinden. Indien teruggave, onherroepelijke vernietiging of verwijdering niet mogelijk is, stelt Verwerker Verwerkingsverantwoordelijke daarvan onmiddellijk op de hoogte. In dat geval garandeert Verwerker dat hij de Persoonsgegevens vertrouwelijk zal behandelen en niet langer zal verwerken.

Artikel 12. Intellectuele eigendomsrechten

12.1. Voor zover de (verzameling van) Persoonsgegevens wordt beschermd door enig intellectueel eigendomsrecht, verleent Verwerkingsverantwoordelijke toestemming aan Verwerker de Persoonsgegevens te gebruiken in het kader van de uitvoering van deze Verwerkersovereenkomst.

Artikel 13. Slotbepalingen

13.1. De overwegingen maken onderdeel uit van deze Verwerkersovereenkomst.
13.2. In geval van nietigheid c.q. vernietigbaarheid van een of meer bepalingen uit deze Verwerkersovereenkomst, blijven de overige bepalingen onverkort van kracht.
13.3. In alle gevallen waarin deze Verwerkersovereenkomst niet voorziet beslissen Partijen in onderling overleg.
13.4. Op deze Verwerkersovereenkomst is Nederlands recht van toepassing.
13.5. Partijen zullen zich inspannen conflicten in onderling overleg op te lossen. Hierbij is inbegrepen de mogelijkheid het geschil te beëindigen door een in onderling overleg vast te stellen mediation of arbitrage.
13.6. Geschillen over of in verband met deze Verwerkersovereenkomst worden uitsluitend voorgelegd aan de daartoe in de Overeenkomst aangewezen rechtbank of arbiter(s).

GGD West-Brabant	Yource Operations B.V. (Cendris Customer Contact B.V.)
[redacted]	[redacted]

Plaats: _____

Datum:_____

Plaats: _____

Datum: _____

Bijlage 1: Overeenkomsten, omschrijving Persoonsgegevens, aard verwerkingen, etc.

Deze Verwerkersovereenkomst is een bijlage bij de volgende Overeenkomsten en heeft betrekking op de volgende verwerkingen van Persoonsgegevens.

Ingangs-datum contract	Kenmerk / nummer / titel contract	Korte omschrijving diensten	Aard van de verwerking	Soort Persoonsgegevens	Categorieën van betrokkenen	Doeleinden van de verwerking	Goedgekeurde subverwerkers	Afspraken bewaartermijnen
01-12-2022	HSCDOC-1368817716-1091 Raamovereenkomst Inzake bron- en contactonderzoeken	*De uitvoering van bron- en contactonder-zoeken*	***Artikel 1*** *Bijv. Verwerking patiënt gegevens,*	***Artikel 2*** *Bijv. NAW gegevens, medische gegevens, financiële gegevens, etc.*	***Artikel 3*** *Bijv. Patiënten, familieleden, personeelsleden*	***Artikel 4*** *Bijv. Verlenen en organiseren van zorg, interne bedrijfsvoeringsdoel-einden, etc*		

Bijlage 2: Omschrijving nadere beveiligingsmaatregelen

[*Hier de meer concrete beveiligingsmaatregelen specificeren*]

Bijlage 3: Specificatie tarieven

[*Hier uitwerken of en zo ja welke tarieven in rekening mogen worden gebracht voor uit de verwerkersovereenkomst voortvloeiende werkzaamheden*]

Bijlage 4 - **Aanpassingen t.o.v. standaard tekst << OPTIONEEL >>**

Bij voorkeur wordt de gehele tekst van de modelovereenkomst gehandhaafd, uitgezonderd Bijlagen 1, 2 en 3 die per overeenkomst specifiek moeten worden ingevuld.
Mochten er toch additionele wijzigingen in de tekst nodig zijn (na onderhandelingen tussen Opdrachtgever en Opdrachtnemer) dan kunnen de aanpassingen in deze Bijlage 4 beschreven worden onder opgave van

- Artikelnummer,
- Betreffende tekst uit de standaard die vervalt
- Nieuwe vervangende tekst
- Reden van wijziging (bijv. n.v.t., eis niet acceptabel voor Opdrachtnemer, onderhandeld, etc.)

Art.	Tekst die vervalt	Vervangende tekst	Reden

Instructies behandeling datalekken Bron- en Contact Onderzoek (BCO)

Binnen BCO kunnen datalekken plaatsvinden. GGD GHOR Nederland heeft contracten met de verschillende partijen die callcenter capaciteit leveren aan de regionale GGD'en. Indien een datalek zich voordoet, moet dit door de verwerkingsverantwoordelijke aan de Autoriteit Persoonsgegevens (AP) en/of betrokkene (de persoon van wie de gegevens zijn uitgelekt) worden gemeld. Om duidelijk te maken wie welke melding behandelt, is deze korte procedure opgesteld.

Datalekken bij een landelijke BCO-partner (BCO callcenter)

Indien een datalek ontstaat bij een landelijke BCO-partner wordt dit, conform artikel 6 van de verwerkersovereenkomst, gemeld bij GGD GHOR Nederland door het meldingsformulier[1] (bijlage 3 verwerkersovereenkomst landelijke partners) te mailen naar **privacy@ggdghor.nl**. Het is van belang dat de gelekte informatie, bijvoorbeeld de verkeerd gestuurde mail met daarin contactgegevens, mee wordt gestuurd met het meldingsformulier. Zo kan gecontroleerd worden of betrokkenen op basis van de gelekte informatie makkelijk te traceren zijn. Er zijn binnen BCO twee types datalekken, die als volgt worden afgehandeld:

1. **Datalek is voorgekomen bij werkzaamheden voor een regionale GGD**

In dit geval wordt de melding die bij GGD GHOR Nederland binnenkomt direct doorgestuurd naar de regionale GGD. GGD GHOR Nederland functioneert in deze datalekken enkel als verdeelstation en zorgt dat het meldingsformulier bij de desbetreffende GGD terechtkomt, zodat de regionale GGD een adequate beoordeling kan uitvoeren. Een voorbeeld van een categorie 1 datalek, is een brief verstuurd naar de verkeerde ontvanger.

De regionale GGD handelt zelfstandig het datalek af en stelt de privacy officer van GGD GHOR Nederland (via **privacy@ggdghor.nl**) op de hoogte van de afhandeling van het datalek en eventuele melding aan de AP en/of betrokkenen.

De volgende informatie heeft GGD GHOR nodig om het datalek adequaat te registeren in het datalekregister:

Is er naar aanleiding van het datalek een melding gedaan bij de AP? Licht toe waarom wel/niet.	
Is er naar aanleiding van het datalek een melding gedaan bij de betrokkenen? Licht toe waarom wel/niet.	
Welke maatregelen zijn genomen naar aanleiding van het datalek?	
Indien er een melding is gedaan bij de AP, is GGD GHOR vermeld als 'andere betrokken organisatie' in de zin van §1.2 Meldingsformulier datalek van de AP?	

2. **Datalek is voorgekomen op landelijk niveau**

Indien een GGD merkt dat een datalek is veroorzaakt door een medewerker van de landelijke schil van BCO en het datalek zich op een landelijk niveau speelt, dan dient de GGD het aan GGD GHOR te melden. In dit geval is het van belang dat het datalek op landelijk niveau wordt opgepakt en wordt

[1] Ter volledigheid is het meldingsformulier bijgevoegd op pagina 3.

behandeld volgens de procedure van GGD GHOR Nederland. Een voorbeeld van een categorie 2 datalek, is fraude met gegevens van betrokkenen van verschillende regio's door een landelijke BCO-medewerker.

De GGD vult daarvoor het meldformulier in zoals opgenomen in bijlage 3 van de verwerkersovereenkomst en op pagina 3 van deze instructie. De GGD stelt GGD GHOR Nederland **zo snel mogelijk**, maar **uiterlijk binnen 48 uur**, op de hoogte van het lek.

Extra toelichting met betrekking tot type datalekken

Om de datalekken te kunnen onderscheiden, moet worden gekeken waar het datalek heeft plaatsgevonden en wat de invloed is van het datalek. Als het datalek enkel (mogelijke) invloed heeft op één regionale GGD, dan moet de desbetreffende GGD het datalek zelf in behandeling nemen. Als het datalek (mogelijk) invloed heeft op meerdere GGD'en, dan moet GGD GHOR Nederland het datalek behandelen.

Voorbeelden van datalekken die enkel invloed hebben op één GGD, zijn de volgenden:

- Een brief wordt verstuurd aan een verkeerde persoon. Het gaat hier om een persoon, die enkel onder één GGD valt. Dit heeft geen gevolgen voor andere mensen bij andere GGD'en;
- Een BCO-medewerker wil verschillende mogelijk besmette contacten tegelijkertijd waarschuwen en zet de ontvangers van de waarschuwingsmail in CC in plaats van BCC, zodat alle contacten inzicht krijgen in elkaars contactgegevens;

Voorbeelden van datalekken die (mogelijk) invloed hebben op meerdere GGD'en, zijn de volgenden:

- Fraude met gegevens. Als een medewerker van de landelijk BCO-schil fraude heeft gepleegd, dan is het aannemelijk dat deze dat bij meerdere GGD'en waar deze actief is heeft gedaan of zich toegang heeft verschaft tot landelijke gegevens. In dat geval zijn er wellicht slachtoffers op landelijk niveau, waardoor dit ook op landelijk niveau moet worden onderzocht;
- Een BCO-medewerker die op social media screenshots deelt van privacygevoelige gegevens uit HP Zone Lite.

Meldingsformulier landelijke partners (zoals opgenomen in bijlage 3 van de verwerkersovereenkomst)

Afspraken betreffende Inbreuk in verband met persoonsgegevens ex artikel 4 sub 12 AVG in verband met Persoonsgegevens

1) Wanneer zich bij Verwerker Inbreuk in verband met persoonsgegevens voordoen in de zin van artikel 4 sub 12 als aangeduid sub ii definitie Inbreuk in verband met persoonsgegevens, dan wel Verwerker daarmee bekend raakt, levert Verwerker de volgende informatie zo snel mogelijk, **maar uiterlijk binnen 48 uur**, aan de Verwerkingsverantwoordelijke.

2) Contactgegevens melder (Naam, functie, emailadres, telefoonnummer)

3) Gegevens over het Inbreuk in verband met persoonsgegevens
Geef een samenvatting van de Inbreuk in verband met persoonsgegevens en in hoeverre de beveiliging van de persoonsgegevens in het gedrang is;

4) Van hoeveel personen zijn Persoonsgegevens betrokken bij de inbreuk? (Vul de aantallen in.)

a) Minimaal: (vul aan)
b) Maximaal: (vul aan)

5) Omschrijf de groep mensen van wie Persoonsgegevens zijn betrokken bij de inbreuk;

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

a) Op (datum)
b) Tussen (begindatum periode) en (einddatum periode)
c) Nog niet bekend

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

a) Lezen (vertrouwelijkheid)
b) Kopiëren
c) Veranderen (integriteit)

d) Verwijderen of vernietigen (beschikbaarheid)

e) Diefstal
f) Nog niet bekend

8) Om welk type Persoonsgegevens gaat het? (U kunt meerdere mogelijkheden aankruisen.)

a) Naam -, adres - en woonplaatsgegevens
b) Telefoonnummers
c) E - mailadressen of andere adressen voor elektronische communicatie

d) Toegangs - of identificatiegegevens (bijvoorbeeld inlognaam/wachtwoord of huisarts/ zorggroepnummer)
e) Financiële gegevens (bijvoorbeeld rekeningnummer, creditcardnummer)

f) Burgerservicenummer (BSN)
g) Paspoortkopieën of kopieën van andere legitimatiebewijzen
h) Geslacht, geboortedatum en/of leeftijd
i) Bijzondere Persoonsgegevens (bijvoorbeeld ras, etniciteit, criminele gegevens, politieke overtuiging, vakbondslidmaatschap, religie, seksuele leven, gegevens over de gezondheid)

j) Overige gegevens, namelijk (vul aan)

9) Welke gevolgen kan de inbreuk hebben voor de persoonlijke levenssfeer van de betrokkenen? (U kunt meerdere mogelijkheden aankruisen.)
a) Stigmatisering of uitsluiting
b) Schade aan de gezondheid

c) Blootstelling aan (identiteits)fraude

d) Blootstelling aan spam of phishing

e) Anders, namelijk (vul aan)

10) Vervolgacties naar aanleiding van het Datalek
Welke technische en organisatorische maatregelen heeft uw organisatie getroffen om de inbreuk aan te pakken en om verdere inbreuken te voorkomen?

11) Technische beschermingsmaatregelen
Zijn de Persoonsgegevens versleuteld, gehasht of op een andere manier onbegrijpelijk of ontoegankelijk gemaakt voor onbevoegden? (Kies een van de volgende opties en vul waar nodig aan.)
a) Ja
b) Nee
c) Deels, namelijk: (vul aan)

Als de Persoonsgegevens geheel of deels onbegrijpelijk of ontoegankelijk zijn gemaakt, op welke manier is dit dan gebeurd? (Beantwoord deze vraag als u bij de vorige vraag gekozen heeft voor optie a of optie c. Als u gebruik heeft gemaakt van encryptie, licht dan ook de wijze van versleutelen toe.)

12) Internationale aspecten
Heeft de inbreuk betrekking op personen in andere EU-landen? (Kies een van de volgende opties.)

a) Ja
b) Nee
c) Nog niet bekend

Wob-verzoek SOLV/ICAM datalek 2021 coronasysteem

4.0 Tekst Wob-verzoek en register documenten

Tekst verzoek (iv)

Audits, rapportages, analyses en onderzoeken (intern of door derde partijen) met betrekking tot privacy(risico's) en beveiliging(srisico's) in verband met CoronIT, HPZone en HPZone Lite, waaronder in ieder geval:

a) Risicoanalyse uitgevoerd over de test- en traceerketen d.d. 22 december 2020; [voetnoot 2: Kamerstukken II 2020-2021, 27 529, nr. 252]
b) Analyse KPMG interne systemen d.d. 20 januari 2020; [voetnoot 3: Kamerstukken II 2020-2021, 27 529, nr. 235, p. 9]
c) IT-assessment op het IT landschap van de COVID-19 bestrijding door GGD GHOR Nederland van december 2020; [voetnoot 4: Kamerstukken II 2020-2021, 27 529, nr. 234, vraag 51]
d) IT-audit KPMG d.d. 18 december 2020; [voetnoot 5: Feitenrelaas inzake gebeurtenissen omtrent coronatest-IT-systeem van de GGD, p. 6]

Register

Een screenshot van de verkennerpagina van map 4:

1. ETHISCHE OVERWEGINGEN

1.1 Verordening

Relevante documenten / declaraties / richtlijnen / wetgeving:

- Declaration of Taipei (uitbreiding op declaration of Helsinki) (11)
- Algemene verordening gegevensbescherming (AVG)
- Wet Publieke Gezondheid (WPG)

Relevante artikelen uit de AVG en WPG zijn weergegeven in bijlage 1. De studie wordt verricht volgens de principes van de 'Declaration of Helsinki' en de 'Declaration of Taipei'. *Informed consent* is een punt waaraan deze studie niet helemaal kan voldoen (toelichting in 12).

Data over besmettingen worden binnen de wettelijke taak primair verzameld om inwoners zorg te verlenen en om het verspreidingsrisico in te schatten en te verminderen. Gebruik van deze data voor beleidssturing op populatieniveau is een secundair doel, dat ethische overwegingen oproept. Deze heb betrekking hebben op de uitwisseling en koppeling van privacygevoelige data die herleidbaar zijn tot het individu. Er dient een afweging te worden gemaakt tussen de potentiële privacy schade dat een individu zou kunnen ondervinden (AVG) van deze datakoppeling en de potentiële winst die het oplevert voor de volksgezondheid (WPG). Deze afweging staat beschreven in paragraaf 1.4.

1.2 Aanwerving en geïnformeerde toestemming

Omdat dit project een secundaire analyse op reeds verzamelde data betreft, is geen sprake geweest van recruitment. De studie is gebaseerd op registratiedata die primair is verzameld voor het leveren van passende covid-zorg en preventie van verdere verspreiding van infectieziekten en niet voor onderzoeksdoeleinden. Hierdoor is geen *informed consent* gevraagd. Wij zijn van mening dat dit een het vragen van uitdrukkelijke toestemming onmogelijk is of een onevenredige inspanning kost (zie 1.4).

1.3 Bezwaren door minderjarigen of wilsonbekwame subjecten (indien van toepassing)

Niet van toepassing. Het betreft hier secundaire data-analyse. De mensen in het onderzoek ondergaan geen behandeling. De privacy-punten die in dit hoofdstuk worden benoemd, zijn op iedereen van toepassing. Er zitten relatief weinig

minderjarigen in de dataset. Belangrijker is dat ook voor jongeren geldt dat zij op geen enkele manier herleidbaar zijn voor de onderzoekers, conform de AVG.

1.4 Baten en risico evaluatie, groep gerelateerd; AVG versus WPG

De AVG schrijft voor dat bijzondere persoonsgegevens (in dit project gegevens over besmettingen) bij uitzondering gebruikt mogen worden voor onderzoeksdoeleinden wanneer kan worden verantwoord dat:

a) het onderzoek het algemeen belang dient
b) toestemming vragen aan elke individuele deelnemer van het onderzoek onmogelijk blijkt of een onevenredige inspanning kost en
c) de persoonlijke levenssfeer van de betrokkenen niet onevenredig wordt geschaad.

Ad a. Het onderzoek dient een algemeen belang namelijk het verkrijgen van betrouwbare resultaten over de achtergrondkenmerken van individuen die een GGD teststraat bezoeken. Op basis van de resultaten kan de GGD het testbeleid beter afstemmen op groepen die niet- of ondervertegenwoordigd zijn. Dit draagt bij aan het beter indammen van het coronavirus en het gezondheidspotentieel van alle inwoners optimaal te ontwikkelen.

Ad b. In de registratiedata zijn honderdduizenden personen opgenomen. Het benaderen van al deze personen zou een grote administratieve inspanning vergen voor de onderzoekspartijen. Daarnaast zou het expliciet vragen van toestemming onrust kunnen creëren, bijvoorbeeld in het geval dat personen nog herstellende zijn van Covid-19 of dat personen juist overleden blijken te zijn. Tenslotte zou de kwaliteit en representativiteit van de uitkomsten van het onderzoek kunnen afnemen door een lage deelnamegraad van bepaalde bevolkingsgroepen: er is een grote kans dat er dan een selectiebias ontstaat waardoor de resultaten van het onderzoek onbruikbaar worden. Samenvattend is te stellen dat het een onevenredige inspanning vergt (in tijd en kosten) om al deze personen alsnog om toestemming te vragen.

Ad c. De personen die de data analyses zullen uitvoeren zijn niet de personen die de data zullen aanleveren aan het CBS. Door deze strikte scheiding zijn de onderzoekers die aan de slag gaan met de gepseudonimiseerde data (zonder het Burgerservicenummer erin) niet in staat het individu in de originele databron te

herleiden. Resultaten zullen alleen op geaggregeerd niveau worden gerapporteerd en gecommuniceerd. Wanneer een bepaalde doelgroep zo klein is dat de herleidbaarheid in het geding komt zal deze niet worden gerapporteerd. Hiervoor zal een minimale 'cell count' van 10 per subgroep worden gehanteerd. Hierbij kan bijvoorbeeld worden gedacht aan tijdelijke arbeidsmigranten uit een bepaald land van herkomst of inwoners met een migratieachtergrond in een heel dun bevolkte geografisch gebied.

Het voordeel is helder. Ons project levert een belangrijke bijdrage voor drie taken binnen de WPG (bijlage 1) omdat de resultaten van epidemiologische analyses direct zullen worden gebruikt voor lokale invulling van de preventieve covid-19 zorg.

Overall achten wij het risico op nadelige effecten voor deelnemers minimaal. Er is een punt van aandacht, te weten het risico op stigma wanneer blijkt dat specifieke populatiegroepen niet- of ondervertegenwoordigd zijn. Hoewel de rapportage heel feitelijk van aard zal zijn, zal zorgvuldig worden omgegaan met formuleringen. Deze zullen worden gekozen op basis van een combinatie van kwantitatieve en kwalitatieve waarnemingen.

1.5 Schadeloosstelling bij letsel

Niet van toepassing.

1.6 Incentives (indien van toepassing)

Niet van toepassing.

Bijlage 1. Citaat van relevante artikelen uit de WPG en de AVG

Binnen de WPG voert de GGD onder andere de volgende wettelijke taken uit:

- Artikel 2a: het verwerven van, op epidemiologische analyse gebaseerd, inzicht in de gezondheidssituatie van de bevolking
- Artikel 2c: het bewaken van gezondheidsaspecten in bestuurlijke beslissingen en
- Artikel 2d: het bijdragen aan opzet, uitvoering en afstemming van preventieprogramma's, met inbegrip van programma's voor de gezondheidsbevordering

De verwerking van *bijzondere* persoonsgegevens (zoals gezondheidsgegevens) is in beginsel verboden. Deze verwerking is alleen toegestaan wanneer een beroep kan worden gedaan op één van de zes grondslagen voor het verwerken van persoonsgegevens èn één van de 10 wettelijke uitzonderingsregels genoemd in de AVG (Artikel 9 AVG). Bij eventuele verwerking van bijzondere persoonsgegevens kan een beroep worden gedaan op: de verwerking is noodzakelijk met het oog op de archivering in het algemeen belang, wetenschappelijk of historisch onderzoek of statistische doeleinden (Artikel 9 lid 2 sub j AVG).

De Uitvoeringswet op de AVG stelt enkele eisen voor een beroep op de noodzaak van de persoonsgegevens voor wetenschappelijk onderzoek:

a) de verwerking moet noodzakelijk zijn met het oog op wetenschappelijk of historisch onderzoek of statistische doeleinden.
b) het wetenschappelijk onderzoek moet een algemeen belang dienen.
c) het vragen van uitdrukkelijke toestemming onmogelijk blijkt of een onevenredige inspanning kost
d) bij de uitvoering is voorzien in zodanige waarborgen dat de persoonlijke levenssfeer van de betrokkene niet onevenredig wordt geschaad.

Aanbiedingsformulier MT GGD WB

Datum vergadering	16-11-2020
Agendapunt	2.6
Onderwerp	Verzoek tot instemming ethische overwegingen secundair gebruik Covid-19 data.
Naam indiener	[redacted]
Doel	ter vaststelling
Vraag aan MT	Het MT wordt gevraagd om mee te gaan met de ethische overwegingen van GGD ZHZ, GGD Rotterdam-Rijnmond en GGD Zeeland, beschreven in de bijlage, om zonder *informed consent* van het individu secundair gebruik te maken van privacy-gevoelige CoronIT- en HPzone-data.
Toelichting	In een Brabantbreed onderzoek willen we onderzoeken of de geteste personen op Covid-19 in Noord-Brabant een doorsnede zijn van de Brabantse bevolking wat betreft hun sociaaleconomische positie. Met de resultaten kan het GGD-testbeleid beter worden afgestemd op groepen die niet- of ondervertegenwoordigd zijn. Data (lees CoronIT- en HPzone-data) over besmettingen worden binnen de wettelijke taak primair verzameld om inwoners zorg te verlenen en om het verspreidingsrisico in te schatten en te verminderen. Gebruik van deze data voor beleidssturing op populatieniveau is een secundair doel, dat ethische overwegingen oproept. Deze hebben betrekking hebben op de uitwisseling en koppeling van privacygevoelige data die herleidbaar zijn tot het individu. Er dient een afweging te worden gemaakt tussen de potentiële privacy schade dat een individu zou kunnen ondervinden (AVG) van deze data-uitwisseling en data-koppeling en de potentiële winst die het oplevert voor de volksgezondheid (WPG). Deze afweging is al gemaakt door GGD ZHZ, GGD Rotterdam-Rijnmond en GGD Zeeland in een gezamenlijk wetenschappelijk onderzoek van deze GGD-en. De conclusie daarvan is dat: 1. er geen *informed consent* kan worden gevraagd doordat het vragen van uitdrukkelijke toestemming onmogelijk is of een onevenredige inspanning kost. Het gaat hier om ruim 400.000 individuen. 2. Bovendien ondergaan de individuen geen behandeling en zitten er relatief weinig minderjarigen in de data set. 3. Tenslotte geldt dat individuen op geen enkele manier herleidbaar zijn voor de onderzoekers.
Vergaderstukken	Ethische overwegingen.docx
Financiële consequenties	Niet van toepassing.

Advies ontvangen van	[redacted] heeft geadviseerd dat advies van [redacted] niet nodig is, omdat we hier meeliften op de hier boven genoemde conclusies van de functionaris gegevensbescherming van GGD ZHZ.
Besluit/ Vervolgstappen:	Het MT besluit: Niet zonder meer akkoord te gaan met de ethische overwegingen van GGD ZHZ, GGD Rotterdam-Rijnmond en GGD Zeeland, beschreven in de bijlage, om zonder *informed consent* van het individu secundair gebruik te maken van privacy-gevoelige CoronIT- en HPzone-data. Voordat dit kan, dienen eerst SMA's en FGB betrokken worden op de vragen als in bespreking genoemd.
Communicatie:	
Doorgeleiding naar OR	☐ ter informatie ☐ ter instemming ☐ ter advisering ☐ niet van toepassing

Handtekening (Algemeen) Directeur:

Brabant-Zuidoost

Betreft: advies [redacted] GGD BZO inzake Corona Dashboard
Datum: 19 oktober 2020

Dag [redacted]

Graag licht ik mijn standpunt toe ter zake waarom de gegevens in CoronIT onder andere onder de Wpg worden verzameld en daarmee toestemming van de betrokkene niet vereist is voor wat betreft het verdere gebruik van deze gegevens voor het dashboard en mogelijke andere statistische- of onderzoekdoeleinden.

Ik ben het eens met [redacted] dat het testen van mensen op COVID-19 op de teststraten geen Wpg-taak is. Hier komt de WGBO om de hoek heen kijken. Echter, is het belangrijk om een goed onderscheid te blijven maken tussen gegevens die verkregen zijn op grond van de Wpg en de WGBO, ondanks de vermening van Wpg en WGBO. Dit geldt zowel voor CoronIT en HPZone. Daarnaast worden de gegevens in CoronIT niet zonder meer enkel verkregen op basis van de uitgevoerde coronatesten op de teststraat. Alle gegevens (met uitzondering van de monsters, registratie daarvan en adviezen) van de betrokkene worden verkregen door het callcenter en/of burgerportaal en de labs.

Wet publieke gezondheid (Wpg)

I. CoronIT bestaat uit Wpg en voor een bepaald gedeelte uit WGBO (ten minste voor wat betreft de afgenomen monsters, registratie daarvan en adviezen). Vanuit Wpg kunnen gegevens verder worden verwerkt voor statistische of onderzoeksdoeleinden (zolang die in het kader van de Wpg zijn aangeleverd en er natuurlijk wordt voldaan aan andere eisen van de AVG). Normaliter krijgt de GGD op grond van artikel 21 en 24 Wpg meerdere gegevens aangeleverd in het kader van infectieziektebestrijding. Het gaat om de volgende gegevens:

> ***a****. de naam, het adres, het geslacht, de geboortedatum, het burgerservicenummer en de verblijfplaats van de betrokken persoon,*
>
> ***b.*** *de infectieziekte dan wel een beschrijving van het ziektebeeld, de eerste ziektedag, de vaccinatietoestand, het gebruik van chemoprofylaxe, de vermoedelijke infectiebron, de datum van vermoeden of vaststelling van infectie, de wijze van vaststelling van die infectieziekte, en*
>
> ***c.*** *indien nodig, of de betrokken persoon dan wel een persoon in zijn directe omgeving beroeps- of bedrijfsmatig betrokken is bij de behandeling van eet- of drinkwaren of bij de behandeling, verpleging of verzorging van andere personen.*

Deze pandemie heeft ervoor gezorgd dat de werkwijze heeft moeten afwijken van de standaard. Het zijn niet meer de artsen die bovenstaande gegevens aanleveren, maar dit gebeurt vanuit CoronIT (het callcenter), nu het niet mogelijk was om artsen hiervoor te gaan inzetten. Alhoewel in het kader hiervan vaak geen sprake is van een arts zoals bedoeld in de Wpg (door de bijzondere inrichting van het callcenter en de teststraten en coronIT), wordt de Wpg naar analogie gebruikt. Dit gebeurt op grond van artikel 6 Wpg. Dit is in overleg met het VWS bepaald. Dit betekent dat wij op grond van artikel 6 Wpg (naar analogie van

artikel 21 en 24 Wpg) recht hebben op bovenstaande gegevens. Onze grondslag om deze gegevens in CoronIT (en deels HPZone) te verwerken is om die reden op grond van de Wpg. Wij hebben recht op bovenstaande gegevens en kunnen deze gebruiken om in het kader van volksgezondheid een beeld te krijgen op de ontwikkeling van de verspreiding van het virus (los van het BSN uiteraard). Er zit een noodzaak aan vast. Uiteraard moeten wij dit goed verantwoorden, maar toestemming als grondslag voor verwerking is dan niet nodig. Immers, op grond van de AVG is verdere verwerking op grond van statistische- of onderzoeksdoeleinden verenigbaar met het doel waarvoor de gegevens in beginsel zijn verwerkt (Wpg). Dit betekent dat de Wpg als grondslag voor de verdere verwerking dient.

II. Ook krijgen wij op grond van artikel 25 lid 2 en 3 Wpg gegevens van het laboratorium. Het betreft dan:

> ***2*** *Onverminderd artikel 22 meldt het hoofd van het laboratorium de vaststelling van een verwekker van een infectieziekte behorend tot groep A, B1, B2 of C aan de gemeentelijke gezondheidsdienst van de gemeente waarin de arts die het onderzoek bij het laboratorium heeft aangevraagd zijn praktijk heeft.*
>
> ***3*** *De melding bevat de volgende gegevens: de naam van de arts, de naam, de geboortedatum en het burgerservicenummer van de betrokken persoon.*

Ook deze gegevens verwerkt de GGD op grond de Wpg. Indien de GGD deze gegevens verder verwerkt voor statistische- of onderzoekdoeleinden, om zo een beeld te krijgen op de ontwikkeling van de verspreiding van de ziekte, is de toestemming van de betrokkene niet nodig. Immers, ook hier is de verwerking verenigbaar met het doel waarvoor de persoonsgegevens in beginsel worden verwerkt.

III. Indien de arts (deze is nu niet van toepassing, maar het idee is niet anders) andere gegevens dan zoals boven genoemd aan de GGD wil strekken (dus eigenlijk als wij in het dasboard andere gegevens meenemen dan zoals hierboven vermeld), dan moet aan de betrokkene wel om toestemming worden vragen. Denk aan telefoonnummer en e-mailadres die in CoronIT worden verwerkt. Immers, deze 'extra' gegevens zijn niet verkregen op grond van de Wpg -> art. 24 lid 4 Wpg vermeldt:

> *De arts verstrekt aan de gemeentelijke gezondheidsdienst uitsluitend andere medische gegevens over de betrokken persoon indien:*
>
> ***b.*** *de betrokken persoon daarvoor toestemming geeft.*

WGBO

Het benoemen van onderzoek in het kader van WGBO is begrijpelijk, doch lijkt in beginsel dat GGD geen onderzoeken uitvoert als bedoeld in de WGBO. Denk aan onderzoek waarbij de monster worden geanalyseerd om de werking van het virus te begrijpen. Het doel van de GGD is de focus op de ontwikkeling van de verspreiding van het virus in het kader van volksgezondheid. Indien en voor zover de GGD'en ook onderzoek in het kader van de WGBO uitvoeren, dan geldt het volgende vanuit de WGBO. De gegevens van de 'patiënt' van het medische dossier kan aan een ander worden verstrekt in het kader van statistische doeleinden. Dit zou dus in basis de monsters betreffen. Het klopt dat toestemming niet nodig is als het vragen van die toestemming onmogelijk is.

Echter, is dit 1 van de 2 uitzondering. De tweede uitzondering wordt niet benoemd. De tweede uitzondering is;

'het vragen van toestemming, gelet op de aard en het doel van het onderzoek, in redelijkheid niet kan worden verlangd en de hulpverlener zorg heeft gedragen dat de gegevens in zodanige vorm worden verstrekt dat herleiding tot individuele natuurlijke personen redelijkerwijs wordt voorkomen.'

De wet legt de tweede uitzondering als volg uit: *'Met de woorden 'in redelijkheid niet te verlangen' heeft de wetgever speciaal gedacht aan onderzoeken waarbij zo grote aantallen patiënten zijn betrokken dat redelijkerwijs niet kan worden gevergd dat inspanningen worden gedaan om hen allen te bereiken, dan wel, in uitzonderlijke omstandigheden, aan onderzoeken van zodanige aard dat het vragen van toestemming zou leiden tot een selectieve respons en daarvan een vertekend beeld van het onderzoeksresultaat als reëel gevolg moet worden gevreesd (NvW 4, Kamerstukken II, 21561, 20, p. 3)'*

Op grond van bovenstaande zou gesteld kunnen worden, indien en voor zover de analyses van de GGD'en kunnen worden gezien als onderzoeken in het kader van de WGBO (wat te betwijfelen valt), op grond van de tweede uitzondering een mogelijkheid bestaat om de toestemming van de betrokkene te 'passeren'. Uiteraard moet er dan voor gezorgd worden, zoals de tweede uitzondering stelt, dat herleiding tot individuele natuurlijke personen redelijkerwijs wordt voorkomen. Dit zal voor ons tijdens de verwerking lastiger zijn, nu wij natuurlijk ook de herleidbare gegevens hebben, maar uiteraard moeten de gegevens in het onderzoek zelf zodanig worden uitgezet, dat uit een analyse of onderzoek zelf de betrokkene rederlijkwijs niet herleidbaar is.

Conclusie

Zoals hierboven vermeld is de toestemming van betrokkene niet nodig indien de gegevens op grond van de Wpg worden verzameld, hetgeen in verre weg de meeste gevallen het geval is. Indien er sprake zou zijn van de WGBO, kan gebruik worden gemaakt van de tweede uitzondering voor wat betreft het niet hoeven vragen om toestemming. Let wel dat te allen tijde goed moeten worden gemotiveerd waarom geen toestemming wordt gevraagd. Enige uitzondering waarvoor wel toestemming moet worden gevraagd, betreft die gegevens zoals vermeld in artikel 24 lid 4 Wpg, namelijk gegevens die zowel niet zijn verzameld op grond van de Wpg als niet op grond van de WGBO.

Hopende jullie hier van voldoende informatie te hebben voorzien.

Met vriendelijke groeten,

[redacted]

Beste [redacted],

Hierbij willen wij je informeren over het landelijke, digitale registratiesysteem CoronIT. CoronIT is een systeem dat het uitvoeren van de COVID-19 testprocessen bij GGD'en en laboratoria efficiënt kan ondersteunen. Deze webapplicatie wordt vergoed door het ministerie van VWS en gaat op zeer korte termijn live bij alle GGD'en. Het is de bedoeling dat GGD'en uiterlijk op 8 mei werken met CoronIT of bezig zijn met de implementatie daarvan. Het projectleiderschap van CoronIT is in handen van GGD GHOR Nederland.

Registratiesysteem CoronIT

Het doel van de CoronIT is het automatiseren, vergemakkelijken, versnellen en zoveel mogelijk centraliseren van de administratie behorende bij het testproces op COVID-19. CoronIT maakt het mogelijk om het proces van triage, aanvraag tot het terugkoppelen en het delen van een testuitslag te vereenvoudigen en te versnellen. Hierdoor wordt het mogelijk om de opgeschaalde testcapaciteit van de laboratoria gericht en efficiënt in te zetten. Met behulp van het registratiesysteem kunnen GGD'en en externe aanvragers bij vermoeden van besmetting, personen snel en efficiënt laten testen op COVID-19.

Informatie met betrekking tot CoronIT

In het project is een FG betrokken, die risico's in kaart brengt en adviezen geeft over adequate bescherming van persoonsgegevens. Wij gaan alle relevante informatie met u te delen, maar zijn op dit moment nog zoekende naar de meest optimale manier daarvoor. Zodra dit bekend is, stellen wij u op de hoogte en krijgt u toegang tot de informatie. Op dit moment werken wij nog aan de DPIA op de webapplicatie. Wij houden u op de hoogte van relevante ontwikkelingen.

Vragen

Wellicht was u nog niet op de hoogte van de implementatie van het registratiesysteem CoronIT. In eerste instantie zijn de bij ons bekende contactpersonen van de teststraten van de GGD'en geïnformeerd. Hebt u vragen naar aanleiding van dit bericht, de webapplicatie of specifieke vragen over de privacy en security aspecten van CoronIT, dan kunt u per mail contact opnemen met het projectteam implementatie via coronit@ggdghor.nl.

Wij hopen u hiermee vooralsnog voldoende te hebben geïnformeerd.

Met vriendelijke groet,
Namens het [redacted]

Cyber Inc. Security bv
Koraalrood 125
2718 SB Zoetermeer
Nederland

+31 85 0602 444
hello@cyberinc.nl
https://cyberinc.nl

Ggd West-Brabant
Doornboslaan 225
4816 CZ Breda
Nederland

[redacted]

[redacted]

Offerte 2020 / 107: Phishing simulatie -GGD W.B.

Beste [redacted]

Als antwoord op de mailwisseling met [redacted] is het Cyber Inc. een plezier om Ggd West-Brabant een voorstel te sturen. Het betreft een offerte voor de een eenmalige phishing simulatie. Dit heeft als doel de privacy- en security risico's te verkleinen, waarbij de menselijke factor een rol speelt. De resultaten van de medewerkers zal meetbaar worden vastgelegd voor de aantoonbaarheid in het kader van de relevante ISO-normeringen.

Mocht je binnen 3 maanden besluiten om het online security awareness programma af te nemen, dan verrekenen we deze offerte. Er zijn namelijk al 4 phishing simulaties inclusief bij het programma..

Wanneer je vragen en/of opmerkingen bent kun je te allen tijde contact opnemen met ondergetekende, via telefoonnummer +31(0)6 1348 5555 of via ons kantoor op +31(0)85 0602 444

Wij vertrouwen er op je met plezier te hebben geïnformeerd en zien je reactie met belangstelling tegemoet.

[redacted]

Met vriendelijke groet,

[redacted]
Cyber Inc. security BV

Het gedrag van de medewerkers binnen de organisatie moet aangepast worden, om de dreigingen en risico's van informatiebeveiliging en privacy het hoofd te bieden. Maar de meeste medewerkers zitten daar niet op te wachten. Ze vinden dat het prima gaat zoals het nu gaat. Ze vinden de onderwerpen saai en hebben eigenlijk geen tijd. Hierdoor kan je als organisatie risico's lopen door het verlies van gevoelige informatie, fraude en reputatieschade.

Onze diensten richten zich juist op deze groep medewerkers. Door ze nieuwsgierig te maken naar het onderwerp, motiveren we ze om te leren. Daarbij maken we het persoonlijk. Niet jij als medewerker, maar jij als persoon speelt de hoofdrol. We laten aan de hand van dagelijkse privé- en zakelijke situaties zien waarom deze onderwerpen belangrijk voor je zijn en wat je hieraan zelf kunt doen.

Phishing simulatie
De phishing simulatie die we aanbieden zal op het eerste moeilijkheidsniveau plaatsvinden en de score zal vergeleken kunnen worden met andere organisaties. Zo krijgt een score meer waarde. We meten hoeveel medewerkers de phishing hebben geopend, geklikt, data achter gelaten en de hacker gemaild hebben. We versturen of slaan geen wachtwoorden op, wel het account waarmee de medewerker inlogt. De simulatie wordt gedaan om medewerkers te helpen phishing te herkennen of ze te laten inzien dat ook zij slachtoffer kunnen worden.

Rapportage
De phishing campagne duurt ongeveer 2 weken. Na de campagne ontvang je een uitgebreid rapport. Hier hebben we al een voorbeeld van gestuurd naar Faris. Je weet dan niet alleen hoeveel medewerkers de phishingmail geopend hebben, hoeveel op de link geklikt hebben of hoeveel hun gegevens hebben achtergelaten. We laten ook zien wat de resultaten van deze simulatie bij andere organisaties is geweest en wat de resultaten zijn ten opzichte van de vorige simulaties indien je bij ons het awareness programma afneemt of meerdere phishing simulaties laat doen. Tevens laten we weten welke medewerkers de "hacker" hebben gemaild.

Onderstaand vind je de prijsopgave. Ik ben voor de prijs uitgegaan van 350 deelnemers voor een eenmalige phishing campagne.

Nummer	Datum
2020 / 107	20/05/2020

Beschrijving	Aantal	Stukprijs	Btw	Totaal
ph001: Phishing simulatie (eenmalig)	350	[redacted]	21%	[redacted]
		Totaal excl. btw		
		Btw 21%		
		Totaal incl. btw		
		Totaal te betalen		

*Alle genoemde prijzen hebben alleen betrekking op Ggd West-Brabant, ex btw en 30 dagen geldig na 20/05/2020. Op al onze aanbiedingen en overeenkomsten zijn de Algemene voorwaarden van Cyber Inc Security bv van kracht.

Beide partijen verklaren zich akkoord met de inhoud van de offerte.

Cyber Inc. Security bv
[redacted]

Ggd West-Brabant
[redacted]

Ondertekening
Aldus overeengekomen en in tweevoud ondertekend,
Ingangsdatum: 20 -5 - 2020

GGD West-Brabant,
Directeur Publieke Gezondheid

namens deze: [redacted]

plaats: Breda

datum: 20 -5 -2020

Cyber Inc. security b.v.,

namens deze: [redacted]

plaats: Zoetermeer

datum: 14-05-2020

HPZone autorisatie wijziging
export Bijzondere Persoonsgegeven
Voorstel

Versie 0.4

Auteurs;

- [redacted], [redacted], GGD GHOR
- [redacted], [redacted], GGD GHOR

Inhoudsopgave

Huidige situatie 3
Doelen 3
Oplossing 3
Uitgangspunten 3
Acties, Planning 4
Huidig aantal toegekende information officer rollen 5
Vragen/ opmerkingen? 5

Huidige situatie

In de huidige situatie is het niet mogelijk om bijzondere persoonsgegevens te exporteren uit HPZone. Na het datalek in januari 2021 zijn alle export mogelijkheden m.b.t. bijzondere persoonsgegevens weggehaald.
Het ontbreken van de bijzondere persoonsgegevens heeft een impact op lopende (gesubsidieerde)onderzoeken en analyses. Zonder de bijzondere persoonsgegevens is het in sommige gevallen niet mogelijk het onderzoek verder uit te voeren.

Doelen

1. Mogelijk maken om alle gegevens te exporten in HPZone incl. de bijzondere persoonsgegevens
2. Zorgen dat risico van misbruikt van Bijzondere Persoonsgegevens zo klein mogelijk is.

Oplossing

Het inrichten van de Information Officer rol t.b.v. het exporteren van alle data uit HPZone. Daarna de rol op een verantwoorde manier laten toekennen aan 2 tot 5 gebruikers per regionale GGD (ongeacht de grootte van de GGD):

- Minimaal 2 personen per regionale GGD kunnen Bijzondere Persoonsgegevens exporteren
- Maximaal 5 personen per regionale GGD kunnen Bijzondere Persoonsgegevens exporteren

Uitgangspunten

Veiligheidsprinciepes toekennen Information officer rol
Ter behoeve van het beheersen van de dienstverlening aan de regionale GGD'en is het nodig om inzicht te hebben in de toekenning van de information officer rol zodat er, bij vragen aan de servicedesk, getoetst kan worden of deze persoon geautoriseerd is om bepaalde datavragen/autorisaties te vragen.

- Vaste dienstelling binnen de regionale GGD
- Geen functionele gebruikers accounts (bots/applicaties etc.) ivm NEN7510/NEN7513 richtlijnen

Uitsluiting
Functioneel en Technisch beheerders kunnen de information officer rol niet uitvoeren.

Acties, Planning

Actie	Wat	Wie	Afgerond?
1	Opdracht ontvangen voor uitvoer van de wijziging	DPG raad/Directie GGD GHOR Nederland	Ja
2	Opstellen planning en inventariseren impact/risico's	IM BCO GGD GHOR Nederland	Ja
3	Opvolging en uitvoer toekennen	IM BCO GGD GHOR Nederland	Ja
4	RfC & wijzigingsdocumentatie opstellen	PM BCO GGD GHOR Nederland	Ja
5	Gebruikers verwijderen uit de rol van information officer	Regionale GGD (Coördinatie via IM)	Week 46-47
6	Rechten toekennen information officer rol	Infact	Week 47
7	Delen van de lijst met gebruikers die de nieuwe rol gaan ontvangen (zie *"Invullijst gebruikers nieuwe information officer rol HPZone.xlsx"*)	Regionale GGD (Coördinatie via IM)	Week 46-47
8	Communicatie livegang nieuwe rechten	PM BCO GGD GHOR Nederland	Week 47/48
9	Toekennen nieuwe rol via regionale IT afdeling (regionale GGD)	Regionale GGD (Coördinatie via IM)	Week 46-48

Manager PCO en Directeur regionale GGD voorzien in handhaving en controle van (on)terechte uitgifte Bijzondere Persoonsgegevens Export autorisaties en toekenning rol "Information Officer".

* De lijst met personen die geautoriseerd worden, dient te bevatten;
- voornaam
- achternaam
- functie
- gebruikersnaam
- GGD e-mailadres
- reden gebruik

Huidig aantal toegekende information officer rollen

Hieronder een overzicht van de toekenning van de information officer rol.

Rijlabels	HPZone-Information-Officer
[redacted]	[redacted]
ggdwestbrabant.nl	3
[redacted]	[redacted]

Staat de GGD er niet bij? Dan zijn er van die desbetreffende GGD geen mensen aan de Information Officer rol gekoppeld.

Vragen/ opmerkingen?

- [redacted]
- [redacted]

Informatieveiligheidsbeleid

2018 - 2022

Het Service Centrum

Versie: 1.0

Datum: 22-03-2018

Inhoudsopgave

Versiebeheer 3

Vaststelling door MT HSC 3

Informatieveiligheidsbeleid 4

1. Aanleiding en doel 4

Visie 4

Waarom informatiebeveiliging? 4

Doel 5

Doelstelling 5

Scope 5

Toepassingsgebied 5

Uitgangspunten 6

Werking, evaluatie en herziening 6

2. Definitie informatiebeveiliging 7

3. Verantwoordelijkheden en organisatie 8

4. Risicomanagement en continuïteit 9

Risicomanagement 9

Continuïteit 11

5. Naleving van wet- en regelgeving 12

Versiebeheer

Versie	Datum	Auteur(s)	Status	Opmerking
01	27-02-2018	[redacted]	Under construction	Aanpassen van het totale informatieveiligheidsbeleid omdat scope gewijzigd is in verband met organisatiewijzigingen. En de norm NEN7510 is gewijzigd, er is een nieuwe uitgave. NEN7510:2017
1.0	22-3-2018	[redacted]	Vastgesteld	

Vaststelling door MT HSC

Versie	Datum	Datum vaststelling MT HSC
01	18-01-2017	n.v.t. zie opmerking versiebeheer
02[1]	27-02-2018	22-03-2018

[1] Bij vaststelling door het MT HSC wijzigt versie 02 in versie 1.0

Informatieveiligheidsbeleid

1. Aanleiding en doel

Voor de dienstverlening en bedrijfsvoering van Hét Service Centrum (HSC) is informatiebeveiliging een must. Wij voelen ons ervoor verantwoordelijk dat de beveiliging van informatie en informatiesystemen op orde is. Het is belangrijk dat vanuit strategisch oogpunt wordt bepaald, vastgelegd en gecommuniceerd hoe HSC informatie ontvangt, gebruikt en deelt met andere partijen en de moederorganisaties. Voor een effectieve beveiliging is het noodzakelijk dat de gegevens die aan de basis liggen van informatie, voldoen aan de gestelde eisen ten aanzien van vertrouwelijkheid, integriteit en beschikbaarheid. Effectieve beveiliging wordt bereikt door het werken met gepaste gedragsregels, in overeenstemming met de wetgeving, navolgen van vastgesteld beleid en gewenste richtlijnen uit de praktijk.
Binnen een Information Security Management Systeem (ISMS) is het informatieveiligheidsbeleid een belangrijk basisdocument. Om beveiligingsdoelstellingen, risico's en maatregelen goed te beheersen, wordt informatiebeveiliging cyclisch ingericht. HSC richt het ISMS in op basis van de NEN7510:2017. De aanpak van informatiebeveiliging is gebaseerd op risicobeheersing. De werking van het ISMS wordt in een apart document beschreven.

Visie
Wij willen dat onze partners, klanten en medewerkers kunnen beschikken over en vertrouwen op een betrouwbare en veilige informatievoorziening en de privacy afdoende wordt beschermd. Dat doen we door de bedrijfsvoering op die onderdelen veilig te stellen die met informatievoorziening te maken hebben en wettelijke verplichtingen na te komen.

Waarom informatiebeveiliging?
Informatie is één van de belangrijkste bedrijfsmiddelen van onze organisatie. Toegankelijke en betrouwbare informatie is essentieel voor onze dienstverlening en bedrijfsvoering en voor de organisaties waar wij voor werken. Het verlies van gegevens, uitval van ICT, of het door onbevoegden kennisnemen of manipuleren van bepaalde informatie kan ernstige gevolgen hebben voor de bedrijfsvoering maar ook leiden tot imago en/of financiële schade. Ernstige incidenten hebben mogelijk negatieve gevolgen voor burgers, (keten)partners en de moederorganisaties. Informatieveiligheid is daarom van groot belang. Informatiebeveiliging (IB) is het proces dat dit belang ondersteunt.

Doel

Het doel van informatiebeveiliging binnen HSC is om structureel een adequate set van maatregelen te hebben getroffen om op gepast niveau mogelijke (gevolg)schade van risico's die uit de risicoanalyses naar voren komen, te beperken.

Doelstelling

Dit informatieveiligheidsbeleid is het kader voor passende technische en organisatorische maatrelen om informatie te beschermen en te waarborgen en dat HSC voldoet aan relevante wet- en regelgeving. HSC streeft ernaar om in control te zijn en daarover op professionele wijze verantwoording af te leggen.
In control betekent in dit verband dat HSC weet welke maatregelen genomen zijn en dat er een planning is van de maatregelen die nog niet genomen zijn en als laatste dat dit geheel verankerd is in de PDCA-cyclus.

Scope

Informatiebeveiliging is meer dan ICT, computers en automatisering. Het gaat om alle uitingsvormen van informatie (analoog, digitaal, tekst, video, geluid, geheugen, kennis) en alle informatie verwerkende systemen (de programmatuur, systeemprogrammatuur, databases, hardware, bijbehorende bedrijfsmiddelen), maar vooral ook om mensen en processen.
De scope van dit beleid omvat de medewerkers van HSC en de HSC-processen van:

- Financiën
- Salarisadministratie
- Post en archivering
- Inkoop
- ICA
- en de onderliggende informatiesystemen, informatie en gegevens van HSC.

Buiten de scope vallen de primaire en ondersteunende diensten en processen, informatiesystemen en informatie en medewerkers van de moederorganisaties.

Toepassingsgebied

Het beleid voor informatieveiligheid is van toepassing op de gehele organisatie van HSC. Het beleid richt zich op alle HSC-medewerkers, tijdelijk HSC-personeel en op personeel dat door derden wordt ingezet om diensten te verlenen aan HSC. Het beleid is van toepassing op alle ontwikkelde, operationele en te ontwikkelen (HSC)-informatiesystemen, inclusief alle (HSC)-informatie die ze bevatten. En het is ook van toepassing op de gegevensuitwisseling van HSC met andere organisaties. Het beleid is niet van toepassing op de ondersteunende diensten die direct onder de moederorganisaties vallen, zoals HR, C&I, FM, deze worden meegenomen in het managementsysteem van de betreffende moederorganisatie.

Uitgangspunten

Bij de toepassing van informatiebeveilingsbeleid binnen HSC worden de volgende uitgangspunten gehanteerd:

- Door het uitbrengen van dit informatieveiligheidsbeleid geeft het MT HSC aan dat zij belang hecht aan een goed ingericht en werkend informatiebeveiligingssysteem en dat zij dit beleid van harte ondersteunt.
- HSC streeft ernaar aantoonbaar te voldoen aan de normen op het gebied van informatiebeveiliging NEN7510:2017 en aan hieruit volgende normen, op het gebied van vertrouwensbasis voor gegevensuitwisseling en logging.
  Certificering volgens NEN7510 betekent dat HSC in control is. Dit betekent geen 100% veiligheid, omdat dit een niet-werkbare situatie creëert tegen onverantwoord hoge kosten.
- Beveiliging van informatie is een onderdeel van de integrale managementverantwoordelijkheid.
- MT HSC stelt de noodzakelijke voorzieningen (mensen, materialen, middelen) voor de opzet en uitvoering van het ISMS beschikbaar.
- Samenwerking met externe partijen moet voldoen aan de door HSC gestelde eisen t.a.v. informatieveiligheid.
- Het melden van beveiligingsincidenten wordt voor zover mogelijk opgenomen in het bestaande incidentmeldingssysteem.
- Alle HSC-medewerkers, tijdelijk HSC-personeel en medewerkers van externe partijen die informatievoorzieningen van HSC gebruiken worden geïnformeerd over het algemeen geldende informatieveiligheidsbeleid.
- Verantwoordelijkheden, rollen, bevoegdheden en taken m.b.t. informatieveiligheid zijn gedefinieerd en vastgesteld.
- De kosten van de maatregelen moeten in balans zijn, zowel met de waarde van het bedrijfsmiddel als met de schade die kan ontstaan uit een incident.
- Gedrag van medewerkers en de cultuur van HSC over informatiebeveiliging vraagt permanente aandacht, daar wordt op verschillende manieren aandacht aan geschonken.

Werking, evaluatie en herziening

Het beleid treedt in werking na vaststelling door het MT HSC. Het beleid wordt minimaal eens per vijf jaar geëvalueerd en indien nodig naar aanleiding van belangrijke veiligheidsincidenten, nieuwe kwetsbaarheden of wijzigingen in de organisatorische of technische infrastructuur aangepast.

2. Definitie informatiebeveiliging

Informatiebeveiliging is het geheel van maatregelen, procedures en processen die de beschikbaarheid, integriteit en vertrouwelijkheid (exclusiviteit) van alle vormen van informatie binnen de organisatie garanderen, met als doel de continuïteit van de informatie en de informatievoorziening te waarborgen en de eventuele gevolgen van beveiligingsincidenten tot een acceptabel, vooraf bepaald niveau te beperken.

Beschikbaarheid: *de informatie moet op de gewenste momenten beschikbaar zijn.*
Integriteit: *de informatie moet juist en volledig zijn en de informatiesystemen moeten juiste en volledige informatie opslaan en verwerken.*
Vertrouwelijkheid (exclusiviteit): *de informatie moet alleen toegankelijk zijn voor degene die hiervoor bevoegd is en de informatie kan niet uitlekken.*

De definitie is conform NEN7510, norm Informatiebeveiliging voor de zorg (2017)

3. Verantwoordelijkheden en organisatie

Er is voor gekozen om op voorhand alleen de primair benodigde rollen voor het inrichten en onderhouden van het ISMS te benoemen. De overige rollen volgen uit risicoanalyses.

De manager HSC is opdrachtgever en eindverantwoordelijke voor de ontwikkeling van het ISMS, dat moet leiden tot veilig omgaan met informatie en een NEN7510-certificering. De manager HSC geeft volledige steun aan de ontwikkeling van informatiebeveiliging. De daarvoor noodzakelijke middelen en inspanningen worden beschikbaar gesteld en toegepast. Het MT HSC evalueert de ontwikkeling van het ISMS. Het MT HSC functioneert als de stuurgroep informatiebeveiliging en bewaakt de doelstellingen en uitvoering van activiteiten die betrekking hebben op de informatiebeveiliging. In het werkoverleg IB-BC (informatiebeveiliging – business continuïteit) worden o.a. risico's en de te nemen acties met betrekking tot informatieveiligheid besproken, bepaald en gemonitord. Deelnemers van het werkoverleg zijn manager HSC, controller, adviseurs informatiebeveiliging en projectleider met aandachtsgebied informatiebeveiliging en kwaliteit.

De managers dragen zorg voor een cultuur en werkomgeving waarin veilig en juist omgaan met informatie en informatiebeveiliging structureel ontwikkeld wordt. Zij dragen bij aan het benoemen van veiligheidsaspecten in en het naleven van de HSC-processen. Daarnaast zorgen zij voor een werkklimaat waarin het voor medewerkers veilig is om datalekken, incidenten en risico's te melden.

Iedere medewerker draagt er zorg voor veilig om te gaan met informatie en informatiesystemen. Medewerkers dragen bij aan informatiebeveiliging door zich ervan bewust te zijn met welke informatie zij werken, door datalekken en veiligheidsincidenten te melden en inzichtelijk te werken volgens de vastgestelde procedures, instructies en protocollen.

De adviseurs informatieveiligheid zijn aanjagers en toetsers van informatiebeveiliging en het ISMS. Zij zijn echter niet verantwoordelijk. De verantwoordelijkheid ligt bij de manager HSC. De adviseurs ondersteunen de manager HSC bij het opstellen en vaststellen van relevante beleidsdocumentatie en het implementeren van het ISMS.

In de informatiebeveiliging is een bijzondere rol weggelegd voor medewerkers in het ICT-domein. Voor nagenoeg al deze medewerkers geldt dat zij vooral beheer- en inrichtingsactiviteiten uitvoeren. Software- en systeemontwikkeling vindt nagenoeg helemaal plaats bij en door ICT-leveranciers. Daarnaast worden steeds meer ICT-activiteiten verplaatst naar de cloud. Dit houdt in dat activiteiten rondom informatiebeveiliging zich concentreren op beheertaken en op de (operationele) aansturing van leveranciers.

4. Risicomanagement en continuïteit

Risicomanagement

Beveiligen gebeurt met een duidelijk beeld voor ogen van de waarde van datgene wat beveiligd wordt. Dat betekent dat bewustzijn van waarde en van risico's van mogelijke schade, de grondslag is van dit beleid en daarmee sturend moet zijn in het nemen van maatregelen. Het is de taak van het MT HSC om ervoor te zorgen dat dit bewustzijn aanwezig is.

Om reproduceerbaar en eenduidig de waarde van informatie en informatiesystemen en gepaste beheersmaatregelen te kunnen bepalen heeft HSC een cyclisch proces voor risicomanagement ingericht. In dit proces worden de risico's geïdentificeerd, geanalyseerd en bepaald of er maatregelen genomen moeten worden. En geverifieerd of de genomen maatregelen voldoen of dat er additionele maatregelen getroffen moeten worden of dat het restrisico aanvaard wordt.

Alle informatie, informatiesystemen en informatiemiddelen hebben een eigenaar. De waarde van de informatiesystemen en informatiemiddelen worden vastgesteld door de eigenaar op basis van een uniforme methodiek voor classificatie van beveiligingsniveaus voor informatiesystemen of informatiemiddelen zie tabel 1. De waarde wordt bepaald door de schade die verlies van beschikbaarheid, integriteit en vertrouwelijkheid toebrengt aan de mogelijkheid tot het op een hoogwaardig niveau kunnen leveren van de HSC-processen.

Tabel 1. Classificatieschema voor informatiesystemen en informatiemiddelen

Classificatie	Kenmerken
Vitaal	Het uitvoeren van de bedrijfsprocessen of het tot stand komen van producten/diensten is (nagenoeg) onmogelijk zonder de inzet van het informatiesysteem / informatiemiddel. De inzet ervan is van levensbelang voor een goede uitvoering van het bedrijfsproces. Het informatiesysteem / informatiemiddel is wezenlijk voor de beheersing of besturing van de bedrijfsactiviteiten **(Onontbeerlijk voor het proces)**
Aanzienlijk	Het informatiesysteem / informatiemiddel levert een aanzienlijke bijdrage aan de activiteiten binnen het proces en/of het tot stand komen van producten / diensten. Slechts met grote, onevenredige inspanning is voortzetting van het proces mogelijk indien het informatiesysteem / informatiemiddel niet beschikbaar is. Inzet ervan heeft een positief effect op de doeltreffendheid en doelmatigheid van de organisatie. **(Groot belang voor de ondersteuning – hoge beschikbaarheidseis)**
Nuttig	Het informatiesysteem / informatiemiddel levert een belangrijke bijdrage aan de activiteiten binnen het proces en/of het tot stand komen van producten /

Classificatie	Kenmerken
	diensten. Voortzetting van het proces is mogelijk door het volgen van alternatieve procedures / activiteiten. Inzet ervan heeft een positief effect op de doeltreffendheid en doelmatigheid van de organisatie **(Belangrijke ondersteuning voor het proces)**
Support / Ondersteunend	Het informatiesysteem / informatiemiddel geeft support bij de activiteiten binnen het bedrijfsproces en is 'handig om te hebben'. **(Kan eventueel gemist worden)**

Voor informatiesystemen of informatiemiddelen geclassificeerd als ***Nuttig*** of lager geldt een basis beveiligingsniveau. Voor de informatiesystemen of informatiemiddelen geclassificeerd als ***Vitaal*** of ***Aanzienlijk*** dienen bovenop het basisbeveiligingsniveau additionele beheersmaatregelen te worden overwogen. Informatiesystemen of informatiemiddelen die de classificatie Vitaal of Aanzienlijk krijgen behoren tot de groep kritieke systemen.

Naast het classificeren van informatiesystemen en informatiemiddelen dient ook de informatie in of op deze systemen en middelen geclassificeerd te worden naar één van de drie niveaus van vertrouwelijkheid zie tabel 2.

Tabel 2. Classificatieschema voor informatie

Classificatie	Kenmerken
Openbaar	Deze informatie kent geen eisen ten aanzien van vertrouwelijkheid en integriteit en is daardoor voor **iedereen** beschikbaar en toegankelijk.
Intern	Dit betreft informatie die toegankelijk mag of moet zijn voor alle **medewerkers** van HSC. De eisen ten aanzien van vertrouwelijkheid zijn gering.
Vertrouwelijk	Dit betreft informatie die alleen toegankelijk mag zijn voor een **beperkte** groep gebruikers. De informatie wordt beschikbaar gesteld op basis van het ***need to know principe***[2]. Schending van deze classificatie kan directe of indirecte schade toebrengen aan HSC. De eisen ten aanzien van vertrouwelijkheid zijn aanzienlijk.
Zeer vertrouwelijk	Dit betreft informatie die alleen toegankelijk mag zijn voor een **nog beperktere groep** gebruikers. De informatie wordt beschikbaar gesteld op basis van het ***need to know principe***. Schending van deze classificatie kan directe of indirecte schade toebrengen aan personen en/of HSC. De eisen ten aanzien van vertrouwelijkheid zijn groot.

[2] Need to know principe houdt in dat medewerkers slechts toegang hebben tot die informatie die zij nodig hebben voor het uitoefenen van hun functie.

Continuïteit

Informatiebeveiliging heeft als doel om risico's met betrekking tot informatiebeveiligingsincidenten te reduceren tot een, door het management vastgesteld, acceptabel niveau. Ondanks goede beheersmaatregelen kan een incident zich voordoen. Voor kritieke processen / diensten en informatiesystemen is een continuïteitsplan of uitwijkplan aanwezig. Hierin is opgenomen hoe, in geval van calamiteiten, de getroffen processen / diensten en/of informatiesystemen zo snel mogelijk operationeel gemaakt kunnen worden.

5. Naleving van wet- en regelgeving

HSC dient zich te houden aan alle relevante wet- en regelgeving die van toepassing zijn op het uitvoeren van de dagelijkse werkzaamheden De relevante wet- en regelgeving is waar nodig vertaald naar richtlijnen en gedragscodes die van toepassing zijn op alle medewerkers van HSC, voor tijdelijk HSC-personeel en op personeel dat door derden wordt ingezet om diensten te verlenen aan HSC.

HSC volgt de richtlijnen met betrekking tot privacy en gedragscodes zoals die zijn opgesteld in de moederorganisatie GGD Hart voor Brabant.

Daarnaast gelden de afspraken die contractueel gelden met leveranciers waarmee HSC afspraken heeft gemaakt.

Verdere informatie en samenvattingen van de wetgeving met betrekking tot het informatieveiligheidsbeleid van HSC is te vinden in de ondersteunende richtlijnen en/of gerelateerde documenten.

Indien HSC schade ondervindt door nalatigheid bij het gebruik of het opzettelijk misbruik van informatievoorzieningen zullen de vigerende wet- en regelgeving worden toegepast en op basis daarvan maatregelen worden genomen door of namens het MT HSC.

xxx

DRAFT Risk Register Van Geloven

					Initieel Risico								
Risico ID	Generiek Risico Statement	Risico ID	Risico Statement	Risico Rationale (observaties)	I	K	R	Impact	Kans	Mitigerende maatregelen	Status beschrijving (genomen maatregelen)	Status	Restrisico
1	Niet voldoen aan basisvereisten uit de Algemene Verordening Gegevensbescherming (AVG) wat leidt tot imagoschade en financiële schade in de vorm van opgelegde boetes/sancties.	1.1	Een datalekprocedure is niet beschikbaar waardoor het correct (wettelijk) afhandelen van een datalek in het geding komt.	- Wanneer een datalek niet tijdig en juist wordt afgehandeld voldoet de verantwoordelijke niet aan de vereisten vanuit de AVG. Hiermee ontstaat het risico op imagoschade en boetes/sancties door autoriteiten en claims van getroffen betrokkenen. Zie ook risico's omtrent afspraken met leveranciers over het vastleggen van afspraken over afhandeling van datalekken wanneer deze bij de verwerker plaatsvinden cq. worden ontdekt.				De impact is hoog, doordat datalekken niet, niet juist of niet tijdig worden opgemerkt en opgevolgd. Impact op de betrokkene (bijzondere persoonsgegevens) en de organisatie in de vorm van imagoschade, fnanciële schade en bedreiging voor de continuïteit van CoronIT.	De kans dat het risico zich voordoet is hoog. Er bestaat onduidelijkheid over de werkprocessen en er bestaan nog beperkt geformaliseerde afspraken tussen partijen. Dit vergroot de kans op datalekken en daarmee de effectuering van de impact.	- Binnen het project een datalekprocedure of -protocol opstellen. - Deze procedure voorleggen aan Informatiemanager en manager bedrijfsvoering binnen GGD GHOR Nederland ten behoeve van afstemming huidige aanpak datalekken binnen GGD GHOR Nederland. - Na afstemming de procedure onderdeel laten uitmaken van de afspraken met de betrokken partijen (gebruikers CoronIT, de leveranciers).	Met Topicus is in de verwerkersovereenkomst afgestemd hoe met datalekken om moet worden gegaan. Met GGD'en is in het convenant vastgelegd hoe datalekken moeten worden gemeld. Leverancier is gecertificeerd volgens ISO 27001 en NEN-7510, waarin specificaties zijn gegeven rond logging. Binnen GGD GHOR Nederland is een datalekkenprocedure opgesteld, zodat gemelden incidenten kunnen worden afgehandeld.	Afgerond	
		1.2	Doelbinding, grondslag en daarmee de bewaartermijnen voor de persoonsgegevens in CoronIT zijn niet vastgesteld waardoor gegevens te lang of niet op de juiste wijze worden verwerkt.	- Door onduidelijkheid over het doel en daarmee de grondslag van verwerking (zie risico's onder 4), is onduidelijk welke bewaartermijnen van toepassing zijn voor de persoonsgegevens die middels CoronIT verwerkt worden. Indien verwerking plaatsvindt na aflopen van de van toepassing zijnde bewaartermijn, is de verantwoordelijke in overtreding van de AVG, met het risico op imagoschade en boetes/sancties door autoriteiten tot gevolg. - Door onduidelijkheden over bewaartermijn en doelmatigheid komt voor dat het proces langer wordt uitgevoerd dan voor het doel noodzakelijk is. Het einde van het project, of in ieder geval een beschrijving hoe lang de dataverzameling door zal lopen en voor welke doelen, is noodzakelijk. Gebeurt dit niet, dan is het voor de betrokkene niet duidelijk hoelang het project loopt en de dataverzameling zal voortduren. Ook vereist de AVG een vooraf welbepaald duidelijk doel en dit impliceert dat duidelijk is hoelang een gegevensverwerking loopt.				De impact is midden. Effectueren van het risico betekent non-compliance met de AVG, met imagoschade, boetes/financiële schade tot gevolg. De risico's voor de betrokkene zijn in deze gemiddeld, het betreft veelal medewerkers die toegang dienen te hebben tot de gegevens, enkel niet na de verstreken doelmatigheid.	Kans dat het risico zich voordoet is hoog. De onduidelijkheid bestaat gedurende de ontwikkeling van CoronIT, (geautomatiseerde) regels voor retentie van gegevens worden niet of niet juist geïmplementeerd. Werkprocessen dienen voorzien te worden van de juiste richtlijnen, die nog niet geformaliseerd zijn.	- Binnen het project bepalen en vaststellen welk doel CoronIT dient, enkel als registratie- en ondersteuningssysteem om op snelle wijze op grote schaal testen te bewerkstellingen, of daarnaast ook als medisch dossier op basis waarvan behandelingen zullen worden geregistreerd? Afhankelijk van het doel is de grondslag en de bewaartermijn respectievelijk Wet publieke gezondheid (5 jaar) en WGBO (20 jaar). Gelet op het feit dat GGD GHOR en GGD'en deze taak po basis van Wet publieke gezondheid uitvoeren is er dan geen ruimte om CoronIT als medisch dossier te gebruiken. - Het doel, grondslagen en bewaartermijnen duidelijk communiceren naar alle partijen die toegangs- en invoerrechten hebben in CoronIT, dit opnemen in de gebruiksvoorwaarden van CoronIT, gedragscodes en werkprocessen, in de afspraken met de betrokken partijen (GGD'en, leverancier, overige gebruikers CoronIT) en in de privacyverklaring voor de betrokkenen. - CoronIT conform het doel inrichten (geen open velden voor bijvoorbeeld de behandeling, bewaartermijnen by default inzetten, autorisaties inrichten, etc).	Doel van de applicatie is registreren van geteste personen en uitslagen. Grondslagen en bewaartermijnen zijn bepaald in de Wet publieke gezondheid en vastgelegd in de DPIA en overeenkomsten. Het doel van de applicatie is vastgelegd in het convenant met de GGD en in de gebruiksvoorwaarden voor de andere gebruikers. Naar aanleiding van dit doel is de grondslag en de bewaartermijn bepaald. Bij het inrichten van de applicatie is daarnaast rekening gehouden met de Wet publieke gezondheid. Daarnaast zijn ook autorisaties ingericht op basis van rollen.	Afgerond	Maatregelen om te zorgen dat de bewaartermijn niet wordt overschreden, worden nog ingericht.
		1.3	Voor betrokkene is het onduidelijk waar rechten kunnen worden uitgeoefend doordat de verantwoordelijke niet voldoet aan de informatieplicht uit de AVG.	- Doordat de doelen en daardoor de grondslagen en de bewaartermijnen niet welbepaald zijn en de verantwoordelijkheden nog niet geformaliseerd zijn (zie risico's onder 1 en 4) is de privacyverklaring niet volledig of onjuist. Hierdoor wordt de betrokkene onjuist en onvolledig geïnformeerd waardoor niet voldaan wordt aan de vereiste vanuit de AVG en de betrokkene haar rechten niet kan uitvoeren.				De impact is midden. Effectueren van het risico betekent non-compliance met de AVG, met imagoschade, boetes/financiële schade tot gevolg. De risico's voor de betrokkene zijn in deze gemiddeld, het is geen directe inbreuk op de persoonsgegevens. Wel op de rechten die een betrokken moet kunnen uitvoeren.	De kans dat het risico zich voordoet is hoog. Er bestaat onduidelijkheid over de werkprocessen en er bestaan nog beperkt geformaliseerde afspraken tussen partijen. Hierdoor is het nog niet mogelijk geweest de privacyverklaring eenduidig af te ronden.	- Het doel, grondslagen en bewaartermijnen duidelijk communiceren naar alle partijen die toegangs- en invoerrechten hebben in CoronIT, dit opnemen in de gebruiksvoorwaarden van CoronIT, gedragscodes en werkprocessen, in de afspraken met de betrokken partijen (GGD'en, leverancier, overige gebruikers CoronIT) en in de privacyverklaring voor de betrokkenen. - In de werkprocessen en werkafspraken tussen de betrokken partijen de aanpak van en de verantwoordelijkheden rondom een dergelijk verzoek opnemen en met elkaar afstemmen.	In het convenant is bepaald dat de GGD'en zelf uitvoering moeten geven aan de rechten van de betrokkenen. In de gebruiksvoorwaarden is geregeld dat de gebruiker verantwoordelijk is om gehoor te geven aan de rechten van de betrokkenen, aangezien ze zelf verantwoordelijk zijn voor de verwerking. voor de rechten waar geen uitvoering aan kan worden gegeven door de gebruiker, is de gebruiker via de gemaakte apspraken (covenant, gebruiksvoorwaarden en communicatie met de partijen) op de hoogte gebracht over waar zij een verzoek kunnen indienen.	Afgerond	
2	Maatregelen voor informatiebeveiliging zijn onvoldoende ingericht wat leidt tot datalekken, imagoschade en financiële schade in de vorm van opgelegde boetes/sancties en claims van betrokkenen.	2.1	Beschikbaarheid, integriteit en vertrouwelijkheid van verzamelde (persoons)gegevens zijn in het geding door gebrekkige validatie van technische inrichting van vereiste beveiligingsaspecten.	- Door onvoldoende inzicht in de technische inrichting van CoronIT is onduidelijk op welke wijze beveiligingsmaatregelen zijn geïmplementeerd en of deze de technische bedreigingen voldoende mitigeren. Naast bedreigingen voor de correcte werking van de applicatie, zijn mogelijk technische kwetsbaarheden aanwezig, die door kwaadwillende geëxploiteerd kunnen worden. Effectuering van het risico leidt tot verminderde beschikbaarheid van de applicatie, inbreuk op vertrouwelijkheid van de (persoons)gegevens die verwerkt wordt en/of verminderde integriteit (juistheid/volledigheid) van de (persoons)gegevens.				De impact is hoog. Het project is onder hoge tijdsdruk uitgevoerd waarbij beperkt inzicht is voor de projectgroep in de technische inrichting. Indien zich kwetsbaarheden in de applicatie bevinden, die zich openbaren (zij het in processen of door invloed van buitenaf) heeft dit een directe impact op de beschikbaarheid, integriteit en vertrouwelijkheid van CoronIT en de gegevensverwerking.	De kans dat het risico zich voordoet is hoog. Er gaat gewerkt worden met een applicatie waarvan de technische inricht beperkt is gevalideerd. Door de betrokkenheid van veel verschillende partijen alsmede de gevoeligheid van het onderwerp (trekt aandacht), is de kans groot dat eventuele kwetsbaarheden aan het licht komen en een weg naar de publiciteit vinden.	- Het (laten) uitvoeren van een technische securitytest (penetratietest) om kwetsbaarheden in de beveiliging te testen en waar nodig tijdig te kunnen herstellen. - Het (laten) uitvoeren van een beeoordeling van de applicatie (pre-implementatiereview) op techniek, code en werking van gewenste beheersmaatregelen in de processen. - In de verwerkersovereenkomst met Topicus dienen de volgende zaken te worden opgenomen: • Voldoen aan NEN7510 (in bijzonder 7512/7513), of indien op korte termijn niet haalbaar ISO27001; • Periodiek uitvoeren van technische security testen • Behoud van Right to Audit voor verwerkingsverantwoordelijke om periodiek de applicatie te (laten) beoordelen op vertrouwelijkheid, integriteit en beschikbaarheid.	Een Security Assessment wordt uitgevoerd door FOX-IT. Deze is gestart op 6 mei en duurt 10 dagen. Indien nodig, zal deze test worden uitgebreid tot de labkoppeling, maar initieel is gekozen om deze test te beperken tot de webapplicatie. Deze test houdt een pentest en applicatietest in. Topicus is ISO 27001 gecertificeerd en is bezig met het invoeren van de eisen van de NEN-7510. In de verwerkersovereenkomst is gesteld dat ze werken conform NEN-7512 en NEN-7513. In de verwerkersovereenkomst is opgenomen dat GGD GHOR het right to audit heeft en dat Topicus periodiek security testen zal uitvoeren. De frequentie daarvan moet nog worden bepaald. Ten slotte is de applicatie voor livegang uitvoering getest door een aantal GGD'en om te controleren of het systeem naar behoren werkt. 28092020: Topicus heeft documenten in laten zien en beide certificatie voorgelegd van NEN7510 en ISO27001. Daarnaast is technische documentatie getoond.	Afgerond	
		2.2	De getroffen technische maatregelen voor bescherming van persoonsgegevens zijn niet passend voor de bescherming van bijzondere persoonsgegevens en bij het doel van de verwerking met mogelijke datalekken met ernstige gevolgen voor de betrokkene tot gevolg.	- In het ontwikkelproces van CoronIT zijn keuzes gemaakt voor technische beveiligingsmaatregelen die mogelijk niet passend zijn (geen Privacy by Design) voor de bescherming van de bijzondere persoonsgegevens die verwerkt worden. Dit leidt tot datalekken met een ernstige impact op de levenssfeer van de betrokkene en tot sancties/boetes en daarmee financiële schade voor de verantwoordelijke. - Indien de AP het proces aan een onderzoek onderwerpt, leidt dit tot vertraging in het proces, financiële implicaties voor de verantwoordelijke en een bedreiging van continuïteit van gebruik van CoronIT.				De impact is hoog. Het project is onder hoge tijdsdruk uitgevoerd waarbij beperkt inzicht is voor de projectgroep in de technische inrichting. Indien zich kwetsbaarheden in de applicatie bevinden, die zich openbaren (zij het in processen of door invloed van buitenaf) heeft dit een directe impact op de beschikbaarheid, integriteit en vertrouwelijkheid van CoronIT en de gegevensverwerking.	De kans dat het risico zich voordoet is hoog. Er gaat gewerkt worden met een applicatie waarvan de technische inricht beperkt is gevalideerd. Door de betrokkenheid van veel verschillende partijen alsmede de gevoeligheid van het onderwerp (trekt aandacht), is de kans groot dat eventuele kwetsbaarheden aan het licht komen en een weg naar de publiciteit vinden.	- Het (laten) uitvoeren van een technische securitytest (penetratietest) om kwetsbaarheden in de beveiliging te testen en waar nodig tijdig te kunnen herstellen. Advies is om in het weekend van 25 april een securitytest uit te (laten) voeren en na opvolging van eventuele bevindingen een nieuwe test om opvolging te toetsen. Daarnaast adviseren we om tenminste testen uit te voeren om de beschikbaarheid en functionaliteit van de applicatie te beoordelen. Uitgebreide testen dienen ook na livegang plaats te vinden. - In de verwerkersovereenkomst met Topicus dienen de volgende zaken te worden opgenomen: • Voldoen aan NEN7510 (in bijzonder 7512/7513), of indien op korte termijn niet haalbaar ISO27001; • Periodiek uitvoeren van technische security testen • Behoud van Right to Audit voor verwerkingsverantwoordelijke om periodiek de applicatie te (laten) beoordelen op vertrouwelijkheid, integriteit en beschikbaarheid.	Een Security Assessment wordt uitgevoerd door FOX-IT. Deze is gestart op 6 mei en duurt 10 dagen. Indien nodig, zal deze test worden uitgebreid tot de labkoppeling, maar initieel is gekozen om deze test te beperken tot de webapplicatie. Deze test houdt een pentest en applicatietest in. Topicus is ISO 27001 gecertificeerd en is bezig met het invoeren van de eisen van de NEN-7510. In de verwerkersovereenkomst is gesteld dat ze werken conform NEN-7512 en NEN-7513. In de verwerkersovereenkomst is opgenomen dat GGD GHOR het right to audit heeft en dat Topicus periodiek security testen uitvoert. ten slotte is een privacyspecialist/FG ingehuurd voor het project. Voor belangrijke beslissingen wordt advies gevraagd. Verder worden de risico's in the go genoteerd en wordt on the go een DPIA uitgevoerd. Indien een zwakheid wordt geconstateerd of een inbreukop de wetgeving/niet optimale situatie in de verwerking wordt geconstateerd, adviseert de privacyspecialist?FG hierover aan de projectleider, zodat dit kan worden opgepakt.	Afgerond	
		2.3	Vertrouwelijkheid en integriteit van de persoonsgegevens zijn in het geding door onvoldoende maatregelen voor authenticatie.	- Multi-factor authenticatie (MFA) is in CoronIT momenteel enkel van toepassing bij het opstarten van de applicatie. Daarna zal enkel de gebruikersnaam/wachtwoordcombinatie gebruiktworden om opnieuw in te loggen. De AP stelt dat voor gezondheidsinformatiesystemen waarin gegevens over de gezondheid worden verwerkt, altijd sprake dient te zijn van MFA bij het aanloggen in een applicatie. Dit is bij CoronIT niet het geval en zijn de getroffen maatregelen daarom niet passend met datalekken en financiële schade tot gevolg. - De snelheid waarmee ingelogd dient te worden door de gebruikers is het argument om te zoeken naar praktische toepassing van MFA. Deze gebruikers werken in omstandigheden (bijv.: beschermende kleding), die een gebruiksvriendelijke toepassing van MFA belemmeren. MFA is daarmee als aandachtspunt voor fase 2 opgenomen. - Het is voor de projectgroep onbekend op welke wijze een time-out van de sessie wordt ingericht om te voorkomen dat een sessie langer open blijft staan dan noodzakelijk voor de specifieke verwerking met in de tussentijd de mogelijkheid voor onrechtmatige inzage.				De impact van het risico is hoog. De impact van effectuering is inzage door onbevoegden in de gegevens. Dit is een impact op de levenssfeer van de betrokkene en leidt voor de betrokken organisaties tot datalekken, imagoschade en boetes/financiële schade.	De kans van het risico is hoog. Door de combinatie van geen time out van de sessie en beperkte authenticatie is de kans groot dat onbevoegden toegang krijgen tot gegevens. Schermen blijven te lang open staan en het is eenvoudiger om inloggegevens te achterhalen indien geen MFA gebruikt wordt. Het betreft een webapplicatie die voor kwaadwillende te identificeren is. Zonder MFA kunnen kwetsbaarheden in het inlogproces (of door social engineering) misbruikt worden.	- Toepasssen van MFA oplossingen voor het inloggen in CoronIT. Indien er praktische bezwaren gelden waardoor een traditioneel token niet werkt, kunnen alternatieven toegepast worden, zoals gebruik van een pasje of een certficaat op het apparaat waar mee wordt gewerkt.	Elke keer als wordt ingelogd, moet dit via mulitfactor authenticatie. Daarnaast vergendeld de applicatie zich autmatisch na 30 minuten. De tweede factor die wordt gebruikt voor MFA, is een authenticator applicatie.	Afgerond	

		2.4	Beschikbaarheid en vertrouwelijkheid van persoonsgegevens is in het geding door onvoldoende borging van maatregelen voor back-up en restore.	- Het is voor de projectgroep onbekend of de back-ups van CoronIT alleen lokaal worden bewaard of (ook) op een externe locatie, of back-ups fysiek of digitaal worden opgeslagen, hoe lang de gemaakte back-ups worden bewaard en tot op welk detailniveau de back-ups te restoren zijn. Daarnaast is het onbekend wat de leverancier verstaat onder het periodiek uitvoeren van restoretesten of in de 2 datacenters de data realtime wordt gerepliceerd en welke beveiligingsmaatregelen hierbij zijn getroffen voor het borgen van de vertrouwelijkheid van gegevens in opslag en transport. Het tijdig of in zijn geheel niet meer beschikbaar hebben van persoonsgegevens is een datalek op basis van de bepalingen in de AVG.				De impact van het risico is hoog. Indien de maatregelen die getroffen zijn niet effectief zijn dan gaan gegevens verloren. Dit zorgt voor imagoschade en mogelijk boetes door het datalek, maar heeft geen directe impact op de vertrouwelijkheid. De vetrouwelijkheid is in het geding door onvoldoende treffen van maatregelen voor beveiliging van backup, hierover is onvoldoende bekend.	De kans is midden. In de verkregen documentatie staat beschreven dat er maatregelen getroffen zijn voor back-up en restore. Het is onbekend op welke wijze deze zijn getroffen en door de hoge tijdsdruk is het mogelijk dat een aspect als vertrouwelijkheid over het hoofd is gezien.	- in de technische documentatie dient verantwoord te worden op welke wijze back-up en restore wordt uitgevoerd en welke maatregelen voor beschikbaar, vertrouwelijkheid en integriteit van de gegevensverwerking hierbij in acht worden genomen (gegevens en opslag/transport). - back-up en restore is onderdeel van de gevraagde informatiebeveiligingsstandaarden waaraan Topicus zich dient te comformeren op basis van de afspraken in de verwerkersovereenkomst.	Er worden back-ups gemaakt.	Openstaand	Het is niet bekend hoe deze back-ups worden gemaakt, hoe vaak ze worden gerefresht en hoe ze zijn beveiligd. Dit onderdeel wordt uitgevraagd bij topicus.
		2.5	Vertrouwelijkheid en integriteit van persoonsgegevens is in het geding door onvoldoende borging van maatregelen voor logging en monitoring.	- Het is voor de projectgroep onbekend op welke wijze logging in CoronIT wordt toegepast (wat wordt er gelogd, wie heeft er toegang tot de log en op welke wijze wordt de log beveiligd). Daarnaast zijn afspraken over de evaluatie/monitoring van logging niet vastgelegd/beschikbaar. Hierdoor ontstaan risico's voor de vertrouwelijkheid van persooonsgegevens. In combinatie met risico's ten aanzien van autorisatiebeheer en authenticatie is logging cruciaal om detectief afwijkingen (van de gewenste situatie) te kunnen vaststellen en vervolgacties te bepalen. Logging dient als controlemiddel om vast te stellen of inzage in persoonsgegevens rechtmatig is geschied.				De impact is midden. Logging is een controlemiddel voor detectie van ongeautoriseerde handelingen. De impact is dat dergelijke handelingen niet, of niet tijdig worden geïdentificeerd waardoor passende maatregelen niet (tijdig) kunnen worden doorgevoerd.	De kans is midden. In de verkregen documentatie staat beschreven dat er maatregelen getroffen zijn voor logging en monitoring. Het is voor de projectgroep onbekend welke maatregelen het zijn, wie ze beheerd en op welke manier ze bijdragen aan de vertrouwelijkheid van de gegevensverwerking.	- Voor CoronIT dient bepaald te worden welke handelingen in de applicatie kritisch zijn, hoe en of deze gelogd worden en op welke wijze deze logging proactief wordt geevalueerd. Waar mogelijk dient ook signalering toegepast te worden in het geval van een handeling die een bepaalde regel triggert - de logging dient conform Privacy by Design te worden ingericht (logging bevat geen live gegevens) en opgeslagen te worden met in achtname van maatregelen voor vertrouwelijkheid. - met GGD'en moet worden vastgelegd wie de loggingcontrole uitvoert.	Op het systeem wordt logging toegepast. Hierin worden twee zaken gelogd. Ten eerste de breaking-the-glass pogingen, waarin wordt vermeld waarom het dossier in wordt gezien. Ten tweede is logging aangezet op toegang tot het systeem en kan worden gezien wanneer een gebruiker inlogt, welke dossiers een gebruiker opent, of de gebruiker iets in het dossier muteert. Voor controle op de logging wordt een plan opgezet om de logging te controleren. GGD'en hebben geen toegang tot logging. Zij zijn geïnformeerd dat zij met verzoeken contact op moeten nemen met de servicedesk. Deze handelswijze is in lijn met de procedure voor andere applicaties waar GGD GHOR NEderland het functioneel beheer over heeft.	Openstaand	Controle van de logging moet worden geautomatiseerd
		2.6	De integriteit van persoonsgegevens is in het geding door onvoldoende borging van maatregelen voor juistheid van gegegevensinvoer en gegevensvalidatie in CoronIT.	- Vanuit het functioneel ontwerp wordt niet helder welke checks en controles in de applicatie worden uitgevoerd op de juistheid van de informatie (in FO enkele openstaande vragen over invoervalidatie). Indien dergelijke (applicatieve) controles niet worden uitgevoerd (bijv.: controle op juistheid BSN nummer), is de integriteit van de gegevensverwerking niet geborgd.				De impact is hoog. Indien er foutieve invoer plaatsvindt, dan heeft dat een directe impact op de integriteit van de testresultaten. Hierbij kunnen zowelgegevens over de resultaten zelf als de geteste betrokken foutief zijn. Dit heeft een impact op de betrouwbaarheid van de gehele gegevensverwerking met datalekken en een impact op de levenssfeer van de betrokkene als gevolg.	De kans is midden. In het FO staat beperkt vermeld welke invoercontroles zijn ingericht. De kans is aanwezig dat onvoldoende onderzocht is op welke wijze invoercontroles fouten in de processen kunnen ondervangen.	- onderzoek welke velden kritisch zijn bij het opvoeren van gegevens en onderzoek mogelijkheden voor borgen van integriteit van gegevens in die velden	In de applicatie kan enkel met twee velden worden ingevoerd en vervolgens de persoon worden opgeveord. Dit betekent dat telkens twee velden moeten worden ingevoerd om iemand op te halen, wat een waaarborg biedt voor de juistheid van de opgehaalde gegevens.	Afgerond	
		2.7	Beschikbaarheid, integriteit en vertrouwelijkheid van verzamelde (persoons)gegevens zijn in het geding door vastgestelde kwetsbaarheden in CoronIT en gekoppelde systemen.	Fox-IT heeft een Security Assessment uitgevoerd en hieruit zijn 15 bevindingen gekomen, namelijk: 1 Remote Code Execution via Server Side Template Injection 2 SOAP API kan uitgevoerd worden door gebruikers zonder autorisatie 3 Beheer API kan uitgevoerd worden door gebruikers zonder beheer privileges 4 Persistente Cross-Site Scripting (XSS) 5 Geen validatie bij het uploaden van bestanden bij correspondenties 6 DOM based reflected Cross-Site Scripting (XSS) 7 Wachtwoorden plain-tekst in website broncode 8 HTTP Content-Security-Policy response header ontbreekt 9 Verouderde JavaScript libraries 10 Applicatie geeft debug-informatie vrij 11 Webservers geven versienummers vrij 12 Webserver geeft intern IP-adres vrij 13 Web server staat toegang tot configuratiebestanden toe 14 Gebruik van externe scripts zonder subresource integriteit checks 15 HTTP Strict Transport Security ontbreekt Deze resultaten zijn voortgekomen uit een test op de applicatie, maar nog niet alles is gescand. Daarnaast zijn de koppelingen in de eerste test niet meegenomen omdat het gezien de tijdsdruk belangrijk was om te weten of de applicatie zelf op orde is. Fox-IT heeft een tweede Security Assessment uitgevoerd op CoronIT, waarbij de applicatie verder is getest. Deze test bestond uit een interne pentest en een webappicatie test. Hieruit zijn de volgende resultaten gekomen. 1 Ongeautoriseerde toegang tot NFS shares 2 Redis server zonder authenticatie 3 Redis server kwetsbaar voor Remote Code Execution kwetsbaarheid				De impact is hoog. De applicatie (en het portaal) zullen breed bekend worden en daarmee ook een mikpunt voor hackers. In de applicatie worden gevoelige persoonsgegevens verwerkt, zoals BSN en medische gegevens. Als deze uitlekken, is sprake van een datalek, en daarnaast imagoschade. Dit heeft tevens financiële gevolgen.	De kans dat het risico zich voordoet is groot. Door de aandacht die aan de allpicatie zal worden gegeven, zal dit interessant zijn voor kwaadwillenden. De gevonden (en potentiële) kwetsbaarheden zorgen ervoor dat kwaadwillenden zich toegang kunnen verschaffen tot (delen van) het systeem en/of (delen van) de data die in het systeem worden verwerkt.	Maak een schema waarin wordt gesteld welke kwetsbaarheid wanneer wordt gemitigeerd, waarbij wordt gezorgd dat de meest kritieke kwetsbaarheden het snelst worden opgelost, wanneer dit gebeurt en hoe de kwetsbaarheden worden opgelost. Daarbij is het van belang dat de bevindingen die een kritiek en hoog risico hebben eerst worden opgelost. Dit schema moet worden gedeeld met de opdrachtgever, zodat zij weten wat Topicus zal doen en Topicus moet de opdrachtgever op de hoogte houden van de stand van zaken van dit schema. Voor de niet geteste onderdelen waar persoonsgegevens in worden gewerkt, wordt geadviseerd een security assessment uit te laten voeren, zodat alle delen van het systeem worden doorgelicht en zo alle kwetsbaarheden duidelijk zijn. Voer een hertest uit als de kwetsbaarheden zijn opgelost, zodat kan worden onderzocht of de risico's nog bestaan.	Topicus heeft de eerste risico´s reeds verholpen. Daarvoor hebben zij intern een prioritering opgesteld. Fox-IT heeft de opdracht gekregen van GGD GHOR Nederland om verder te testen op de koppelingen, zodat duidelijk is waar nog kwetsbaarheden worden gevonden. Met Fox-IT is afgesproken dat, als alles getest is en de kwetsbaarheden zijn verholpen, de onderdelen opnieuw zullen worden getest omte controleren of de kwetsbaarheden weg zijn.	Openstaand	Het testproces is nog bezig. Daarom is nog niet duidelijk welke kwetsbaarheden er exact zijn. De bekende kwestbaarheden worden volgens een schema verholpen door Topicus. Dit schema is bekend.
		2.8	Beschikbaarheid, integriteit en vertrouwelijkheid van verzamelde (persoons)gegevens zijn in het geding door continue ontwikkelingen in het systeem, waardoor nieuwe kwetsbaarheden ontstaan die niet zijn ontdekt in eerder uitgevoerde testen.	CoronIT wordt nog steeds verder ontwikkeld door Topicus, wat betekent dat er wijzigingen in de applicatie en de code worden aangebracht die niet mee worden getest door Fox-IT (of een andere derde partij). Dit betekent dat kwetsbaarheden in deze ontwikkelingen over het hoofd worden gezien, of nieuwe kwetsbaarheden ontstaan op delen die wel getest zijn en waar veranderingen in de applicatie ontstaan.				De impact is hoog. Omdat in de webapplicatie gevoelige gegevens worden verwerkt, heeft het uitlekken hiervan grote gevolgen voor de betrokkenen van wie de gegevens worden gelekt. Daarnaast leidt dit tot imagoschade en financiële schade.	De kans dat het risico zich voordoet is midden. Het systeem is al eens getest en er worden geen grote wijzigingen doorgevoerd. Daarnaast test Topicus de webapplicatie en wordt deze getest door de GGD'en. Dit biedt echter geen garantie dat alle kwetsbaarheden worden vastgesteld.	Wijzigingen in het systeem moeten, zeker als dit grote wijzigingen betreft, worden getest door Topicus. Hierbij moet rekening worden gehouden dat moet worden getest of er kwetsbaarheden zijn ontstaan door de wijzigingen in de applicatie. De wijzigingen die na het testen door Fox-IT zijn gebeurd, moeten worden vastgelegd, zodat duidelijk is waar de applicatie nog moet worden getest als deze is opgeleverd.	Topicus test wijzigingen in het systeem om na te gaan of het goed werkt en het niet zorgt voor kwetsbaarheden. Deze testen worden echter niet tot in detail uitgevoerd. Fox-IT wordt ingeschakeld om het gehele systeem grondig te testen. Telkens als een deel is getest, worden de resultaten daarvan besproken met de partijen.	Openstaand	De applicatie is nog een tijd in ontwikkeling. Testen worden uitgevoerd, maar de ontwikkeling houdt in dat kwetsbaarheden kunnen ontstaan.
		2.9	Vertrouwelijkheid van persoonsgegevens is in het geding door de mogelijkheid tot inzien en printen van het afsprakenoverzicht.	Binnen CoronIT is het afsprakenoverzicht voor diverse functies inzichtelijk en te printen. De noodzaak tot inzage is divers. Dit kan zijn om inzicht te hebben in het feit of iemand al een afspraak heeft, maar geldt voornamelijk om op locatie te kunnen kijken in het overzicht en iemand te kunnen testen. Het printen is aangezet om een noodlijst te hebben. Als de systemen uitvallen, kan in dit geval worden doorgegaan met testen.				De impact is hoog.De print van het afsprakenoverzicht bevat gegevens als BSN. Indien dit onrechtmatig wordt verwerkt, leidt dit tot fraude, imagoschade en financiële schade.	De kans is midden. De printfunctie is ingericht en enkel daarbij is het BSN inzichtelijk. De mogelijkheid tot printen is geen instructie. Het is daarom niet ver verspreid dat er een mogelijkheid is tot printen. Daarom is de kans midden dat iemand toch een print maakt, vooral aangezien het niet wijd gecommuniceerd is dat BSN wel te zien is in de print.	Zet de printfunctie enkel open voor bepaalde rollen die de prints moeten kunnen draaien. Maak het afsprakenoverzicht enkel toegankelijk voor de rollen die hier toegang tot moeten hebben. Zorg voor logging op het afsprakenoverzicht en het printen en voor hier periodieke controle op uit.	Inzage van het afsprakenoverzicht wordt gelogd. Na datalek januari is de printfunctie uitgezet.	Openstaand	

DRAFT Risk Register Van Geloven

3	Afspraken omtrent het beheer van CoronIT zijn onduidelijk en/of niet geformaliseerd wat leidt tot datalekken, imagoschade en financiële schade in de vorm van opgelegde boetes/sancties en kosten voor herstelwerkzaamheden.	3.1	Beschikbaarheid, integriteit en vertrouwelijkheid van verzamelde (persoons)gegevens zijn in het geding door onduidelijke en niet-geformaliseerde afspraken rondom het beheer van CoronIT.	- Rondom het beheer van de applicatie bestaat onduidelijkheid welke taken/verantwoordelijkheden belegd zijn of dienen te worden. Onder de beheeromgeving wordt (onder meer) verstaan het beheren van toegang tot de applicatie, de rechten binnen de applicatie, functionele/technische wijzigingen aan de applicatie en beheer in het kader van beschikbaarheidsborging (back-up, monitoring). Indien deze beheertaken niet eenduidig zijn vastgesteld en belegd, ontstaat onduidelijkheid over het dagelijks beheer van de applicatie waardoor autorisaties niet (juist) worden ingericht, wijzigingen met een negatieve impact op de applicatie worden doorgevoerd of eventuele incidenten (bijv.: ongeautoriseerde inzage) niet juist of tijdig worden opgemerkt en/of opgevolgd.				De impact is hoog. De aspecten toegangs/autorisatie/wijzigingenbeheer zijn cruciaal voor een betrouwbare gegevensverwerking. Indien het beheer niet juist wordt uitgevoerd heeft dat datalekken tot gevolg en wordt niet voldaan aan het treffen van passende maatregelen voor bescherming van gegevens. Datalekken, imagoschade en financiele schade zijn de gevolgen.	De kans dat het risico zich voordoet is hoog. Er bestaat onduidelijkheid over beheer van de applicatie en de tijdsdruk waarmee de applicatie is ontwikkeld is hoog. Hierdoor is vaak onvoldoende oog voor het beheer na de ontwikkelfase.	- Formaliseer de afspraken rondom beheer van de applicatie, waar taken en verantwoordelijkheden worden beschreven voor technisch en functioneel beheer.	Topicus heeft het technisch beheer, GGD GHOR Nederland het functioneel beheer. Daarnaast zijn taken met betrekking tot het beheer vastgelegd in de overeenkomsten die zijn gesloten en wordt gecommuniceerd over hoe en wie de beheertaken uitvoert. Ook zijn een aantal van deze zaken, zoals hoe met datalekken en rechten van betrokkenen moet worden omgegaan, al vastlegegd.	Afgerond	
		3.2	Vertrouwelijkheid van persoonsgegevens is in het geding door onvoldoende borging van maatregelen voor autorisatiebeheer.	- Het is onduidelijk op welke wijze gebruikers van CoronIT toegang krijgen tot de applicatie en welke autorisaties daarbij van toepassing kunnen zijn. Hierdoor worden autorisaties te breed toegekend, met verlies van vertrouwelijkheid tot gevolg. Op basis van de AVG betreft een onrechtmatige inzage een datalek. Door ineffectief autorisatiebeheer worden autorisaties niet tijdig gewijzigd of ingetrokken waardoor gebruikers langer inzage hebben in de gegevens dan toegestaan. - Indien een gebruiker reeds over een account beschikt op een andere door Topicus geleverde applicatie, is het niet mogelijk om een account aan te maken voor CoronIT op basis van hetzelfde e-mailadres. Dit zorgt voor praktische problemen bij de reset van het wachtwoord of de vraag om een ander mailadres te gebruiken. Het is de verantwoordelijke niet toegestaan op basis van AVG om het privémailadres te verwerken, hiervoor is geen grondslag. Daarnaast is het gebruik van e-mail buiten de omgeving van de gebruikende organisatie onveilig met mogelijke datalekken tot gevolg.				De impact is hoog. De aspecten toegangs/autorisatie/wijzigingenbeheer zijn cruciaal voor een betrouwbare gegevensverwerking. Indien het beheer niet juist wordt uitgevoerd heeft dat datalekken tot gevolg en wordt niet voldaan aan het treffen van passende maatregelen voor bescherming van gegevens. Datalekken, imagoschade en financiele schade zijn de gevolgen.	De kans dat het risico zich voordoet is hoog. Er bestaat onduidelijkheid over beheer van de applicatie en de tijdsdruk waarmee de applicatie is ontwikkeld is hoog. Hierdoor is vaak onvoldoende oog voor het beheer na de ontwikkelfase. De kans wordt vergroot door technische beperkingen zoals beschreven in de observaties.	- Formaliseer de afspraken rondom beheer van de applicatie, waar taken en verantwoordelijkheden worden beschreven voor technisch en functioneel beheer in het bijzonder rondom toegangsbeheer.	Rollen zijn door GGD GHOR Nederland vormgegeven. Autorisaties worden bepaald door GGD'en en ingericht door GGD GHOR Nederland. GGD GHOR bepaald wat je in een bepaalde rol kan, maar wie die krijgt is voorbehouden aan de GGD. De centrale servicedesk richt het in voor de GGD'en. Servicedeskmedewerkers kunnen rollen en rechten aanpassen, maar veranderingen aanbrengen in de autorisaitesschema's kan alleen worden gedaan door een zeer beperkte groep mensen bij GGD GHOR Nederland. Dat zijn op dit moment twee medewerkers. Alle wijzigingen worden vastgelegd in Topdesk, zodat achteraf kan worden achterhaald wie de opdracht heeft gegeven en wie de wijzigingen heeft doorgevoerd. De rollen zullen periodiek worden herzien. GGD'en zijn verantwoordelijk om de autorisaties die zijn gegeven te blijven controleren.	Afgerond	
		3.3	Beschikbaarheid van persoonsgegegens is niet volledig ingericht, waardoor GGD GHOR Nederland geen volledige toegang heeft tot haar gegevens.	Tableau wordt tijdelijk gebruikt voor het opstellen van rapportages. GGD GHOR Nederland heeft als afgevaardigde van de GGD'en om hun taken deels uit te voeren, noodzaak om bij de data te kunnen als hier een noodzaak toe is. Topicus geeft echter aan dat GGD GHOR Nederland op basis van verzoeken informatie kan ontvangen. Dit betekent dat op dit moment niet vrij kan worden gewerkt in de rapportageomgeving en niet direct een nieuwe rapportage kan worden gedraaid/een volledig beeld bestaat over de beschikbare data.				De impact is laag. Het niet tijdig ontvangen van een rapportage betekent dat gegevens, waaronder stuurdata, iets later worden aangeleverd. Hierdoor kan stuurinformatie iets later komen.	De kans dat dit voorkomt is midden. Rapportages kunnen wijzigen en GGD'en kunnen wensen hebben om hun data inzichtelijk te hebben, zodat ze zelf ook analyses kunnen maken die helpen bij het nemen van beslissingen.	De data van GGD'en moeten direct toegankelijk worden gemaakt voor GGD'en (en GGD GHOR Nederland als deze in opdracht van de GGD'en iets moet uitvoeren). Tableau is een tijdelijk oplossing. In de nieuwe oplossing is directe toegang tot gegevens noodzakelijk, voor GGD GHOR Nederland op landelijk niveau voor rapportages aan het RIVM, voor GGD'en op het nivrau van de regio waar zij verantwoordelijk voor zijn.		Openstaand	Tableau is een tijdelijke oplossing.
		3.4	Vertrouwelijkheid en integriteit van persoonsgegevens is in het geding door vermenging van rechten van verschillende systemen die worden gehost op hetzelfde platform.	Gebruikers van iTBC, dat ook is gebouwd op het Synaps platform en daar rechten en autorisaties hebben en vervolgens ook toegang en rechten voor CoronIT krijgen, kunnen toegang behouden tot beide systemen, zelfs als ze later niet meer worden ingezet op een van de twee taken. GGD´en vergeten daarbij dit door te geven, zodat de rechten kunnen worden ingetrokken en de gebruiker nog toegang heeft tot de systemen, zelfs als ze niet meer in dienst zijn van de GGD. Voor medewerkers die uit dienst gaan en toegang hebben tot een systeem, moeten ook de rechten worden ingetrokken, zodat ze geen misbruik kunnen maken van de teogang tot het systeem.				De impact is hoog. Als een medewerker uit dienst gaat en nog toegang heeft tot de gegevens, leidt dit tot onrechtmatige inzage en onrechtmatige verspreiding van de gegevens.	De kans dat het risioc zicht voordoet is midden. Er is een beperkte groep medewerkers met dubbele rechten. De groep mensen die uit dienst gaan, worden vaker afgemeld als onderdeel van het uit dienst gaan.	GGD`en moeten worden gewezen op hun verantwoordelijkeid om rechten in te laten trekken als een medewerker niet meer werkzaam is in een van beide applicaties.	Communicatie met GGD'en om hen erop te wijzen dat rechten moeten worden ingetrokken als iemand uit dienst gaat.	Afgerond	
4	Overeenkomsten met betrokken partijen en leveranciers en afspraken over verantwoordelijkheid zijn niet duidelijk en/of niet geformaliseerd wat leidt datalekken, imagoschade en financiële schade in de vorm van opgelegde boetes/sancties.	4.1	Onduidelijkheid over verantwoordelijkheden voor verwerken zorgt ervoor dat betrokkenen niet voldoende worden geïnformeerd over de verwerking en waar de betrokkene haar rechten kan uitoefenen.	- Onduidelijkheid welke partijen door betrokkene aangesproken dienen te worden in het geval van uitoefening rechten of melden van klachten. Betrokkenen zijn sneller geneigd melding te doen bij autoriteiten (om media-aandacht te zoeken) met imagoschade en financiële schade als mogelijk gevolg. - De verwerkingsverantwoordelijke kan niet voldoen aan de informatieplicht vanuit de AVG wanneer onduidelijkheid bestaat over de verschillende verantwoordelijkheden van de betrokken partijen.				De impact is midden. Effectueren van het risico betekent non-compliance met de AVG, met imagoschade, boetes/financiële schade tot gevolg. De risico's voor de betrokkene zijn in deze gemiddeld, het is geen directe inbreuk op de persoonsgegevens. Wel op de rechten die een betrokken moet kunnen uitvoeren.	De kans dat het risico zich voordoet is midden. Er bestaat onduidelijkheid over de werkprocessen en er bestaan nog beperkt geformaliseerde afspraken tussen partijen. Hierdoor is het nog niet mogelijk geweest de privacyverklaring eenduidig af te ronden.	- Het doel, grondslagen en bewaartermijnen duidelijk communiceren naar alle partijen die toegangs- en invoerrechten hebben in CoronIT, dit opnemen in de gebruiksvoorwaarden van CoronIT, gedragscodes en werkprocessen, in de afspraken met de betrokken partijen (GGD'en, leverancier, overige gebruikers CoronIT) en in de privacyverklaring voor de betrokkenen. - In de werkprocessen en werkafspraken tussen de betrokken partijen de aanpak van en de verantwoordelijkheden rondom een dergelijk verzoek opnemen en met elkaar afstemmen. "	Rechten van betrokkenen moeten door de GGD worden uitgevoerd. Dit zou duidelijk moeten zijn vermeld op de website van de GGD'en. Deze structuur is ook vastgelegd in het convenant. Voor de informatieplicht is een privacyverklaring opgesteld, waarnaar GGD'en kunnen verwijzen op hun website. Verstandig is dat GGD'en verwijzen naar de privacyverklaring op de website van GGD GHOR, omdat deze kan wordengewijzigd en zo altijd wordt verwezen naar de meest recente versie. Indien de GGD'en een verzoek niet zelf kunnen uitvoeren, nemen zij contact op met de servicedesk bij GGD GHOR Nederland met een motivatie, zodat zij het verzoek kunnen doorvoeren.	Afgerond	
		4.2	Beschikbaarheid, integriteit en vertrouwelijkheid van verzamelde (persoons)gegevens zijn in het geding doordat de verwerkersovereenkomst met Topicus niet is geformaliseerd en onduidelijkheid ontstaat over de (verdeling van) taken en verantwoordelijkheden	- De onderhandelingen met de leverancier (Topicus) lopen moeizaam en de garanties die Topicus kan geven over de beveiligingsmaatregelen zijn niet helder en dus ook niet opgenomen in de huidige conceptversie van de verwerkersovereenkomst. Zonder een ondertekende verwerkersovereenkomst of duidelijkheid over de beveiligingsmaatregelen en gelet op de mate van afhankelijkheid van de gebruikers van de applicatie in deze cruciale tijden is het onverantwoord om een applicatie met zoveel gevoelige (persoons)gegevens live te laten gaan. - Op dit moment is niet bekend of er nog andere verwerkers zijn, of partijen waar gegevens mee worden uitgewisseld, waarbij het noodzakelijk is om afspraken te maken over de omgang met deze gegevens.				De impact is hoog. Bij onduidelijke afspraken kunnen geschillen ontstaan over verantwoordelijkheid. Door onduidelijkheid over de afspraken ontstaan fouten en misverstanden in de werkprocessen en het dagelijks beheer van de applicaties met mogelijk datalekken tot gevolg of verminderde beschikbaarheid van CoronIT.	De kans dat het risico zich voordoet is midden. Er bestaat onduidelijkheid over de gewenste versie van de verwerkersovereenkomst. Het is voor alle betrokkenen helder dat een dergelijke overeenkomst geformaliseerd dient te worden.	-De verwerkersovereenkomst met Topicus formaliseren. De verwerkersovereenkomst zoals die eerder is overeengekomen voor ITBC is voldoende zolang in de te formaliseren verwerkersovereenkomst ten minste de volgende maatregelen benoemd zijn: - Voldoen aan NEN7510 (in bijzonder 7512/7513), of indien op korte termijn niet haalbaar ISO27001; - Periodiek uitvoeren van technische security testen - Behoud van Right to Audit voor verwerkingsverantwoordelijke om periodiek de applicatie te (laten) beoordelen op vertrouwelijkheid, integriteit en beschikbaarheid. In kaart brengen van partijen waar gegevens mee worden uitgewisseld, kwalificeren van deze partijen en opstellen van documenten met daarin de afgestemde afspraken.	Een verwerkersovereenkomst is gesloten met Topicus. Deze is op basis van iTBC, maar aangepast naar de huidige wetgeving en stand van techniek. Gezien de snelheid waarmee de applicatie moet worden geïmplementeerd, is besloten de overeenkomst opnieuw te beoordelen over 2 tot 3 maanden om te beoordelen of dit voldoet aan de eisen die de wetgeving stelt voor de verwerking. In de huidige overeenkomst is opgenomen dat Topicus een ISO 27001 certificering heeft, werkt aan de NEN 7510 en handelt conform NEN-7512 en NEN-7513. Daarnaast is het right to audit opgenomen. Gebruikersovereenkomst is opgesteld voor gebruikers die zelfstandig verantwoordelijk zijn, zoals bedrijfsartsen en laboratoria. De meeste partijen zijn in kaart gebracht. Als een nieuwe partij wordt aangesloten, wordt deze in het overzicht van partijen van de categorie opgenomen en zullen de gebruiksvoorwaarden worden voorgelegd.	Openstaand	De gebruiksvoorwaarden zijn opgesteld en worden spoedig aan de partijen voorgelegd.
		4.3	De vertrouwelijkheid van verzamelde (persoons)gegevens (testresultaten) is in het geding door onduidelijkheid of CoronIT een registratiesysteem of een medisch dossier wordt, wat leidt tot het niet voldoen aan wettelijke vereisten (o.a. AVG, WGBO)	- Het is onduidelijk met welk doel CoronIT wordt uitgerold. GGD'en opereren op basis van de Wpg, niet WGBO tenzij bij Wpg aangegeven. Medisch dossier = WGBO, registratiesysteem testresultaten (bedoeld voor registratie/terugkoppeling/ondersteuningssysteem om op snelle wijze op grote schaal testen te bewerkstellingen) = WPG. Wanneer het doel en daarmee de grondslag niet van tevoren welbepaald en dus onduidelijk is, kunnen hierdoor ook niet de juiste autorisaties en de bewaartermijnen worden ingericht. Bij te brede autorisaties of te lange bewaartermijnen worden gegevens onrechtmatig verwerkt. Ook bij te korte bewaartermijnen terwijle lange aan de orde zijn is sprake van onrechtmatige verwerking van persoonsgegevens namelijk als de gegevens dus te vroeg worden verwijderd.				De impact is hoog. Indien niet de juiste doelstelling en grondslag wordt vastgesteld is de verantwoordelijke in overtreding van haar eigen wettelijke taken en daarmee ook van de AVG voor de verwerking van persoonsgegevens.	De kans dat het risico effectueert is laag. Het risico is beken en het besluit dient genomen te worden door de projectgroep. De projectgroep is voldoende om de juiste afwegingen te maken en waar nodig vervolgstappen voor dit besluit te kunnen nemen.	- Binnen het project bepalen en vaststellen welk doel CoronIT dient, enkel als registratie- en ondersteuningssysteem om op snelle wijze op grote schaal testen te bewerkstellingen, of daarnaast ook als medisch dossier op basis waarvan behandelingen zullen worden geregistreerd. Afhankelijk van het doel is de grondslag en de bewaartermijn respectievelijk Wet publieke gezondheid (5 jaar) en WGBO (20 jaar). Gelet op het feit dat GGD GHOR en GGD'en deze taak op basis van Wet publieke gezondheid uitvoeren is er dan geen ruimte om CoronIT als medisch dossier te gebruiken. Dit wordt dan voor nu en in de toekomst afgeraden. - CoronIT conform het doel inrichten (geen open velden voor bijvoorbeeld de behandeling, bewaartermijnen by default inzetten, autorisaties inrichten, etc). - Indien anders wordt besloten dient de volledige keten en de basis waarop uitvoering wordt gegeven aan de taken van die keten te worden herzien.	Binnen het project is vastgelegd dat CoronIT een registratiesysteem is, waardoor de Wpg van toepassing is. Binnen CoronIT is daarom geregeld dat invulvelden zijn opgenomen die overeenkomen met de velden die verplicht zijn volgens de Wpg. Op basis daarvan is ook de bewaartermijn vastgesteld. In de applicatie zijn nog open velden aanwezig. Deze worden ingevuld indien de betrokkene dit wenst. Te denken valt aan de partnernaam/geboortenaam.	Afgerond	

5	Processen om de testresultaten te verwerken en te communiceren (gehele keten) zijn niet eenduidig gedefinieerd wat leidt tot datalekken, imagoschade en financiële schade in de vorm van opgelegde boetes/sancties en kosten voor herstelwerkzaamheden.	5.1	Verlies in vertrouwelijkheid van persoonsgegevens door onduidelijkheid over de wijze waarop testresultaten verstrekt dienen te worden.	- Op basis van Wpg (art. 22) meldt de arts die bij een door hem onderzocht persoon het coronavirus vermoedt of vaststelt, dit bij GGD. De beoogde situatie met CoronIT is dat diverse groepen in de maatschappij, te beginnen met de zorgmedewerkers en daarna ook medewerkers in het onderwijs, door hun werkgever kunnen worden aangemeld voor de test. Degene die de betrokkene aanmeldt krijgt tevens de terugkoppeling van de resultaten. Deze aanvrager kan ook de manager of instellingsarts zijn. Dit is in strijd met Wpg maar ook met arbeidswetgeving en AVG aangezien bijzondere persoonsgegevens worden verstrekt aan een onrechtmatige ontvanger. Gegevens die worden ingezien door een manager of instellingsarts, is een onrechtmatige inzage, die, gezien de keuzes die zijn gemaakt, vaak voorkomt. Dit leidt tot klachten bij betrokkenen instellingen en AP met boetes/sancties en imagoschade tot gevolg. - De onduidelijkheid zorgt voor misverstanden in verwerking door de verwerkende instanties met mogelijke datalekken tot gevolg. - De wijze waarop testresultaten voor de ontvanger zichtbaar worden gemaakt is niet bekend voor de projectgroep. Het risico is aanwezig dat 'oude' testresultaten zichtbaar zijn wanneer nieuwe resultaten worden opgevraagd met onrechtmatige inzage tot gevolg.				De impact is hoog. Het betreft de vertrouwelijkheid van bijzondere persoonsgegevens, en het handelen in strijd met de wettelijke uitvoering van taken. Naast datalekken leidt dit ook op basis van andere wettelijke bepalingen tot boetes, sancties en bedreiging voor de continuïteit van CoronIT.	De kans dat het risico zich voordoet is hoog. Het betreft hier een combinatie van verschillende factoren die er allen toe kunnen leiden dat testgegevens ongeautoriseerd ingezien worden. Er is beperkt inzicht in de wijze waarop dit ingericht gaat worden en welk proces hiervoor van toepassing zal zijn.	- Het besluit nemen dat de aanvrager van de test enkel de bedrijfsarts van de werkgever is die de werknemer (de betrokkene) kan aanmelden voor de test. De restresultaten zouden enkel aan de betrokkene moeten worden teruggekoppeld. Gelet op de schaal en de snelheid van de verspreiding van het virus zou het tevens verantwoord kunnen zijn om de terugkoppeling aan de bedrijfsarts te doen. De instellingsarts (als het om de zorgmedewerkers gaat en deze arts niet de bedrijfsarts is) of de manager zijn niet bevoegd om de test aan te vragen of terugkoppeling te ontvangen. - In de DPIA verantwoorden waarom de testen niet direct via de huisarts maar via de bedrijfsarts worden aangevraagd en waarom de terugkoppeling niet naar de huisarts of enkel de betrokkene gaat maar juist naar de bedrijfsarts. - Deze maatregelen doorvoeren in het proces en neem het op in de procesbeschrijving. - De werkwijze op basis van de maatregelen duideijk communiceren naar de aanmelder en betrokkene. - Nadenken over en implementeren van een wijze die veilig en verantwoord is om de testresultaten te communiceren aan de betrokkene waarbij aan de juistheid, actualiteit en vertrouwelijkheid van de resultaten niet valt te twijfelen.	Het proces is op dit moment nog niet helemaal helder met betrekking tot de aanvraag. De opties die op dit momenet worden bekeken zijn aanvraag door de bedrijfsarts, aanvraag door de huisarts en/of aanvraag door de betrokkene zelf. Indien hier meer over bbekend is, wordt dat in de DPIA aangevuld. De gegevens zullen niet onbeveiligd worden gemaild naar de betrokkene. De betrokkene zal echter wel altijd direct op de hoogte worden gebracht, zodat er direct zekerheid is voor de betrokkene over het moeten treffen van maatregelen. Er wordt nu gekeken welke beveiligde optie zal worden gebruikt. Tot die tijd zullen betrokkenen telefonisch op de hoogte worden gebracht van de uitslag. In de privacyverklaring is beschreven hoe dit proces loopt, zodat de betrokkene op de hoogte is van het proces. Betrokkenen kunnen zich nu aanmelding via het callcenter en binnenkort via het burgerportaal. In het burerportaal kan de uitslag worden ingezien. Nu wordt de uitslag teruggebeld door GGD'en bij een positieve uitslag en een callcenter medewerker bij een negatieve uitslag. Hierdoor worden niet heel veel aanvragen meer door bedrijfsartsen gedaan en kunnen zorgmedewerkers ook kiezen de aanvraag voor een test via het callcenter en later het burgerportaal te laten lopen.	Afgerond	
		5.2	Verlies van vertrouwelijkheid of integriteit van persoonsgegevens door onjuiste voorlichting of beschikbaarheid van procedurebeschrijvingen.	- De beschikbare functionele documentatie bevat oude beschrijvingen ten aanzien van de werkwijze (bijv.: FSB leidende partij). Een nieuwe procesbeschrijving is niet beschikbaar, waardoor onduidelijkheid ontstaat over de te hanteren werkwijzes. Dit leidt tot verschillende interpretaties waardoor gegevens mogelijk onrechtmatig worden ingezien of onjuist worden verwerkt met een verlies van integriteit van gegevens tot gevolg (juistheid/volledigheid). Bij verlies van vertrouwelijkheid en integriteit is sprake van een datalek in termen van de AVG met boetes/sancties en imagoschade tot gevolg. - Door onjuist/onvolledig inzicht in het beoogde proces is het niet mogelijk om de passende technische, maar vooral organisatotische maatregelen te treffen die een adequate bescherming van persoonsgegevens dienen te borgen. - Een richtlijn of protocol voor de omgang met en de vernietiging van zowel de digitale als geprinte persoonsgegevens (bijv.: in rapportages) in niet gedefinieerd. Het is onduidelijk voor de projectgroep of de rapportages op het digitale dashboard te printen zijn. Voor zover deze mogelijkheid bestaat, is onduidelijk of dit ook het printen van privacygevoelige informatie omvat. Hierdoor ontstaan risico's voor de vertrouwelijkheid en de integriteit van persoonsgegevens.				De impact is hoog. Het is van belang dat iedereen op dezelfde wijze handelt, anders kunnen fouten worden gemaakt in het proces. Dit kan leiden tot onrechtmatige verwerking van persoonsgegevens.	De kans is midden. Medewerkers zijn allemaal op de hoogte van het proces en hoe gehandeld dient te worden. Daarnaast zijn een aantal werkwijzen opgesteld.	- De oude procesbeschrijvingen herzien of nieuwe opsitellen die aansluiten bij de beoogde situatie. Houd in de procesbeschrijvingen rekening met de in dit risicoregister voorgeschreven maatregelen. - De uitvoeringspraktijk conform de procesbeschrijvingen laten plaatsvinden door de procesbeschrijvingen te communiceren en het proces te bewaken. - Nadenken over en implementeren van een mechanisme om het proces te bewaken en te sturen. - In de procesbeschrijvingen of in een afzonderlijk protocol (of gedragscode)aangeven hoe zowel digitale als geprinte persoonsgegevens om te gaan. De vernietiging van digitale persoonsgegevens na het verstrijken van de bewaartermijnen kan door middel van by design oplossingen. Voor de omgang en vernietiging van onjuiste of irrelevante invoer van digitale gegevens of geprinte persoonsgegevens zullen echter in een gedragscode moeten worden uitgewerkt en worden gecommuniceerd naar de gebruikers. - Terughoudend omgaan met het afdrukken van persoonsgegevens uit CoronIT. Indien dit noodzakelijk is dan in de procesbeschrijvingen toelichten wanneer dit het geval is of juist dat dat niet de bedoeling is.	Voor medewerkers zijn werkinstructies opgesteld zodat ze voor iedere stap in het proces weten hoe ze moeten werken en dus met de persoonsgegevens om moeten gaan. Daarnaast wordt gezorgd voor Q&A sessies en een Q&A pagina die kan worden geraadpleegd. Op deze wijze wordt gezorgd dat medewerkers weten hoe ze in het proces moeten handelen. ten slotte is een rocesoverzicht opgemaakt. Indien het proces helemaal vast ligt, zal het proces verder worden uitgewerkt, zodat een volledige beschrijving bestaat. Daarnaast is het mogelijk om aan de GGD GHOR vragen te stellen als zaken in het proces onduidelijk zijn. Deze mogelijkheid zal ook bij de GGD zelf mogelijk zijn.	Afgerond	
		5.3	Verlies van vertrouwelijkheid of integriteit van testresultaten door onvoldoende verificatie van persoonsgegevens.	- Ingave en verificatie van de persoonsgegevens kan op twee manieren: 1. Ingave van de persoonsgegevens van de betrokkene en het opvragen van het BSN. 2. Invoeren van het BSN en het opvragen van de gegevens van de betrokkene. De eerste wijze bevat een grotere kans op fouten in de gegevens van de geteste persoon doordat er diverse spellingsmogelijkheden van een naam mogelijk zijn. Het gebruik van verkeerde gegevens, betekent dat een uitslag aan de verkeerde persoon wordt gekoppeld of aan de verkeerde persoon wordt gegeven. Dit betekent dat juistheid zoals gesteld in de AVG niet wordt nageleefd (datalek) en het treffen van juiste vervolgstappen voor de betrokkene wordt bedreigd.				De impact is hoog. Indien er foutieve invoer plaatsvindt, dan heeft dat een directe impact op de integriteit van de testresultaten. Hierbij kunnen zowelgegevens over de resultaten zelf als de geteste betrokken foutief zijn. Dit heeft een impact op de betrouwbaarheid van de gehele gegevensverwerking met datalekken en een impact op de levenssfeer van de betrokkene als gevolg.	De kans is midden. In het FO staat beperkt vermeld welke invoercontroles zijn ingericht. De kans is aanwezig dat onvoldoende onderzocht is op welke wijze invoercontroles fouten in de processen kunnen ondervangen.	- By design inrichten dat het ophalen van de gegevens van betrokkene enkel mogelijk is als [redacted] - By design inrichten dat zolang beide velden niet zijn ingevuld (en gedurende het typen van de gegevens) zoekresultaten niet worden getoond. Zo voorkom je onbevoegde inzage in persoonsgegevens van andere betrokkenen. - Aangezien CoronIT in de toekomst eventueel uitgebreid kan worden om andere groepen dan zorg- en onderwijsmedewerkers te testen, in het onwerp rekening houden met het feit dat niet alle inwoners van Nederland over een BSN beschikken (denk aan V-nummers).	n de applicatie kan enkel met twee velden worden ingevoerd en vervolgens de persoon worden opgeveord. Dit betekent dat telkens twee velden moeten worden ingevoerd om iemand op te halen, wat een waaarborg biedt voor de juistheid van de opgehaalde gegevens. In het ontwerp is ook meegenomen dat niet iedereen een BSN heeft. Hiervoor kan een nummer worden aangemaakt zodat toch kan worden getest.	Afgerond	
		5.4	De vertrouwelijkheid van verzamelde (persoons)gegevens (testresultaten) is in het geding doordat communicatie met betrokkenen onveilig is.	- In het functioneel ontwerp is uitgegaan van terugkoppeling van de testresultaten per e-mail. E-mail is ongeschikt voor het communiceren van medische testresultaten (bijzondere persoonsgegevens). - De testuitslag wordt per e-mail aan de arts en bekend gemaakt. Het e-mailadres van de arts wordt handmatig in het dossier ingevuld door de arts. Er vindt geen actieve controle op de juistheid van het e-mailadres plaats met verlies van integriteit en vertrouwelijkheid van gegevens tot gevolg. - De betrokkene ontvangt een e-mail met daarin de testuitslag.				De impact is hoog. Indien de mail uitlekt of verkeerd wordt bezorgd, ziet een onrechtmatige ontvanger de gegevens in. Daarnaast kan een mail worden onderschept. Dit is heeft een impact op de betrouwbaarheid en met datalekken en een impact op de levenssfeer van de betrokkene als gevolg.	De kans is hoog. Er zullen veel uitslagen worden gecommuniceerd en dus veel mails worden verstuurd, waardoor de kans op fout verzenden of onderschepping sterk aanwezig is.	- De mogelijkheid overwegen om een platform (bijv.: portaal) te bouwen voor betrokkenen voor het inzien van hun testresultaten. - Tot het moment waarop dit portaal beschikbaar is de resultaten telefonisch aan de betrokkene communiceren. E-mail kan alsnog worden gebruikt om de betrokkene te informeren dat testresultaten klaar staan, zonder de daadwerkelijke resultaten te verstrekken. De testresultaten kunnen dan op het portaal ingezien worden.	Het bouwen van een portaal neemt teveel tijd in beslag om te realiseren voor het ingebruiknemen van de applicatie. Daarom zullen betrokkenen eerst telefonisch op de hoogte worden gesteld door de GGD of arts. Er wordt intussen gewerkt om een beveiligde functie op te bouwen, ofwel door een beveiligde mail met SMS-authenticatie ofwel door een mail die kan worden geopend in een beveiligde webpagina of portaal door middel van SMS-authenticatie, ofwel de uitslag telefonisch melden zodat verificatie mogelijk is. Artsen ontvangen wel een e-mail dat een bericht klaarstaat en kunnen zich inloggen op een beveiligde omgeving met SMS-verificatie.	Afgerond	
		5.5	Vertrouwelijkheid, integriteit en beschikbaarheid van persoonsgegevens zijn in het geding door onvoldoende inzicht in koppelingen van CoronIT met andere applicaties in de omgeving van gebruikende organisaties.	- Er bestaat geen eenduidig overzicht van koppelingen van CoronIT met andere applicaties van betrokken en gebruikende organisaties (GGD'en, laboratoria, Topicus en eventueel organsiaties die aanvraag voor een test invoeren en indien medisch dossier, de zorginstellingen die aangesloten (zouden) moeten worden). Hierdoor is onvoldoende controle op de gegevensstromen buiten CoronIT met onrechtmatige verwerkingen tot gevolg. De integriteit van gegevens kan niet worden geborgd indien de gegevens buiten CoronIT om worden verwerkt. Naast onduidelijkheid over verantwoordelijkheden leidt het risico tot datalekken en imagoschade voor de betrokken organisaties. - Door onvoldoende inzicht in de infrastructuur waarin CoronIT gebruikt wordt en de koppelingen naar andere omgevingen is het risico aanwezig dat de koppelingen onvoldoende beveiligd worden om de vertrouwelijkheid, integriteit en beschikbaarheid van de gegevensverwerking middels die koppelingen te borgen.				De impact is hoog. Als koppelingen niet goed zijn beveiligd of gekoppeld wordt met verkeerde systemen, betekent dit dat persoonsgegevens onrechtmatig worden verwerkt.	De kans is midden. De koppelingen worden allemaal beoordeeld en er wordt gekeken waar de gegevens naartoe gaan. Er mist echter een overzicht, waardoor niet direct kan worden overzien wat exact waar naartoe gaat.	- Technische documentatie updaten, in kaart brengen welke koppelingen van toepassing zijn, risico inschatting per koppeling in kaart brengen.	Er is een overzicht van alle koppelingen die worden gebruikt. De koppelingen voor het lab voldoen aan de NICTOZ standaarden.	Openstaand	De koppelingen zijn nog niet weergegeven in een uitgebreide procesplaat.

Wob-verzoek SOLV/ICAM datalek 2021 coronasysteem

5.0 Tekst Wob-verzoek en register documenten

Tekst verzoek (v)

Audits, rapportages, analyses en/of onderzoeken (intern of door derde partijen) ten aanzien van de effectiviteit van (beveiligings-)maatregelen doorgevoerd na publiek bekend worden van het datalek, waaronder in ieder geval:

a) Rapportage functionele beveiligingstest uitgevoerd door Fox-IT; [voetnoot 6: Door de Tweede Kamer ontvangen op 28 april 2021, zoals blijkt uit Kamerstukken II 2020-2021, 25295, nr. 1179, p. 41.]

b) Extern onderzoek naar de kwaliteit van de software en de kwaliteit van de dienstverlening van de software-leverancier van HPZone; [voetnoot 7: Stand van zakenbrief digitale ondersteuning pandemiebestrijding d.d. 12 februari 2021.]

c) Gateway reflectie en Gateway Review op verbeterplannen; [voetnoot 8: Kamerstukken II 2020-2021, 25 295, nr. 995, p. 38-39.]

d) Externe (technische en cultuur) audits genoemd in Kamerbrief d.d. 23 maart 2021; [voetnoot 9: Kamerstukken II 2020-2021, 25 295, nr. 1063, p. 33.]

Register

Een screenshot van de verkennerpagina van map 5:

GGD en haar data – Hoe zit het echt?
- Een repliek -

GGD-medewerkers opereren al ruim 10 maanden in de vuurlinie, net als al die andere zorgprofessionals. Met man en macht wordt gewerkt aan dat ene ultieme doel: het coronavirus bestrijden. Een missie waar wij vol voor gaan door te testen, vaccineren en het doen van bron- en contactonderzoek. Deze week zijn wij allemaal opgeschrikt door het bericht over het onzorgvuldig omgaan met bijzondere persoonsgegevens en het stelen van data uit onze GGD-systemen. Een uitermate serieus en schokkend incident. Er is sprake van een ernstig misdrijf met grote impact. Voor ons en eigenlijk voor iedereen in Nederland.

De afgelopen week is er veel gesproken, geschreven en gespeculeerd over deze zaak. Verhalen over de GGD en de veiligheid en beveiliging van onze data en ICT-systemen volgden elkaar in rap tempo op. Verhalen vol feiten en verzinsels, onjuistheden en onvolledigheden, terechte en onterechte kritiek. Maar hoe zit het nu echt? Een repliek.

Spijt

Deze ernstige situatie roept heel begrijpelijk allerlei emoties op. Bij ons als GGD'ers en ook bij mensen in Nederland. Mensen die zich hebben laten testen, vaccineren en mee hebben gedaan aan bron- en contactonderzoek. Emoties als verontwaardiging, verdriet en frustratie. Bezorgdheid en boosheid. Ongeloof en onbegrip. Wij begrijpen dat heel goed. Wij voelen ook die pijn. Het spijt ons dat dit zo heeft kunnen gebeuren. Omdat dit afleidt van waar we ons in het land allemaal mee bezig zouden moeten houden: ervoor zorgen dat we dat verwoestende en ontwrichtende coronavirus onder controle krijgen én houden. Daar zou alle focus en energie op gericht moeten zijn. Ook die van ons.

Hart voor de publieke gezondheid

Het versterken van de publieke gezondheid en de veiligheid. Dat is de taak en rol van GGD'en in ons Nederlandse systeem. Een taak en rol die wij met hart en ziel uitoefenen. De gezondheid van ons allemaal drijft ons. Daarom zijn wij al maandenlang in de weer. Alle dagen van de week. Met vele duizenden mensen. En dat aantal groeit nog iedere dag. Duizenden gedreven mensen die hart hebben voor hun werk en de publieke gezondheid. Duizenden mensen die zich volledig focussen op het bestrijden van het coronavirus. Daar is alles wat we doen op gericht. Voorkomen dat mensen ziek worden. Of erger. Op een integere en betrokken manier.

Geen bewijs grootschalige verkoop of verhandeling

Maar de zaken zijn zoals ze zijn. Niet iedereen blijkt met deze integere en betrokken intentie bezig te zijn geweest. Mensen die werken voor een GGD zijn op een onjuiste en onzorgvuldige manier omgegaan met persoonsgegevens. Persoonsgegevens van burgers zijn gestolen. En het lijkt erop dat zij die gegevens uit onze GGD-systemen te koop hebben aangeboden of gedeeld met onbevoegden. Voor de duidelijkheid: wij (GGD en politie en justitie) hebben vernomen dat er datasets worden

aangeboden, maar er is niet waargenomen dat deze ook daadwerkelijk zijn verkocht of verhandeld. Dit is allemaal nog onderdeel van het grootschalige en grondige onderzoek van politie en justitie. Zij nemen deze situatie zeer hoog op. En daar zijn wij blij mee.

De gelegenheid maakt de dief

Hoe het ook precies blijkt te zitten, wij kunnen er niet omheen dat dit heeft *kunnen* gebeuren. Mensen hebben misbruik *kunnen* maken van data omdat ze daar ruim toegang toe hadden. De gelegenheid maakt de dief. Wij hebben naar eer en geweten keihard gewerkt en keihard ons best gedaan. Maar het was niet genoeg. Er zijn fouten gemaakt. Daar lopen wij niet voor weg.

Wij willen hier wel wijzen op de context waarin wij keuzes hebben gemaakt en hebben moeten maken. Het coronavirus golfde en golft nog steeds over het land. Al onze focus lag op de gezondheid van ons allemaal en het bestrijden van het virus. Ervoor zorgen dat zoveel mensen zo snel mogelijk getest konden worden. Dat was de opdracht die we kregen. In die strijd hebben we lastige keuzes moeten maken over systemen en de inrichting daarvan.

En waar keuzes worden gemaakt, worden óók fouten of verkeerde keuzes gemaakt. Niet bewust of opzettelijk. Maar wel fouten of verkeerde keuzes, omdat je achteraf moet constateren dat ze tot onwenselijke situaties hebben geleid. Zoals nu. Kwaadwillenden zijn moedwillig en onrechtmatig aan de haal gegaan met persoonsgegevens. Dat had niet mogen gebeuren.

Twee systemen

GGD'en werken met twee systemen. CoronIT en HPZone. CoronIT is het administratiesysteem voor het test- en vaccinnatieproces en de communicatie hierover. Dus als iemand een afspraak maakt voor een coronatest over een vaccinatieafspraak, komen zijn of haar persoonsgegevens in CoronIT. Daarnaast werken we met HPZone. Dat is een elektronisch dossier dat we gebruiken bij het bron- en contactonderzoek. Speciaal voor de bestrijding van de coronapandemie wordt er gewerkt met een uitgeklede versie van HPZone: HPZone Lite.

CoronIT

CoronIT is een relatief nieuw systeem. Hier zijn de GGD'en mee gaan werken toen wij de opdracht kregen van het ministerie van VWS om mensen te gaan testen op het coronavirus. Dit was tot dat moment geen rol van de GGD. Alles is in zeer korte tijd en onder zeer hoge druk opgetuigd. Want het virus wachtte niet. Er moesten zo snel mogelijk teststraten komen. En een systeem waarin de gegevens kwamen te staan. Een goed en veilig systeem– en dat is het ook.

Is het perfect? Zeker niet. Werken we continu aan het verbeteren van het systeem? Bijvoorbeeld op het gebied van informatieveiligheid en privacy, controles en analyses? Absoluut. Overigens zijn er in het najaar van 2020 naar aanleiding van berichten in de media vragen aan ons gesteld door de Autoriteit Persoonsgegevens (AP) over CoronIT. Deze vragen hebben wij beantwoord, waarna de AP geen aanvullende vragen had.

Voor zover wij nu kunnen overzien zijn er persoonsgegevens van individuen uit CoronIT gehaald. Geen datasets met gegevens van duizenden (of meer) mensen. En voor zover wij nu kunnen overzien heeft dit weinig tot niets te maken met het falen, disfunctioneren of de eventuele onveiligheid van het systeem. In dit geval gaat niet om systeemfouten, maar om boosaardige opzet en de drang om over de rug van anderen wat te verdienen.

Als kwaadwillende mensen moedwillig gegevens uit een systeem halen, dan is dat bijna niet te voorkomen. Elk systeem is zo sterk als de zwakste schakel en meestal zijn de mensen de zwakste schakel. Dat lijkt ook in dit geval zo te zijn. Wij zijn blij dat er afgelopen weekend – toen bekend werd dat er persoonsgegevens buiten onze 'poorten' terecht waren gekomen - direct twee mensen zijn gearresteerd. En afgelopen week nog meerdere.

HPZone

En dan hebben we nog HPZone. Een systeem uit 2003. Een systeem dat al jarenlang gebruikt werd door 23 GGD'en voor de infectieziektebestrijding. Een systeem waar een kleine groep artsen en verpleegkundigen mee werkte als ze te maken kregen met een lokale uitbraak van een infectieziekte. Een systeem dus voor en van specialisten waar zij al buitengewoon lange tijd op zeer kleine schaal en binnen elke GGD apart probleemloos mee werkten.

Toen corona uitbrak is er onder hoge druk en in korte tijd de keuze gemaakt om HPZone als basis te blijven gebruiken voor het uitvoeren van bron- en contactonderzoek; dit werd HPZone Lite. We hadden niks beters. Zo konden we snel van start en snel handelen. En dat wilden wij ook, want corona dreigde ons land te overspoelen.

En ja, wij weten en wisten dat HPZone (Lite) niet geschikt is om zo grootschalig en zo intensief te worden gebruikt als nu nodig is bij het bestrijden van de coronapandemie. Daar zijn wij al maanden heel transparant en eerlijk over. Als geen ander kennen wij de beperkingen van het systeem. Het is echter onvermijdelijk dat HPZone een relatief open systeem is. Dit is nodig om dat te doen waar het systeem bij moet helpen: infectieziektebestrijding. Dus daar is bij de keuze van de inrichting vanuit gegaan. Ook toen in plaats van een handvol gespecialiseerde artsen en verpleegkundigen duizenden mensen in het systeem gingen werken.

Van die openheid hebben bepaalde lieden nu misbruik gemaakt. Zij hebben tegen de regels en voorschriften in persoonsgegevens uit HPZone gehaald en die te koop aangeboden. Om hoeveel gegevens het gaat en van wie, daar kunnen we nu nog niets over zeggen. De fout zit hier in de menselijke keuze om iets volstrekt laakbaars te doen in combinatie met een systeem dat relatief open (en daardoor kwetsbaar) is.

Dat is ook precies de reden waarom we - samen met het ministerie van VWS - al maanden werken aan een nieuw systeem. Een systeem dat voldoet aan de huidige eisen (qua veiligheid en gebruikersvriendelijkheid) en omstandigheden (het indammen van een landelijke pandemie waar duizenden mensen dagelijks mee bezig zijn). Alles is erop gericht om dit systeem GGD Contact – samen met het bijbehorende BCO-portaal – in maart operationeel te hebben voor de coronabestrijding. Dan kunnen we afscheid nemen van HPZone Lite bij de bestrijding van de coronapandemie. Het is uiteraard wel belangrijk dat dit systeem dezelfde functionaliteiten heeft die cruciaal zijn in deze pandemiebestrijding. Zoals de koppeling met het RIVM. Daar werken we ook aan.

En nu?

Nu gaan we in eerste instantie ‘gewoon’ door met het bestrijden van de pandemie. En daarbovenop werken we met vereende krachten aan het vergroten en verbeteren van de veiligheid van onze systemen en het opsporen van onrechtmatigheden. We werken nauw en intensief samen met politie, justitie en data- en cybercrimespecialisten om fouten die zijn gemaakt door mensen én systemen te traceren. Mensen die buiten hun boekje zijn gegaan zullen worden ontslagen. Heel simpel. En zwakke plekken in de beveiliging zullen worden opgespoord en verstevigd.

We nemen allerlei beheermaatregelen om de veiligheid en vertrouwelijkheid beter te kunnen waarborgen. Bepaalde functionaliteiten gaan ‘op slot’ voor de meeste gebruikers. Helemaal ‘op slot’ kunnen we HPZone Lite niet zetten. Eenvoudigweg omdat we dan de infectieziektebestrijding in het slot zouden gooien. Dat mag natuurlijk nooit gebeuren. Het virus is nog allesbehalve onder controle. Bovendien laten we een externe audit uitvoeren naar het gebruik van de data door de GGD en onze partners.

Door al deze daden willen wij het vertrouwen herstellen. Want juist omdat wij staan voor die publieke gezondheid, weten wij als geen ander dat vertrouwen een cruciaal element is om onze rol in de virusbestrijding goed te vervullen. We kunnen er niet omheen. Door deze datadiefstal heeft het vertrouwen van mensen in de GGD en in het werk dat we doen een forse deuk opgelopen. Zij vragen zich – begrijpelijkerwijs – af of hun zeer gevoelige en persoonlijke informatie bij ons wel in veilige handen is. Het heeft nu topprioriteit om die veiligheid te vergroten en het vertrouwen te herstellen.

Speciaal nummer voor mensen met vragen

Wij begrijpen heel goed dat mensen van wie de gegevens in onze systemen zitten ongerust zijn en vragen hebben. Daarom hebben wij een speciaal telefoonnummer ingesteld waar zij terecht kunnen met hun vragen en zorgen. Dit nummer is vanaf 29 januari 2021 bereikbaar van 09.00 tot 21.00 uur, 7 dagen in de week.

Aan de burgemeesters VRMWB
Aan de AB-leden AB GGD WB,
Raadsleden en ambtenaren.

Kenmerk: [redacted] Datum: 5 februari 2021
Behandeld door: [redacted] E-mail: [redacted]
Onderwerp: Incident rondom de data uit de landelijke GGD-systemen

Geachte burgemeesters VR MWB, leden van ons algemeen bestuur, raadsleden en ambtenaren,

In de media is momenteel veel aandacht voor het incident rondom de data uit de landelijke GGD-systemen. Wij kunnen ons voorstellen dat dit bij u vragen oproept en dat u behoefte heeft aan informatie om met uw raad te delen. Daarvoor ontvangt u onderstaande toelichting.

De afgelopen week is er veel gesproken, geschreven en gespeculeerd over de gestolen data uit de GGD-systemen. Van essentieel belang is eerst en vooral dat het onderzoek van de politie daarnaar nog loopt. Wel heeft GGD GHOR Nederland het nodig gevonden om over het incident te communiceren. Via deze link vindt u een repliek vanuit GGD GHOR Nederland die op 29 januari jl. werd gepubliceerd. Daarnaast vindt u hier een overzicht met **veel gestelde vragen en antwoorden over het incident.**

Daarnaast is er uit de aard der zaak veel en intensief contact met de Autoriteit Persoonsgegevens (AP), in het kader van het toezicht dat de AP dient te houden op de veiligheid van de gegevens in de GGD-systemen en de naleving van de Algemene Verordening Gegevensbescherming (AVG). Het mag geen verbazing wekken dat dit toezicht naar aanleiding van het incident de afgelopen week is geïntensiveerd. Het intensiveren van het toezicht houdt in dat inspecteurs van de AP nauwlettend de ontwikkelingen volgen en controles zullen uitvoeren.

Aandacht binnen GGD'en
Als GGD'en werken we aan de virusbestrijding, met de benodigde functionaliteiten op een zo veilig mogelijke manier. GGD'en doen alles wat in het vermogen ligt om ervoor te zorgen dat gegevens van mensen die zich laten testen, vaccineren en betrokken zijn bij bron- en contactonderzoek in veilige handen zijn. Zo zorgt de GGD voor controle aan de poort (VOG en geheimhoudingsverklaring), is er breed in de organisatie ruime aandacht voor het onderwerp door extra communicatie, aangescherpte werkwijzen en gesprekken met medewerkers over privacy en geheimhouding en vinden er steekproefsgewijs checks plaats op noodzakelijke toegang dossiers. De functionaris

gegevensbescherming is hier nauw bij betrokken, als ook een interne projectgroep die is ingesteld voor de verdere optimalisatie van de processen, zowel in de systemen als in de communicatie.

Verkenning verwijdering (persoons)gegevens
Mensen kunnen op grond van de Algemene Verordening Gegevensbescherming (AVG) bij de GGD alwaar zij getest of gevaccineerd zijn een verzoek doen tot het verwijderen van hun persoonsgegevens. Vanuit GGD GHOR Nederland wordt op dit moment gewerkt aan de precieze invulling van het recht op gegevensverwijdering en de procedure die daarvoor ingericht wordt. Zo wordt bijvoorbeeld uitgezocht welke gegevens in welke gevallen en met inachtneming van welke termijnen verwijderd mogen c.q. moeten worden. Naast de AVG hebben we bijvoorbeeld ook te voldoen aan de Wet Publieke Gezondheid (Wpg), die o.a. eisen stelt aan de bewaartermijn van medische gegevens.

Vanuit GGD GHOR Nederland en de GGD-en wordt alle medewerking verleend aan instanties die op grond van hun wettelijke taken toezicht houden, vragen stellen en controles uitvoeren. Wij zien het maatschappelijke belang daarvan en ons gezamenlijke doel is het herstel van vertrouwen.
Indien er nieuwe ontwikkelingen zijn dan informeer ik u daarover.

Met vriendelijke groet,

Directeur Publieke Gezondheid

Change readiness status (09-06-2021) GGD West Brabant

GGD GHOR Nederland

22-06-2021

Dashboard

Gedurende de afgelopen maanden zijn er periodiek change readiness surveys (t.b.v. transitiegereedheid) ingevuld door de transitiecoördinatoren van de GGD'en. In deze surveys wordt op verschillende aspecten geïnventariseerd hoe de GGD'en zijn voorbereid op de transitie naar GGD Contact. De aspecten die zijn onderzocht zijn: Organisatie, communicatie, transitieteam, veranderbereidheid, training en security/privacy. Per aspect zijn er vragen over meerdere onderwerpen gesteld (deze worden op de komende slides toegelicht). Dit change readiness dashboard toont de status van GGD West Brabant van de meest recente survey (09-06-2021), een beschrijving van de gap tussen de IST- en SOLL-situatie, en aanbevelingen voor mitigerende maatregelen.

Readiness status overzicht

Hoog 9

Aanspreekpunten; medewerker informatie; versturen nieuwsbrieven; teamvolledigheid; teamcommunicatie; urgentieherkenning; urgentiecommunicatie; probleemverwachting; werkinstructies

Middel 11

Key-users; werkwijzeverandering; medewerker updates; gebruik nieuwsbrieven; probleembewustheid; voordeelbekendheid; acceptatieverwachting; opleidingsbehoefte; lokale coaches; security/privacy inzicht; security/privacy voortgang

Laag 0

Status en mitigerende maatregelen

Onderwerp	Change readiness status	Mitigerende maatregelen
Aanspreek-punten 	Om te borgen dat de live-gang en het werken met GGD Contact zo soepel als mogelijk verloopt is het van belang dat medewerkers weten wie de juiste aanspreekpunten zijn bij vragen over de implementatie, vragen over de applicatie zelf, storingen en verbeterideeën. De transitie coördinator geeft aan dat (bijna) alle medewerkers weten wie de juiste aanspreekpunten zijn.	N.v.t.
Medewerker informatie 	Een van de meest essentiële voorwaarden voor een succesvolle transitie is dat medewerkers überhaupt ermee bekend zijn dat HPZone(Lite) wordt vervangen door GGD Contact. Bij GGD West Brabant is dit volledig het geval.	N.v.t.
Versturen nieuwsbrieven 	De wekelijkse nieuwsbrieven, welke relevante informatie over ontwikkelingen rondom GGD Contact omvatten, worden door de transitie coördinator met de medewerkers bij GGD West Brabant gedeeld. Medewerkers worden geïnformeerd over de urgentie van de vervanging van HPZone(Lite), de voordelen van GGD Contact, het uitgebreide test- en verbeteringsproces, de juiste aanspreekpunten bij vragen/storingen, en verdere informatie.	N.v.t.
Team-volledigheid 	Voor een succesvolle transitie is het essentieel dat de juiste functionarissen zijn betrokken bij de lokale voorbereidingen op de transitie. De transitie coördinator geeft aan dat zijn transitie team samen met een functionaris gegevensbescherming, CISO, IT service desk, communicatieadviseur, opleidingscoördinator en BCO-coördinator volledig is.	N.v.t.

Status en mitigerende maatregelen

Onderwerp	Change readiness status	Mitigerende maatregelen
Team-communicatie 	De transitie coördinatoren zijn gevraagd om samen met het lokale transitieteam regelmatige overleggen te houden waarin de teamleden zich over de voortgang en eventuele uitdagingen op hun verantwoordelijkheidsgebieden kunnen uitwisselen. Ook bij GGD West Brabant vinden deze gezamenlijke afstemmingsmomenten plaats.	N.v.t.
Urgentie-herkenning 	Voor een hoge veranderbereidheid en gebruikersacceptatie is het van belang dat medewerkers de urgentie van de vervanging van HPZone(Lite) middels een veiligere, efficiëntere en gebruikersvriendelijkere applicatie begrijpen. Volgens de transitie coördinator wordt de urgentie volledig herkend door de medewerkers.	N.v.t.
Urgentie-communicatie 	De gebruikersacceptatie van een nieuwe applicatie is hoger wanneer de urgentie duidelijk door directie en management wordt gecommuniceerd richting medewerkers. Volgens de transitie coördinator wordt de urgentie van de implementatie van GGD Contact volledig gecommuniceerd door hem, de DPG en het management team van GGD West Brabant.	N.v.t.
Probleem-verwachting 	De transitie coördinator verwacht dat de transitie bij GGD West Brabant probleemvrij gaat verlopen.	N.v.t.

Status en mitigerende maatregelen

Onderwerp	Change readiness status	Mitigerende maatregelen
Werkinstructies 	Het opleidingsmateriaal voor GGD Contact is opgesteld met het uitgangspunt dat er geen grote verschillen bestaan tussen de huidige landelijke werkinstructies en de werkwijze bij een bepaalde GGD. Indien de werkwijze van BCO medewerkers significant afwijkt van de landelijke werkinstructies, kan het opleidingsmateriaal mogelijk de gap tussen de huidige en de nieuwe werkprocessen niet volledig afdekken. Bij GGD West Brabant komt de werkwijze volledig overeen met de landelijke werkinstructies.	N.v.t.
Key-users 	De transitie coördinatoren zijn gevraagd om tenminste 8 key-users per GGD aan te stellen, welke na live-gang als eerste aanspreekpunt bij vragen dienen en het incidenten- en wijzigingsproces faciliteren. GGD West Brabant beschikt grotendeels over key-users.	Voor GGD Contact gaat de voorkeur uit naar minimaal 8 key-users, desgewenst uit te breiden naar bijv. 1 key-user per 25 medewerkers. Daarnaast heeft het de voorkeur om 1 key-user als aanspreekpunt te laten fungeren voor de huidige projectorganisatie van GGD Contact. Proactieve ondersteuning van collega's t.b.v. een plezierige en snelle adoptie maar ook het tijdig opmerken, inventariseren, categoriseren en melden van issues en verbeteringen zijn belangrijke en primaire taken van een key-user.
Werkwijze-verandering 	Met de transitie naar GGD Contact gaat ook de BCO werkwijze op sommige aspecten veranderen. Het is belangrijk dat medewerkers ervan op de hoogte zijn dat hun werkprocessen deels anders gaan verlopen, zodat ze zich hierop kunnen voorbereiden. Bij GGD Rotterdam Rijnmond is dit grotendeels het geval.	Bijvoorbeeld de GGD Contact toolkit en de wekelijkse nieuwsbrieven bevatten informatie die medewerkers ervan op de hoogte stelt dat er met GGD Contact een verandering aan komt die ook invloed heeft op hun manier van werken.

Status en mitigerende maatregelen

Onderwerp	Change readiness status	Mitigerende maatregelen
Medewerker updates 	Om te borgen dat GGD Contact de medewerkers niet als een verassing bereikt, inventariseren wij in hoeverre zij op de hoogte zijn over de voortgang van het ontwikkel- en implementatietraject van GGD Contact. De transitie coördinator geeft aan dat medewerkers bij GGD West Brabant grotendeels op de hoogte zijn.	Wij bevelen aan om de belangrijkste informatie over GGD Contact, die medewerkers in de laatste maanden hebben gemist te delen (bijv. de GGD Contact toolkit, beweegredenen voor de vervanging, gekozen uitrolstrategie, eerste ervaringen met de applicatie tijdens de testfase, aanspreekpunten en processen bij vragen/storingen).
Gebruik nieuwsbrieven 	De GGD Contact nieuwsbrieven zijn een centraal informatieproduct, waarmee medewerkers op de hoogte worden gehouden over de voor hun relevante ontwikkelingen rondom de implementatie van GGD Contact. Het is belangrijk om inzichtelijk te hebben in hoeverre de medewerkers de nieuwsbrieven lezen en hoe goed de informatie hun bereikt. Bij GGD West Brabant worden de nieuwsbrieven deels door medewerkers gelezen.	Het risico is dat medewerkers niet voldoende zijn geïnformeerd over GGD Contact en zodoende geen vertrouwen in de applicatie hebben, wat gebruikersweerstand kan veroorzaken. Om dit te voorkomen is het belangrijk om medewerkers mee te nemen in de transitie, het gesprek over GGD Contact te voeren en informatieproducten zoals nieuwsbrieven, video's en de toolkit met hun te delen. Hiernaast kunnen ook communicatiekanalen van de eigen GGD van meerwaarde zijn, zoals bijvoorbeeld dagstart meetings of zelfgemaakte video's over GGD Contact.
Probleem-bewustheid 	Voor de veranderbereidheid in de vervanging van een huidige applicatie is het belangrijk dat medewerkers zich bewust zijn van de beweegredenen voor de verandering en de noodzaak van de vervanging. De transitie coördinator van GGD West Brabant geeft aan dat medewerkers deels bekend zijn met de problemen betreffende HPZone(Lite).	Bijvoorbeeld het hoofdstuk "Waarom GGD Contact?" en het overzicht met verschillen tussen de applicaties in de GGD Contact toollkit kunnen erbij helpen de beweegredenen te verduidelijken. Naast het delen van de toolkit is het belangrijk om dit beter onder de aandacht van medewerkers te brengen.

Status en mitigerende maatregelen

Onderwerp	Change readiness status	Mitigerende maatregelen
Voordeel-bekendheid 	Voor de veranderbereidheid van medewerkers en de voorbereiding op de ingebruikname van een applicatie is het belangrijk om medewerkers goed te informeren over de voordelen van de nieuwe applicatie. De transitie coördinator van GGD West Brabant geeft aan dat medewerkers grotendeels bekend zijn met de voordelen van GGD Contact.	De GGD Contact toolkit bevat een overzicht dat de verschillen tussen HPZoneLite en GGD Contact weergeeft en de voordelen van de nieuwe applicatie uitlicht. Dit onder de aandacht van medewerkers te brengen is een mitigerende maatregel.
Acceptatie-verwachting 	Om mogelijke weerstand en/of problemen bij de ingebruikname zo vroeg als mogelijk te herkennen en er op te kunnen reageren, is het belangrijk om de verwachte gebruikersacceptatie goed in beeld te hebben. De transitie coördinator schat zelfs in dat de gebruikersacceptatie van GGD Contact bij GGD West Brabant grotendeels gemakkelijk gaat verlopen.	Voor een hoge gebruikersacceptatie is het essentieel dat medewerkers vertrouwen hebben in de applicatie, bekend zijn met de noodzaak en voordelen van de vervanging, én voldoende opgeleid en ondersteund worden. De transitie coördinator speelt een belangrijke rol in het creëren van een draagvlak voor GGD Contact binnen de eigen GGD. Hiernaast is het ook een taak van de key-user om enthousiasme over GGD Contact te verspreiden.
Opleidings-behoefte 	Om te borgen dat medewerkers voldoende zijn getraind om te kunnen werken met de nieuwe applicatie is het van belang om te onderzoeken in hoeverre het aanbod aan opleidingsmaterialen en aanvullende ondersteuning de opleidingsbehoefte bij een specifieke GGD regio afdekt. Volgens de transitie coördinator is de opleidingsbehoefte van GGD West Brabant door het e-learning, de werkinstructie, de FAQ website, de IT service desk, de landelijke coaches en de BCO webinars grotendeels afgedekt.	Wanneer er verwacht wordt, dat medewerkers niet voldoende kunnen worden opgeleid middels de benoemde trainingsmaterialen en ondersteuning, is het belangrijk om vroegtijdig aan te geven welke aanvullende support resources benodigd zijn. Het projectteam kan helpen bij het organiseren van ondersteuning.

Status en mitigerende maatregelen

Onderwerp	Change readiness status	Mitigerende maatregelen
Lokale coaches 	Naast de landelijke coaches, welke de key-users gaan trainen en ondersteunen in hun nieuwe rol in de periode rond en kort na de live-gang, is het ook wenselijk om lokale coaches aan te wijzen. Dit zijn collega's met de rol 'Coach' in Academy GGD GHOR. Zij kunnen de voortgang van medewerkers inzien t.a.v. de e-learning. Bij GGD West Brabant is deze rol deels afgedekt.	Indien er nog niet voldoende lokale coaches met de rol 'coach' in Academy GGD GHOR zijn aangesteld, bevelen wij aan om deze voordat medewerkers de e-learning doorlopen aan te wijzen.
Security/ privacy inzicht 	Omdat informatiebeveiliging en privacy twee van de meest belangrijke factoren zijn in het project rondom de vervanging van HPZone(Lite), is het noodzakelijk dat de transitie coördinator zicht heeft op de te treffen maatregelen. Hij geeft aan dat hij hier grotendeels zicht op heeft.	Goede communicatielijnen naar de CISO/ISO en de FG zijn essentieel om inzicht te hebben in de relevante maatregelen die door de GGD te treffen zijn. Bijvoorbeeld is er vanuit het project een tweetal vragenlijsten opgesteld om inzicht te geven in de privacy en security volwassenheid van de GGD'en.
Security/ privacy voortgang 	Voor transitie coördinatoren is het belangrijk om de voortgang rondom de implementatie van de privacy en informatiebeveiligingsmaatregelen goed inzichtelijk te hebben, zodat issues tijdig kunnen worden besproken en vóór de live-gang aan alle eisen wordt voldaan. De transitie coördinator van GGD West Brabant geeft aan dat hij hier grotendeels inzicht in heeft.	Regelmatige stand-up meetings met het transitieteam kunnen helpen om op de hoogte te zijn t.a.v. de voortgang bij de verschillende verantwoordelijkheidsgebieden, zoals o.a. security en privacy. Hiernaast kunnen voortgangsrapportages en checklists de status inzichtelijker maken.

Archived: donderdag 12 mei 2022 11:44:16
From: [redacted]
Sent: vrijdag 5 februari 2021 17:43:31
To: [redacted]
Subject: FW: Wijzigingen HPZone en HPZoneLite
Importance: Normal
Sensitivity: None

Hi collega's,

Hebben jullie deze al ontvangen via een ander kanaal???

Hartelijke groeten,

[redacted]

[redacted]

GGD West-Brabant

Doornboslaan 225-227, Breda

www.ggdwestbrabant.nl

Heeft u vragen over het Corona virus? Bel 085-0785810.

Van: [redacted]
Verzonden: vrijdag 5 februari 2021 10:18
Aan: [redacted]
Onderwerp: Wijzigingen HPZone en HPZoneLite

Beste collegae,

Er zijn recent maatregelen getroffen in HPZone en HPZoneLite om datalekken in de toekomst zoveel mogelijk te voorkomen. De maatregelen komen neer op:

1. **Queryfuncties voor cases en contacten (in HPZone en HPZone Lite):**

- Query views kunnen niet meer worden geprint.
- Query downloads zijn alleen beschikbaar voor de volgende rollen:
  - Administrative Officer (geeft ook toegang tot "Administration")
  - Coördinator
- In deze beperkt toegankelijke queries is BSN-informatie niet meer aanwezig.
  - Wel aanwezig zijn: naam, voor en achternaam, 4-cijferige postcode (PC4), en geboortedatum, berekende leeftijd, echter geen adresgegevens.
  - Er wordt een voorstel uitgewerkt om ook PC6 op te nemen om GGD-en lokale analyses te kunnen laten doen.
  - Als er in CoronIT een BSN staat, zal een koppeling van de melding naar HPZone blijven functioneren.
  - Door de ontbrekende BSN in data-output is de voor datamanagers tot nu toe gebruikte koppeling tussen CoronIT en HPZone via BSN onmogelijk. Deze moet worden vervangen door koppelingen op naam/geboortedatum en postcode.

2. **Customqueries:**

- Er zijn customqueries door gebruikers aangemaakt die BSN- en adresgegevens bevatten. De bestaande customqueries zijn **per onmiddellijke ingang verwijderd** uit zowel HPZone als HPZoneLite.
- Wilt u functioneel noodzakelijke customqueries in HPZone en HPZone Lite opnieuw aanmaken, dan zullen die alleen gegevens mogen bevatten die aan de privacy-eisen voldoen. BSN- en adresgegevens zijn dus niet meer toegestaan.

Met vriendelijke groet,

[redacted]

[redacted]

GGD West-Brabant
E [redacted]

Doornboslaan 225-227, Breda

www.ggdwestbrabant.nl

www.brabantscan.nl

[redacted]

Aanwezig op: ma-di-wo-do-vr

Benieuwd naar de gezondheid van West-Brabanders? Bezoek dan de Brabantscan!

Archived: donderdag 12 mei 2022 11:43:59
From: [redacted]
Mail received time: Fri, 12 Feb 2021 13:16:06
Sent: Fri, 12 Feb 2021 14:15:56
To: [redacted]
Subject: Fwd: Bericht over KennisNet
Importance: Normal
Sensitivity: None

Ter info

Gr [redacted]

Begin doorgestuurd bericht:

Van: [redacted]
Datum: 12 februari 2021 om 14:15:00 CET
Aan: [redacted]
Kopie: [redacted]
Onderwerp: FW: Bericht over KennisNet

Hallo allemaal,

Hierbij ook naar jullie ter info. Toelichting op het besluit om Kennisnet offline te halen.

Met vriendelijke groet,

[redacted]

Van: [redacted]
Verzonden: donderdag 11 februari 2021 18:15
Aan: [redacted]
Onderwerp: Bericht over KennisNet

Beste collega's,

Ter informatie ontvangen jullie het onderstaande bericht dat vanmiddag op onze website is gezet.

GGD Kennisplatform offline, onderzoek loopt

Na de recente datadiefstal uit systemen van GGD GHOR Nederland zijn wij extra alert als het gaat om de beveiliging van onze systemen. Het ministerie van VWS heeft na overleg met ons een aantal van onze systemen laten bekijken door een zogenaamd 'Red team' van ICT-deskundigen. Dit team heeft gesignaleerd dat de toegang tot het kennisplatform KennisNet tekortkomingen kent. KennisNet wordt gebruikt voor kennisuitwisseling door professionals, werkzaam in de publieke gezondheidszorg en bevat onder meer werkinstructies en handleidingen. Naast een publiek toegankelijk deel waren er besloten groepen waar specifieke personen voor toegelaten konden worden.

Forensisch onderzoek is gestart om te bepalen of personen toegang hebben gehad tot het systeem die niet tot de doelgroep van dit platform horen. Ook wordt onderzocht of personen toegang hebben gehad tot informatie op het platform die vertrouwelijk is of die niet op het platform gedeeld had mogen worden. Dat zal het onderzoek moeten uitwijzen. Om het onderzoek niet te schaden, kunnen we hierover op dit moment geen verdere mededelingen doen.

Het systeem is op dinsdag 2 februari offline gehaald, nadat we de logging files en bestanden veilig hebben gesteld. Tevens hebben we een voorlopige melding gedaan bij AP, die opdracht heeft gegeven tot nader onderzoek. Deze week is het forensisch onderzoek van start gegaan. Het offline halen van KennisNet is vervelend voor de gebruikers, maar heeft geen onoverkomelijke gevolgen voor de bestrijding van het coronavirus.

Met vriendelijke groet,

[redacted]

[redacted]

GGD GHOR Nederland
Zwarte Woud 2
3524 SJ Utrecht

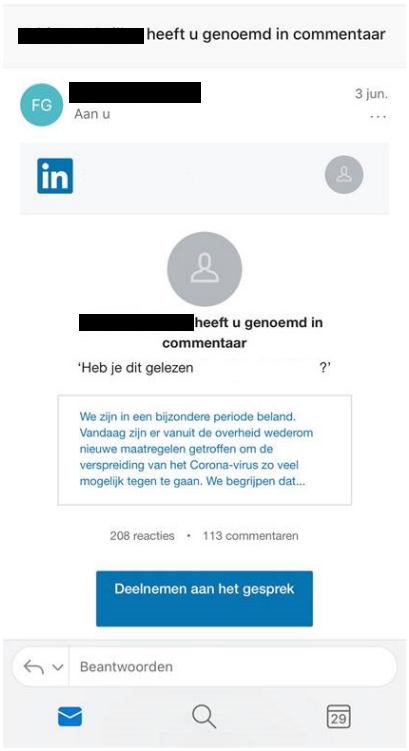
E-mail [redacted]
Telefoon [redacted]
Website www.ggdghor.nl
Twitter @GGDGHORNL

Phishing e-mail simulatie bij de GGD West-Brabant:

DE UITSLAG!

Op 3 juni heeft er een phishing e-mail simulatie plaatsgevonden, uitgevoerd door een extern bedrijf, onder alle medewerkers van de GGD West-Brabant.

Phishing is een vorm van internetfraude waarbij internetcriminelen op geraffineerde wijze proberen persoonlijke gegevens of wachtwoorden te stelen. Jij, of iemand anders in je organisatie, heeft op een verkeerde link geklikt, een verkeerde bijlage geopend of misschien verkeerd gereageerd op een e-mail.



Met deze gegevens kunnen criminelen inbreken op onze systemen en bijvoorbeeld bestanden 'gijzelen', die pas na het betalen van losgeld weer vrijgelaten worden.
We weten dat met name door de bestrijding van Corona de GGD ook extra belangstelling geniet van internetcriminelen over heel de wereld, met alle risico's voor de beschikbaarheid en vertrouwelijkheid van de gegevens van de inwoners van West-Brabant van dien!

076 528 20 00
www.ggdwestbrabant.nl

Hoe is er te werk gegaan en wat is de uitkomst?

Op woensdag 3 juni zijn in totaal **337** berichten met tussenpozen verstuurd. **297** collega's hebben hier ook daadwerkelijk iets mee gedaan.

Er is gemeten dat bij **190** collega's **(64%)** daadwerkelijk 'code' is uitgevoerd.

Hiermee verifieer je e-mailadres en kunnen hackers deze verder gebruiken in hun aanval naar jou of juist je collega's. Hackers weten ook dat je aan het werk bent, vanaf welke locatie, op welk tijdstip en welk apparaat je hebt.

142 **(47,8%)** collega's hebben één of meerdere keren op de link geklikt. Sommige waren zo nieuwsgierig dat ze **9** keer op dezelfde link hebben geklikt. **22** medewerkers klikte meer dan **3** keer op de link.

Het klikken op een malafide link kan er voor zorgen dat :

- Er automatisch op de achtergrond malware gedownload wordt.
- Je naar een misleidende site worden gebracht, zoals nu, die kan lijken op een betrouwbare website.

Er zijn **46** collega's **(15,5%)** geweest die hebben ingelogd op de nep pagina.
22 collega's deden dit met een GGD West-Brabant e-mail adres. Zij lieten wachtenwoorden achter.

Het achterlaten van data (zoals dat bij 22 mensen gebeurde) brengt het meeste risico met zich mee. Hiermee kunnen kwaadwillenden direct toegang krijgen tot een vertrouwelijke omgeving en mogelijk tot de omgeving van de GGD.

Hoe scoort de GGD ten opzichte van andere organisaties?

47,8% van de collega's heeft geklikt. Dit is **7,8% hoger** dan gemiddeld bij andere organisaties met dezelfde soort mails.

15,5% van de collega's heeft gegevens achtergelaten. Dit is **0,1% lager** dan gemiddeld bij andere organisaties.

Waar herken ik een phishing e-mail als deze aan?

Er waren een aantal punten waardoor je kon zien dat dit een phishing e-mail was:

- Ten eerste zou het ongebruikelijk moeten zijn dat **social mediaberichten** op je
- **zakelijke e-mailadres komen**. Zeker als je geen LinkedIn account hebt.
- De afzender: [redacted]**@nl-message.com** komt van een **onbekend domein**
- De **opmaak** van het bericht wijkt af van het origineel
- [redacted] heeft **geen foto** in het bericht en de ontvanger zelf ook niet
- Alle linkjes verwijzen naar: http://**54.195.53.179**/?rid=5CCh6UR
- Dit is **geen secure website** (dan zou het beginnen met https://)

Wat het geloofwaardig maakt is dat:

- Het een persoonlijk bericht is
- Je wordt nieuwsgierig gemaakt door dat je genoemd wordt in een bericht waar je dus eerst voor moet inloggen.

Nog meer tips!

- Gebruik bij voorkeur niet je zakelijke (ggdwestbrabant.nl) e-mail adres voor social-media (zoals LinkedIn, facebook ed.)
- Let op wat je in je out-of-office bericht schrijft. Dergelijke berichten bieden criminelen ook vaak weer ene schat aan namen, telefoonnummers, perioden van afwezigheid e.d.

Blijf alert!

Archived: donderdag 12 mei 2022 11:44:02
From: [redacted]
Sent: maandag 8 februari 2021 11:04:48
To: [redacted]
Cc: [redacted]
Subject: Remaining questions re BCO Capacity Planning & data exports
Importance: Normal
Sensitivity: None

Beste collega's,

In de mail met als onderwerp 'Remaining questions re BCO Capacity Planning' staat een passage over **data exports**. Het is goed om daarover het volgende te weten.

Data exports door menselijk handelen zijn op basis van de behandeling in de Tweede Kamer van het datalek per direct:

- Toegewezen aan de rollen Administrator en HPZone Coördinator voor HPZone, en aan de rol van HPZone Coördinator binnen HPZone Lite
- Géén van de exports bevat nog BSN en NAW-gegevens anders dan postcode 6 (na correctie afgelopen vrijdag; was initieel nog postcode 4, werd vrijdag postcode 6)

Vriendelijke groet,
[redacted]

Van: [redacted]
Verzonden: maandag 8 februari 2021 09:08
Aan: [redacted]
CC: [redacted]
Onderwerp: FW: Remaining questions re BCO Capacity Planning

Hoi [redacted],

Kun jij aangeven wanneer jij [redacted] een antwoord hebt verzonden op onderstaande? We zitten te wachten op de oplevering en kunnen niet verder zo.

Met vriendelijke groet,
[redacted]

[redacted]

E-mail: [redacted]
Mobiel: [redacted]

Adres:
Zwarte Woud 2
3524 SJ Utrecht
www.ggdghor.nl

De uitbraak van het Coronavirus vraagt dat ook wij, in lijn met de maatregelen van de Rijksoverheid, zoveel mogelijk thuiswerken. U kunt mij goed bereiken via e-mail of via mijn mobiele telefoon.

Van: [redacted]
Verzonden: donderdag 4 februari 2021 11:24
Aan: [redacted]
CC: [redacted]
Onderwerp: Re: Remaining questions re BCO Capacity Planning

Dear [redacted]

Probably best to check with [redacted] re the latest restrictions.

Regards

[redacted]

On 4 Feb 2021, at 10:14, [redacted] wrote:

[redacted]

Could you please respond to [redacted]?

[redacted]: You which restrictions there currently are on export of data.
Please check if these restrictions are also applied on the export possibility in the new RFC.

Met vriendelijke groet,
[redacted]

[redacted].

<image001.jpg>E-mail: [redacted]

Mobiel: [redacted]

Adres:

Zwarte Woud 2
3524 SJ Utrecht
www.ggdghor.nl De uitbraak van het Coronavirus vraagt dat ook wij, in lijn met de maatregelen van de Rijksoverheid, zoveel mogelijk thuiswerken. U kunt mij goed bereiken via e-mail of via mijn mobiele telefoon.

Van: [redacted]
Verzonden: donderdag 4 februari 2021 11:11
Aan: [redacted]
CC: [redacted]
Onderwerp: Re: Remaining questions re BCO Capacity Planning

Dear [redacted]

Please could you confirm that UAT has been completed on all aspects of the RfC. Please could you also confirm if all screens and exports within this RfC have been checked in line with the new restrictions that we have been instructed to implement recently.

Regards
[redacted]

On 4 Feb 2021, at 08:28, [redacted] wrote:

Daear [redacted],

Testing has been done. Could you inform us when you can update the production environment?

Met vriendelijke groet,
[redacted]

[redacted]

<image001.jpg>

E-mail: [redacted]

Mobiel: [redacted]

Adres:
Zwarte Woud 2, 3524 SJ Utrecht
www.ggdghor.nl

De uitbraak van het Coronavirus vraagt dat ook wij, in lijn met de maatregelen van de Rijksoverheid, zoveel mogelijk thuiswerken. U kunt mij goed bereiken via e-mail of via mijn mobiele telefoon.

Van: [redacted]
Verzonden: woensdag 27 januari 2021 22:14
Aan: [redacted]
Onderwerp: Re: Remaining questions re BCO Capacity Planning

Dear All,

Please find attached the Release Notes for the new Capacity Planning functionality. This is now available on the UAT site for your verification.

We will wait to hear from you,

Regards

[redacted]

<image003.png>

On 19 Jan 2021, at 16:43, [redacted] wrote:

Good afternoon [redacted],

Please find our remarks in red. Could you please confirm that all is clear now and we can proceed to get this solution to production before the first of February?

Met vriendelijke groet,
[redacted]

<image001.jpg>

E-mail: [redacted]

Mobiel: [redacted]

Adres:

Zwarte Woud 2
3524 SJ Utrecht
www.ggdghor.nl

De uitbraak van het Coronavirus vraagt dat ook wij, in lijn met de maatregelen van de Rijksoverheid, zoveel mogelijk thuiswerken. U kunt mij goed bereiken via e-mail of via mijn mobiele telefoon.

Van: [redacted]
Verzonden: dinsdag 19 januari 2021 10:35
Aan: [redacted]
CC: [redacted]
Onderwerp: Re: Remaining questions re BCO Capacity Planning

Morning [redacted]

Thank you for the responses. We have gone through the responses and included our comments below. Please could you come back to us as soon as you can

Thanks

[redacted]

On 18 Jan 2021, at 19:42, [redacted] wrote:

> Good evening [redacted],
>
> Below you'll find our remarks on the remaining questions. Please let me know a.s.a.p. if there are any comments or questions from your side.
>
> A. Definitions for complexity, medium, high and very high
>
> *Medium: >5 contacts, Asymptomatic, Immunocomprimised, Vaccinated, Reinfection*
>
> *\fi708High: Health Professionals,, Elderly>70 years, Children <18 years, extramural, hospitalised*
>
> *\fi708 Very High: Language Issues, Intramural , Passed Away Index, Asylum Centre, Penitentiary, Food-Processing industry, Index living abroad*

inFact 19/01/21: We need succinct definitions for each category so that we can add

to the app. The above may confuse Users as each definition is a list of aspects which may change. Best to think of generic definitions to allow the GGDs to adapt more readily. Also, we suggested 4 categories, as you see below. This is because having 3 categories, will insight Users to sit on the fence and use Medium the majority of the time. It would be good to have a Routine category with an appropriate definition.

These are the definitions, it will not confuse users, this is part of our job. These are generic defnitions, please stop thinking for our users.

B. What to do with the status Completed

A case should be marked as Completed when BCO work has been done and monitoring (follow-up) will start.
The capacity planning view will not directly being used by the monitoring team since they can make an export of the active monitors / con trolpage.

inFact 19/01/21: The above does not really answer the question, which is when a Case is "Completed", what will happen to that Case in terms of Capacity Planning. In our concept, it will have to disappear from the Capacity Planning Matrix. Failing this, that matrix will continue to grow for ever and the whole matrix becomes unmanageable. So the question remains: If the Case is removed from the matrix - what is the process flow for it?

If the cases pops-up with our cross check's we'll change the status accordingly. Also, see "C".

C. Together with InFact we should think about a solution to 'remove' cases from the capacity planning view

Proposal: For the first version we think it would be good not show cases in this view when they have the status 'Closed' (lock is shown). Remark: In this way a case stays accessible via the capacity planning view for a longer time (14 days or more) because a case is being closed after follow-up has been executed. Because the capacity planning view is mostly being used for bulk assigning cases instead of a view to check if cases are closed. For a first release the export-possibilities from the dashboard will solve the problem (if there is any) that casefiles are shown longer in the dashboard. Does InFact has a proposal for this?

inFact 19/01/21: I am not sure if you are suggesting that we keep Cases which have been closed in the Capacity Planning Matrix? - possibly for 14 days? This will be problematic as the matrix will over populated (see above), plus the closed status is independent of Capacity Planning as the Status categories only includes Completed. We think that if the contact tracing of the Case has been 'Completed", then it should not stay in the Capacity Planning matrix. The "closure" of the Case is more related to the management of the Case and should be treated elsewhere from the Capacity Planning. Please could you kediscuss this as we are not clear about what your suggestion is in respect of this point.

*No this is exactly what we are **not** proposing: "For the first version we think it would be good not show cases in this view when they have the status 'Closed' (lock is shown)", overpopulation is not an issue since there are filter-possibilities, we disagree with your arguments and have thought this through.*

C. When are cases set to completed by accident

\fi708A cross check can be done by looking at the open actions (Follow-up // GP // Context actions etc should be open). Additionally a

cross-check on Osiris data (for example if this is "Gefiatteerd" the case should not be completed). This information can be accessed via the capacity planning view.

inFact 19/01/21: Are you suggesting that the User manually checks that the number of remaining Actions is 0 and is then free to check "Completed" for the Case. This is a good idea in principle. I dont think the checking of "Completed" should be made automatically as Users are highly likely to have closed certain actions or sent to Osiris by mistake and then the Case will disappear from the matrix. We will therefore go with the manual check.

Perfect.

D. How a case will be returned to a GGD

Case will be set to Completed

Not completed cases can be returned to GGD using the preset action: [[GGD]] BCO Terug naar GGD

inFact 19/01/21: From the above, we understand that we do nothing in this scenario as you are suggesting that the preset actions will take over.

Finally, there still remains the question below, if you could let us have an answer as soon as possible please

- What happens when a User non-intentionally has set the Index Status to "Complete" or "Index Not Accessible". In such scenario, we need to know what happens to the record as it will disappear from the capacity planning matrix.

This doesn't matter, since there are cross-checks as explained previously. Wel'l change the status back. Index Not accessible will just be marked as completed if we can't reach them.

Met vriendelijke groet,
[redacted]

[redacted]

<image001.jpg>

E-mail: [redacted]

Mobiel: [redacted]

Adres:
Zwarte Woud 2
3524 SJ Utrecht
www.ggdghor.nl

De uitbraak van het Coronavirus vraagt dat ook wij, in lijn met de maatregelen van de Rijksoverheid, zoveel mogelijk thuiswerken. U kunt mij goed bereiken via e-mail of via mijn mobiele telefoon.

Van: [redacted]
Verzonden: zondag 17 januari 2021 19:52
Aan [redacted]
Onderwerp: RE: Remaining questions re BCO Capacity Planning

Hi [redacted]

Thanks for your email.

You'll receive an answer tomorrow around 17:00 hour!

Met vriendelijke groet,
[redacted]

[redacted]

<image001.jpg>

E-mail: [redacted]

Mobiel: [redacted]

Adres:
Zwarte Woud 2
3524 SJ Utrecht
www.ggdghor.nl

De uitbraak van het Coronavirus vraagt dat ook wij, in lijn met de maatregelen van de Rijksoverheid, zoveel mogelijk thuiswerken. U kunt mij goed bereiken via e-mail of via mijn mobiele telefoon.

Van: [redacted]
Verzonden: vrijdag 15 januari 2021 14:18
Aan: [redacted]
CC: [redacted]
Onderwerp: Remaining questions re BCO Capacity Planning

Hi [redacted]

We urgently need your responses to the remaining questions below, as highlighted at the meeting on Tuesday. What happens when a User non-intentionally has set the Index Status to "Complete" or "Index Not Accessible". In such scenario, we need to know what happens to the record as it will disappear from the capacity planning matrix.

Definitions for routine, medium, high and very high Complexity What happened to a record with Status = Completed or Status = Index Not Accessible

Your early responses would be much appreciated

Regards

[redacted]

On 13 Jan 2021, at 18:15, [redacted]

Good evening [redacted]

Because the items about what to do with the status completed en how should a case be left out of the view are already on our list, we take your feedback about non-intentionally set a status to completed also into account.

Assigning a case back to the GGD will be done using the pre-set actions.

For now I would like you to inform us about a planning when the complete solution can be used in production. I asked for this this morning and really would like to receive this today since it is clear since Thursday that there are no big changes to the original design.

Hope to receive your answer as soon as possible. Best regards,

Met vriendelijke groet,
[redacted]

[redacted]

<image001.jpg>

E-mail: [redacted]

Mobiel: [redacted]

Adres:
Zwarte Woud 2
3524 SJ Utrecht
www.ggdghor.nl

De uitbraak van het Coronavirus vraagt dat ook wij, in lijn met de maatregelen van de Rijksoverheid, zoveel mogelijk thuiswerken. U kunt mij goed bereiken via email of via mijn mobiele telefoon.

Van: [redacted]
Verzonden: woensdag 13 januari 2021 10:23
[redacted]
Onderwerp: Re: Feedback on BCO Capacity Planning PPT **Urgentie:** Hoog

Hi [redacted]

I have just thought of something else we did not have time to discuss yesterday. Please could you also include in the list below feedback or confirmation on **Assign an Index Back to the GGD**.

Thanks

[redacted]

On 13 Jan 2021, at 08:27, [redacted] wrote:

Morning [redacted],

Please could you add to the list below the process flow for when a User non-intentionally has set the Index Status to "Complete" or "Cannot be contacted". In such scenario, we need to know what happens to the record as it will disappear from the capacity planning matrix.

Thanks

[redacted]

On 13 Jan 2021, at 08:24, [redacted] wrote:

Hi [redacted]
Thank you for your email. As agreed we'll provide the following input:

- Definitions for routine, medium, high and very high Answer the question about the
- status Completed Together with InFact we think about possibilities to remove cases
- from the capacityplanning view when BCO is completed

We would like to receive an planning today when the complete solution can be used in production.

Thanks in advance for your reply.

Met vriendelijke groet,
[redacted]

[redacted]

<image001.jpg>
E-mail: [redacted]
Mobiel: [redacted]

Adres: Zwarte Woud 2
3524 SJ Utrecht
www.ggdghor.nl

De uitbraak van het Coronavirus vraagt dat ook wij, in lijn met de maatregelen van de Rijksoverheid, zoveel mogelijk thuiswerken. U kunt mij goed bereiken via e-mail of via mijn mobiele telefoon.

Van: [redacted]
Verzonden: dinsdag 12 januari 2021 15:56
Aan: [redacted]
CC: [redacted]
Onderwerp: Re: Feedback on BCO Capacity Planning PPT

Hi [redacted]

Please find attached a copy of the PPT this afternoon - changes agreed at the meeting today are highlighted in red for your convenience

Regards

[redacted]

On 9 Jan 2021, at 11:44, [redacted] wrote:

Hi [redacted]

That's great - thank you. I look forward to hearing from you on Monday

Regards

[redacted]

On 9 Jan 2021, at 11:29 [redacted] wrote:

Hi [redacted],

Thanks for the quick response. I just went through all the highlight ed questions and think I can on Monday answer all of the together with [redacted].
I just need to check if we can manage a meeting in both our agenda's (which are a bit full fl), before Monday noon. Get back to you on that asap.

Met vriendelijke groet,

[redacted]

Van: [redacted]
Datum: vrijdag 8 januari 2021 om 14:53
Aan: [redacted]
CC: [redacted]
Onderwerp: Re: Feedback on BCO Cappacity PlanningPPT

Hi [redacted]

Thanks again for your very hard work meeting with 25 GGDs and capturin g essentia l info rmat ion for the Capacity Planning RfC. We are pleased to see that our solution design version 1 was not too far off the mark.

We have reviewed all the feedback for which we are grateful. Please find attached a document which provides answers to questions raised by the Capacity Planning Coordinators as well as Actions we would like you to help us with. Please could you do your best to let us your responses by noon Monday so that we have just enough time to include them in our present action on Tuesday . We have highlighted these actions in yellow for your convenience.
Best regards

[redacted]

On 7 Jan 2021, at 19:35, [redacted] wrote:

Dear [redacted]
Attached you 'll find the document with feedback from all 25GGDS (end-USerleVel). Overall response: 'happy with the proposal, when Can we Start wo r king with it I don't think that there are many changes needed on the original design. once developed and In use I think that there are a few Changes need to be made because Users only then Can experience what iS does and what's missing. If any questions please don't hesitate to Contact me. We'll meet next Tuesday to discuss the feedback!

BeSt regardS, MetVriendeliJke groet,
[redacted]

[redacted] <image003.Jpg> [redacted]

Mobiel: [redacted]
AdreS:ZwarteWoUd2
3524SJ, UtreCht
www.ggdghor.nl

De Uitbraak Van het CoronaVirUS Vraagt dat ook wiJ,in liJn met de maatregel en Van de RiJkSoVerheid, zoVeel mogeliJk thUiS werken. U kUnt miJ goed bereiken Via e-mail of Via mijn mobieletelefoon.

w w w . i n-f a c t. c o m |+44(0)1274585365

Van: [redacted]
Verzonden: maandag 4 JanUari 2021 18:12
Aan: [redacted]
CC: [redacted]
onderwerp: BCO CapaCity Planning PPT

Hi [redacted]
Please find attached the BCO Capacity Planning presentation.
Kind regards, [redacted]

In Fact Support Team |
support@infact.com<image004.png>infactukltd|**specialistsinpublichealthsoftwar**<image005.png>

Veelgestelde vragen en antwoorden over datadiefstal

Laatste update: 29 januari 2021 10.00 uur

Hier vindt u veelgestelde vragen en de antwoorden over de datadiefstal die recent heeft plaatsgevonden uit de systemen van de GGD. U kunt uw vraag vinden door te navigeren via de linker kolom.

We kunnen ons voorstellen dat de datadiefstal vragen oproept en mogelijk uw vertrouwen in ons heeft geschaad. Dit vinden wij heel erg. We willen u zo goed mogelijk informeren en daarom vullen wij deze veelgestelde vragen steeds aan met nieuwe informatie.

Er loopt op dit moment een politieonderzoek, waardoor we nog niet precies weten hoe groot de datadiefstal is. Ook mogen we bepaalde details nog niet delen, omdat dit mogelijk het onderzoek in gevaar brengt.

Heeft u een vraag die hier niet bij staat? Bel dan met ons speciale nummer: 085-1308226, elke dag bereikbaar van 9:00 uur tot 21:00 uur.

HOE ZIT HET ECHT? EEN REPLIEK

Top 3 meest gestelde vragen

Wat is er precies gebeurd?
Er zijn persoonsgegevens gestolen door medewerkers van de GGD. Deze gegevens gaan over het testen op het COVID-19-virus en mogelijk het bron- en contactonderzoek en bevatten onder andere naam, adres, BSN, telefoonnummer, e-mailadres, testuitslag en testlocatie. Of de gegevens ook zijn verkocht en om wiens gegevens het gaat, maakt deel uit van het politieonderzoek. Meer informatie is te vinden op de site van de politie

Zijn mijn gegevens gestolen?
Dat kunnen wij nu nog niet zeggen. Dit maakt onderdeel uit van het politieonderzoek. Op het moment dat vast komt te staan dat uw gegevens gestolen zijn, dan informeren wij u daar over.

Wat zijn de mogelijke gevolgen? Welk risico loop ik als criminelen mijn persoonsgegevens hebben? En waarop moet ik letten?

- U loopt het risico slachtoffer te worden van oplichting. Criminelen bellen of mailen u bijvoorbeeld uit naam van een voor u geloofwaardige instantie zoals uw bank. Ze zouden uw vertrouwen kunnen winnen, omdat ze persoonlijke informatie noemen (zoals uw geboortedatum of woonadres). Voordat u het weet, heeft u een betaling voor iets gedaan – maar feitelijk op een phishinglink geklikt. Ontdek hier hoe u zich kunt beschermen tegen phishing.
- Een ander risico is identiteitsfraude. De fraudeur gebruikt uw persoonsgegevens bijvoorbeeld om producten en diensten te krijgen op uw naam. Of om een bankrekening te openen of een creditcard aan te vragen. Ontdek hier meer informatie over identiteitsfraude.

- Activeer tweestapsverificatie op uw social media accounts, e-mail. Een overzichtelijke manier hoe u dit kunt inschakelen treft u hier aan.
- Maakt u gebruik van WhatsApp? Criminelen maken steeds vaker gebruik van de 'vriend in nood fraude'. Ons advies is om hier ook een extra beveiliging in te stellen. Hoe u dat doet leest u hier.

Doe altijd aangifte als u slachtoffer wordt van cybercrime.

Vragen over de datadiefstal

Hoe is GGD GHOR Nederland er achter gekomen dat er werd gehandeld in privégegevens afkomstig uit CoronIT
Naar aanleiding van vragen die ons zijn gesteld door een journalist van RTL nieuws.

Wat is er precies gebeurd?
Er zijn persoonsgegevens gestolen. Deze gegevens gaan over het testen op het coronavirus en mogelijk het bron- en contactonderzoek en bevatten onder andere naam, adres, BSN, testuitslag en testlocatie. Of de gegevens ook zijn verkocht en om wiens gegevens het gaat, maakt deel uit van het politieonderzoek. Meer informatie is te vinden op de site van de politie.

Hadden jullie dit zelf niet moeten ontdekken?
Wij controleren op verschillende manieren hoe onze medewerkers omgaan met de informatie in onze systemen. En dat leidt tot de ontdekking van onregelmatigheden en tot het nemen van maatregelen. Daarnaast beschermen we ons tegen aanvallen op onze systemen van buitenaf. Deze diefstal is in onze controles niet naar voren gekomen.

Wat hebben jullie gedaan na deze vragen?
We hebben meteen onderzoek ingesteld. Vervolgens contact opgenomen met de politie, aangifte gedaan en een melding gedaan bij de Autoriteit Persoonsgegevens. Vervolgens hebben wij zelf controles uitgevoerd in onze systemen én volledige toegang verstrekt aan de politie om de opsporing zo goed mogelijk plaats te kunnen laten vinden.

Welke privégegevens worden via welk medium/platform aangeboden?
Hierover kunnen wij voor nu geen uitspraken doen, dit is onderdeel van het onderzoek van politie en justitie.

Van hoeveel mensen zijn privégegevens verkocht? In welke periode?
Hierover kunnen wij voor nu geen uitspraken doen, dit is onderdeel van het onderzoek van politie en justitie.

Hoeveel GGD-medewerkers hebben in deze privégegevens gehandeld?
Hierover kunnen wij voor nu geen uitspraken doen, dit is onderdeel van het onderzoek van politie en openbaar ministerie.

Welke actie is genomen richting de betreffende medewerkers?
Er zijn in ieder geval twee medewerkers gearresteerd. Maar onderzoek van politie en justitie loopt. Zij zullen hierover communiceren zodra ze dat kunnen.

Vragen over systemen

Uit welke systemen is er sprake geweest van datadiefstal?
Het gaat om CoronIT. Dit is het administratiesysteem voor het testen en vaccineren en de communicatie hierover. Dus wanneer u een afspraak maakt voor een COVID-19-test via het callcenter, de COVID-19-test website of een arts, komen uw persoonsgegevens in CoronIT. Ook wanneer u een afspraak maakt voor een vaccinatie.

Daarnaast lijkt er ook sprake te zijn van diefstal van persoonsgegevens uit HPZone. We hebben vernomen dat gestolen persoonsgegevens worden aangeboden, maar hebben nog niet kunnen vaststellen dat ze feitelijk verhandeld zijn. Dat is onderwerp van het onderzoek dat de politie nu doet.

HPZone is een elektronisch dossier wat de GGD'en gebruiken om het bron- en contactonderzoek uit te voeren. Als iemand een positieve testuitslag heeft en deze gemeld wordt bij de GGD, dan wordt een dossier van deze persoon in HPZone aangemaakt.

Zijn mijn gegevens wel veilig bij jullie?
Geen enkel IT-systeem is onfeilbaar. De GGD doet alles wat in haar vermogen ligt om ervoor te zorgen dat gegevens van mensen die zich laten testen in veilige handen zijn. Daarom hebben we ook na dit incident maatregelen genomen. Om dit soort incidenten in de toekomst te voorkomen. Maar helaas kunnen we dit niet 100% uitsluiten. Hoe wij ervoor zorgen dat uw gegevens zo veilig mogelijk zijn, leest u bij het kopje ***Beveiliging***.

Zijn de systemen voor testen, bron- en contact onderzoek en vaccineren strikt gescheiden?
Gegevens van testen en vaccineren bevinden zich in CoronIT. De medische gegevens die bij vaccinaties worden vastgelegd zijn afgeschermd en niet zichtbaar voor medewerkers die zich met testen bezighouden. Wel is er een koppeling waardoor een testuitslag altijd te zien is, wanneer iemand in het systeem kijkt bij een vaccinatie afspraak. Dit is zo ingericht omdat het nodig kan zijn om te bepalen of iemand gevaccineerd kan worden.

De gegevens van het Bron- en contactonderzoek bevinden zich in HPZone.

Hoeveel Nederlanders staan er in CoronIT en HPzone?
In CoronIT staan gegevens van circa ca. 5,5 miljoen mensen. In HPZone van circa 1 miljoen

Hoeveel medewerkers hebben toegang tot CoronIT?
In totaal gaat dit om ca. 26.000 medewerkers. Zowel bij de GGD'en als bij bedrijven die gecontracteerd zijn voor de COVID-19-bestrijding.

Wat doen de medewerkers in CoronIT en HPZone?
Medewerkers van het callcenter die telefoontjes ontvangen kunnen via CoronIT testafspraken en vaccinatieafspraken maken. Verder kunnen de medewerkers die uitgaande telefoontjes plegen de testuitslagen zien, zodat ze die kunnen meedelen.
Bron- en contactonderzoekers leggen alle gegevens rondom een besmetting vast in HPZone.

CoronIT

Wat is er precies gestolen uit CoronIT?
CoronIT is het administratiesysteem voor het test- en vaccinatieproces. Het gaat daarbij om de

persoonsgegevens van losse personen. Niet om het downloaden van complete datasets. Er zijn twee verdachten gearresteerd op verdenking van het te koop aanbieden van persoonsgegevens uit de systemen die de GGD gebruikt voor de COVID-19 testen.

Is het normaal dat zoveel medewerkers toegang hebben tot deze gegevens? En waarom is dit nodig?
De GGD'en willen het COVID-19-virus zo goed mogelijk bestrijden. Daarbij zijn zeer veel medewerkers betrokken. Elke callcenter medewerker die telefoontjes aanneemt (inbound) moet afspraken kunnen maken. En iedere callcenter medewerker die mensen belt (outbound) moet uitslagen door kunnen gegeven als deze binnen zijn.

Wat doen we aan extra controles in CoronIT?
We verbeteren onze systemen continue. Aan de hand van dit incident hebben we wederom verdere aanscherpingen gedaan. We maken de mogelijkheden om te zoeken naar mensen in de systemen veel beperkter door de zoekfunctie aan te passen. De zoekacties die gedaan worden, worden gelogd. FOX IT doet op dit moment forensisch onderzoek naar onze logging (de handelingen die in het systeem verricht zijn). En tot de lancering van vol-automatisch en continu controleren eind maart, blijft FOX IT voor ons de loggings controleren. Zo proberen we verdacht gedrag te ontdekken. Bovendien hebben we een team dat 7 dagen per week handmatig verdachte handelingen opspoort.

Wat betekent het beperken van de toegang voor de toegankelijkheid van testen en bron- en contactonderzoek?
Beperkingen in toegang van mensen tot gegevens vertraagt de snelheid waarmee wij ons werk kunnen doen en verlengt de doorlooptijden. Bijvoorbeeld de snelheid waarmee we testuitslagen kunnen doorgeven en testafspraken kunnen maken.

HPZone

Waarom werken jullie (nog) met HPZone?
HPZone was het enige systeem dat voorhanden was om in maart 2020 in vliegende vaart aan de slag te gaan. We hebben aan het begin geconstateerd dat HPZone niet aan de eisen van deze tijd voldoet, hebben aanpassingen gepleegd, maar wisten ook dat een nieuw systeem nodig was.

We waren al bezig om over te gaan naar een nieuw, beter systeem. Dat zal versneld gaan gebeuren. Het exacte moment dat we overgaan kunnen wij nog niet noemen.

Wie heeft er allemaal toegang tot HPZone?
In HPZone hebben de eigen GGD-artsen en verpleegkundigen toegang en alle (tijdelijke) medewerkers die bron- en contactonderzoek doen.

Klopt het dat er datasets uit HPZone zijn aangeboden?
We hebben vernomen dat datasets worden aangeboden, maar hebben nog niet kunnen vaststellen dat ze feitelijk verhandeld zijn. Dat is onderwerp van het onderzoek dat de politie nu doet.

Hoe kan het dat er sprake is van het exporteren van een dataset?
In CoronIT kan dit niet. In HP Zone kon dit wel.
Om een goed beeld te hebben van de COVID-19 crisis maken GGD-epidemiologen rapportages op

basis van datasets. De meeste daarvan zijn anoniem en bevatten alleen aantallen. Daarnaast krijgen GGD'en als zij dat willen exports van de gegevens van mensen die in hun GGD-regio getest of gevaccineerd zijn, zodat zij die kunnen gebruiken voor het maken van rapporten voor bijvoorbeeld de gemeenten. De rechten worden beheerd door de GGD'en en de exports worden gelogd.

Klopt het dat die functie nu is uitgezet?
Ja, de belangrijkste export mogelijkheden hebben we uitgezet. We werken ook aan het aanpassen van alle overige exportmogelijkheden. De rechten voor gebruik van de resterende, benodigde exportfunctionaliteit zijn aan minder mensen toegekend op basis van beperktere rollen.

Wat betekent het afsluiten van deze export functie voor het werk van BCO-mensen?
Onder andere de werkverdeling is per direct lastiger geworden.

HP Zone en HP Zone Lite. Wat is het verschil?
HP Zone Lite is een variant van HPzone waarmee alleen COVID19 data beschikbaar wordt gesteld aan gebruikers.

Waarom hebben jullie HPZone Lite geïmplementeerd (in augustus)?
HPZone Lite is bedoeld om grote aantallen medewerkers makkelijk te laten werken aan bron- en contactonderzoek. In de eerste golf liepen GGD regio's over en konden andere GGD regio's hen niet helpen. Dat hebben we opgelost in HPZone Lite, door het systeem zo in te richten dat GGD'en elkaar wel konden helpen. hierdoor konden veel meer bron- en contactonderzoeker hun werk doen.

Kan een medewerker van GGD-regio Groningen in een bron-en contactonderzoek casus van GGD regio Utrecht?
Nee, in principe niet. Soms blijven bron- en contactmedewerkers toegang houden tot gegevens van GGD-regio's, waar ze eerder voor gewerkt hebben. Zodat ze snel weer kunnen inspringen als dit nodig is voor virusbestrijding.

Wat gaan jullie doen om de tijd tot de introductie van het nieuwe systeem wel veilig te overbruggen?
GGD GHOR Nederland heeft een gespecialiseerd bureau opdracht gegeven tot het in kaart brengen en realiseren van alle noodzakelijke wijzingen om het systeem te laten voldoen aan veiligheidseisen.

Persoonlijke gegevens

Welke informatie van mensen staat in Coronit en HP Zone?
In CoronIT staan onder andere naam, adres, woonplaats, telefoonnummer/e-mailadres, BSN, geslacht, geboortedatum, test- en/of vaccineerafspraken en testresultaten. Contra-indicaties en COVID-19 klachten.

In HPZone staan naam, adres, woonplaats, telefoonnummer, geslacht, geboortedatum en BSN van een persoon. Verder wordt in HPZone ook de informatie uit de bron- en contactonderzoek gesprekken vastgelegd. Dit is onder andere: noodzakelijke medische gegevens (bijvoorbeeld klachten/symptomen en huisarts), waar iemand is geweest en met wie hij/zij in contact is geweest. Ook wordt informatie vastgelegd van bron(nen) en nauwe contacten.

De gegevens zoals geregistreerd in CoronIT zijn opgenomen in de privacyverklaring CoronIT. Hetzelfde geldt voor HPZone, deze zijn terug te vinden in de privacyverklaring van bron- en contactonderzoek in het kader van COVID-19.

Waarom zijn mijn volledige persoonsgegevens en BSN nodig voor het maken van een testafspraak?
Volledige persoonsgegevens zijn nodig, zodat wij zeker weten dat wij een test of vaccinatie afspraak maken met de juiste persoon.

Het BSN is belangrijk, zodat in ons systeem automatisch de juiste persoonsgegevens geregistreerd worden in plaats van dat alle persoonsgegevens handmatig ingevoerd moeten worden (met het risico op administratieve fouten). Daarnaast is het BSN gekoppeld aan DigiD, wat het mogelijk maakt om de uitslag online in te zien. Het woonadres is nodig, zodat we de uitslag ook per brief kunnen toesturen indien er onverhoopt een verkeerd telefoonnummer is geregistreerd en daardoor iemand de uitslag niet heeft kunnen ontvangen.

Welke gegevens van een persoon kunnen de medewerkers inzien?
Dat hangt van de rol van de gebruiker af: De gebruiker ziet alleen die gegevens die hij of zij op dat moment voor zijn werk nodig heeft. Voor mensen die werken bij het callcenter dat testafspraken maakt zijn bijvoorbeeld de gezondheidsverklaringen die voor vaccinaties worden ingevuld niet zichtbaar. Registratie van bijwerkingen is alleen toegankelijk voor mensen met medische autorisatie.

Staan de gegevens van alle Nederlanders in CoronIT en HPZone?
Nee, in CoronIT staan alleen de gegevens van personen die een test of vaccinatie afspraak bij de GGD hebben gemaakt.

In HPZone staan alleen de gegevens van de personen die een positieve COVID-19 test hebben ontvangen en van mensen die als huisgenoot of als nauw contact uit bron- en contactonderzoek kwamen.

Beveiliging

Welke controle mechanismen hebben jullie om datadiefstal te voorkomen in Coronit en HP Zone?
Dat zijn er verschillende:

- Mensen moeten een Verklaring Omtrent het Gedrag (VOG) aanleveren en een geheimhoudingsverklaring ondertekenen. Daarmee is duidelijk dat ze aansprakelijk zijn op het moment dat zij zich niet aan de voorwaarden van de overeenkomst houden
- Privacy en geheimhouding zijn een doorlopend onderwerp van onze trainingen en tijdens gesprekken.
- Wij controleren het gebruik van onze systemen door de medewerkers, en hebben onze controles steeds verder verbeterd. Vanwege het belang van de virusbestrijding en de gevraagde snelheid zijn wij – op diverse manieren – met steekproefsgewijze controles van start gegaan. Specifiek over Coronit heeft de Autoriteit Persoonsgegevens ons in oktober

vragen gesteld. Deze hebben wij beantwoord, waarna er tot een paar dagen geleden geen aanvullende vragen zijn gesteld over de werkwijze. De manier waarop wij in Coronit en HPZone controleren verschilt. Dat komt door de technische mogelijkheden

- Alleen mensen die voor hun werk inzage moeten hebben in een persoonsdossier voor hun werk, mogen dit dossier inzien. Hierop controleren we zoals gezegd steekproefsgewijs. Bij niet voor het werk noodzakelijke inzage volgt ontslag en indien nodig aangifte. Enkele tientallen mensen zijn om die reden ontslagen.
- We verwachten we eind maart systemen te implementeren die automatisch en continue niet-noodzakelijke toegang controleren. Om zo verdacht gedrag op te sporen

Hoe gaat de GGD voorkomen dat de illegale handel van gegevens uit CoronIT en HPzone in de toekomst kan plaatsvinden?
We werken intensief samen met de politie om daders op te sporen en er voor te zorgen dat gegevens niet verder gedeeld kunnen worden. Daarnaast zijn we continu bezig om onze werkprocessen te verbeteren en de veiligheid van onze systemen te vergroten. Welke maatregelen we precies nemen kunnen we, omwille van de veiligheid, niet toelichten. Anders dan de maatregelen die we reeds noemen.

Testen

Kan ik me nog wel veilig laten testen?
Ja, het is belangrijk dat u zich laat testen, vaccineren en deelneemt aan bron- en contactonderzoek. De datadiefstal gaat om incidenten, waarbij we alles op alles zetten om daders aan te geven en voorzorgsmaatregelen te treffen. We zijn continu bezig om onze werkprocessen te verbeteren en de veiligheid van onze systemen te vergroten.

Ik heb een COVID-19 test gedaan bij een andere organisatie dan de GGD. Staan mijn gegevens nu ook in jullie systemen?
Als uw testuitslag negatief is niet. Als u een positieve testuitslag had, dan worden uw gegevens in HPZone opgenomen. Alleen positieve uitslagen zijn andere organisaties verplicht aan ons te melden.

Ik heb een test gedaan en was negatief. Sta ik dan ook in het systeem?
Als u zich bij de GGD heeft laten testen en de uitslag was negatief dan staat u in CoronIT. Als u zich bij een andere partij heeft laten testen en uw uitslag was negatief dan staat u niet in onze systemen.

Vaccineren

Kan ik me nog wel veilig laten vaccineren?
Ja, het is belangrijk dat u zich laat testen, vaccineren en deelneemt aan bron- en contactonderzoek. De datadiefstal gaat om incidenten, waarbij we alles op alles zetten om daders aan te geven en voorzorgsmaatregelen te treffen. We zijn continu bezig om onze werkprocessen te verbeteren en de veiligheid van onze systemen te vergroten.

Hebben evenveel mensen toegang tot mijn gegevens bij vaccineren als bij de COVID19-testen?
Gegevens van zowel testen en vaccineren bevinden zich in CoronIT. De medische gegevens die bij vaccinaties worden vastgelegd zijn afgeschermd en niet zichtbaar voor medewerkers die zich met testen bezighouden. Wel is er een koppeling waardoor een testuitslag altijd te zien is, wanneer iemand in het systeem kijkt bij een vaccinatie afspraak. Omdat dat nodig kan zijn om te bepalen of u gevaccineerd kunt worden.

Hoe helpen wij u?

Wat doet u om te voorkomen dat mensen van wie nu de gegevens in omloop kunnen zijn, geen slachtoffer worden van fraude?
We werken intensief samen met de politie om daders op te sporen en er voor te zorgen dat gegevens niet verder gedeeld kunnen worden. Verder proberen we op deze pagina tips te geven hoe men zich kan wapenen tegen cybercriminelen.

Op het moment dat vast komt te staan dat uw gegevens gestolen zijn, dan zullen wij u hierover informeren.

Kunnen jullie controleren of mijn gegevens gestolen zijn bij de datadiefstal?
Nee, dat kunnen wij op dit moment niet. De politie doet namelijk nog onderzoek naar welke gegevens gestolen zijn. Het is nu nog onduidelijk welke data er gestolen zijn en om wiens gegevens het gaat. Het is onze plicht om mensen te informeren als hun gegevens betrokken zijn bij datadiefstal. Maar daar valt nu helaas nog niets over te zeggen.

Kunnen mijn gegevens ook verwijderd worden uit jullie systemen nadat ik getest ben / er bron- en contact onderzoek heeft plaatsgevonden ?
U heeft het recht om een verzoek te doen tot verwijdering of anonimisering van uw gegevens. Let wel, met het anonimiseren of verwijderen van uw gegevens is het voor de GGD minder goed mogelijk om de verspreiding van het virus te monitoren of tegen te gaan.

Wilt u dit toch, dan is hier een procedure voor via uw regionale GGD. U kunt hiervoor contact opnemen met uw regionale GGD. U vindt deze contactgegevens op www.ggd.nl.

Ik wil een klacht indienen over de manier waarop jullie met mijn persoonsgegevens omgaan.
Dat kan. U kunt zich wenden tot onze functionaris gegevensbescherming via fg@ggdghor.nl.

Krijg ik een vergoeding als blijkt dat mijn data bij de datadiefstel zijn betrokken?
Daarover kunnen we nu nog niets zeggen. De politie doet op dit moment namelijk nog onderzoek naar de datadiefstal. Als het daadwerkelijk zou gaan om uw gegevens, wordt u hierover geïnformeerd.

Welk risico loop ik als criminelen mijn persoonsgegevens hebben? En waarop moet ik letten?
De website van de politie beschrijft de mogelijke gevolgen goed:

U loopt het risico slachtoffer te worden van oplichting. Criminelen bellen of mailen u bijvoorbeeld uit naam van een voor u geloofwaardige instantie zoals uw bank. Ze zouden uw vertrouwen kunnen winnen, omdat ze persoonlijke informatie noemen (zoals uw geboortedatum of woonadres). Voordat u het weet, heeft u een betaling voor iets gedaan – maar feitelijk op een phishinglink geklikt. Ontdek hier hoe u zich kunt beschermen tegen phishing.
Een ander risico is identiteitsfraude. De fraudeur gebruikt uw persoonsgegevens bijvoorbeeld om producten en diensten te krijgen op uw naam. Of om een bankrekening te openen of een creditcard aan te vragen. Ontdek hier meer informatie over identiteitsfraude.
Activeer tweestapsverificatie op uw social media accounts, e-mail. Een overzichtelijke manier hoe u dit kunt inschakelen treft u hier aan.
Maakt u gebruik van WhatsApp? Criminelen maken steeds vaker gebruik van de 'vriend in nood fraude'. Ons advies is om hier ook een extra beveiliging in te stellen. Hoe u dat doet leest u hier.

Doe altijd aangifte als u slachtoffer wordt van cybercrime.

Ik ben onlangs slachtoffer geworden van phishing/cybercrime. Kan dit komen doordat de GGD mijn gegevens had? En wat moet ik doen?
Als u slachtoffer bent van phishing/cybercrime, doe dan altijd aangifte op het politiebureau.
De politie doet op dit moment namelijk nog onderzoek naar welke gegevens gestolen zijn bij de GGD. Het is nu nog onduidelijk welke data er gestolen zijn en om wiens gegevens het gaat.

Wat kan ik doen als ik zie dat iemand online of via een chatdienst persoonsgegevens verkoopt?
Bel direct de politie op 0900 8844. Of anoniem op 0800 7000. Melding doen, heeft altijd zin. Hiermee voorkomt u slachtoffers en kan de politie direct verdachten opsporen en hun criminele praktijken stoppen.

Onze medewerkers

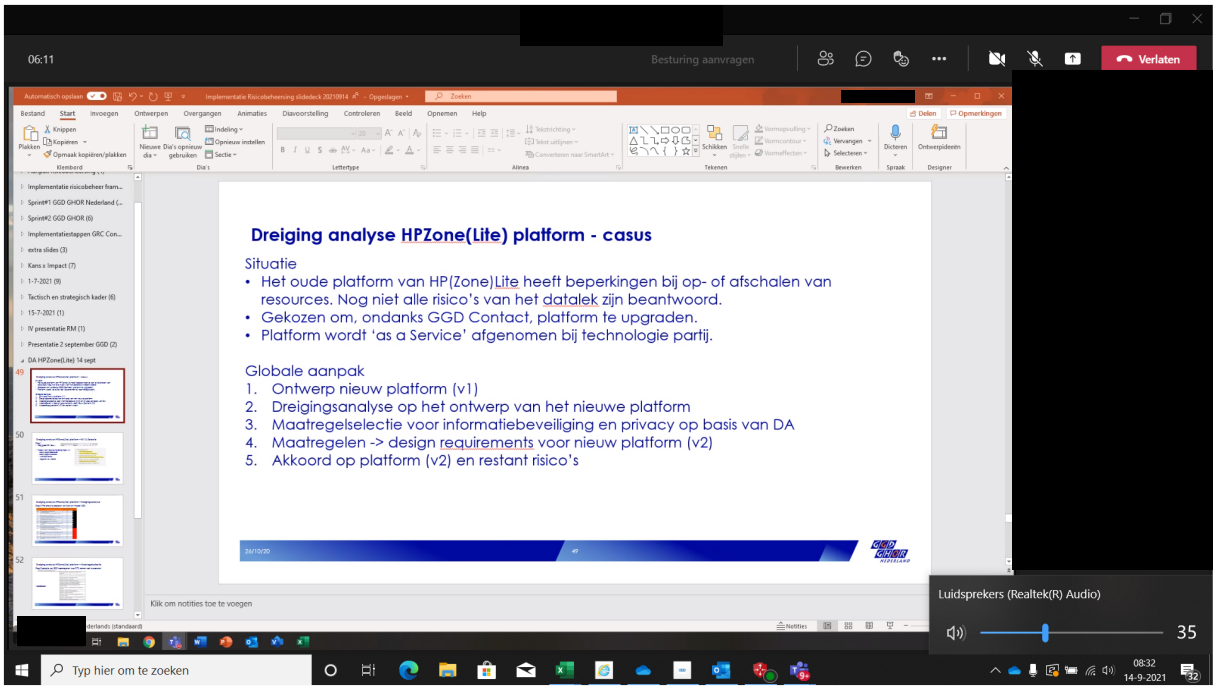
Klopt het dat u uw medewerkers verbiedt om te spreken met de pers of onder druk zet om dit niet te doen?
Nee, dit klopt niet. Wij staan alle pers te woord. Daarbij vragen wij onze medewerkers om in geval van persvragen contact op te nemen met onze persvoorlichters.

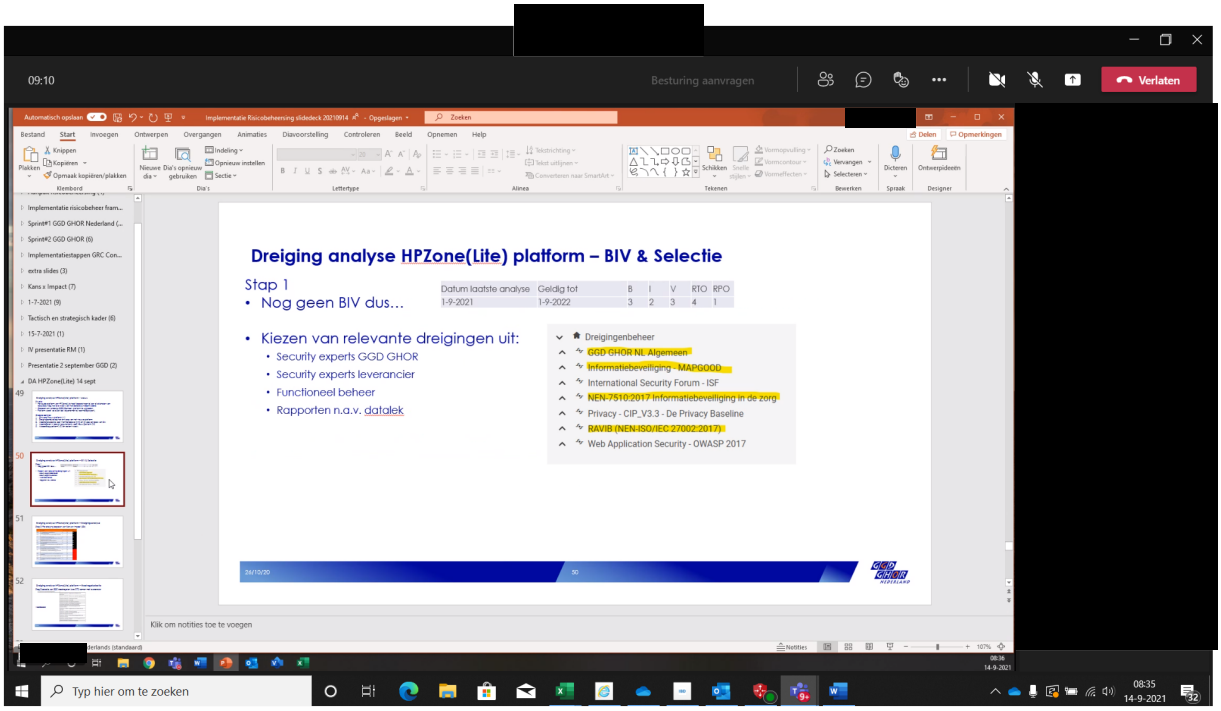
Klopt het dat u medewerkers boetes oplegt als ze naar buiten treden over hun werk?
Nee, dit klopt niet. Wel is het zo dat al onze medewerkers een geheimhoudingsverklaring ondertekenen. Dat doen we omdat onze medewerkers met gevoelige informatie zoals persoonsgegevens omgaan.

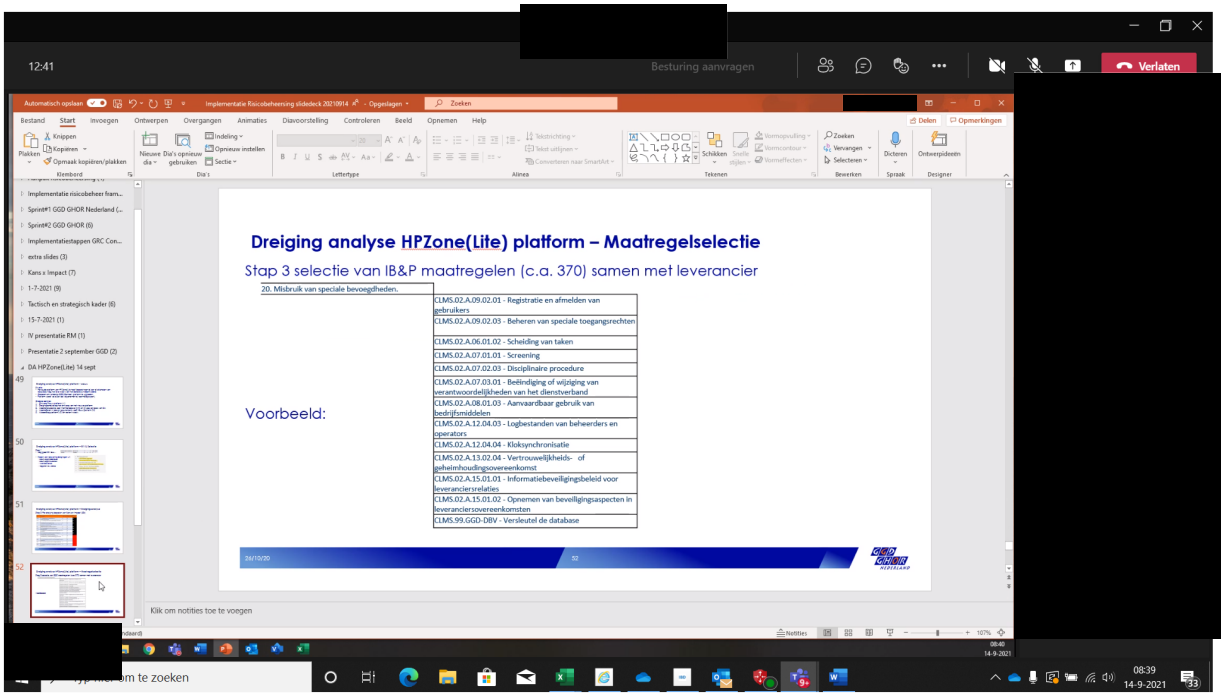
Contact

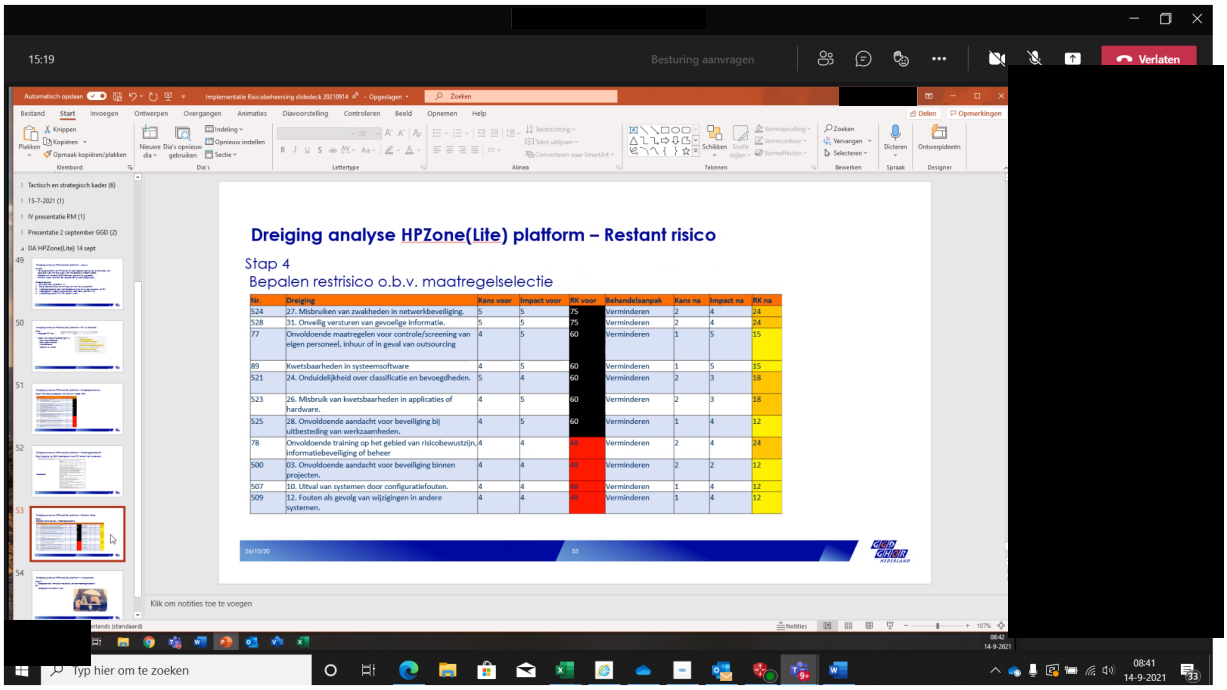
Met wie kan ik contact opnemen voor vragen en klachten?
Heeft u vragen dan adviseren wij u om deze lijst met veelgestelde vragen goed door te nemen. Zit

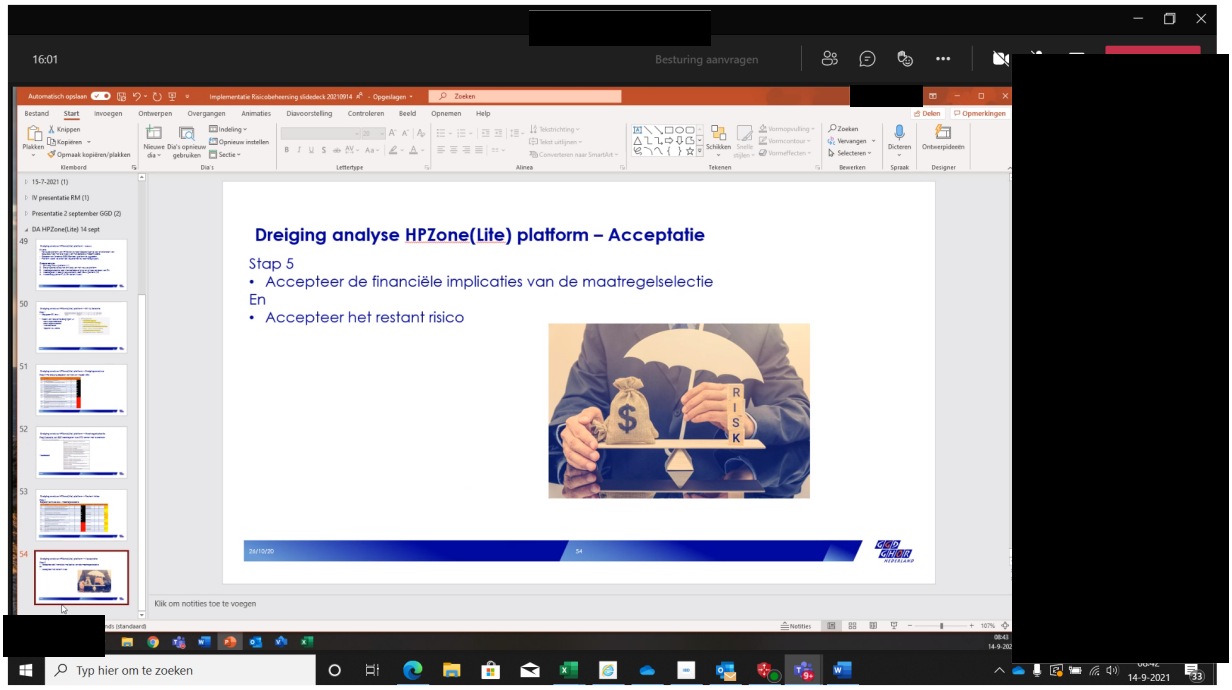
het antwoord op uw vraag er niet bij, neemt u dan contact op met het speciale nummer voor deze datadiefstal: 085-1308226 elke dag bereikbaar van 9:00u tot 21:00u.


06:11
Besturing aanvragen
Verlaten
Dreiging analyse HPZone(Lite) platform - casus
Situatie
• Het oude platform van HP(Zone)Lite heeft beperkingen bij op- of afschalen van resources. Nog niet alle risico's van het datalek zijn beantwoord.
• Gekozen om, ondanks GGD Contact, platform te upgraden.
• Platform wordt 'as a Service' afgenomen bij technologie partij.
Globale aanpak
1. Ontwerp nieuw platform (v1)
2. Dreigingsanalyse op het ontwerp van het nieuwe platform
3. Maatregelselectie voor informatiebeveiliging en privacy op basis van DA
4. Maatregelen -> design requirements voor nieuw platform (v2)
5. Akkoord op platform (v2) en restant risico's
Luidsprekers (Realtek(R) Audio)
35
Typ hier om te zoeken
08:32
14-9-2021


09:10
Besturing aanvragen
Verlaten
Dreiging analyse HPZone(Lite) platform – BIV & Selectie
Stap 1
• Nog geen BIV dus…
Datum laatste analyse | Geldig tot | B | I | V | RTO | RPO
1-9-2021 | 1-9-2022 | 3 | 2 | 3 | 4 | 1
• Kiezen van relevante dreigingen uit:
• Security experts GGD GHOR
• Security experts leverancier
• Functioneel beheer
• Rapporten n.a.v. datalek
Dreigingenbeheer
GGD GHOR NL Algemeen
Informatiebeveiliging - MAPGOOD
International Security Forum - ISF
NEN-7510:2017 Informatiebeveiliging in de zorg
Privacy - CIP_V3.3 - De Privacy Baseline
RAVIB (NEN-ISO/IEC 27002:2017)
Web Application Security - OWASP 2017
Klik om notities toe te voegen
Typ hier om te zoeken
08:35
14-9-2021


12:41
Besturing aanvragen
Verlaten
Dreiging analyse HPZone(Lite) platform – Maatregelselectie
Stap 3 selectie van IB&P maatregelen (c.a. 370) samen met leverancier
Voorbeeld:
20. Misbruik van speciale bevoegdheden.
CLMS.02.A.09.02.01 - Registratie en afmelden van gebruikers
CLMS.02.A.09.02.03 - Beheren van speciale toegangsrechten
CLMS.02.A.06.01.02 - Scheiding van taken
CLMS.02.A.07.01.01 - Screening
CLMS.02.A.07.02.03 - Disciplinaire procedure
CLMS.02.A.07.03.01 - Beëindiging of wijziging van verantwoordelijkheden van het dienstverband
CLMS.02.A.08.01.03 - Aanvaardbaar gebruik van bedrijfsmiddelen
CLMS.02.A.12.04.03 - Logbestanden van beheerders en operators
CLMS.02.A.12.04.04 - Kloksynchronisatie
CLMS.02.A.13.02.04 - Vertrouwelijkheids- of geheimhoudingsovereenkomst
CLMS.02.A.15.01.01 - Informatiebeveiligingsbeleid voor leveranciersrelaties
CLMS.02.A.15.01.02 - Opnemen van beveiligingsaspecten in leveranciersovereenkomsten
CLMS.99.GGD-DBV - Versleutel de database
Klik om notities toe te voegen
08:39
14-9-2021


15:19
Besturing aanvragen
Verlaten
Dreiging analyse HPZone(Lite) platform – Restant risico
Stap 4
Bepalen restrisico o.b.v. maatregelselectie
Nr. | Dreiging | Kans voor | Impact voor | RK voor | Behandelaanpak | Kans na | Impact na | RK na
524 | 27. Misbruiken van zwakheden in netwerkbeveiliging. | 5 | 5 | 75 | Verminderen | 2 | 4 | 24
528 | 31. Onveilig versturen van gevoelige informatie. | 5 | 5 | 75 | Verminderen | 2 | 4 | 24
77 | Onvoldoende maatregelen voor controle/screening van eigen personeel, inhuur of in geval van outsourcing | 4 | 5 | 60 | Verminderen | 1 | 5 | 15
89 | Kwetsbaarheden in systeemsoftware | 4 | 5 | 60 | Verminderen | 1 | 5 | 15
521 | 24. Onduidelijkheid over classificatie en bevoegdheden. | 5 | 4 | 60 | Verminderen | 2 | 3 | 18
523 | 26. Misbruik van kwetsbaarheden in applicaties of hardware. | 4 | 5 | 60 | Verminderen | 2 | 3 | 18
525 | 28. Onvoldoende aandacht voor beveiliging bij uitbesteding van werkzaamheden. | 4 | 5 | 60 | Verminderen | 1 | 4 | 12
78 | Onvoldoende training op het gebied van risicobewustzijn, informatiebeveiliging of beheer | 4 | 4 | 48 | Verminderen | 2 | 4 | 24
500 | 03. Onvoldoende aandacht voor beveiliging binnen projecten. | 4 | 4 | 48 | Verminderen | 2 | 2 | 12
507 | 10. Uitval van systemen door configuratiefouten. | 4 | 4 | 48 | Verminderen | 1 | 4 | 12
509 | 12. Fouten als gevolg van wijzigingen in andere systemen. | 4 | 4 | 48 | Verminderen | 1 | 4 | 12
24/10/20
53
Klik om notities toe te voegen
Typ hier om te zoeken
08:41
14-9-2021

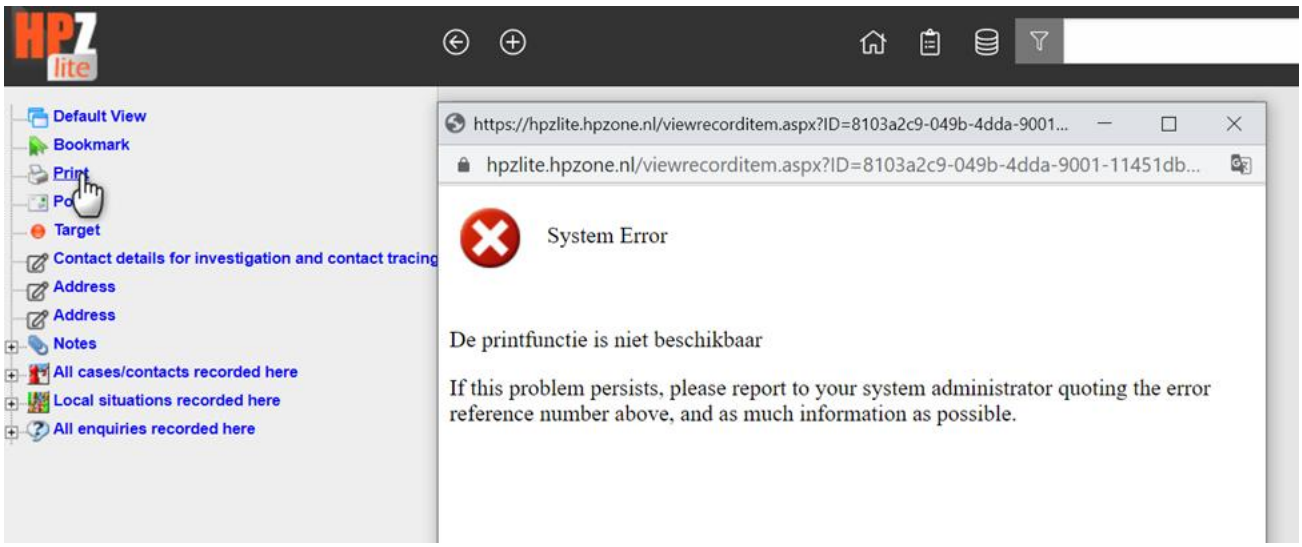

16:01
Besturing aanvragen
Dreiging analyse HPZone(Lite) platform – Acceptatie
Stap 5
• Accepteer de financiële implicaties van de maatregelselectie
En
• Accepteer het restant risico
R I S K
Klik om notities toe te voegen
Typ hier om te zoeken
14-9-2021

Archived: donderdag 12 mei 2022 11:44:10
From: [redacted]
Sent: vrijdag 5 februari 2021 10:57:58
To: [redacted]
Subject: Wijzigingen HPZone en HPZlite
Importance: Normal
Sensitivity: None
Attachments:
Adminstrative officer rollen.xlsx; Autorisaties HPZone.docx;

Goedemorgen heren,

Even een kort resumé m.b.t. de door GGDGhor uitgevoerde wijzigingen HPZone en HPZoneLite om toekomstige datalekken in de toekomst zoveel mogelijk te voorkomen:

1. Queriefunctie is uitsluitend nog beschikbaar voor de rollen 'Administrative Officer' en 'Coördinator' (in de bijlage een overzicht van personen binnen GGDWestbrabant
2. Alle tot op heden aanwezige custom queries binnen HPZLite zijn verwijderd;
3. Nieuwe queries mogen geen BSN en adresgegevens meer bevatten?! Je kunt nog wel een querie draaien, het exporteren ervan naar welk format dan ook en met of zonder 'core values' is niet meer mogelijk. [redacted]: geldt dit ook voor jou?!
4. Ook de 'print' functie in HPZLite is niet meer beschikbaar (zie screendump)



5. Wat mij betreft moet er nog aandacht komen voor de 'printscreen'-functie van de laptops. Deze zou beter kunnen worden uitgeschakeld. Echter is het met je telefoon nog altijd mogelijk een foto te maken van je scherm.
6. In de bijlage tevens een document met wat achtergrond informatie Infact mbt rollen en rechten.

Ik hoop jullie hiermee voldoende te hebben geïnformeerd, zo niet , laat me dit dan nog even weten.

Met vriendelijke groet,

[redacted]

[redacted]

GGD West-Brabant
E [redacted]

Doornboslaan 225-227, Breda

www.ggdwestbrabant.nl

www.brabantscan.nl

[redacted]

Aanwezig op: ma-di-wo-do-vr

Benieuwd naar de gezondheid van West-Brabanders? Bezoek dan de Brabantscan!

Wob-verzoek SOLV/ICAM datalek 2021 coronasysteem

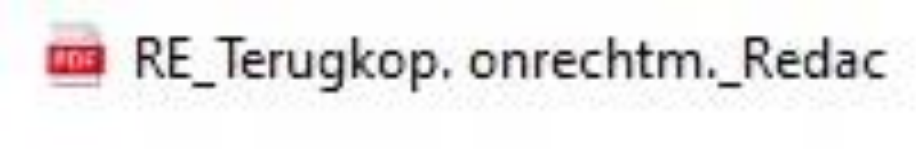
7.0 Tekst Wob-verzoek en register documenten

Tekst verzoek (vii)

Informatie over de verschillen in beveiliging tussen het reeds voor de coronacrisis bestaande systeem HPZone en het later ontwikkelde HPZone Lite.

Register

Een screenshot van de verkennerpagina van map 7:



Archived: donderdag 12 mei 2022 11:45:13
From: [redacted]
Sent: woensdag 31 maart 2021 11:14:43
To: [redacted]
Cc: [redacted]
Subject: RE: Terugkoppeling onrechtmatig inzage in HPZone dossiers
Importance: Normal
Sensitivity: None

Beste [redacted]

Bedankt voor de uitgebreide terugkoppeling.

Vooruitlopend op een eventueel uitgebreid advies van mijn zijde middels deze weg alvast een eerste korte reactie.

Is er sprake van een inbreuk in verband met persoonsgegevens ('datalek') als gevolg van een onrechtmatige verwerking i.c. een onrechtmatige inzage van een HP zone dossier?

Om te beoordelen of er eventueel sprake is van een (meldplichtig) datalek is het op de eerste plaats van belang dat je onomstotelijk bewijst dat de inzage in de HPzone dossier(s) door de betrokkene -rechtmatig- was.

Uit de terugkoppeling met betrekking tot bijvoorbeeld nummer [redacted] wordt dit niet direct duidelijk.

Ook het per ongeluk inzien van een medisch dossier waarbij er geen noodzaak bestaat kan kwalificeren als datalek en is in veel gevallen ook (wettelijk) meldplichtig.

Mijn aanbeveling is dan ook om per geval te analyseren of de inzage echt rechtmatig was. Mocht dit niet het geval zijn, of twijfel je hieraan, dan adviseer ik de inbreuk in verband met persoonsgegevens (zekerheidshalve) te melden aan de AP (Autoriteit Persoonsgegevens) via [redacted]

Opstellen en naleven 'procedure controle rechtmatigheid dossierinzage'

Mijn tweede aanbeveling zou zijn om te starten met het opstellen van een: 'procedure controle rechtmatigheid dossierinzage HP zone'.

Ingevolge artikel 5 lid 1 van het Besluit elektronische gegevensverwerking door zorgaanbieders (zie: https://wetten.overheid.nl/BWBR0040238/2020-10-01) is de GGD verplicht om stelselmatig en consequent te controleren op (onrechtmatige) toegang tot (medische) dossiers.

Doel van deze toekomstige procedure is dan ook om concrete handvatten te creëren voor het daadwerkelijk uitvoeren van controles op toegang tot dossiers en op deze wijze invulling te geven aan deze wettelijke verplichting.

Mede gelet op het grote aantal mensen dat (potentieel) toegang heeft tot de systemen is mijn advies hier prioriteit aan te geven.

In dit kader wil ik graag wijzen op de recente boete van 440.000 euro die recent is opgelegd aan het Onze Lieve Vrouwe Gasthuis in Amsterdam (zie: https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/boetebesluit_olvg.pdf)

Met name de passages vanaf pagina 9 ('controle op logging') zijn in dit kader interessant.

Mvg,

[redacted]

[redacted]

GGD West-Brabant RAV Brabant Midden-West-Noord

M: [redacted]

E: [redacted]

Wil je weten wat de privacywet (AVG) voor jou betekent? Kijk op hulpbijprivacy.nl#hulpbijprivacy

---

Van: [redacted]
Verzonden: woensdag 31 maart 2021 10:08
Aan: [redacted]
CC: [redacted]
Onderwerp: Terugkoppeling onrechtmatig inzage in HPZone dossiers
Urgentie: Hoog

Goedemorgen allen,

Gisteren heb ik [redacted] gesproken over de zorgen dat er medewerkers van BCO in reguliere IZB dossiers hebben gekeken/gezeten.

Afgesproken met [redacted] dat ik een verslag ervan maak ter terugkoppeling, zodat we het goed kunnen vastleggen.

Hierbij terugkoppeling wat we tot nu gedaan hebben en wat de bevindingen zijn:

- Op vrijdag 26-03-21 constateerde [redacted] dat er een aantal medewerkers van BCO in reguliere IZB dossier hebben gezeten. Dit is in HPZone zichtbaar via 'Change History'. Daar zie je wie wanneer iets wordt bewerkt in een dossier. In HPZone is niet te herleiden wanneer iemand alleen in een dossier heeft gekeken.
- Op vrijdag 26-03-21 en zaterdag 27-03-21 hebben [redacted] en ik bij de betreffende medewerkers van BCO nagevraagd waarom zij in de dossiers zaten.
- Hier onder opgesomd om wie het gaat, welk hpzone dossier het betreft, in het rood erachter zijn de reacties die we hebben verkregen van de medewerkers.
  - [redacted]: [redacted]: [redacted] heeft aan [redacted] gevraagd wat hij precies in dit dossier heeft gedaan. Hij heeft het dossier ontkoppeld van de situation. Deze hepatitis B index stond dan gekoppeld aan een Covid context/ situation. Ik heb gevraagd of hij dit voortaan in een event wil zetten. Dit gaat hij doen. [redacted] heeft bij [redacted] nagevraagd; zij kwam het dossier tegen toen ze een situation compleet aan het maken was, in het algemeen geeft ze aan dat het vaker voorkomt dat er in niet-Covid gerelateerde cases preset actions worden aangemaakt die dan bij BCO terecht komen. Afgesproken indien ze dit tegenkomt dat er een event wordt aangemaakt en benoemt waarom ze in het dossier zat en wat ze erin gedaan heeft.
  - [redacted]: [redacted]: heeft alleen in het dossier gekeken, niets veranderd.
  - [redacted]: [redacted]: Er stond een actie aangemaakt op WB dossier sluiten.
  - [redacted]: [redacted]: Er stond een actie aangemaakt op WB dossier sluiten.

- Bij de verpleegkundigen van team IZB die de reguliere meldingen doen heb ik bij [redacted] onder de aandacht gebracht dat zij géénn preset actions moeten gebruiken waar “LS” of “WB” voorstaan. Dit zijn acties die in het Covid proces terecht komen bij BCO
- In overleg met [redacted] hebben we direct aparte preset actions aangemaakt voor het reguliere IZB team, voor de preset action staat dan “IZB”.
- Om wat meer achtergrond te geven aan dit probleem… HPZone is inprincipe bedoelt voor reguliere IZB meldingen en HPZone Lite is gemaakt voor alle Covid meldingen. Echter bij BCO en vooral in het Clusterteam is het lastig dat niet alle functionaliteiten in HPZone Lite aanwezig zijn om het werk goed uit te voeren en clusters in beeld te krijgen. Dit maakt dat er diverse collega’s van BCO toegang hebben tot HPZone. Hieronder is een opsomming gemaakt waarom medewerkers van het clusterteam en MV-ers nog steeds toegang hebben tot HPZone. De redenen waarom medewerkers van het clusterteam in HPZone werken, gaan we nogmaals goed na, om kritisch te kijken of zij alsnog niet in HPZoneLite moeten gaan werken. Dat HPZone gebruiken gemakkelijker is, moet dan geen reden zijn om niet vanuit HPZoneLite te werken. Dus dit pakken we verder op.

HPzone vs. HPlite

1. In HPlite wordt de geschiedenis functie snel gesloten, hierdoor kan je erg moeilijk situations uitwerken, je moet dan namelijk telkens de betreffende dossiers opnieuw opzoeken
1. Niet reproduceerbaar, graag verduidelijken

2. Dit probleem is hetzelfde bij query’s, deze moet je telkens opnieuw uitdraaien in HPlite om erin te komen. Query’s draaien kan je terug naar history in HPzone, dit kan niet in HPlite want dan moet je hem opnieuw draaien
2. Niet reproduceerbaar, graag verduidelijken

3. Je kan geen contexten opzoeken op naam in Hplite
3. Waarom heb je dit nodig? Bij koppeling aan situation, zoek je vanuit situation. Wel is er een lijst beschikbaar met alle contexten van open cases.

4. Als je een nieuwe cluster aanmaakt kan je niet [redacted] aanklikken als ‘Manager’
4. Klopt, dit is nu opgelost.

5. Hoop query’s zijn niet zichtbaar in Hplite
5. Klopt, maar deze kunnen we zelf toevoegen wanneer nodig.

6. MV’ers moeten nog in adminstration hp kunnen om admin contexten aan te maken, daarnaast gebruiken wij dit wanneer er een verkeerde situation is verwijderd om die terug te halen.
6. Eens, MV'ers moeten in Hpzone/Administrator kant om dit te doen.

7. In HPlite kunnen wij de complete contextlijsten niet meer inzien.
7. In Hplite staan lijsten met alle contexten. Graag verduidelijken.

Mochten er nog vragen zijn n.a.v. mijn mail dan hoor ik dat graag.

[redacted] is mede betrokken om medewerkers van BCO de juiste rechten toe te kennen voor HPZone en HPZLite.

Met vriendelijke groet,

[redacted]

[redacted]

[redacted]

Team Infectieziekten
BIG-nummer: [redacted]

GGD West-Brabant

Doornboslaan 225-227
4816 CZ Breda

www.ggdwestbrabant.nl

085-0782979

[redacted]

Wob-verzoek SOLV/ICAM datalek 2021 coronasysteem

6.0 Tekst Wob-verzoek en register documenten

Tekst verzoek (vi)

Verslagen en notulen Regiegroep DOTT en Landelijke Coördinatiestructuur Testcapaciteit (LCT) met betrekking tot CoronIT en HPZone (Lite)

Register

Geen documenten aanwezig.

Wob-verzoek SOLV/ICAM datalek 2021 coronasysteem

9.0 Tekst Wob-verzoek en register documenten

Tekst verzoek (i)

Het gehanteerde beveiligings- of privacybeleid omtrent het omgaan met persoonsgegevens en datalekken in verband met testen, vaccineren en bron- en contractonderzoek, waaronder het beleid ten aanzien van toegangsrechten en autorisatiebeheer en logging en monitoring.

Register

Een screenshot van de verkennerpagina van map 9:

Beste [geanonimiseerd]

Een belangrijk aandachtspunt, waar ook de AP op wijst in haar eindbrief, is het maken van -duidelijke afspraken- op het vlak van informatiebeveiliging.
Het stuk wat er nu ligt geeft hier geen gevolg aan.

Het gaat hier om (in potentie) een grootschalige verstrekking van medische gegevens. Mijn klemmende advies is dan ook de beveiligingsafspraken te concretiseren en in lijn te brengen met het uitvoeringsbesluit van de Europese Commissie van afgelopen zomer (zie pagina 12 van het stuk dat is toegevoegd).

Op deze manier kan je in maart ook aan de AP rapporteren dat je op dit punt vooruitgang hebt geboekt.

Met vriendelijke groet,

[redacted]

GGD West-Brabant RAV Brabant Midden-West-Noord

M: [redacted]
E: [redacted]

Bijlage 2

Beveiligingsmaatregelen

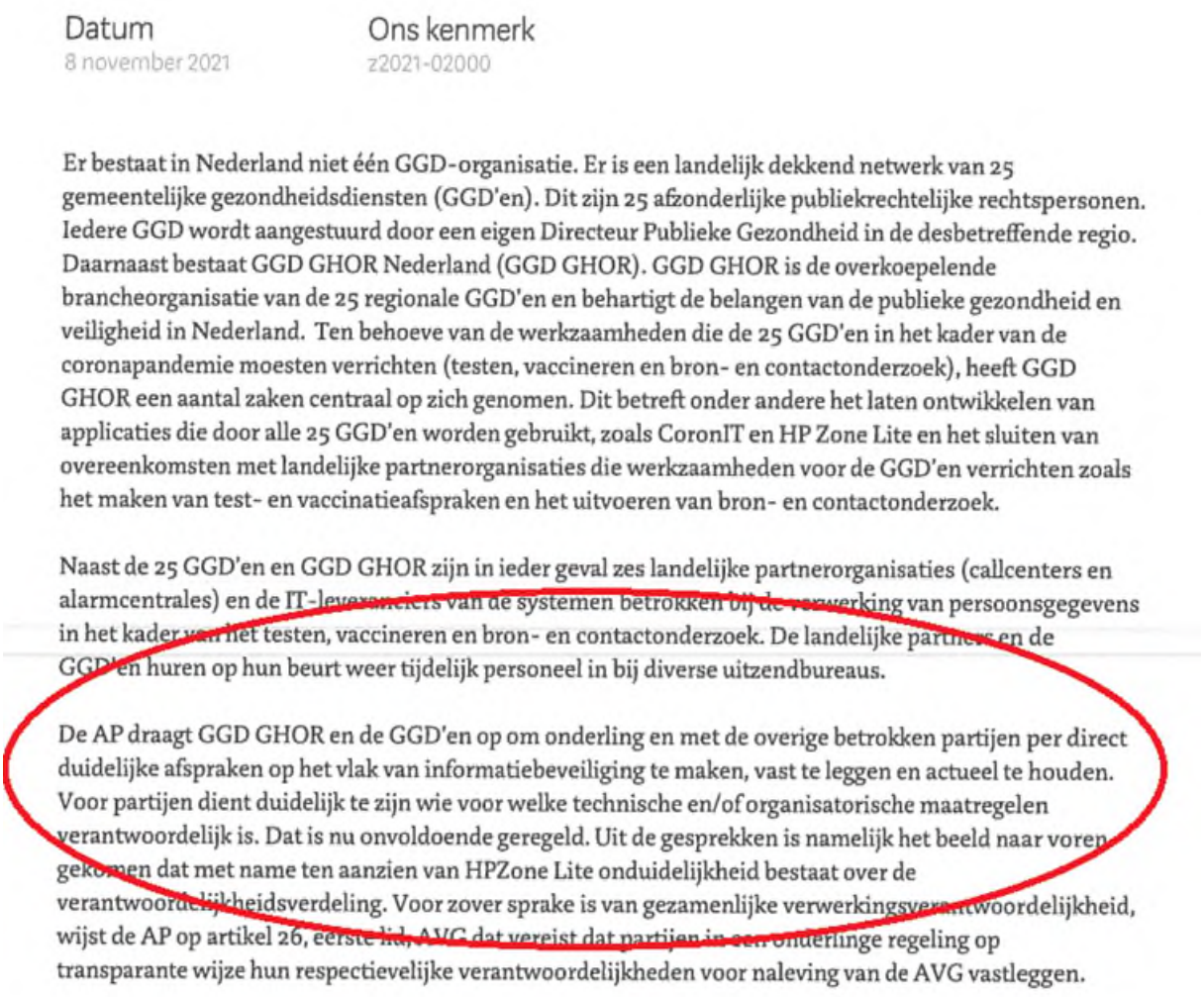
Verwerker werkt aantoonbaar in overeenstemming met IS027001 en NEN 7510 en heeft een passend, geschreven beveiligingsbeleid geïmplementeerd voor de verwerking van Persoonsgegevens, waarin in ieder geval de in het derde lid van dit artikel 2 genoemde maatregelen uiteen zijn gezet.

Indien een of meerdere van de hierboven genoemde normen wijziging ondergaat of wordt vervangen door een nieuwe norm, zal Verwerker vanaf het bekend worden van die nieuwe normering, de beveiliging van de Persoonsgegevens uitvoeren conform de nieuwe normering.

Verklaring van toepasselijkheid wordt op verzoek van de Verwerkingsverantwoordelijke toegezonden.

Verwerker voldoet aantoonbaar aan de veiligheidseisen voor netwerkverbindingen.

Verwerker voldoet aantoonbaar aan de eisen ten aanzien van logging.



Datum
8 november 2021

Ons kenmerk
z2021-02000

Er bestaat in Nederland niet één GGD-organisatie. Er is een landelijk dekkend netwerk van 25 gemeentelijke gezondheidsdiensten (GGD'en). Dit zijn 25 afzonderlijke publiekrechtelijke rechtspersonen. Iedere GGD wordt aangestuurd door een eigen Directeur Publieke Gezondheid in de desbetreffende regio. Daarnaast bestaat GGD GHOR Nederland (GGD GHOR). GGD GHOR is de overkoepelende brancheorganisatie van de 25 regionale GGD'en en behartigt de belangen van de publieke gezondheid en veiligheid in Nederland. Ten behoeve van de werkzaamheden die de 25 GGD'en in het kader van de coronapandemie moesten verrichten (testen, vaccineren en bron- en contactonderzoek), heeft GGD GHOR een aantal zaken centraal op zich genomen. Dit betreft onder andere het laten ontwikkelen van applicaties die door alle 25 GGD'en worden gebruikt, zoals CoronIT en HP Zone Lite en het sluiten van overeenkomsten met landelijke partnerorganisaties die werkzaamheden voor de GGD'en verrichten zoals het maken van test- en vaccinatieafspraken en het uitvoeren van bron- en contactonderzoek.

Naast de 25 GGD'en en GGD GHOR zijn in ieder geval zes landelijke partnerorganisaties (callcenters en alarmcentrales) en de IT-leveranciers van de systemen betrokken bij de verwerking van persoonsgegevens in het kader van het testen, vaccineren en bron- en contactonderzoek. De landelijke partners en de GGD'en huren op hun beurt weer tijdelijk personeel in bij diverse uitzendbureaus.

De AP draagt GGD GHOR en de GGD'en op om onderling en met de overige betrokken partijen per direct duidelijke afspraken op het vlak van informatiebeveiliging te maken, vast te leggen en actueel te houden. Voor partijen dient duidelijk te zijn wie voor welke technische en/of organisatorische maatregelen verantwoordelijk is. Dat is nu onvoldoende geregeld. Uit de gesprekken is namelijk het beeld naar voren gekomen dat met name ten aanzien van HPZone Lite onduidelijkheid bestaat over de verantwoordelijkheidsverdeling. Voor zover sprake is van gezamenlijke verwerkingsverantwoordelijkheid, wijst de AP op artikel 26, eerste lid, AVG dat vereist dat partijen in een onderlinge regeling op transparante wijze hun respectievelijke verantwoordelijkheden voor naleving van de AVG vastleggen.

Van: [geanonimiseerd]
Verzonden: donderdag 11 november 2021 12:59
Aan: [redacted]
Onderwerp: FW: Voorbereidende acties voor mogelijk in moeten zetten prio procedure BCO: verzoek ondertekening (eigen tekenblad bij de) verwerkersovereenkomst

Hartelijke groet,

[geanonimiseerd]

Van: [geanonimiseerd]
Verzonden: donderdag 11 november 2021 08:59

Aan: [geanonimiseerd]
CC: [geanonimiseerd]
Onderwerp: FW: Voorbereidende acties voor mogelijk in moeten zetten prio procedure BCO: verzoek ondertekening (eigen tekenblad bij de) verwerkersovereenkomst

Hoi collega's

Willen jullie voor ondertekening zorgen? En zorgen voor de verzending naar GGD GHOR (zie hieronder in geel) met ons in de cc.

Alvast bedankt

groeten
[geanonimiseerd]

Van: [geanonimiseerd]
Verzonden: donderdag 11 november 2021 08:46
Aan: [geanonimiseerd]
CC: [geanonimiseerd]
Onderwerp: FW: Voorbereidende acties voor mogelijk in moeten zetten prio procedure BCO: verzoek ondertekening (eigen tekenblad bij de) verwerkersovereenkomst

Goedemorgen allemaal,

Ter info onderstaande mail die gisteravond is verstuurd naar jullie DPG'en. De verwerkingsovereenkomst voor het inzetten van de mailservice van de prio procedure. Belangrijk dat deze ondertekend wordt als jullie hier gebruik van willen gaan maken.

Met vriendelijke groet,

[geanonimiseerd]
Corona organisatie GGD GHOR
[geanonimiseerd]

From: [geanonimiseerd]
Date: 10 November 2021 at 21:22:12 CET
To: Directie GGD GHOR Nederland <directie@ggdghor.nl>
Subject: Voorbereidende acties voor mogelijk in moeten zetten prio procedure BCO: verzoek ondertekening (eigen tekenblad bij de) verwerkersovereenkomst

Beste DPG-en,

De 'Prio Procedure BCO' is ontwikkeld om GGD'en handvatten te bieden als zij door zeer hoge besmettingsaantallen niet meer alle indexen eenmalig kunnen bellen in het kader van BCO. Het gaat dus om de situatie waarbij het acteren in fase 5 van het BCO niet meer mogelijk is. Onderdeel van de procedure is het verzenden van een beveiligde mail richting indexen waarin zij geattendeerd worden op hun besmetting en advies krijgen hoe zij virusverspreiding kunnen voorkomen. Ook wordt hen gevraagd het BCO voor te bereiden en

worden zij erop geattendeerd dat de GGD mogelijk geen tijd heeft om met iedere index contact op te nemen.

Het proces voor het verzenden van een beveiligde mail aan de index kan op verzoek van de regionale GGD worden gefaciliteerd door GGD GHOR Nederland. Wij vragen jullie akkoord op de verwerkingsovereenkomst die ten grondslag ligt aan dit proces. In de bijlage vinden jullie de betreffende verwerkingsovereenkomst en een oplegger met een nadere toelichting op de procedure. Tevens zijn tekenbladen per GGD toegevoegd. Het staat een GGD uiteraard vrij om te besluiten geen gebruik te maken van deze procedure en het informeren van indexen op een andere wijze te organiseren. Indien jouw GGD in geval van capaciteitstekort wel gebruik wil maken van het proces voor het verzenden van beveiligde mails verzoeken wij je om de het tekenblad van jouw GGD getekend retour te zenden aan: bcocorona@ggdghor.nl. Ook als je verwacht het nu niet nodig te hebben, is het advies om alles wel getekend en ingeregeld te hebben, zodat de procedure direct ingezet kan worden mocht het onverhoopt toch nodig blijken.

Met vriendelijke groet,

-

GGD GHOR Nederland
Zwarte Woud 2
3524 SJ Utrecht

E-mail [redacted]
Telefoon [redacted]
Website www.ggdghor.nl
Twitter@GGDGHORNL

Ministerie van VWS
Directie Publieke Gezondheid
[redacted]
Postbus 20350
2500 EJ DEN HAAG

Datum: 4 november 2020
Kenmerk: 20-088.AR
Betreft: **Doorgeven gegevens meldingsplicht A-ziekte**

Geachte [redacted]

Via deze brief verzoek ik u om een aantal acties, teneinde per direct en in de toekomst de doorlooptijd tussen een positieve besmetting met een meldingsplichtige infectieziekte in de categorie A en het daaropvolgende bron- en contactonderzoek (hierna: BCO) te minimaliseren, de werkdruk voor betrokken GGD'en te verkleinen en hiermee de slagkracht in de strijd tegen pandemieën (zoals de huidige SARS-CoV-2-pandemie) in algemene zin te vergroten. In deze brief schets ik in het kort een beeld van de huidige praktijksituatie waarmee alle GGD'en worden geconfronteerd. Vervolgens ga ik in op de achtergrond van deze situatie, met in het bijzonder aandacht voor het juridische kader. Tenslotte vraag ik u om een drietal acties in te zetten.

Actualiteit t.a.v. meldingen van positieve casussen
Momenteel leveren de GGD'en een maximale krachtsinspanning om zicht en grip op het virus te houden, onze kwetsbaren te beschermen en de zorgcontinuïteit te garanderen. Doorlopend wordt de capaciteit van testafnames en BCO opgeschaald en doen collega's alles wat binnen hun mogelijkheden ligt om landelijk en regionaal het virus in te dammen. Hoewel het aantal besmettingen in Nederland lijkt te dalen, is het bij alle GGD'en nog steeds alle hens aan dek. Ook het BCO staat onder druk; door het hoge aantal besmettingen zijn GGD'en genoodzaakt om het BCO in afgeschaalde versie uit te voeren. Momenteel is dus alle beschikbare (landelijke én regionale) BCO-capaciteit nodig om de ontwikkeling van het virus zo goed mogelijk in beeld te houden. Een effectief BCO is gebaat bij een aantal zaken, waarbij een snelle start cruciaal is om effectief te zijn. Ik ontvang vanuit (vrijwel) alle GGD'en signalen dat zij hierbij sterk gehinderd worden door het feit dat zij niet altijd de beschikking hebben over de juiste gegevens om een BCO op te starten; in het bijzonder gaat het hierbij om het ontbreken van een telefoonnummer. Deze situatie doet zich steeds vaker voor, vooral in gevallen waarbij positieve testuitslagen door (ziekenhuis)labs gemeld worden via een (al dan niet beveiligde) email aan de GGD'en. Indien een afspraak is gemaakt via coronatest.nl of via het landelijke callcenter, beschikt de GGD automatisch over de juiste gegevens – deze zijn immers uitgevraagd via de website of door de callcentermedewerker. Echter, we vernemen dat in (sterk) toenemende mate GGD'en via mail

geconfronteerd worden met positieve testuitslagen, zonder dat deze vergezeld worden door de verplichte en benodigde (contact)gegevens om een BCO op te starten.[1]
Op verzoek van het ministerie hebben wij een aantal GGD'en verzocht om meer in detail de praktijk en gevolgen van bovenstaande te schetsen. Een uitvraag bij 5 GGD'en leert dat de situatie zich wijdverbreid voordoet. Al deze GGD'en geven aan deze problematiek te herkennen, dat hiermee (spaarzame) menskracht verloren gaat aan de uitvraag van corresponderende (contact)gegevens en dat de start van het BCO (en quarantaine van eventuele nauwe contacten) hiermee vertraging oploopt. GGD'en omschrijven het onderzoek naar (contact)gegevens als een speurtocht, waarbij zij van het kastje naar de muur worden gestuurd, omdat laboratoria deze gegevens ook niet van de aanvragend arts hebben ontvangen. Vanaf het moment dat GGD'en de positieven ontvangen moeten zij contactpersonen, labmedewerkers, ondersteunend personeel of soms zelfs aanvragend artsen – allemaal eveneens drukbezet met hun primair proces – benaderen om gegevens te achterhalen. Op de vraag welk percentage van het aantal positieven zonder voldoende gegevens wordt aangeleverd konden 2 GGD'en een inschatting maken. Zij gaven daarbij aan dat ze vermoeden dat het om 10-20% (!) van de ontvangen positieve casuïstiek gaat.
De vertraging die door ontbrekende gegevens ontstaat loopt per regio en casus sterk uiteen. Een aantal GGD'en geeft aan dat het enkele dagen kost om deze gegevens te achterhalen. Soms kost het achterhalen van een enkel telefoonnummer een BCO-medewerker wel 3 uur. Eén grotere GGD geeft aan dat zij momenteel een lijst heeft van 600 indexen waarbij het BCO (nog) niet is opgestart. De gemiddelde tijd tussen ontvangst van positieve uitslagen en de start van het BCO is voor die groep mensen door het ontbreken van gegevens en de hierboven beschreven benodigde actie zelfs meer dan een week (met uitschieters daarboven).
GGD'en proberen op verschillende wijze deze vertraging het hoofd te bieden. Eén GGD heeft een senior medewerker opdracht gegeven doorlopend contact met laboratoria en ketenpartners te onderhouden, teneinde de samenwerking en doorgifte van gegevens te verbeteren. Alle GGD'en zijn (broodnodige) menskracht kwijt om deze gegevens te achterhalen – in de grotere regio's wordt zelfs gesproken over meerdere FTE's. Er zijn bij elke bevraagde GGD meerdere laboratoria die onvolledig zijn in de verstrekking van gegevens. In deze eerste uitvraag geven deze 5 GGD'en aan dat problemen spelen voor 1 tot 9 laboratoria per GGD, in totaal tenminste. Het gaat hierbij onder andere om ziekenhuislaboratoria, maar ook om medisch-microbiologische laboratoria waarbij de testaanvraag niet via CoronIT is gedaan.

Als tussenconclusie lijkt het mij veilig om te stellen dat deze situatie zeer onwenselijk is en contrair aan datgene wij gezamenlijk trachten te bereiken. Hieronder ga ik in op de bredere achtergrond van de discussie over de meldingsplicht, die uiteraard niet alleen voor de huidige pandemie geldt en al langer speelt.

Achtergrond

[1] Ter illustratie: 2 maanden geleden ontving GGD Rotterdam circa 10% van de positieve uitslagen via ZorgMail. Inmiddels is dit opgelopen tot circa 35%. Deze mails vragen handmatige verwerking, deze verwerking is dus foutgevoeliger én de mails zijn (veel) vaker onvolledig qua (contact)gegevens.

Er is al enige tijd een discussie over de gegevens die artsen-microbioloog en behandelaren moeten doorgeven aan de GGD in het kader van de meldingsplicht bij vaststelling (of vermoeden) van een meldingsplichtige infectieziekte in de categorie A, zoals het nieuwe coronavirus. Er worden op dit moment door het laboratorium alleen de persoonsgegevens zoals expliciet genoemd in de Wet publieke gezondheid (Wpg) gemeld, maar geen contactgegevens of diagnostische uitslag. Na melding moet vanuit de GGD ondanks de meldplicht voor hoofden van laboratoria en behandelend artsen nu eerst contact opgenomen worden met de behandelaar voor het verkrijgen van contactgegevens van de patiënt. Bij het bron- en contactonderzoek in het kader van een coronabesmetting levert dit in sommige gevallen een week vertraging op, hetgeen zeer onwenselijk is. Daarnaast worden op dit moment ook de specifieke meetresultaten niet gedeeld. Deze gegevens heeft de GGD nodig om een risico-inschatting te kunnen maken of en hoe besmettelijk een persoon is. Zeker als de GGD geen gegevens krijgt van een behandelend arts – die niet is aangesloten op CoronIT – is het van belang dat de GGD gegevens van het laboratorium krijgt.
Het gaat hierbij om meldingen die plaatsvinden binnen zorginstellingen, bij cliënten/patiënten en/of medewerkers of bezoekers. Dit betreft dus met name positieve uitslagen die gemeld worden buiten CoronIT om. In het geval een ziekenhuis zelf aangeeft contactonderzoek te doen en te testen, dan dient dit ook gemeld te worden bij de GGD. Bij het beschikbaar komen van sneltesten die weer andere diagnostische procedures kennen, wordt dit probleem nog pregnanter.
Deze discussie liep reeds vóór de coronacrisis in het kader van alle meldingsplichtige infectieziekten, maar is nu bijzonder urgent in het kader van het tijdig en effectief kunnen uitvoeren van bron- en contactonderzoek (BCO) en het snel indammen van het virus. Op dit moment worden bij meldingen door laboratoria geen contactgegevens aangeleverd, met als argument dat hier vanuit de Algemene Verordening Gegevensbescherming (AVG) geen juridische basis voor zou bestaan. Verschillende juristen hebben in verband met deze kwestie gekeken naar de Wpg en de AVG. De juridische teksten en aangeleverde argumenten zijn op dit punt echter multi-interpretabel.

Juridisch kader

De GGD heeft op grond van de Wpg de wettelijke taak om bron- en contactopsporing uit te voeren bij een aantal specifieke in de wet genoemde meldingen (artikel 6 lid 1 sub c Wpg).
In de huidige praktijk blijkt zoals gezegd dat bij een groot aantal (mogelijke) besmettingen in een grootschalige epidemie het tijdig en effectief uitvoeren van BCO zeer moeilijk is. Hiervoor is op zijn minst noodzakelijk dat de GGD over de relevante en noodzakelijke gegevens beschikt.

Volgens de wet moet een arts die bij een door hem onderzocht persoon *een A-infectieziekte* vermoedt of vaststelt (artikel 22 lid 1 Wpg) dit onverwijld melden aan de GGD, en bij die melding de volgende gegevens (artikel 24 lid 1 Wpg) doorgeven:

- de naam, het adres, het geslacht, de geboortedatum, het burgerservicenummer en de verblijfplaats van de betrokken persoon,

- de infectieziekte dan wel een beschrijving van het ziektebeeld, de eerste ziektedag, de vaccinatietoestand, het gebruik van chemoprofylaxe, de vermoedelijke infectiebron, de datum van vermoeden of vaststelling van infectie, de wijze van vaststelling van die infectieziekte, en
- indien nodig, of de betrokken persoon dan wel een persoon in zijn directe omgeving beroeps- of bedrijfsmatig betrokken is bij de behandeling van eet- of drinkwaren of bij de behandeling, verpleging of verzorging van andere personen.

Voor het doorgeven van 'andere medische gegevens' is in beginsel toestemming nodig van de betrokken persoon, ofwel een daartoe strekkend verzoek van de burgemeester of voorzitter van de veiligheidsregio (artikel 24 lid 4 Wpg).

Daarnaast moet volgens de wet (artikel 25 lid 2 Wpg jo. artikel 3 lid 1 sub a Regeling publieke gezondheid) het hoofd van een laboratorium – waar de arts een onderzoek heeft aangevraagd – de vaststelling van een *verwekker* van een A-infectieziekte onverwijld melden bij de GGD, en daarbij de volgende gegevens doorgeven:

- de naam van de arts, de naam, de geboortedatum en het burgerservicenummer van de betrokken persoon.

Contactgegevens

Bij BCO is van het grootste belang dat de GGD zo snel mogelijk contact kan opnemen met betrokkene(n). Dat vereist de directe contactgegevens van betrokkene(n), namelijk e-mailadres en telefoonnummer. Volgens de limitatieve opsomming in artikel 24, eerste lid, aanhef en onder a, van de Wpg bevat een melding geen directe contactgegevens, maar enkel het adres en het burgerservicenummer. Dat geldt evenzeer voor de melding van artikel 25, eerste lid, van de Wpg, al ontbreekt in die melding ook het adres. Dat maakt het in de praktijk, in het bijzonder vanwege het grote aantal (mogelijke) besmettingen, onmogelijk om direct en op korte termijn contact te zoeken.

Dit lijkt een lacune in de wetgeving. Bij de overgang van de oude Infectieziektenwet naar de huidige Wpg is aan de opsomming van de bij een melding te verstrekken gegevens het burgerservicenummer toegevoegd. Redenen daarvoor zijn bron- en contactonderzoek mogelijk maken en het bieden van een extra waarborg om de identiteit van betrokkene(n) te verifiëren. In de toelichting bij artikel 24 van de Wpg wordt verder genoemd dat, indien bepaalde gegevens niet bekend zijn bij de arts (bijvoorbeeld woon- of verblijfplaats, of burgerservicenummer), dit de melding niet hoeft te vertragen en de arts de gegevens dient te verschaffen die deze redelijkerwijs heeft kunnen achterhalen. Voorts wordt in de toelichting bij artikel 25 van de Wpg in dat verband gewezen op de centrale rol die het laboratorium (meer nog dan voorheen) speelt in de infectieziektebestrijding.

Gelet op het bovenstaande lijkt het in lijn met de bedoeling van de wetgever dat ook contactgegevens van betrokkene(n) mogen worden verstrekt aan de GGD en dat dit niet alleen beperkt hoeft te blijven tot het verstrekken van het burgerservicenummer maar dat ook telefoonnummer en e-mailadres kunnen

worden doorgegeven. Het vereiste toestemming vragen aan de patiënt (artikel 24 lid 4 Wpg) betreft dan enkel ‘andere medische gegevens’.

Diagnostische uitslag

In het kader van BCO is, naast de melding van de (vermoedelijke) vaststelling van (de verwekker van) de infectieziekte, ook van groot belang om de uitslag van het meetresultaat te kennen. Op basis hiervan is namelijk in te schatten in hoeverre een persoon besmettelijk is.

Op grond van artikel 24, eerste lid, aanhef en onder b, van de Wpg moet een melding – onder meer – bevatten ‘de wijze van vaststelling van de infectieziekte’. Daaronder moet in ieder geval worden verstaan de gebruikte testmethode. Of daaronder ook kan worden verstaan het concrete meetresultaat is minder evident, maar ligt wel in de rede. Het antwoord op de vraag of iemand (vermoedelijk) besmet is, is immers direct afhankelijk van het meetresultaat als uitkomst van het uitgevoerde onderzoek. Dit geldt evenzeer voor de melding ingevolge artikel 25, tweede lid, van de Wpg, die gaat over de vaststelling van de verwekker van de infectieziekte. Temeer omdat het hoofd van het laboratorium op grond van het vijfde lid van voornoemd artikel op verzoek van de GGD nader onderzoek moet verrichten naar de ziekteverwekker en de GGD van het resultaat op de hoogte moet stellen.

Wie heeft meldingsplicht?

Momenteel geldt de wettelijke meldingsplicht voor artsen, hoofden van laboratoria en hoofden van instellingen. Ook als het laboratorium heeft gemeld, heeft de aanvragend/ontvangend arts meldingsplicht en vice versa. De ‘dubbele’ melding van zowel behandelaar als laboratorium voorkomt dat belangrijke signalen te laat worden opgemerkt. Dit impliceert dat iedereen die geen arts, hoofd van een laboratorium of hoofd van een instelling géén wettelijke meldingsplicht aan de GGD heeft. Met het oog op de snelle ontwikkeling van nieuwe vormen van testen (waarbij geen laboratorium nodig is) en ook het commercieel beschikbaar zijn van diagnostische testen voor niet-artsen, kunnen hierdoor meldingen van positieve testen gemist worden. Iedereen kan testen immers aanbieden zonder tussenkomst van een arts of laboratorium en hoeft een positieve uitslag niet te melden. Hierdoor bestaat het risico dat besmettingen gemist worden en we zicht op het virus verliezen.

Via deze brief wil ik u vragen om op korte termijn de volgende onderstaande acties op te pakken:

1. Uitsluitsel en uitleg geven over de toepassing van wet- en regelgeving in het kader van het delen van gegevens

Er is behoefte aan uitsluitsel van het ministerie van VWS over de uitleg van de toepasselijke wet- en regelgeving. Concreet wie meldingplicht heeft en vervolgens welke gegevens aangeleverd moeten worden bij vaststelling of vermoeden van een SARS-CoV-2 infectie (of een andere meldingsplichtige infectieziekte), zonder dat daarbij vooraf toestemming is gevraagd aan de betrokkene(n).
Gelet op het tijdig en effectief kunnen uitvoeren van BCO, is voor de GGD noodzakelijk dat de volgende gegevens worden aangeleverd:

- Naam arts/naam behandelaar;
- De naam, het adres, het geslacht, de geboortedatum, het burgerservicenummer en de verblijfplaats van de betrokken persoon;
- (Indien bekend): functie van betrokkene: patiënt/bewoner/bezoeker/werknemer van afdeling;
- Contactgegevens: e-mailadres en telefoonnummer;
- Methode van vaststelling.

De wettelijke bepaling over de meldingsplicht van het laboratorium biedt de mogelijkheid aan de minister van VWS om nadere regels te stellen omtrent de wijze waarop de melding plaatsvindt (artikel 25 lid 6 Wpg). De minister zou in een algemene maatregel van bestuur kunnen bepalen welke aanvullende gegevens door het laboratorium moeten worden verstrekt. Een vergelijkbare vraag betreft de gegevens die een arts-behandelaar dient aan te leveren. De opsomming in artikel 24 lid 1 dient uitgebreid te worden met e-mailadres en telefoonnummer.

Doel van bovenstaand verzoek is om uitvoerende (lab)professionals in de keten gerust te stellen dat het delen van contactgegevens in lijn is met gewenste handelingsperspectief vanuit het ministerie, afgeleid vanuit de huidige beleidsdoelstellingen.

2. Betrokken medisch (lab)personeel en zorginstellingen attenderen op het verzoek (van GGD'en/VWS) om mee te werken aan het delen van contactgegevens te delen ten behoeve van een spoedige uitvoer van bron- en contactopsporing.

Contactonderzoeken van positieve patiënten en medewerkers en bezoekers verlopen vaak via de afdelingen infectiepreventie, die onder supervisie staan van de arts-microbiologen in het ziekenhuis. De GGD ontvangt idealiter via een beveiligde mail per index (bewezen positieve) de contactlijsten van de indexen. De GGD-adviezen richten zich met name op de thuissituatie van deze contacten. Op deze contactlijsten staan:

- Naam;
- Geboortedatum;
- Opnamestatus contact of functie;
- Contactgegevens: Telefoonnummer (indien mogelijk e-mailadres);
- Datum eerste/ laatste contact van "nauwe" contacten en "overige" contacten conform de LCI-richtlijn;
- Gegevens index.

Contactgegevens zijn voor het zo snel mogelijk opstarten van BCO het meest essentieel. Op dit moment vertraagt het niet aanleveren van contactgegevens door de ziekenhuizen en andere zorginstellingen onnodig het BCO. Vanwege de grote hoeveelheid meldingen is de urgentie van het snel aanleveren van bovengenoemde gegevens zeer hoog, om het contactonderzoek zinvol te kunnen uitvoeren binnen de daarvoor vastgestelde termijnen. Deze gegevens kunnen beveiligd gedeeld worden via ZorgMail.
Doel van dit verzoek is om uitvoerend medisch (lab)personeel in de keten daadwerkelijk te laten handelen in lijn met de gewenste doelen vanuit het testbeleid (zo snel mogelijk BCO opstarten).

3. Bovengenoemde uitwisseling van persoonsgegevens in kader van bron- en contactopsporing faciliteren door deze vast te leggen in wet- en regelgeving

Voor de infectieziektebestrijding in Nederland is het van groot belang dat ook voor andere infectieziekten in de WPG het delen van een bredere set (persoons)gegevens tussen laboratorium en GGD wettelijk wordt gefaciliteerd.

Doel van deze wetswijziging is om huidige en toekomstige bestrijding van infectieziekten te versoepelen.

Ten slotte

We zouden het zeer waarderen als het ministerie van VWS op zeer korte termijn aan ons verzoek tegemoet kan komen.

Mocht deze brief nog vragen oproepen, dan beantwoorden wij die uiteraard graag.

Met vriendelijke groet,

Gegevensbeschermingsbeleid GGD West-Brabant

Versie: 1.3
Classificatie: Intern
Datum: 2 januari 2020

Inhoud

2.1 Aard en positie van dit document 4
3.1 Aanleiding, ambitie en doelstellingen van het beleid 5
3.2 Begripsbepalingen 6
3.3 Juridisch kader 8
3.4 Doelgroep en toepassingsbereik 9
3.5 Inrichtingswijze gegevensverwerking 9
4.1 Rechten van betrokkenen 11
4.2 Recht op informatie en toegang tot gegevens 11
4.3 Recht op inzage en afschrift van gegevens 12
4.4 Recht op rectificatie (correctie, aanvulling) van gegevens 12
4.5 Recht op gegevenswissing 12
4.6 Recht op beperking van de verwerking 13
4.7 Recht op overdraagbaarheid van gegevens (dataportabiliteit) 13
4.8 Recht van bezwaar tegen verwerking 14
4.9 Recht niet te worden onderworpen aan geautomatiseerde individuele besluitvorming waaronder profilering 14
4.10 Klachten en vragen 14
4.11 Informeren van (keten)partners 14
4.12 Rechten en plichten aangaande het medisch dossier 15
5.1 Bewustwording 16
5.2 Verwerking van persoonsgegevens door derden 16
5.3 Documentatie over verwerking van persoonsgegevens 17
5.4 Informatiebeveiliging 18
5.5 Meldplicht voor inbreuken in verband met persoonsgegevens (datalekken) 19
5.6 DPIA’s (Data Protection Impact Assessments) 20
5.7 Beheer van persoonsgegevens 21
6.1 Functies en verantwoordelijkheden 24

1. Samenvatting

De GGD West-Brabant (hierna: “GGD”) verwerkt dagelijks veel gegevens over veel mensen. Bescherming van deze zogenaamde persoonsgegevens tegen oneigenlijk gebruik is noodzakelijk en evident maar tegelijkertijd niet altijd eenvoudig.

Met dit beleid vult de GGD nader in hoe zij uitvoering wenst te geven aan gegevensbescherming. Het document helpt om koers te bepalen, af te bakenen en te zien of er voldoende maatregelen zijn genomen om de persoonsgegevens te beschermen. Daarnaast wordt met naleving van dit beleid voldaan aan een wettelijke plicht en is het een manier waarmee de GGD aan zowel betrokkenen als de Autoriteit Persoonsgegevens toont dat de ze de Algemene verordening gegevensbescherming (“AVG”) naleeft.

Een beleid dat ziet op gegevensbescherming is niet nieuw, maar met de sinds de AVG een wettelijke verplichting voor organisaties die veel (bijzondere) persoonsgegevens verwerken, zoals de GGD.

Typisch vangt een gegevensbeschermingsbeleid aan met een antwoord op de vraag: ‘wat weet een organisatie allemaal over mensen en waarom?’. In dit geval is er voor gekozen om voor dit onderdeel te verwijzen naar het ‘register van verwerkingsactiviteiten’ van de GGD als losstaand document.
Dit document vangt aan met de wijze waarop mensen invloed kunnen uitoefenen of grip kunnen krijgen op (verwerking van) hun persoonsgegevens bij de GGD. Dit wordt ook wel ‘de rechten van betrokkenen’ genoemd.
Voorts worden de (verplichte) procedures en maatregelen beschreven die de GGD hanteert om invulling te geven aan de plichten uit de AVG. Hierbij wordt achtereenvolgens stilgestaan bij:

- bewustmaking van het personeel;
- (contractuele) afspraken bij (het inschakelen van) andere partijen;
- de (verplicht) aan te leggen documentatie;
- (technische én organisatorische) beveiliging van persoonsgegevens;
- (het melden van) datalekken;
- het uitvoeren van risicoanalyses bij verwerking van persoonsgegevens (DPIA’s) en
- het beheer van persoonsgegevens.

Er wordt afgesloten met het vastleggen van de ‘governancestructuur’ op het vlak van gegevensbescherming. Hierbij worden de rollen, taken en verantwoordelijkheden die betrekking hebben op de naleving van de bepalingen uit dit beleid nader uitgewerkt.

2. Inleiding

Op 25 mei 2018 trad de Algemene verordening gegevensbescherming (hierna: “AVG”) in werking. Dat betekent dat vanaf die datum dezelfde privacywetgeving geldt in de gehele Europese Unie. Lidstaten hebben slechts zeer beperkte vrijheid om aanvullende regelgeving vast te stellen. De Nederlandse wetgever bereidde daarvoor de Uitvoeringswet AVG (hierna: “UAVG”) voor. Feitelijk gaat het om modernisering van de wetgeving, die een kans biedt om maatschappelijk vertrouwen in technologie te versterken. Ook stelt het organisaties in de gelegenheid om de beveiliging van waardevolle gegevens te verbeteren en zo te komen tot een ‘AVG- proof’ werkomgeving.

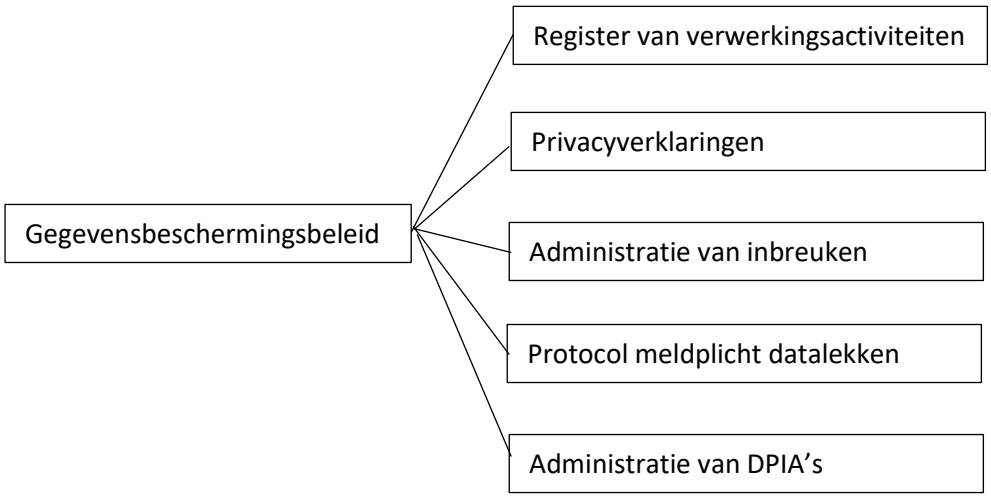
De AVG is dus een verplichting en wel één die ons in positieve zin uitdaagt om een stevige ambitie uit te spreken over het gegevensbeschermingsniveau van zowel cliënten, medewerkers als (keten)partners. Betrokkenen moeten er te allen tijde op kunnen vertrouwen dat hun gegevens bij ons in veilige handen zijn. Daarnaast is ook de samenleving kritischer en veeleisender geworden ten aanzien van de wijze waarop met gevoelige informatie wordt omgegaan.

Het beschermen van privacybelangen wordt vaak gezien als obstakel bij het uitvoeren van werkzaamheden, omdat moet worden getoetst of aan de privacywetgeving wordt voldaan. Maar privacy is een belangrijk grondrecht. In de Grondwet is verankerd dat de overheid niet zomaar persoonlijke gegevens mag gebruiken. Het is een wettelijke verplichting dat de GGD behoorlijk en zorgvuldig omgaat met persoonsgegevens in verband met de privacy van betrokkenen.

Deze ambitie heeft een vertaalslag gekregen in dit beleid en is nader uitgewerkt in onze strategische (beleids)uitgangspunten, een governancestructuur en onderliggende protocollen en werkafspraken.

2.1 Aard en positie van dit document

Dit beleid stelt de algemene kaders vast waarbinnen de GGD gegevensbescherming regelt. Het is een kapstokbeleid dat de basis is voor de uitwerking van alle aspecten van onze bedrijfsvoering, zowel binnen als buiten de organisatie, voor zover daarbij sprake is van de verwerking van persoonsgegevens.
Onderstaand schema toont de relatie van dit beleid met andere documenten.



Om het mogelijk te maken de hoofdstukken ook los van elkaar te lezen komt het incidenteel voor dat begrippen meer dan eens geduid worden.

3. Uitgangspunten

3.1 Aanleiding, ambitie en doelstellingen van het beleid

Binnen de GGD werken we veel met persoonsgegevens: van burgers, medewerkers en (keten)partners. Deze verzamelen we voornamelijk voor het goed uitvoeren van onze taak zoals op gesloten in de Wet publieke gezondheid (hierna: “Wpg”) of de Wet maatschappelijke ondersteuning 2015 (hierna: “Wmo”). Men moet er op kunnen vertrouwen dat wij zorgvuldig en veilig met persoonsgegevens omgaan.
Nieuwe technologische ontwikkelingen, innovatieve voorzieningen, globalisering en een steeds meer digitale overheid stellen andere eisen aan de bescherming van gegevens en privacy. De GGD is zich hier van bewust en zorgt dat de privacy gewaarborgd blijft, onder andere door maatregelen te treffen op het gebied van informatiebeveiliging, dataminimalisatie, transparantie en gebruikerscontrole.

Directe aanleiding voor dit beleid is de inwerkingtreding van de AVG. De AVG staat voor een versterking en uitbreiding van privacyrechten en meer verantwoordelijkheden voor organisaties. De bevoegdheden van de Europese toezichthouders, voor Nederland de Autoriteit Persoonsgegevens (hierna: “AP”), zijn uitgebreid. Een voorbeeld is de bevoegdheid om boetes tot €20 miljoen op te leggen.

De GGD heeft de ambitie, maar ook de wettelijke verplichting om zoveel mogelijk te voldoen aan de (kwaliteits)eisen voor gegevensbescherming uit de AVG. Wij stellen burgers, medewerkers en (keten)partners centraal en vinden dat ze moeten kunnen vertrouwen op een veilige verwerking van persoonsgegevens. Niet alleen vanwege de wettelijke verplichting en het risico op handhaving, maar juist omdat de GGD veel waarde hecht aan de bescherming van de persoonlijke levenssfeer van betrokkenen.
Daarnaast ambieert de GGD een actief gegevensbeschermingsbeleid, dat vooral gericht is op bewustwording, een transparante en kritische cultuur en kennisoverdracht. Bovendien willen wij medewerkers en klanten zoveel mogelijk betrekken bij het onderwerp gegevensbescherming en de bijbehorende dilemma’s. Goede, transparante communicatie met burgers is daarom van groot belang.
De GGD geeft met dit beleid duidelijk richting aan hoe er moet worden omgegaan met privacy en laat zien dat zij de bescherming van persoonsgegevens waarborgt en handhaaft. De GGD wil hiermee onder andere bereiken dat:

- de basis voor een goed geïmplementeerd beleid op het gebied van gegevensbescherming wordt gegarandeerd en dat alle medewerkers zich ten volle bewust zijn van de noodzakelijkheid van een zorgvuldige omgang met persoonsgegevens. Dit vormt de basis voor een toepassing van de wettelijke eisen en voor een respectvolle omgang met de persoonsgegevens van betrokkenen;
- de rechten van betrokkenen worden gerespecteerd en in procedures zijn verankerd;
- het vertrouwen van betrokkenen in de zorg en overheid niet wordt beschaamd;
- uitvoering van dit beleid binnen de GGD gericht wordt opgepakt, zodat de wettelijke eisen goed geïmplementeerd zijn;
- het onderwerp zowel op bestuurlijk- als medewerkersniveau breed wordt gedragen, als onderdeel van zowel uitvoering van de wettelijke opgave, goed werkgeverschap, opdrachtnemer- en opdrachtgeverschap;
- de kans op financiële schade door het oplopen van boetes en reputatieschade voor de GGD wordt geminimaliseerd en bijbehorende risico’s worden beheerst.

3.2 Begripsbepalingen

Accountability (verantwoordingsplicht)
Het kunnen aantonen op welke manier de persoonsgegevens worden verwerkt conform de AVG. Hiertoe dienen passende en effectieve maatregelen te worden genomen, zoals:

- documentatieplicht: het bijhouden van een register van verwerkingen;
- het beschermen van gegevens door ontwerp principes als Privacy by Design en Privacy by Default;
- indien voorkomende gevallen: het uitvoeren van een Data Protection Impact Assessment ("DPIA");
- het treffen van passende technische en organisatorische maatregelen, waaronder juridische en beveiligingsmaatregelen;
- het opstellen van een procedure om beveiligingsincidenten en datalekken te documenteren, alsmede een procedure voor het melden van een datalek aan AP;
- het aanstellen van een Functionaris Gegevensbescherming.

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

Autoriteit Persoonsgegevens
De Autoriteit Persoonsgegevens ("AP") staat voor het grondrecht op bescherming van persoonsgegevens. De AP is de toezichthoudende autoriteit verantwoordelijk voor het toezicht op de toepassing van de Verordening teneinde de grondrechten en fundamentele vrijheden van natuurlijke personen in verband met de verwerking van hun persoonsgegevens te beschermen en het vrije verkeer van persoonsgegevens binnen de Unie te vergemakkelijken.

Betrokkene
Degene op wie de persoonsgegevens betrekking hebben.

Big data
Een of meer datasets, zowel ongestructureerd als gestructureerd, die door middel van koppeling of hergebruik geschikt zijn voor analyse doeleinden, zoals bijvoorbeeld beleidsonderzoek, gedragsonderzoek, of (medisch) wetenschappelijk onderzoek.

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

DB
Het Dagelijks Bestuur van de GGD West-Brabant.

Derde
Een natuurlijke persoon of rechtspersoon, een overheidsinstantie, een dienst of een ander orgaan, niet zijnde de betrokkene, noch de verwerkingsverantwoordelijke, noch de verwerker, noch de personen die onder rechtstreeks gezag van de verwerkingsverantwoordelijke of de verwerker gemachtigd zijn om de persoonsgegevens te verwerken.

Functionaris voor gegevensbescherming

De functionaris voor gegevensbescherming (hierna: “FG”) is de interne toezichthouder op de verwerking van persoonsgegevens. De FG dient in alle onafhankelijkheid zijn werkzaamheden te kunnen uitvoeren en ontvangt daarbij geen instructies van opdrachtgevers of verwerkers. Hij is aangemeld bij de AP als contactpersoon en aanspreekpunt bij de meldingen van datalekken. Hij functioneert als tussenpersoon tussen verschillende belanghebbenden en is daarmee ook verlengstuk van de AP.

Geautomatiseerde (individuele) besluitvorming en profilering
Elke vorm van geautomatiseerde verwerking van persoonsgegevens waarbij aan de hand van persoonsgegevens bepaalde persoonlijke aspecten van een natuurlijke persoon worden geëvalueerd, met name met de bedoeling zijn beroepsprestaties, economische situatie, gezondheid, persoonlijke voorkeuren, interesses, betrouwbaarheid, gedrag, locatie of verplaatsingen te analyseren of te voorspellen.

Gegevensbescherming
Bescherming van persoonsgegevens tegen oneigenlijk gebruik.

Gegevensbeschermingseffectbeoordeling (Data protection impact assessment/DPIA)
Een instrument waarmee het effect van beoogde verwerkingsactiviteiten op de bescherming van persoonsgegevens op een gestructureerde en heldere manier in beeld in kaart wordt gebracht om vervolgens maatregelen te kunnen nemen om de risico’s te verkleinen.
Een analyse van de gevolgen voor gegevensbescherming als een project, beleid, dienst, product of ander initiatief wordt gestart of ingevoerd en het nemen van eventueel noodzakelijke mitigerende acties om een negatieve impact te voorkomen dan wel te verkleinen.

Governance
De wijze waarop de daadwerkelijke implementatie van richtlijnen en strategie is gegarandeerd, zodat vereiste processen op de juiste manier worden gevolgd om te kunnen voldoen aan weten regelgeving. Governance bevat het definiëren van rollen en verantwoordelijkheden, meten en rapporteren, nemen van acties om geïdentificeerde kwesties op te lossen.

Inbreuk in verband met persoonsgegevens (datalek)
Een inbreuk op de beveiliging die al dan niet per ongeluk op onrechtmatige wijze leidt tot de vernietiging, het verlies, de wijziging of de ongeoorloofde verstrekking van of de ongeoorloofde toegang tot doorgezonden, opgeslagen of anderszins verwerkte persoonsgegevens.

Informatiebeveiliging
Een verzameling van processen die zijn ingericht om de betrouwbaarheid van informatie te beschermen. Informatiebeveiliging heeft betrekking op:
- Beschikbaarheid: het zorg dragen voor het beschikbaar zijn van informatie en informatie verwerkende bedrijfsmiddelen op de juiste tijd en plaats voor de gebruikers;
- Integriteit: het waarborgen van de correctheid, volledigheid, tijdigheid en controleerbaarheid van informatie en informatieverwerking;
- Vertrouwelijkheid: het beschermen van informatie tegen kennisname en mutatie door onbevoegden. Informatie is alleen toegankelijk voor degenen die hiertoe geautoriseerd zijn.

Persoonsgegevens
Alle informatie over een geïdentificeerde of identificeerbare natuurlijke persoon.
Bij de GGD worden onder andere de volgende categorieën persoonsgegevens verwerkt:

- Personalia en identificatiegegevens

Persoonsgegevens, die betrekking hebben op persoonlijke bijzonderheden van betrokkene (naam, adres, woonplaats e.d.) om een persoon te kunnen identificeren.

- Medische gegevens

Persoonsgegevens, direct of indirect betrekking hebbend op de lichamelijke of geestelijke gesteldheid van betrokkene, verzameld door een beroepsbeoefenaar op het gebied van de (publieke) gezondheidszorg in het kader van zijn beroepsuitoefening.

- Financiële en administratieve gegevens

Gegevens die in de administratie van de GGD en de persoonsdossiers zijn opgenomen, niet zijnde personalia, identificatie-, medische of psychologische gegevens, die noodzakelijk zijn voor de financiering en/of administratieve afhandeling van de zorgverlening.

Toestemming van betrokkene
Elke vrije, specifieke en op informatie berustende ondubbelzinnige wilsuiting waarmee de betrokkene door middel van een verklaring of een ondubbelzinnige actieve handeling aanvaardt dat zijn persoonsgegevens worden verwerkt.

Tracking
Het volgen van mobiele datadragers zoals telefoons, bijvoorbeeld door Wifi- of bluetooth apparatuur waarbij (persoons)gegevens worden verzameld uit die datadragers.

Verwerker
Een verwerker is een persoons of organisatie die op basis van een opdracht van de verwerkingsverantwoordelijke en conform de aanwijzingen van deze verwerkingsverantwoordelijke persoonsgegevens verwerkt.

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

Verwerkingsverantwoordelijke
Een persoon of instantie die, alleen of samen met een ander, het doel en de middelen voor de verwerking van de persoonsgegevens vaststelt.
Binnen de GGD is het DB de verwerkingsverantwoordelijke. Het DB stelt het doel en de middelen vast voor de verwerking van persoonsgegevens. Het bestuur kan bepaalde taken overdragen aan de directeur publieke gezondheid (hierna: “DPG”) die hiermee de bevoegdheid krijgt om in naam van het bestuur besluiten te nemen.

3.3 Juridisch kader

3.3.1 Bij dit beleid wordt in aanmerking genomen:

- Burgerlijk Wetboek, Boek 7 (Wet op de geneeskundige behandelingsovereenkomst, ”WGBO”);
- Wet op de Beroepen in de individuele gezondheidszorg (Wet Big);
- Wet kwaliteit, klachten en geschillen zorg (“Wkkgz”);
- Algemene Verordening Gegevensbescherming (“AVG”);

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

3.4 Doelgroep en toepassingsbereik

3.4.1 Dit beleid is van toepassing op de gehele organisatie en op alle processen, onderdelen, objecten en gegevensverzamelingen van de GGD waarin persoonsgegevens worden verwerkt. Dit betreft zowel de taken die GGD op grond van de gemeenschappelijke regeling, al dan niet in mandaat, uitvoert voor de bestuursorganen van de gemeenten, alsmede de taken die de GGD uitvoert als openbaar lichaam in het kader van de Wet gemeenschappelijke regelingen (“Wgr”) en als werkgever. De GGD geldt hierbij als verwerkingsverantwoordelijke in de zin van de AVG.

3.4.2 Dit gegevensbeschermingsbeleid en een juiste uitvoering hiervan richt zich tot alle interne en externe medewerkers binnen de organisatie. Het is vooral gericht op diegenen die werken met persoonsgegevens, dan wel persoonsgegevens laten verwerken door externe partners.

3.4.3 Het beleid heeft betrekking op de hele “data levenscyclus”: van het genereren of verzamelen van persoonsgegevens, het dagelijkse gebruik ervan en de gegevensopslag tot en met de archivering en vernietiging ervan.

3.4.4 Het gegevensbeschermingsbeleid staat niet op zichzelf. Het heeft raakvlakken of vertoont overlap met andere beleidsthema’s als informatiebeveiliging, integriteit, kwaliteitszorg, personeel en organisatie en communicatie.

3.5 Inrichtingswijze gegevensverwerking

3.5.1 Door het cyclische karakter van de aangegeven maatregelen en door de bescherming van persoonsgegevens onderdeel te laten zijn van het managementsysteem van de GGD ontstaat een continu proces van veranderen en verbeteren. De kwaliteit van het omgaan met gegevensbeschermingsvraagstukken wordt immers verhoogd door op verschillende niveaus en vanuit verschillende rollen telkens weer de cyclus van plan-do-check-act (“PDCA”) te

doorlopen. Hierdoor ontstaat een evenwichtig beheersingssysteem. De GGD werkt zo actief aan bewustzijn, het opbouwen van kennis bij medewerkers en aan verantwoorde procesuitvoering op het gebied van gegevensbescherming.

3.5.2 Het borgen van de gegevensbescherming is onlosmakelijk verbonden met informatiebeveiliging. In dat kader werkt de GGD nauw samen met ‘Hét Service Centrum‘ (“HSC”).

4. Rechten van betrokkenen

4.1 Rechten van betrokkenen

4.1.1 De AVG brengt betrokkenen sterkere en nieuwe privacyrechten. Organisaties die persoonsgegevens verwerken krijgen meer verplichtingen. De nadruk ligt op de ‘accountability’, ofwel de verantwoordelijkheid van de GGD om te kunnen aantonen de organisatie zich aan de wet houdt.

4.1.2 De rechten van de betrokkene zijn binnen de GGD op transparante ingericht. Betrokkenen hebben recht op:

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

4.1.3 De GGD geeft hieraan onder andere uitvoering door betrokkenen op de website helder te informeren hoe van deze rechten kan worden gebruik gemaakt.

4.1.4 Om gebruik te maken van hun rechten kunnen de betrokkenen een verzoek indienen. Iemand kan een verzoek tot uitoefening van zijn of haar rechten via de website van de GGD of via andere gangbare publieksdienstverleningskanalen van de GGD doen. Dit verzoek is geldig ongeacht het middel waarmee het verzoek wordt gedaan onder voorwaarde van een deugdelijke identiteitsvaststelling.

4.1.5 Een beslissing op een verzoek wordt behandeld als een besluit in de zin van de Algemene wet bestuursrecht (“Awb”). Hiertegen kan bezwaar worden gemaakt.

4.2 Recht op informatie en toegang tot gegevens

4.2.1 Tijdens het eerste contact met een cliënt informeert de hulpverlener betrokkenen over de wijze waarop zijn persoonsgegevens worden verwerkt. Er wordt dan informatie verstrekt over het (a) doel van de gegevensverwerking, (b) de aard van de gegevens die worden verwerkt, (c) de grondslag van de verwerking, (d) de rechten die ten aanzien van de gegevensverwerking kunnen worden ingeroepen en (e) de identiteit van de verantwoordelijke.

4.2.2 Als het niet mogelijk is om de betrokkene tijdens het eerste contact te informeren, dan zorgt de hulpverlener dat de betrokkene zo spoedig als de situatie toe laat, alsnog over de gegevensverwerking wordt geïnformeerd.

4.2.3 Van het (uitstellen of niet) informeren van de betrokkene kan een aantekening worden gemaakt in het dossier.

4.2.4 De GGD verzamelt gegevens om haar taken te kunnen uitvoeren. Indien dit persoonsgegevens betreft en indien betrokkenen hiervan niet op de hoogte zijn informeert de GGD hen actief over de verwerking van hun persoonsgegevens zoals het doel daarvan, welke persoonsgegevens worden verwerkt, wie daarvoor verantwoordelijk is en of de gegevens aan anderen worden verstrekt.

4.2.5 De GGD informeert betrokkene, uiterlijk binnen vier weken na de verzameling van persoonsgegevens, indien de persoonsgegevens van derden afkomstig zijn.

4.3 Recht op inzage en afschrift van gegevens

4.3.1 Patiënten, medewerkers en andere betrokkenen kunnen altijd hun persoonsgegevens inzien wanneer zij hier om vragen en kunnen er op vertrouwen dat deze gegevens correct zijn dan wel worden aangepast wanneer noodzakelijk of door de betrokkene is aangegeven dat deze aangepast dienen te worden, voor zover een (wettelijke) verplichting dit niet onmogelijk maakt.

4.3.2 Betrokkenen hebben de mogelijkheid om te controleren of en op welke manier hun gegevens worden verzameld en verwerkt en het recht op inzage en afschrift van zijn dossier [1]. Uitzondering op deze regel is als de persoonlijke levenssfeer van een ander daardoor wordt geschaad. Bijvoorbeeld informatie die een partner aan een hulpverlener heeft verstrekt in het vertrouwen dat betrokkene deze informatie niet te zien krijgt.

4.3.3 De GGD verstrekt de betrokkene, binnen vier weken na ontvangst van het verzoek, kosteloos een kopie van de persoonsgegevens die worden verwerkt.

4.3.4 Indien de termijn van vier weken onhaalbaar blijkt, verlengt de GGD de termijn met twee maanden en brengt de betrokkene hier schriftelijk van op de hoogte.

4.3.5 Indien de betrokkene om bijkomende kopieën vraagt, kan de GGD een vergoeding rekenen niet hoger dan de kostprijs.

4.4 Recht op rectificatie (correctie, aanvulling) van gegevens

4.4.1 Als de GGD persoonsgegevens van betrokkenen verwerkt die naar hun oordeel onjuist zijn, kunnen zij een verzoek indienen bij de GGD om feitelijke onjuistheden in het dossier te corrigeren. Het gaat dan bijvoorbeeld om onjuiste adresgegevens. Niet wordt bedoeld dat de bijvoorbeeld de diagnose mag worden gewijzigd.

4.4.2 Er kan ook een verklaring aan het medisch dossier worden toegevoegd, bijvoorbeeld eigen visie van de betrokkene, ook als de hulpverlener het niet eens is met de verklaring moet deze worden opgenomen.

4.5 Recht op gegevenswissing

4.5.1 Betrokkenen hebben het recht persoonsgegevens te laten verwijderen indien de GGD niet langer een goede grond heeft voor het gebruik hiervan, bijvoorbeeld indien betrokkenen een

[1] Artikel 7:456 BW en artikel 15 van de AVG

gegeven toestemming intrekken, indien de gegevens onjuist zijn of de gegevens niet langer nodig zijn.

4.5.2 Het AVG recht op gegevenswissing geldt in principe niet voor medische dossiers. De betrokkene heeft het recht om op hem betrekking hebbende gegevens te laten verwijderen en op grond van de Wgbo heeft hij bovendien het recht dossiergegevens te laten vernietigen ongeacht of dit relevante gegevens zijn[2].

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

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

4.6 Recht op beperking van de verwerking

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

4.7 Recht op overdraagbaarheid van gegevens (dataportabiliteit)

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

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

4.7.3 De GGD treft voorzieningen in het kader van dataportabiliteit.

[2] Artikel 7: 455 BW

4.8 Recht van bezwaar tegen verwerking

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

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

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

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

4.10 Klachten en vragen

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

4.10.2 Binnen vier weken beoordeelt de GGD of het verzoek ontvankelijk is. De GGD laat binnen die termijn weten wat er met het verzoek gaat gebeuren, waaronder of de GGD de behandeling van het verzoek met twee maanden verlengt. De GGD behandelt het verzoek volgens de daarvoor door haar vastgestelde en bekendgemaakte procedure[3].

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

4.10.4 Indien naar de mening van de klant de beslissing op een klacht niet tot het gewenste resultaat heeft geleid, wordt gewezen op de mogelijkheid om diens klacht voor te leggen aan de Autoriteit Persoonsgegevens, Postbus 93374, 2509 AJ 's Gravenhage.

4.11 Informeren van (keten)partners

4.11.1 De GGD informeert relevante ketenpartners indien het verzoek wordt ingewilligd. Dit betreft o.a. organisaties met wie een verwerkersovereenkomst dan wel een gebruiksovereenkomst of een overeenkomst tot derde verstrekking is afgesloten. Indien relevant vraagt de GGD

[3] Klachtenregeling GGD West-Brabant 2017

actief om bevestiging van de betreffende ketenpartner(s) dat aan het betreffende verzoek is voldaan.

4.12 Rechten en plichten aangaande het medisch dossier

4.12.1 De Wet op de geneeskundige behandelingsovereenkomst (“WGBO”) verplicht de hulpverlener van de GGD om een medisch dossier in te richten. In het medisch dossier neemt de hulpverlener alle gegevens op over de gezondheid van de betrokkene en over de uitgevoerde verrichtingen, voor zover dit voor een goede hulpverlening noodzakelijk is.

4.12.2 De betrokkene kan de hulpverlener niet van deze verplichting ontheffen. De gegevens vallen onder het medisch beroepsgeheim: de hulpverlener heeft een geheimhoudingsplicht.

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

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

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

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

4.12.6 Een hulpverlener van de GGD mag uitsluitend een (medisch) dossier aanleggen in de hiervoor bestemde en door de GGD aangewezen (zorg)informatiesystemen.

5. Verplichte maatregelen en procedures

5.1 Bewustwording

5.1.1 De GGD zorgt voor bewustzijn op het gebied van gegevensbescherming voor al haar medewerkers. Hierbij dienen zij minimaal op de hoogte te zijn van de voor hun relevante wet- en regelgeving en bepalingen zodat zij deze in hun dagelijkse werk kunnen toepassen. Hierbij kan gedacht worden aan regels over toegang tot medische gegevens, maatregelen ter bescherming van bijzondere persoonsgegevens, datalekken en zwijgplicht.

5.1.2 Concreet kan de GGD bewustwording vormgeven door enerzijds te voorzien in algemene en op het thema afgestemde specifieke voorlichtingen op het gebied van gegevensbescherming. Anderzijds wil de GGD het bewustzijn op dit gebied door gegevensbescherming tot terugkerend agendapunt te maken van de verschillende overleggen. Daarmee worden dilemma's op het gebied van gegevensbescherming bespreekbaar en stimuleert de GGD medewerkers om beveiligingsincidenten en datalekken te melden. Tenslotte kan bewustwording bevorderd worden door bijvoorbeeld e-learning, nieuwsbrieven en informatie op het intranet.

5.2 Verwerking van persoonsgegevens door derden

Verwerkers en verwerkersovereenkomst(en)

5.2.1 Wanneer de GGD een externe partij of (keten)partner inschakelt om ten behoeve van de GGD persoonsgegevens te verwerken en het verwerken van de persoonsgegevens een hoofdzaak is van deze partij, kan deze partij worden beschouwd als verwerker.

5.2.2 De GGD schakelt enkel verwerkers in die afdoende garanties bieden met betrekking tot het toepassen van passende technische, procesmatige, communicatieve en organisatorische maatregelen[4].

5.2.3 De instructies omtrent verwerking(en) door een verwerker worden schriftelijk vastgelegd in een verwerkersovereenkomst[5] voordat de dienstverlening aanvangt.

5.2.4 De belangrijkste verwerkers zullen minstens eens per jaar door de GGD, middels de leveranciersbeoordeling, gecontroleerd worden op borging en naleving van de verplichtingen uit de verwerkersovereenkomst. Een dergelijke controle kan o.a. bestaan uit het opvragen van relevante certificeringen. Minder kritische verwerkers worden periodiek gecontroleerd.

5.2.5 De GGD hanteert als modelovereenkomst: (a) de gemeentelijke standaard verwerkersovereenkomst[6] of (b) de standaard model verwerkersovereenkomst voor de zorgsector[7].

[4] Artikel 28 lid 1 van de AVG
[5] Artikel 28 lid 3 van de AVG
[6] Zie: https://www.informatiebeveiligingsdienst.nl/product/handreiking-standaard-verwerkersovereenkomst-gemeenten/
[7] Zie: https://www.vgn.nl/nieuws/standaard-model-verwerkersovereenkomst-voor-de-zorgsector

5.2.6 Verwerkingen mogen niet plaatsvinden in landen die geen passend beveiligingsniveau kunnen bieden. Hiervan kan worden afgeweken met uitdrukkelijke toestemming van de betrokkenen of andere waarborgen die de autoriteiten hebben goedgekeurd. Een lijst met landen met een passend beveiligingsniveau is te vinden op: https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en

De GGD als verwerker

5.2.7 In voorkomende gevallen treedt de GGD op als verwerker voor derden. Hierbij zijn derden verwerkingsverantwoordelijk.

5.2.8 De GGD streeft na om voor deze verwerkingen heldere en eenduidige voorwaarden op te stellen die ook toepasbaar zijn voor gelijksoortige verwerkingen.

5.2.9 De GGD biedt daarbij aan de verwerkingsverantwoordelijke voldoende garanties voor het zorgvuldig verwerken van gegevens door het toepassen van passende technische en organisatorische maatregelen.

5.2.10 De afspraken omtrent de verwerking worden schriftelijk vastgelegd in een verwerkersovereenkomst, voordat de dienstverlening door de GGD aanvangt.

De GGD als gezamenlijke verwerkingsverantwoordelijke

5.2.11 Indien de GGD met een andere partij samenwerkt, die geen verwerker is, maar waarmee wel persoonsgegevens worden uitgewisseld waarbij een gezamenlijke verwerkingsverantwoordelijkheid bestaat maakt de GGD passende afspraken. In dat geval zal de GGD een regeling[8] sluiten omtrent de verwerking van persoonsgegevens, of samen met de andere partij een regeling vaststellen, waarin de respectievelijke verantwoordelijkheden worden vastgelegd.

5.2.12 De GGD plaatst genoemde regeling op haar website[9].

5.3 Documentatie over verwerking van persoonsgegevens

5.3.1 De FG schrijft namens de GGD de verwerkingen van persoonsgegevens waarvoor meld- of registratieplicht geldt bij in het daartoe bestemde register, daarin bijgestaan door de adviseur gegevensbescherming en de portefeuillehouder kwaliteit van het verantwoordelijke team.

5.3.2 Alle nieuwe of niet geregistreerde verwerkingen worden actief door de betreffende medewerker(s) (daar waar de verwerking plaatsvindt) aangemeld bij de FG.

Bij de inschrijving worden in ieder geval de volgende gegevens[10] vermeld:

a. de naam van de verwerking;
b. wie de verantwoordelijke is voor de verwerking;

[8] Artikel 26 lid 1 van de AVG
[9] Artikel 26 lid 2 van de AVG
[10] Artikel 30 lid 1 van de AVG

c. het doel van de verwerking;
d. de groep van personen van wie persoonsgegevens worden verwerkt (betrokkenen);
e. de categorie persoonsgegevens die bij de verwerking worden gebruikt;
f. de ontvangers van de gegevens;
g. de rechtmatige grondslag voor de verwerking van de persoonsgegevens;
h. eventuele verstrekkingen aan andere landen buiten de Europese Economische Ruimte;
i. de verwijderingstermijnen die in acht genomen worden;

5.3.3 De FG houdt toezicht op de volledigheid, juistheid en rechtmatigheid van de in het register ingeschreven verwerkingen van persoonsgegevens.

5.3.4 Bij wijzigingen van de bij de inschrijving opgenomen gegevens draagt de portefeuillehouder kwaliteit van het verantwoordelijke team. zorg voor wijziging hiervan in het register en informeert de FG hierover.

5.3.5 De GGD maakt het register van verwerkingsactiviteiten niet openbaar op de website.

5.4 Informatiebeveiliging

5.4.1 Het waarborgen van de beschikbaarheid, integriteit en vertrouwelijkheid van persoonsgegevens is een voorwaarde om te garanderen dat betrokkenen hun rechten op adequate wijze kunnen uitoefenen.

5.4.2 De GGD streeft de bepalingen uit de NEN 7510, NEN 7512, NEN 7513 en NTA 7516 normen na, ter bescherming van de verwerking van medische gegevens.

5.4.3 De GGD controleert steekproefsgewijs op toegang tot persoonsgegevens door onbevoegden.

Passende beschermende technische en organisatorische maatregelen

5.4.4 Wanneer de GGD persoonsgegevens verwerkt of laat verwerken door een derde, zorgt de GGD ervoor dat passende beveiligingsmaatregelen worden getroffen om de betreffende persoonsgegevens te beschermen tegen de verschillende risico's.

5.4.5 De GGD slaat gegevens zo op dat voldaan kan worden aan de wettelijke kaders van de AVG, dit betekent in verband met de doelbinding vaak gescheiden opslag. Concreet betekent dit bijvoorbeeld dat medische gegevens van klanten nooit worden opgeslagen in een boekhoudkundig systeem.

5.4.6 De GGD houdt actief, per informatiesysteem, een autorisatiemix bij en controleert steekproefsgewijze achteraf op (eventueel ongeautoriseerde) toegang.

5.4.7 De GGD beperkt de toegang tot inzage en wijzigen van gegevens tot degenen die dit vanuit hun functie nodig hebben; medewerkers worden actief aangesproken in geval van overschrijding van toegangsbevoegdheden.

5.4.8 De GGD beschermt persoonsgegevens onder andere door het aggregeren, versleutelen en anonimiseren van deze gegevens. Hierdoor wordt de mate waarin de verwerkte persoonsgegevens kunnen worden herleid tot een individu verminderd.

5.4.9 In beginsel, in het bijzonder bij gegevens aangaande de gezondheid, worden alle gegevensdragers en alle communicatie tussen de GGD en haar klanten en/of (keten)partners voorzien van encryptie (versleuteling).

5.4.10 Als uitgangspunt kiest de GGD voor technische maatregelen om 'gegevensbescherming door ontwerp' te waarborgen. Daar waar de technische mogelijkheden ontbreken of disproportioneel hoge kosten met zich meebrengen, zoekt de GGD naar organisatorische en of procesmatige maatregelen als alternatief voor of als aanvulling op de technische maatregelen. Dit wordt uiteraard samen en in overleg met informatiebeveiliging uitgewerkt.

5.4.11 Deze (technische, procesmatige, communicatie en organisatorische) maatregelen omvatten bij de verwerking van persoonsgegevens een op het risico afgestemd beveiligingsniveau. Hierbij wordt rekening gehouden met de stand van de techniek, de uitvoeringskosten, en ook met de aard, de omvang, de context en de verwerkingsdoeleinden etc. Tevens wordt rekening gehouden met de, qua waarschijnlijkheid en ernst, uiteenlopende risico's voor de rechten en vrijheden van personen.

Waar wenselijk omvatten de maatregelen onder meer het volgende:

- De pseudonimisering en versleuteling van persoonsgegevens;
- Het vermogen om op permanente basis de vertrouwelijkheid, integriteit, beschikbaarheid en veerkracht van de verwerkingssystemen en diensten te garanderen;
- Het vermogen om bij een fysiek of technisch incident de beschikbaarheid van en de toegang tot de persoonsgegevens tijdig te herstellen;
- Een procedure voor het op gezette tijdstippen testen, beoordelen en evalueren van de doeltreffendheid van de technische en organisatorische maatregelen ter beveiliging van de verwerking.

5.5 Meldplicht voor inbreuken in verband met persoonsgegevens (datalekken)

5.5.1 Indien zich een informatiebeveiligingsincident voordoet, waarbij bijvoorbeeld gegevens van personen in verkeerde handen kunnen komen of zijn gekomen, handelt de GGD in overeenstemming met de vastgestelde werkwijze in het Protocol Meldplicht en Afhandeling van (vermoedelijke) datalekken[11]. Dit protocol bevat een vastgesteld proces van te doorlopen stappen om de eventuele schade of de kans hierop, bij een 'datalek' te beperken en de getroffen perso(o)n(en) te beschermen.

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

5.5.3 De plicht tot het melden van een (vermoeden van een) 'datalek' geldt als er sprake is van een aanzienlijke kans op ernstige nadelige gevolgen voor betrokkene, dan wel ernstige nadelige gevolgen voor de bescherming van persoonsgegevens. Het betreft situaties van het

[11] Zie 'Protocol Meldplicht en Afhandeling van (vermoedelijke) datalekken'

(mogelijk) lekken van persoonsgegevens uit GGD bestanden en/of gegevens waarvoor de GGD verantwoordelijkheid draagt.

5.5.4 Wanneer er een dergelijk 'datalek' heeft plaatsgevonden, wordt dit zonder onredelijke vertraging, uiterlijk 72 uur nadat er kennis van de inbreuk is vernomen, gemeld aan de AP. Als dit later dan 72 uur is wordt er een motivering voor de vertraging bij de melding gevoegd.

5.5.5 Indien de inbreuk een hoog risico voor de rechten en vrijheden van de betrokkenen met zich meebrengt, word de inbreuk ook in eenvoudige en duidelijke taal aan de betrokkenen gemeld.

5.5.6 De GGD maakt de afweging of het informeren van de betrokkene in diens belang is of dat dit beter achterwege kan blijven om de betrokkene zelf of anderen te beschermen. Indien van informeren wordt afgezien zal de GGD dit besluit registreren en duidelijk motiveren.

5.5.7 De FG houdt namens de GGD een logboek bij waarin alle medeplichtige en niet-medeplichtige datalekken zijn opgenomen.

5.5.8 In het logboek worden in ieder geval de volgende gegevens vermeld:

a. Het onderwerp van het 'datalek'.
b. De datum van het 'datalek';
c. De duur van het 'datalek';
d. de aard van de inbreuk;
e. de instanties waar meer informatie over de inbreuk kan worden verkregen;
f. de aanbevolen maatregelen om de negatieve gevolgen van de inbreuk gevolgen te beperken.
g. een beschrijving van de gevolgen voor de verwerkte persoonsgegevens;
h. de maatregelen die de GGD heeft getroffen of voorstelt te treffen om deze gevolgen te verhelpen;
i. de kennisgeving aan betrokkenen.

5.5.9 De GGD maakt haar register van informatiebeveiligingsincidenten niet openbaar.

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

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

5.6 DPIA's (Data Protection Impact Assessments)

5.6.1 Voor de GGD is een DPIA een instrument waarmee het effect van beoogde verwerkingsactiviteiten op de bescherming van persoonsgegevens op een gestructureerde en heldere manier in beeld in kaart wordt gebracht om vervolgens maatregelen te kunnen nemen om de risico's te verkleinen.

5.6.2 De GGD voert DPIA's uit voor nieuwe maar ook bestaande verwerkingen van persoonsgegevens die een hoog privacyrisico opleveren voor de betrokkenen. De GGD volgt hierbij de lijst van de AP[12].

5.6.3 Indien naar oordeel van de FG sprake is van een verwerking, die gelet op de aard en de omvang, de context en de doeleinden een hoog risico inhoudt voor de rechten en vrijheden van natuurlijke personen dan wordt door middel van een DPIA aangetoond dat de privacy voldoende is gewaarborgd en worden de al dan niet te nemen maatregelen gemotiveerd.

5.6.4 De GGD neemt het initiatief tot het uitvoeren van een DPIA en betrekt relevante medewerkers bij het proces wat gecoördineerd wordt door de adviseur gegevensbescherming.

5.6.5 Voor nieuwe verwerkingen vindt een DPIA plaats voordat met de betreffende verwerking wordt gestart.

5.6.6 Ten aanzien van bestaande verwerkingen voert de GGD een DPIA uit indien de betreffende verwerkingen hier aan onderworpen dient te worden maar deze nog niet heeft plaatsgevonden.

5.6.7 Een DPIA wordt na maximaal 3 jaar herhaald ter evaluatie, alsmede bij wijzigingen waardoor de risico's van de verwerking toenemen.

5.6.8 Bij het uitvoeren van een DPIA wordt de FG altijd vooraf geïnformeerd.

5.6.9 De portefeuillehouder kwaliteit van een team ziet toe op het nemen van maatregelen die blijkens de DPIA nodig zijn om de risico's te verkleinen.

5.6.10 Het resultaat van de DPIA en de genomen maatregelen om het risico te beperken worden aan de FG voorgelegd ter toetsing en opneming in het register van verwerkingen.

5.6.11 Waar het nieuwe verwerkingen betreft wordt - voorafgaand aan de verwerking- de AP om advies gevraagd indien de GGD niet in staat is om voldoende maatregelen te treffen om de risico's te beperken en er een hoog restrisico bestaat.

5.6.12 DPIA's die binnen de GGD worden uitgevoerd vinden plaats volgens een door het MT bepaalde standaard.

5.6.13 De FG geeft over de uitgevoerde DPIA een advies aan het MT.

5.6.14 De GGD maakt de resultaten van uitgevoerde DPIA's niet openbaar. Deze dienen uitsluitend ter vaststelling van managementbeleid.

5.7 Beheer van persoonsgegevens

Big data en tracking

[12] https://autoriteitpersoonsgegevens.nl/nl/zelf-doen/data-protection-impact-assessment-dpia

5.7.1 Gegevens in big data en tracking mogen alleen worden verzameld, opgeslagen en gedeeld, als ze niet herleidbaar zijn tot een persoon en worden alleen verzameld voor onderzoek dat door of namens de GGD wordt uitgevoerd.

5.7.2 Voor big data en tracking wordt uitsluitend gebruik gemaakt van brongegevens die door daartoe geautoriseerde personen zijn verzameld.

5.7.3 Brongegevens die gebruikt worden voor big data toepassingen worden omgezet tot een dataset die geen persoonsgegevens bevat en dus geanonimiseerd is. Indien het noodzakelijk is om af te wijken wordt vooraf toestemming aangevraagd bij de FG die de aanvraag zal beoordelen in het kader van de rechtmatigheid en de doelmatigheid. Alleen bij een goedgekeurde aanvraag mogen de gegevens gepseudonimiseerd in plaats van geanonimiseerd worden.

Cameratoezicht, camerabewaking en overige inzet van camera's

5.7.4 De GGD past op verschillende plekken binnen haar organisatie registratie van bewegende beelden toe. Voorbeelden hiervan zijn beelden van bewakingscamera's in en rond de consultatiebureaus. Bij elke registratie van camerabeelden bepaalt en documenteert de GGD of en hoe lang deze worden bewaard.

5.7.5 De GGD plaatst de camera's niet zodanig dat deze uitsluitend of voornamelijk op de openbare ruimte zijn gericht.

5.7.6 Camerabewaking kan door particuliere bedrijven worden uitgeoefend onder voorwaarde dat indien er camera's in de openbare ruimte worden geplaatst dan wel delen van de openbare ruimte in beeld worden gebracht, er een daartoe strekkend besluit door of namens het MT is genomen en er een overeenkomst met de verantwoordelijke is gesloten voorafgaande aan de verwerking. Deze overeenkomst gaat in ieder geval in op:

- de grondslag voor de verwerking van persoonsgegevens;
- het verzamel- en verwerkingsdoel;
- de organisatorische en technische maatregelen die worden getroffen tegen verlies of onrechtmatige verwerking;
- de bewaartermijn;
- de wijze waarop voldaan wordt aan de meldplicht datalekken.

Bij inzet van camera's voor andere doeleinden dient voorafgaand aan deze inzet advies te worden gevraagd aan de FG.

Cookies en soortgelijke technieken

5.7.7 De GGD plaatst, indien noodzakelijk, alleen cookies die noodzakelijk zijn voor het correct functioneren van de website op de computers van betrokkenen en het analyseren hiervan, zgn. functionele en analytische cookies en maakt geen gebruik van tracking cookies.

Geheimhouding

5.7.8 Persoonsgegevens worden in beginsel niet verwerkt door medewerkers zonder (medisch) beroepsgeheim of zonder ondertekende geheimhoudingsverklaring.

Minimaal gebruik van persoonsgegevens (dataminimalisatie)

5.7.9 De GGD verzamelt (of vraagt om) niet meer gegevens dan strikt noodzakelijk.

5.7.10 De GGD verwerkt alleen gegevens voor het doel waarvoor zij zijn verzameld en verwerkt deze verder alleen op een manier die verenigbaar is met dit doel.

5.7.11 Bij configuratie van systemen kiest de GGD in voorkomende gevallen voor de privacy-vriendelijke variant (privacy by default).

5.7.12 De informatie die de GGD verwerkt is in beginsel correct en actueel.

5.7.13 De GGD maakt geen onnodige kopieën van verzamelingen van persoonsgegevens.

5.7.14 De GGD voert actief beleid om alle overbodige gegevensverzameling (bijvoorbeeld op – gestandaardiseerde- vragenlijsten en invulformulieren) te verwijderen.

5.7.15 Per team zijn de wettelijk verplichte bewaartermijnen per categorie van persoonsgegevens vastgesteld. De GGD bewaart persoonsgegevens niet langer dan strikt noodzakelijk (bijvoorbeeld op basis van de Belastingwet, de Archiefwet etc.) en verwijdert actief wat niet meer nodig is.

5.7.16 De GGD communiceert actief aan ketenpartners wanneer persoonsgegevens verwijderd dienen te worden waaronder begrepen het vragen van bevestiging dat betreffende persoonsgegevens door de ketenpartner zijn verwijderd.

Onderzoek

5.7.17 De GGD ontdoet bij onderzoek alle persoonsgegevens van direct identificerende kenmerken (anonimiseren).

Privacy by design (privacy door ontwerp)

5.7.18 De GGD hanteert achtereenvolgens de volgende acht data- en procesgeoriënteerde privacy strategieën om gegevensbescherming vanaf begin af aan mee te nemen bij het ontwerpen en bouwen van nieuwe systemen.

1. De verwerking van persoonsgegevens wordt zo veel mogelijk beperkt.
2. De verwerking van persoonsgegevens wordt zo veel mogelijk van elkaar gescheiden.
3. Het detail waarin persoonsgegevens worden verwerkt wordt zo veel mogelijk beperkt.
4. Persoonsgegevens worden afgeschermd of onherleidbaar. Er wordt voorkomen dat persoonsgegevens openbaar worden.
5. Klanten worden over de verwerking van hun persoonsgegevens geïnformeerd (voorafgaand aan de start van de nieuwe verwerking).
6. Klanten krijgen regie en invloed over de verwerking van hun persoonsgegevens.
7. Er wordt een privacy vriendelijke verwerking van persoonsgegevens afgedwongen.
8. Er wordt aangetoond dat persoonsgegevens op een privacy vriendelijke wijze zijn verwerkt

6. Governance

6.1 Functies en verantwoordelijkheden

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

1. Portefeuillehouder kwaliteit per team

- Verantwoordelijk voor de borging van de beschikbaarheid, integriteit en vertrouwelijkheid van de door het team verwerkte persoonsgegevens;
- Verantwoordelijk voor aanmelden van nieuwe (of veranderde) verwerkingen van persoonsgegevens bij de FG;
- In voorkomend geval verantwoordelijk voor de uitvoering van een (door de FG getriggerde) DPIA en borging van de hieruit voortvloeiende (verbeter)maatregelen;
- Het behandelen van verzoeken in het kader van de rechten van betrokkenen;
- Het afsluiten van verwerkersovereenkomsten en andere regelingen;
- Het onderzoeken en melden van informatieveiligheidsincidenten;
- Adviezen uit veiligheidsincidenten implementeren, onder supervisie van de adviseur gegevensbescherming

2. Functionaris voor gegevensbescherming (FG)

- Toezichthouder op de verwerking van persoonsgegevens (naleving van privacywetgeving)
- Informeren, adviseren, bewustmaking over AVG verplichtingen, verwerking, incidenten, klachten, DPIA, opstellen van beleid;
- Opzetten en beheer van register van de verwerkingsactiviteiten;
- Ziet, in overleg met de CISO, toe op de controle van de uitvoering van de maatregelen voor gegevensbescherming en informatiebeveiliging;
- Ziet toe op de ontwikkeling en uitvoering van een privacy-auditplan samen met de kwaliteitsfunctionaris en de portefeuillehouder kwaliteit van het betreffende team. Aan de hand hiervan kan de PDCA-cyclus worden doorlopen waarmee continu verbeteren wordt geborgd;
- Rapporteert tenminste jaarlijks aan het MT over de manier waarop de GGD de afgelopen periode met gegevensbescherming is omgegaan. Ook doet hij in zijn rapport aanbevelingen;
- Onderhoud contacten met de AP

3. CISO (Chief Information Security Officer)

- Actueel houden- en coördineren van de uitvoering van informatiebeveiligings- en gegevensbeschermingsbeleid, risicobeheersing en rapportage;
- Aanspreekpunt voor informatieveiligheid en privacy;
- Bevorderen van bewustzijn (veiligheid en privacy);
- Registratie van veiligheidsincidenten en verantwoordelijk voor afhandeling.

4. Privacybeheerder / adviseur gegevensbescherming

- Advisering, uitvoering en naleving van privacy wetgeving

- Beoordelen van- en adviseren over persoonsgegevensverwerking
- Coördineren van privacy werkzaamheden, inzage- en correctie verzoeken
- Afhandeling van veiligheidsincidenten
- Beheer van verwerkingsovereenkomsten, advisering en ondersteuning bij het afsluiten ervan

5. Directeur publieke gezondheid

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

6. Dagelijks- en Algemeen bestuur

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

7. Adviseur Informatiebeveiliging

- (Pro) actief adviseren over informatiebeveiliging en het informatiebeveiligingsbeleid
- Uitvoeren van gapanalyse (nulmeting) en advies over NEN7510/BIO (minimaal benodigde aanpassingen)
- Adviseren en ondersteunen van de GGD om het benodigde niveau van informatiebeveiliging te bereiken dat minimaal voldoet aan de wet- en regelgeving.
- Ervoor zorgdragen dat ondersteunde systemen en processen bij gegevensverwerker HSC voldoen aan wet- en regelgeving. (De behaalde NEN7510 certificering behouden).

8. Functioneel beheerders informatiesystemen

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

7. Slotbepalingen

De AVG is per 25 mei 2018 van toepassing. Dit beleid treedt in werking per 1 januari 2020, na vaststelling door de verantwoordelijke van de GGD. Het DB wordt hiervan in kennis gesteld.

Het beleid wordt elk jaar geëvalueerd en indien nodig herzien. Aanpassingen van dit beleid worden aangekondigd via het intranet. De meest actuele versie van het beleid is te vinden in het Document Management Systeem.

Aldus vastgesteld door het MT van de GGD West-Brabant op 24 december 2019 te Breda,

[redacted] publieke gezondheid GGD West-Brabant,

Naam verwerking	Categorieën betrokkenen van wie persoonsgegevens worden verwerkt	Categorieën verwerkte persoonsgegevens	Verwerkte gevoelige gegevens (indien van toepassing) en toegepaste beperkingen of waarborgen	Aard van de verwerking	Doeleinde(n) waarvoor de persoonsgegevens namens de verwerkingsverantwoordelijke worden verwerkt	Duur van de verwerking
BCO sync extensie			(index)	Overheveling van persoonsgegevens van GGD contact naar Hp zone lite door middel van Google Chrome extensie	Het aantal uur dat GGD per index besteedt aan BCO verminderen, waardoor GGD voor meer indexen BCO kan uitvoeren.	Eenmalig per casus
Registratie HP zone (lite)					Identificatie van contacten, hen informeren over de blootstelling en het risico op besmetting, hen wijzen op maatregelen die genomen moeten worden om verdere verspreiding te voorkomen hen hierin begeleiden.	
Registratie GGD contact	Index, contacten van index	Naam + achternaam Telefoonnummer E-mailadres Datum laatste contactmoment Risicoclassificatie Aandachtspunten Vrij opmerkingsveld Contacttype Of de index het contact zelf al heeft geïnformeerd Dag van aanvang van de symptomen			Identificatie van contacten, hen informeren over de blootstelling en het risico op besmetting, hen wijzen op maatregelen die genomen moeten worden om verdere verspreiding te voorkomen hen hierin begeleiden.	
Registratie in Osiris				Via Hpzone(Lite) wordt een melding gemaakt aan Osiris door het invullen van een questionnaire. Deze melding bevat anonieme gegevens van de index en worden gebruikt voor Surveillance bij het RIVM.		

maatregelen inzake pseudonimisering en versleuteling van persoonsgegevens;

Toepassing versleuteling

- (herstel)sleutelbeheer, bij wie is het belegd en hoe is dit geregeld?
- wat is de omvang van de sleutel (128, 256 bits?)
- is bitlocker standaard geactiveerd op de uitgeleverde machines?

maatregelen die op permanente basis de vertrouwelijkheid, integriteit, beschikbaarheid en veerkracht van de verwerkingssystemen en -diensten garanderen;

- Aanwezigheid effectief beleid en een procedure voor systeemupdates
- Aanwezigheid van effectieve antivirus software
- toepassing MFA

maatregelen die het vermogen garanderen om bij een fysiek of technisch incident de beschikbaarheid van en de toegang tot de persoonsgegevens tijdig te herstellen;

..
- Aanwezigheid effectieve backup procedure
- centraal beheer, inclusief op afstand wissen
-

processen voor het op gezette tijdstippen testen, beoordelen en evalueren van de doeltreffendheid van de technische en organisatorische maatregelen ter beveiliging van de verwerking;

- periodiek doorspreken (effectiviteit) van de maatregelen tijdens corona-IBMF?

maatregelen voor de identificatie en autorisatie van gebruikers;

- Welke rollen en rechten bestaan er voor de uitgeleverde machines?
- Wie kent de machine rechten toe en neemt ze in?
- Welk proces is van toepassing bij het intrekken van rechten?

maatregelen ter bescherming van gegevens tijdens de doorgifte;

- Toepassing versleuteling gedurende transport van data?
- Veilig e-mailen?

maatregelen voor de bescherming van gegevens tijdens de opslag;

- Blokkeren printmogelijkheid
- Blokken wegschrijven gegevens via USB poort
- Toepassing versleuteling?

maatregelen ter waarborging van de fysieke beveiliging van de locaties waar persoonsgegevens worden verwerkt;

- Contractuele verplichting tot geheimhouding?
- Monitoring?
- Gedragscode?

maatregelen om ervoor te zorgen dat incidenten worden geregistreerd;

- Procedure voor melding en registratie incidenten

maatregelen om de systeemconfiguratie, met inbegrip van de standaardinstelling, te waarborgen;

- Werken met ‘standaard images’ / virtual desktop?

maatregelen voor interne governance en beheer op het gebied van IT en IT-beveiliging;

- Overzicht van rollen,taken en verantwoordelijkheden op het gebied van informatiebeveiliging binnen Yource
- Procedure toekenning/inneming (local) adminrechten voor uitgeleverde machines

maatregelen voor certificering/waarborging van processen en producten;

- ISO 9001 / 27001
- VVT

maatregelen om gegevensminimalisering te waarborgen;

- Nvt?
- Volgen beleidskaders m.b.t. uitvoering bron- en contactonderzoek

maatregelen om de kwaliteit van de gegevens te waarborgen;

- Kwaliteitscontroles

maatregelen om te zorgen voor beperkte bewaring van gegevens;

- Nvt?
- Volgen beleidskaders m.b.t. uitvoering bron- en contactonderzoek

maatregelen ter waarborging van de verantwoordingsplicht;

- Register van verwerkingsactiviteiten
- Overzicht van en overeenkomsten met subverwerkers
- Overzicht van beveiligingsmaatregelen
- Informatiebeveiligingsbeleid
- Gegevensbeschermingsbeleid
- ..

maatregelen om gegevensoverdraagbaarheid mogelijk te maken en voor wissing te zorgen.

- Nvt?

Beschrijf voor overdrachten aan (sub)verwerkers ook de specifieke technische en organisatorische maatregelen die de (sub)verwerker moet nemen om de verwerkingsverantwoordelijke bijstand te kunnen verlenen.

Beschrijving van de specifieke technische en organisatorische maatregelen die de verwerker moet nemen om de verwerkingsverantwoordelijke bijstand te kunnen verlenen.

Overzicht van subverwerkers

- Teleknowledge (daarmee wordt gebeld met de index)

Teleknowledge Call Center Solutions B.V.
Energieplein 10
2031 TC Haarlem
Tel. (023) 553 0 553

- VPN services (tbv oude versie Teleknowledge)

- Synergy (uren registratie alle BCO medewerkers)
- Pay4People (loonstroken)

Convenant gegevensuitwisseling gezamenlijk verantwoordelijken

INHOUD

1.	Definities	**4**
2.	Scope	**4**
3.	Ingangsdatum convenant, werkingsduur en opzegging	**5**
4.	Rollen en verhoudingen	**5**
5.	Gegevensverwerking	**6**
6.	Wettelijke grondslag voor gegevensverwerkingen	**6**
7.	Rechten van betrokkenen	**6**
8.	Inbreuk in verband met persoonsgegevens	**7**
9.	Geheimhouding	**7**
10.	Aansprakelijkheid	**7**
11.	Tussentijdse wijzigingen van het convenant en evaluatie	**8**
12.	Toepasselijke recht en geschillenbeslechting	**8**
13.	Contactpersonen	**8**
14.	Overige bepalingen	**8**
15.	Ondertekeningspagina's	**9-34**

Bijlagen

Bijlage I:	Overzicht met verwerkingen van persoonsgegevens	**35**
Bijlage II:	Overzicht met beveiligingsmaatregelen	**36**
Bijlage III:	Verwerkers	**37**

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 mevrouw [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 mevrouw [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 mevrouw [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 mevrouw [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 mevrouw [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 mevrouw [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 de heer [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 mevrouw [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 de heer [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 mevrouw [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 heer [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 mevrouw [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 mevrouw [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 de heer [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 de heer [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 mevrouw [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 de heer [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 mevrouw [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 de [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 de heer [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 de heer [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 de heer [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 de heer [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]
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 de heer [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 mevrouw S.V.H.Baas-Van Leeuwen

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 mevrouw A.M. van den Berg;

.....

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 mevrouw J. Baardman;

.....

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 mevrouw A.S. de Boer;

.....

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 mevrouw S. Dinsbach;

.....

Aldus overeengekomen en ondertekend in Assen, op 4 mei 2020

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 mevrouw K. Eeken;

.....

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 mevrouw C. van Esch;

.....

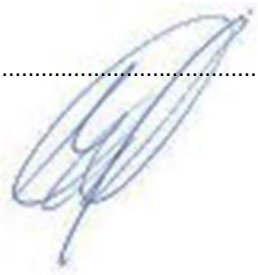
Aldus overeengekomen en ondertekend in Leiden op 29 april 2020

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 de heer J.M.M. de Gouw;

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 mevrouw M.I. de Graaf - Siegers;

.....



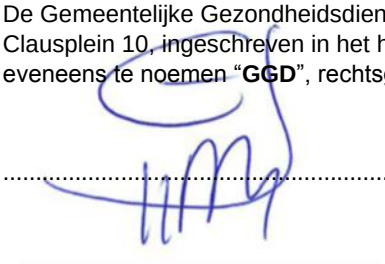
Aldus overeengekomen en ondertekend in Dordrecht, op 30 april 2020

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 heer K.J. van Hengel;

.....

Aldus overeengekomen en ondertekend in Eindhoven op 6 mei 2020

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 mevrouw E. Jeurissen;



.....

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 door de heer F.C.W. Klaassen: A.M.M. Baens

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 mevrouw J. Manshanden;

.....

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 mevrouw J. Gaemers;

.....

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 de heer E.J. Paulina;

E.J. Paulina

.....

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 de heer P. van der Velpen;

.....

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 eveneens te noemen "**GGD**", rechtsgeldig vertegenwoordigd door mevrouw M. Pieters;

.....

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 de heer A.A. Rietveld;

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 mevrouw N.A.M. Rigter;

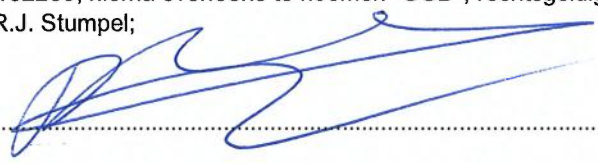
Aldus overeengekomen en ondertekend in Zaanstad, op 6/5/2020

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 de heer F.H.J. Strijthagen;

.....

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

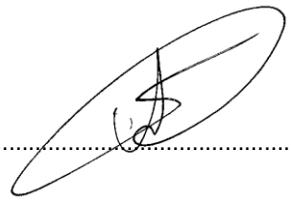
22. De Gemeentelijke Gezondheidsdienst Gooi & Vechtstreek, gevestigd te Bussum aan de Burgemeester de Bordesstraat 80, ingeschreven in het handelsregister onder KvK nummer 32152259, hierna eveneens te noemen "**GGD**", rechtsgeldig vertegenwoordigd door de heer A.R.J. Stumpel;



.....

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 de heer A. van de Velden;



.....

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 de heer C. Verdam;

drs. C. Verdam
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 de heer J.J. Rooijmans;

.....

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 mevrouw A. van der Zijden;

.....

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: C. Mast Contactgegevens: Christiaan.Mast@topicus.com
FG Verwerker:	Naam: Omko Huizenga Contactgegevens: fg.healthcare@topicus.nl

Wob-verzoek SOLV/ICAM datalek 2021 coronasysteem

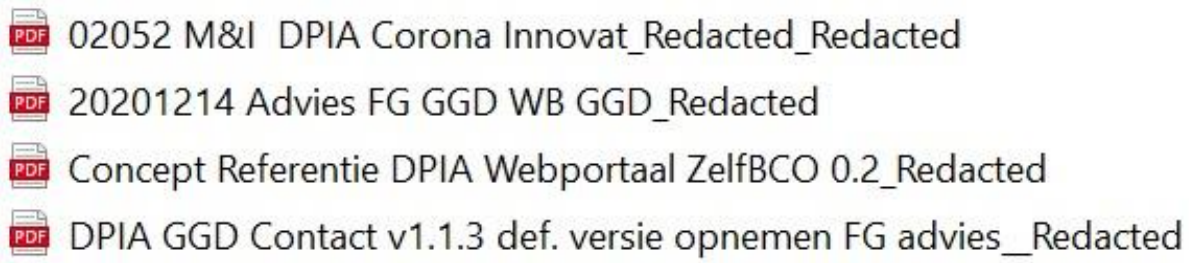
8.0 Tekst Wob-verzoek en register documenten

Tekst verzoek (viii)

Data Protection Impact Assessments (DPIA) ten aanzien van CoronIT, HPZone en HPZone Lite.

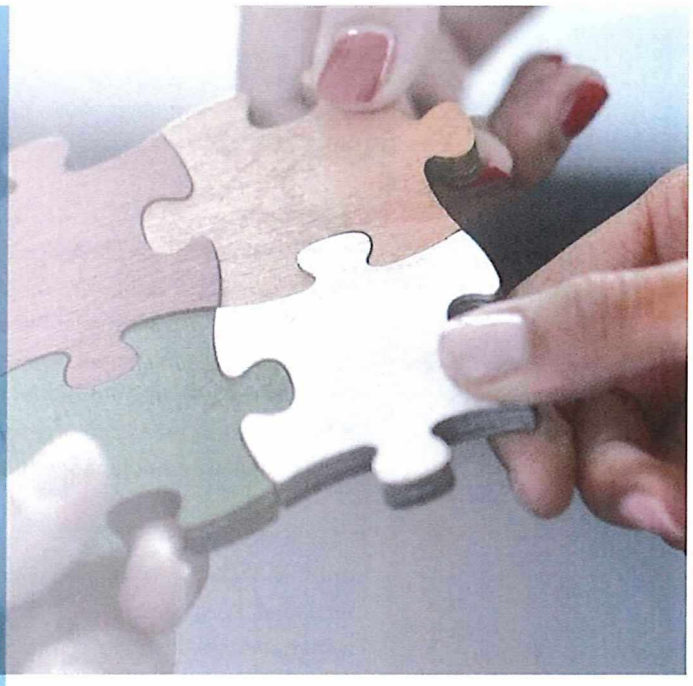
Register

Een screenshot van de verkennerpagina van map 8:



GGD West-Brabant

OFFERTE DPIA CORONA INNOVATIE



Sparrenheuvel 32, 3708 JE Zeist | (030) 2 270 500 | offertebureau@mxi.nl | www.mxi.nl

Project 20282
Versie 1.0 / 23 september 2020

Geachte [redacted]

Op 22 september 2020 hebben wij met uw collega [redacted] gesproken over een innovatieve toepassing die u wil inzetten om gegevens rondom bron- en contactonderzoek (BCO) te analyseren. De gegevens die hierbij verwerkt worden omvatten onder meer gezondheidsgegevens van betrokkenen, daarom is de uitvoering van een DPIA (Data Privacy Impact Assessment) een verplichting.

ONS AANBOD

Wij voeren DPIA's uit conform onze standaard methodiek, die wij later in deze offerte nader toelichten. Door de uitvoering van de DPIA kunt u aantoonbaar voldoen aan wet- en regelgeving.

Resultaat

Bij afronding van deze opdracht heeft u als opdrachtgever:

- Een volledig afgeronde DPIA conform de methodiek van M&I/Partners gericht op de gegevensverwerking binnen de door u beoogde verwerking. Dit bevat tenminste:
  - een beschrijving van de verwerking;
  - een beoordeling van de rechtmatigheid van de verwerking;
  - een analyse en weging van alle risico's die van toepassing zijn op deze verwerking;
  - concrete adviezen over de maatregelen die u kunt treffen om de gevonden privacy risico's te mitigeren;
- Volledige beschikking over de meest actuele versies van de door ons gebruikte sjablonen en methodiek.

Niet in scope:

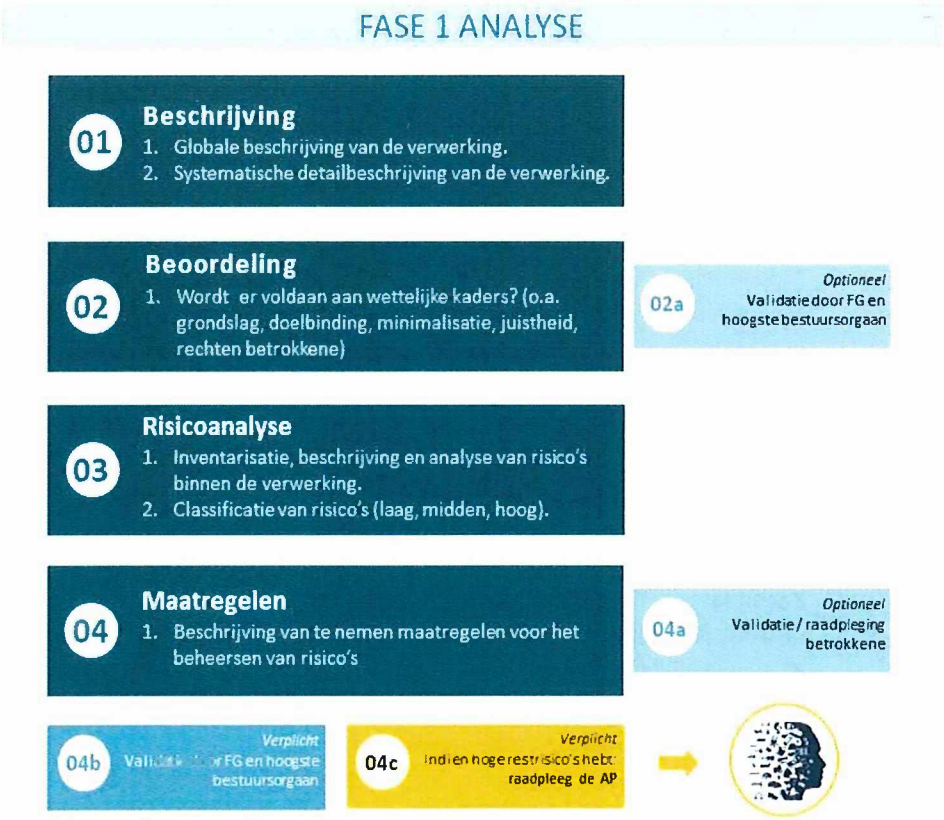
Implementatie van maatregelen op gevonden risico's valt buiten de scope van onze werkzaamheden.

ONZE VISIE

De uitvoering van een DPIA is onder de AVG een verplichting wanneer een verwerking aan specifieke criteria voldoet[1][2]. Vanuit M&I/Partners zijn we ervan overtuigd dat adequate uitvoering van DPIA's van grote toegevoegde waarde is. Een volledige, kritische analyse van een verwerking zorgt er volgens ons namelijk voor, dat de organisatie meer zicht en grip krijgt op de (persoons-) gegevens die gebruikt worden binnen een verwerking, de bewustwording van medewerkers verhoogd wordt en dat de urgentie van het uitvoeren van bepaalde maatregelen concreet onderbouwd met het management gedeeld kan worden.

ONZE AANPAK

Vanuit M&I/Partners hebben we een methodiek ontwikkeld om DPIA's uit te voeren. Deze methodiek is bij verschillende organisaties toegepast, zoals gemeente Amersfoort, gemeente Emmen, Veiligheidsregio Kennemerland, Veiligheidsregio Noord-Holland-Noord, het IFV, GGD GHOR Nederland en GGD Noord-Oost Gelderland. Hieronder geven wij onze aanpak grafisch weer.



[1] https://autoriteitpersoonsgegevens.nl/nl/zelf-doen/data-protection-impact-assessment-dpia#in-welke-gevallen-moet-ik-een-dpia-uitvoeren-5879

[2] https://autoriteitpersoonsgegevens.nl/nl/zelf-doen/data-protection-impact-assessment-dpia#voor-welke-soorten-verwerkingen-is-het-uitvoeren-van-een-dpia-verplicht-6667

Onze opdracht beperkt zicht tot fase 1 van het model. Met de uitkomsten van fase 1 kan Calculus zelf een verbeterprogramma opzetten, om eventueel geconstateerde risico's te mitigeren of beheersen.

Voor ieder van de stappen verrichten we de volgende werkzaamheden.

1 Beschrijving
   - 1.1 Uitvoeren van interviews
   - 1.2 Bestuderen documentatie
   - 1.3 Opstellen beschrijving
   - 1.4 Toetsen beschrijving

2 Beoordeling
   - 2.1 Beoordelen beschrijving o.b.v. van toepassing zijn de wet- en regelgeving
   - 2.2 Afstemming met uw bedrijfsjurist/FG/privacy officer over de beoordeling

3 Risicoanalyse
   - 3.1 Workshop voor het ophalen van risico's
   - 3.2 Uitwerken en wegen van risico's

4 Maatregelen
   - 4.1 Workshop (zelfde als voor de risico's) voor het ophalen van de maatregelen
   - 4.2 Uitwerken van de maatregelen en wegen van restrisico's na toepassen van de maatregelen

Team

[redacted] heeft ruime ervaring met het uitvoeren van DPIA's, hij heeft inmiddels tientallen DPIA's uitgevoerd/begeleid binnen verschillende organisaties.

[redacted]

[redacted]

Ik ben een gedreven, analytische en mensgerichte Privacy en IT-Security consultant die complexe uitdagingen aangaat. Ik weet generieke oplossingen te bedenken voor multidisciplinaire vraagstukken. Daarin bedenk ik niet alleen de oplossingen, maar zorg ik er ook voor dat de oplossingen worden geïmplementeerd. Ik ben in staat om, zowel schriftelijk als mondeling, complexe materie simpel uit te leggen. Terwijl ik me richt op het resultaat houd ik de verschillende belangen in de gaten en zorg ik ervoor dat de groep meebeweegt.

Investering

Wij bieden de uitvoering van deze DPIA aan voor een vast bedrag van [redacted], exclusief btw.

UITVOERING

Organisatie

U bent de opdrachtgever en het eerste aanspreekpunt voor M&I/Partners. [redacted] is het eerste aanspreekpunt vanuit M&I/Partners. Het DPIA-rapport wordt bij afronding opgeleverd aan u als opdrachtgever.

Planning

De uitvoering van een DPIA kost normaliter tussen de zes en acht weken doorlooptijd volgens onze standaard aanpak. Gezien uw wens om de DPIA zo spoedig mogelijk af te ronden, streven we naar een doorlooptijd van drie weken. Het behalen van deze doorlooptijd is met name afhankelijk van de beschikbaarheid van uw interne medewerkers en het tempo waarop informatie wordt aangeleverd.

Kwaliteit

Tevreden opdrachtgevers en het realiseren van oplossingen waar u als klant echt verder mee kan, vinden we bij M&I/Partners belangrijk. Daarom streven wij er naar in onze projecten continu de kwaliteit van de opdracht en onze dienstverlening te optimaliseren en te verbeteren. Leren van eerdere ervaringen is hierbij essentieel. Hiervoor hebben we een kwaliteitssysteem ingericht, waarin we de kwaliteitsbewaking en borging van onze projecten hebben ondergebracht: ISO 9001:2015. Wat betekent dit voor u?

- Voor dit project is [redacted] als de projectpartner eindverantwoordelijk voor de kwaliteit van deze opdracht en het aanspreekpunt rondom de kwaliteitsbewaking.
- Aan het begin van de opdracht voeren wij een risicoanalyse uit om mogelijke risico's te minimaliseren en eventuele voorzorgsmaatregelen te nemen.
- Tijdens de opdracht vinden er één of meerdere tussenevaluaties en/of voortgangsgesprekken plaats om onze kwaliteit continu te verhogen.
- Wij evalueren na afronding de opdracht met u om te groeien in onze professionaliteit.

VOORWAARDEN

Voor deze aanbieding gelden de volgende voorwaarden.

- Alle bedragen zijn exclusief btw.
- Reis- en verblijfkosten binnen Nederland worden niet doorbelast.

- Wij factureren onze werkzaamheden op basis van een vast bedrag. Dit bedrag is geldig onder de in de offerte genoemde condities. Bij gevraagde uitbreiding of wijziging van de werkzaamheden treden wij in overleg om nadere afspraken te maken.
- Wij hanteren het volgende betaalschema: 100% bij oplevering van de opdracht/rapportage.
- Voor deze opdracht gelden onze algemene voorwaarden.
- Deze offerte is geldig tot vijftien dagen na dagtekening.

TOT SLOT

Wij vertrouwen erop dat ons voorstel aansluit op uw wensen. Heeft u vragen of opmerkingen over dit voorstel, neemt u dan gerust contact met ons op. Als u akkoord gaat met ons voorstel, dan ontvangen we graag een ondertekende opdrachtbevestiging terug.

Wij zijn benieuwd naar uw reactie.

Met vriendelijke groet,
M&I/Partners^{bv}

[redacted]

Bijlagen:
1 profielschets;
2 opdrachtbevestiging met 20282.1 .

BIJLAGE 1 PROFIELSCHETSEN

De profielschetsen van de aangeboden adviseurs hebben wij separaat bijgevoegd.

BIJLAGE 2 ONDERBOUWING INVESTERING

BIJLAGE 3 REFERENTIES

BIJLAGE 4 OVER M&I/PARTNERS

M&I/Partners: het ICT-adviesbureau voor de zorg en overheid. Wij zijn al jarenlang een betrouwbare partner voor alle ICT-oplossingen, strategisch en tactisch. We leveren maatwerk en hebben ruim drie decennia ervaring, waarbij meer dan 100 vakgedreven professionals voor u klaar staan. Wij geloven in de kracht van ICT. Ons doel: klantgerichte, effectieve en efficiënte organisaties.

ICT-strategie en realisatie
Wij adviseren u bij het ontwikkelen van uw digitale en *ICT-strategie* en ondersteunen bij de bestuurlijke vragen die daaruit voortvloeien. Ook werken we aan de realisatie van uw plannen in de vorm van *projectleiding*, implementatiemanagement of *interim-management*. Wij gaan voor resultaat, voor (ICT-)oplossingen die werken. Wij kiezen voor opdrachten met maatschappelijke meerwaarde en zijn voornamelijk actief in de *care*, *cure*, *Rijksoverheid*, *lokale overheid* en *veiligheidsregio's*. *Ontdek onze klantsuccessen* waar wij bouwen aan een digitale wereld die mensen écht vooruit helpt.

Sparringpartner
Wij zijn een betrouwbare sparringpartner op elk niveau en durven stelling te nemen. Wij kennen de publieke sector en zijn pragmatisch ingesteld zodat u uw organisatie en ICT naar een hoger niveau kunt brengen. Enthousiasme helpt ons om het beste resultaat te bereiken. Wij nemen onze klant mee in het proces en *delen actief onze kennis.*

Daag ons uit
Daag ons uit met vraagstukken over uw digitale strategie, transformatie en realisatie! Wij helpen u graag met strategisch advies om toekomstbestendig te zijn én te blijven in het huidige digitale tijdperk.

Bekijk onze website voor meer informatie: *www.mxi.nl.*

BIJLAGE 5 OPDRACHTBEVESTIGING

De opdrachtbevestiging hebben wij separaat bijgevoegd.

M&I/Partners/

adviseurs voor management en informatie

OPDRACHTBEVESTIGING 20282.1

De ondergetekenden,

I. GGD West-Brabant, gevestigd te Breda, Doornboslaan 225, hierna te noemen opdrachtgever,

en

II. M&I/Partners^{bv}, gevestigd te Zeist, Sparrenheuvel 32, hierna te noemen M&I/Partners,

zijn als volgt overeengekomen:

1 Opdrachtgever verleent M&I/Partners opdracht en M&I/Partners aanvaardt de opdracht voor het uitvoeren van de volgende werkzaamheden: uitvoeren DPIA.

2 M&I/Partners start zo snel mogelijk met de hiervoor genoemde werkzaamheden en partijen verwachten dat de werkzaamheden zo spoedig mogelijk afgerond zijn.

3 De werkzaamheden worden uitgevoerd door:

Naam	Functie	Vaste prijs (excl. btw)
[redacted]	Adviseur	[redacted]

4 Op deze overeenkomst zijn de algemene voorwaarden van M&I/Partners van toepassing.

5 M&I/Partners heeft de mogelijkheid de opdrachtgever en opdracht als referentie te vermelden. Mocht opdrachtgever hier niet mee akkoord gaan dan volstaat doorhalen van deze zin.

6 Bijzonderheden: zie offerte 20282, versie 1.0 van 23 september 2020.

Aldus overeengekomen:

Breda, datum: 18 sept. 2020

GGD West Brabant

Naam: [redacted]

Functie: bedrijfsarts

Zeist, 23 september 2020

M&I/Partners^{bv}

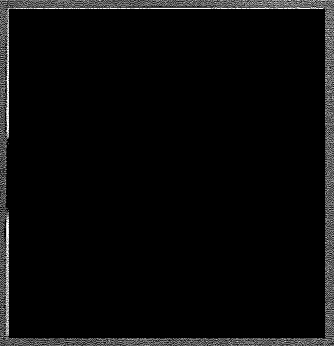
[redacted]

Principal adviseur

[redacted]
Adviseur

[redacted]

Leeftijd:
Woonplaats: [redacted]



Ik ben een gedreven, analytische en een mensgerichte Privacy en IT-Security consultant die complexe uitdagingen aangaat. Ik weet generieke oplossingen te bedenken voor multidisciplinaire vraagstukken. Daarin bedenk ik niet alleen de oplossingen, maar zorg ik er ook voor dat de oplossingen worden geïmplementeerd. Ik ben in staat om, zowel schriftelijk als mondeling, complexe materie simpel uit te leggen. Terwijl ik me richt op het resultaat houd ik de verschillende belangen in de gaten en zorg ik ervoor dat de groep meebeweegt.

ERVARING

4> jaar advieservaring

3> consulent Inkomen

EXPERTISE

Privacywetgeving
Informatiebeveiliging
Privacy By Design
Privacy Risico Analyses (DPIA's)
Big Data/Onderzoek en Privacy
API Security
Privacy Awareness en Serious Gaming

ROLLEN

Adviseur
Verbinder
Inspirator
Procesbeschrijver

MARKTEN

Lokale overheid/gemeenten

UITGELICHT

Het opzetten van een generieke privacy governance voor datagedreven sturing binnen de gemeente Utrecht. Daarin heb ik ervoor gezorgd dat een leek op het gebied van privacy, persoonsgevoelige data kan delen, koppelen en gebruiken (voor o.a. onderzoek en Big Data toepassingen). Hierbij bied ik technische handvatten zoals pseudoniemiseren en anonimiseren. Dat heb ik gedaan door het ontwikkelen van een simpel te gebruiken data privacy framework (stappenplan), met daarin geïmplementeerd een specifieke framework voor Privacy by Design. Het datateam van de Gemeente Utrecht maakt ook gebruik van een Datawarehouse. Hiervoor heb ik een DPIA uitgevoerd, zodat data op een veilige manier wordt geprepareerd en klaargezet.

OPDRACHTEN

Zadkine Rotterdam

Verhogen bewustwording privacy en informatieveiligheid

De opdrachtgever wil bewustwording op het gebied van privacy en informatieveiligheid vormgeven, zodat er structureel bewustwordingsacties worden uitgevoerd en daarmee de bewustwording onder de medewerkers wordt verhoogd. Op basis van meetinstrumenten kan worden bijgehouden hoe bewust medewerkers zijn.

Consultant Privacy & IT Security

september 2020 - december 2020

RUD Zeeland

Uitvoeren nul meting AVG

De opdrachtgever wil weten hoe het ervoor staat binnen de organisatie op het gebied van informatiebeveiliging en privacy. Samen met een collega van M&I Partners voeren we een nul meting BIO & AVG uit.

Consultant Privacy & IT Security

augustus 2020 - oktober 2020

Calculus Software B.V.
Uitvoeren DPIA
Calculus Software B.V. beschikt over een softwareplatform dat gebruikt wordt in de zorg. Onderdeel van dat platform is een applicatie die zorgspecialisten gebruiken om vragenlijsten af te nemen bij patiënten en te monitoren. Om te voldoen aan de AVG voer ik op dat proces een DPIA uit.
Consultant Privacy & IT Security
juli 2020 - september 2020

Gemeente Amersfoort
Begeleiden en adviseren bij DPIA's
M&I Partners heeft in 2019 verschillende DPIA's uitgevoerd en medewerkers opgeleid om zelf DPIA's uit te voeren. De medewerkers die DPIA's uitvoeren worden door mij begeleid en krijgen advies. Daar waar nodig spring ik bij.
Consultant Privacy & IT Security
februari 2020 - juni 2020

Gemeente Emmen
Uitvoeren van DPIA's datagedreven sturing en het geven van workshops DPIA
Het datalab binnen de Gemeente Emmen is in het leven geroepen om datagedreven sturing mogelijk te maken. Het BI team dat onderdeel is van het datalab maakt gebruik van een datawarehouse en werkt nauw samen met onderzoekers. Voor het datawarehouse en het doen van onderzoek voer ik DPIA's uit.
Ook worden workshops voor het doen van DPIA's verzorgd, zodat de gemeente in de toekomst zelf in staat is DPIA's uit te voeren.
Consultant Privacy & IT Security
februari 2020 - juni 2020

Gemeente Emmen
Inrichten privacy governance
Het inrichten van een gemeentebrede privacy governance. Daarbij wordt de huidige situatie in kaart gebracht en wat gedaan moet worden om de gemeente privacyproof te maken (ist and soll). Op basis van input van stakeholders, bestaand beleid en bestaande procesbeschrijvingen zal een op maat gemaakte privacy governance opgeleverd worden.
De privacy governance wordt ondersteund door een plan van aanpak voor de uitvoering ervan en een op maat gemaakt dashboard voor monitoring (PDCA).
Consultant Privacy & IT Security
februari 2020 - juni 2020

Studiecentrum Bedrijf en Overheid
Les geven over Privacy en IT Security
Trends in Big Data en de invloed van privacywetgeving. Datawarehousing in relatie tot privacywetgeving. Basiskennis van cybersecurity. Het integraal borgen van privacywetgeving en IT-security in een organisatie.
Gastdocent
januari 2019 - heden

Gemeente Utrecht
Big Data en Onderzoek in relatie tot Privacy, API security en Bewustwording
Het opzetten van een privacy governance voor Big Data, zodat onderzoekers en data scientisten voldoen aan privacywetgeving en rekening houden met ethiek. Het secure maken van datawarehousing door o.a. een DPIA op te stellen. API-security borgen door het ontwikkelen van een best practice. Privacy by Design inbedden in Enterprise Architectuur, inkoop en projectmanagement methode (waterval). Groot en gemeentebreed privacy bewustwordingsevenement georganiseerd door drie stagiaires (Hogeschool Utrecht, Marketing en Communicatie), onder begeleiding van mij. Daarnaast hebben ze een generieke bewustwordingstoolkit gemaakt voor managers.
Adviseur Privacy & IT Security
januari 2018 - februari 2020

Gemeente Utrecht
Bewustwording, risico analyses en Privacy by Design
Als één van de eerste binnen de Gemeente Utrecht voerde ik DPIA's uit, schreef daarvoor een generieke procesbeschrijving, hielp mee met het uitwerken van een eigen DPIA-methodiek, gaf workshops over "hoe je DPIA's uitvoert" en begeleidde verschillende DPIA-trajecten. Daarnaast creëerde ik op verschillende wijze (quizzen, presentaties, gaming etc.) bewustwording op verschillende afdelingen, voornamelijk IT-organisatie. Het ontwikkelen en implementeren van Privacy by Design methodiek en daarover workshops geven. Adviseren, opstellen en ontwikkelen van overeenkomsten.
Trainee Adviseur Privacy & IT Security
september 2016 - januari 2018

Gemeente Utrecht
Aanjager voor de afdeling Consulenten Inkomen
Verbeteren van werkprocessen (lean methodiek), verbeterplan opgesteld voor de afdeling en het afhandelen van bijstandsaanvragen.
Trainee Allround Inkomensconsulent
maart 2016 - augustus 2016

Gemeente Overbetuwe
Efficiënter werken
Eerste contactpersoon binnen de afdeling Werk en Inkomen voor IT-vragen en heb nieuwe ideeën bedacht, zodat er efficiënter gewerkt wordt.
Key User
januari 2015 - maart 2016

Gemeente Overbetuwe
Beleidsmedewerker
Afhandelen van bijstandsaanvragen, terugvorderingen en kwijtscheldingen. Achtervang WMO.
Consulent Inkomen
juni 2014 - maart 2016

Gemeente Arnhem
Efficiënter werken
Beslisboom gemaakt waarmee voorkomen wordt dat onnodige bijstandsaanvragen ingediend worden, waarvan op voorhand duidelijk is dat de aanvraag wordt afgewezen. Na succesvolle implementatie en resultaten heb ik verschillende organisatieonderdelen daarin geadviseerd.
Procesadviseur
2014

Gemeente Arnhem
Beleidsmedewerker
Afhandelen van bijstandsaanvragen.
Consulent Inkomen
februari 2013 - juni 2015

OPLEIDING

[redacted]

DIPLOMA'S EN CERTIFICATEN
- Certified Information Privacy Professional Europe (CIPP/e)
- Gemeente Utrecht, Agile, Scrum en Lean
- Security Academy, CISSP
- UvA, Masterclass: Privacy the next step

- Nationale AI Cursus
- HAN, Data Protection Officer (DPO)
- Participatiewet

NEVENFUNCTIES

- Gastdocent bij Studiecentrum Bedrijf en Overheid.

Bijlage - Advies [redacted] GGD West-Brabant aangaande de op 'GGD Contact' uitgevoerde DPIA

Inleiding

In opdracht van de leden van GGD GHOR Nederland (hierna: 'de vereniging') heeft de vereniging een gegevensbeschermingseffectbeoordeling ex. artikel 35 AVG (hierna: 'DPIA') uitgevoerd over een nieuw app die het bron- en contactonderzoek moet ondersteunen (hierna: 'GGD contact').
De inzet van GGD contact beoogt een snellere en minder foutgevoelige uitvoering van het bron- en contactonderzoek. De functionaris voor gegevensbescherming van de GGD West-Brabant (hierna: 'FG') is van meet af aan betrokken bij de totstandkoming van de DPIA en heeft lopende de beoordeling geadviseerd. Deze adviezen waren met name gericht op het doel, de grondslag, de noodzaak en evenredigheid en de betrokken partijen. Veel van deze adviezen zijn in het eindrapport verwerkt.

Voorliggend advies beschouwt het eindrapport van de DPIA en gaat achtereenvolgens in op de volgende onderdelen:

- Rechten van betrokkenen;
- Doelbinding;
- Noodzaak- en evenredigheid;
- Manifestatie nieuwe risico's in verband met doorontwikkeling;
- Lokale technische en organisatorische maatregelen ter beveiliging van de verwerking.

De FG concludeert dat slechts met inachtneming van ongenoemde en eerder gestelde adviezen er gestart kan worden met de verwerkingen die gepaard gaan met 'GGD contact'.

Rechten van betrokkenen: vrijwillig gebruik en correctierecht

Informeren index

Mede gelet op het ontbreken van een wettelijke omlijsting is het in de ogen van de FG noodzakelijk index er door de verwerkingsverantwoordelijke, voorafgaand aan de start van het gebruikt van de app, er actief op worden gewezen dat het gebruik -vrijwillig- is en dat het gebruik op ieder gewenst moment kan worden gestaakt.

Recht op correctie en recht op gegevenswissing ("recht op vergetelheid")

De FG acht het van belang dat degene waaraan gevraagd wordt gebruik te maken van GGD contact (hierna: "de index") actief wordt gewezen op het correctierecht ex artikel 12 en 16 uit de AVG. Hoewel het de bedoeling is om juist minder fouten te maken bij het bron- en contactonderzoek is de kans dat abusievelijk onjuiste of onvolledige persoonsgegevens worden doorgegeven door de index aanwezig. Deze moet dan, ook in het belang van de andere betrokkenen (de contacten) een eenvoudige mogelijkheid hebben persoonsgegevens te corrigeren en, of te verwijderen.
Dit recht strekt zich tot de volledige keten van de verwerking, dat wil zeggen vanaf de App tot aan HP zone.
De verwerkingsverantwoordelijke zal haar processen zodanig moeten inrichten dat dit recht kan worden toegekend.

Doelbinding: geen doel? Staken verwerking!

In de DPIA is als hoofddoel van de GGD Contact App omschreven als:

“Het doel van de app GGD Contact is om het aantal uur dat GGD per index besteedt aan bron- en contactopsporing te verminderen, waardoor GGD voor meer indexen bron- en contactopsporing kan uitvoeren.”

Dit betekent dat als uit het evaluatieonderzoek blijkt dat er geen winst wordt gehaald op het gebied van de snelheid van het bron- en contactonderzoek, het doel van de verwerking ontbreekt en daarmee onrechtmatig is.

Het is zaak de verwerking onmiddellijk te staken op het moment dat blijkt dat de verwerking van persoonsgegevens haar doel verliest.

Noodzaak en evenredigheid: geen noodzaak? Staken verwerking!

Aansluitend op bovenstaande passage aangaande de doelbinding geldt voor het doorbreken van het verbod op werkwerking een noodzakelijkheidseis. Op het moment dat blijkt dat het gebruik van de GGD contact app niet noodzakelijk is voor het bron- en contactonderzoek, dient de verwerking onmiddellijk te worden gestaakt. Deze noodzaak kan blijken uit een negatieve uitkomst van het evaluatieonderzoek

Herziening DPIA bij introductie nieuwe risico's

De GGD contact app is nog steeds aan (door)ontwikkeling onderhevig. Mocht het zo zijn dat er een kans bestaat dat er nieuwe risico’s worden geïntroduceerd, dan is het van belang dat de DPIA hierop wordt bijgesteld.

Passende technische maatregelen ter borging van het beveiligingsniveau

Het gebruik van de GGD contact app brengt eveneens wijzigingen met zich mee die betrekking hebben op de inrichting van de technische maatregelen aan de zijde van de GGD. Hieronder valt bijvoorbeeld te denken aan een aanpassing van de zgn. firewall om toegang tot de backend server mogelijk te maken.
Het is van belang om in strikte zin te beoordelen of een of wijziging beveiligingsinstellingen aan de GGD zijde nieuwe risico’s introduceert. Mocht dit zich voordoen, dan zullen hier ook (mitigerende) maatregelen op genomen moeten worden.

Conclusie

De GGD contact app introduceert nieuwe, niet eerder toegepaste verwerkingen van persoonsgegevens. In de ogen van de FG is het derhalve van het grootste belang hier zorgvuldig mee om te gaan en bij voortduring het belang en de positie van de betrokkene(n) in ogenschouw te houden.

Uitsluitend indien het effect van de verwerkingsactiviteiten van ‘GGD contact’ op de bescherming van persoonsgegevens beperkt blijven en mits er actieve opvolging wordt gegeven aan eerder en genoemde adviezen, kan gestart worden met de werking.

Breda, 14 december 2020

[redacted]

[redacted]

GGD West-Brabant RAV Brabant Midden-West-Noord

Referentie Gegevensbeschermingseffectbeoordeling ten behoeve van GGD'en (GEB/DPIA)

Webportaal ZelfBCO

Datum: december 2021
Documentversie: 0.2

TLP:AMBER

Beperkte verspreiding, uitsluitend bestemd voor de organisaties van de deelnemers (meer info zie: https://www.first.org/tlp/docs/tlp-v1-nl.pdf).

Dit Referentiemodel DPIA voor ZelfBCO Webportaal is opgesteld door:

[redacted]

Ministerie van Volksgezondheid, Welzijn en Sport, directie Informatiebeleid, CIO
Programma Realisatie Digitale Ondersteuning COVID-19 bestrijding

Versiebeheer

Datum	Versie	Wie	Toelichting
23-12-2021	0.1	[redacted]	Eerste versie voor pilot regio's
24-12-2021	0.2	[redacted]	Aanscherping AVG-rollen, toevoeging paragraaf Labels, Bijlage 1 (overzicht verwerkte data met grondslag en doelbinding) en Bijlage 2 (overzicht vragen en labels)

Dit referentiemodel is uitgewerkt op basis van het Rijksmodel DPIA

Toelichting versie:

0.1 *Deze DPIA ziet alleen op het Webportaal ZelfBCO. Deze zal als eerste door de pilotregio's in gebruik worden genomen. Deze DPIA is het een eerste concept op basis van het beschreven ontwerp, de door WJZ getoetste juridische analyse op grondslagen en doelbinding. Dit eerste concept is bedoeld om de regio's een basis te geven voor de wijze waarop het portaal is gebouwd, hoe privacy en security by design is toegepast en om procesafspraken te faciliteren om tot een volgende en gereviewde versie te komen. Parallel aan de doorontwikkeling van de webportalen zal tevens deze DPIA worden doorontwikkeld.*

Inhoud

Inleiding 4
A. Beschrijving kenmerken gegevensverwerkingen 5
1. Voorstel: Webportaal ZelfBCO 5
2. Persoonsgegevens 6
3. Gegevensverwerkingen 7
4. Verwerkingsdoeleinden 8
5. Betrokken partijen 8
6. Belangen bij de gegevensverwerking 10
7. Verwerkingslocaties 11
8. Techniek en methode van gegevensverwerking 11
9. Juridisch en beleidsmatig kader 12
10. Bewaartermijnen 13
B. Beoordeling rechtmatigheid gegevensverwerkingen 14
11. Rechtsgrond 14
12. Bijzondere persoonsgegevens 14
13. Doelbinding 14
14. Noodzaak en evenredigheid 14
15. Rechten van de betrokkene 15
C. Beschrijving en beoordeling risico's voor de betrokkenen 16
Risico 1 – Onbevoegden hebben toegang tot persoonsgegevens in Webportaal ZelfBCO 16
Risico 2 – Bij de externe hosting provider vindt een datalek plaats 16
D. Beschrijving voorgenomen maatregelen 17
17. Maatregelen 17

Inleiding

Het Outbreak Management Team (**OMT**) heeft in haar advies aan het kabinet een zeer zorgwekkend beeld geschetst van de COVID19-situatie in Nederland[1]:

- De omikron-variant verspreidt veel sneller dan deltavariant
- Bescherming door eerdere besmetting of vaccinatie lijkt beperkter
- Ziektelast is nog onduidelijk

In dit OMT-advies wordt aandacht gevraagd voor het inrichten en beschikbaar stellen van elektronische systemen voor het melden van positieve zelftesten, en het uitvoeren van bron-contactonderzoek (**BCO**) door de index zelf. Het OMT heeft in haar eerdere adviezen ook aandacht gevraagd voor vormen van zelf BCO. [nog aanvullen met voetnoten]. De minister van Volksgezondheid, Welzijn en Sport (**VWS**) heeft in zijn kamerbrief naar aanleiding van het OMT-advies aangekondigd dat er twee portalen worden gebouwd door VWS:

- ZelfBCO: een Webportaal voor het verzamelen van informatie ten behoeve van BCO van een Index door de GGD (**Webportaal ZelfBCO)**;
- Een zelftesten meldportaal voor het melden van uitslagen van zelftesten (**Zelftestmelden**).

Deze DPIA ziet op Webportaal ZelfBCO. De activiteit die hierin plaatsvindt is te zien als een intake van vragen ten behoeve van het BCO door de GGD.

Niet in scope van deze DPIA zijn het reguliere GGD BCO Proces, GGD Contact / BCO Webportaal (zie daarvoor de recente DPIA GGD Contact) of de verwerking door het RIVM.

[1] Advies n.a.v. 134e OMT (via: https://www.rijksoverheid.nl/documenten/brieven/2021/12/18/advies-vws-nav-omt-134-met-aanpassing)

A. Beschrijving kenmerken gegevensverwerkingen

1. Voorstel: Webportaal ZelfBCO

GGD'en en RIVM hebben beiden belangrijke taken binnen het bestrijden van infectieziekten, die bij wet zijn vastgelegd. Taken van de GGD binnen infectieziektebestrijding zijn o.a. het verwerken van vermoeden of vaststellen van COVID-19, het uitvoeren van BCO, het uitvoeren van analyses en het onverwijld doorgeven van informatie aan het RIVM.

Met de huidige infectiedruk lukt het niet meer om alle positief geteste personen te bereiken en is het uitvoeren van BCO erg lastig. Door met Webportaal ZelfBCO aan de voorkant van het BCO-proces, direct bij het ontvangen van een testuitslag) een vorm van triage toe te passen kan:

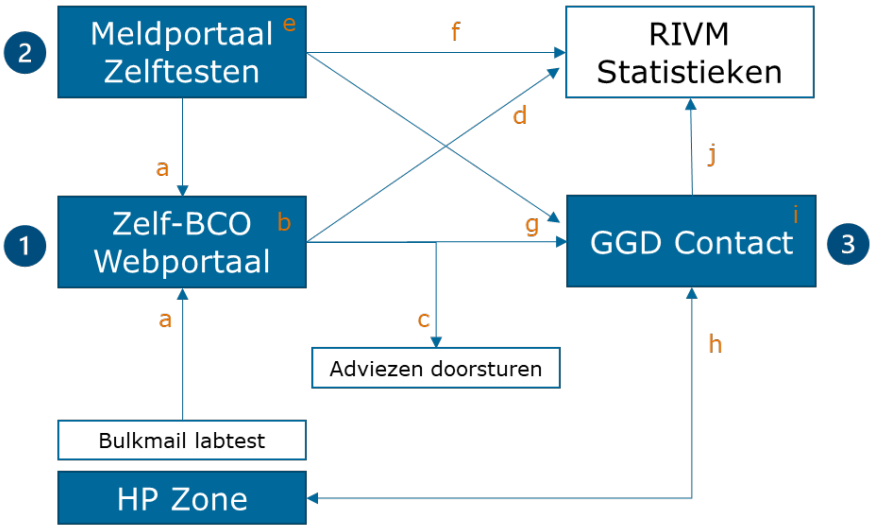
- een index sneller worden voorzien van het juiste handelingsperspectief
- er sneller informatie worden verstrekt en enigszins zicht op de verspreiding van het virus, effectiviteit van vaccins en andere maatregelen worden gehouden.

De activiteit die plaatsvindt in Webportaal ZelfBCO is te zien als zelfintake door de index ten behoeve van het BCO door de GGD. Deelname door de index aan Webportaal ZelfBCO is vrijwillig. GGD'en die van Webportaal ZelfBCO gebruik maken, bereiken daarmee het volgende in het kader van de infectieziektebestrijding:

De Webportaal ZelfBCO en Webportaal Zelftestmelden worden los van elkaar gebruikt. Technisch gezien zijn beide portalen onderdeel van een bredere infrastructuur. Hiervan maken ook de volgende systemen deel van uit:

- CoronIT: systeem van de GGD'en waarin alle positieve testuitslagen worden verwerkt en doorgegeven aan HPZone.
- GGD Contact: systeem dat momenteel is ontwikkeld om HPZone (lite) te kunnen vervangen ten behoeve van BCO. Omdat dit systeem nog niet voorziet in een koppeling met het RIVM, worden alle in GGD Contact verwerkte data gesynchroniseerd met HPZone. GGD Contact bestaat uit GGD Contact App en BCO Portaal.
- HP Zone: het "oude" systeem van de GGD'en voor het uitvoeren van BCO. Van hieruit worden op dit moment indien BCO wel uitgevoerd kan worden gegevens gedeeld met het RIVM.

Schematisch ziet de samenhang van Webportaal ZelfBCO en Webportaal Zelftestmelden er als volgt uit:



Toelichting:

1. **Webportaal ZelfBCO**
   a) Index wordt na een positieve test (conform geldende regelgeving) gewezen op de vragenlijsten en uitgenodigd (via bulkmail) in te loggen, waarbij gebruik wordt gemaakt van een unieke identifier in de link, en wordt zo doorgestuurd naar het Webportaal ZelfBCO.
   b) Index beantwoordt, na DigiD login, een subset vragen van de Osiris[2]-vragenlijst.
   c) Index ontvangt vroegtijdig isolatie-advies en actuele adviezen voor verschillende typen contacten (in de vorm van verwijzingen naar bestaande info) om zelf te delen met eigen netwerk.
   d) RIVM ontvangt gepseudonimiseerde data t.b.v. onderzoekstatistieken.

[Toekomstig]

2. **Meldportaal zelftesten (Webportaal Zelftestmelden)**
   e) Index meldt zelftest op een portaal achter DigiD, beantwoordt een subset vragen van Osiris-vragen en krijgt een handelingsperspectief (isolatieadvies en wel/niet testen).
   f) RIVM ontvangt gepseudonimiseerde data t.b.v. onderzoekstatistieken.

3. **GGD Contact (BCO-portaal)**
   g) Positieve meldingen met ingevulde vragen uit ZelfBCO en Zelftestmelden komen beschikbaar in GGD Contact. Sorteren en prioriteren gebeurt o.b.v. risico indicatie middels labels.
   h) Indien er een bestaand dossier is (d.w.z. dat er een geverifieerd testresultaat aanwezig is) worden de gegevens die door de index zijn ingevuld gekoppeld aan de case in het GGD Contact.
   i) Risico-gestuurd BCO wordt uitgevoerd door BCO'er van de GGD.
   j) Na uitvoering BCO worden via bestaande koppeling gegevens aangeleverd bij RIVM.

2. Persoonsgegevens

In beide Portalen worden de volgenden categorieën persoonsgegevens verwerkt:

- Gegevens om vast te stellen wie je bent en om de informatie die je op deze website geeft op een waardevolle manier te kunnen verwerken.
  - Bij succesvol inloggen met DigiD wordt je BSN verstrekt. Om dit zo veilig mogelijk te doen, worden in het Webportaal ZelfBCO niet de cijfers van het BSN opgeslagen. In plaats daarvan worden deze samen met een aantal andere gegevens versleuteld tot een unieke persoonlijke code, die door anderen dan de GGD niet is te herleiden naar een persoon. Daarmee is het wel

[2] Osiris-vragenlijst is de vragenlijst die tot standkomt in afstemming tussen GGD'en en RIVM ten behoeve van infectieziektebestrijding.

mogelijk om binnen GGD Contact dossiers te koppelen van een uniek persoon, zonder dat we het volledige BSN onnodig lang hoeven op te slaan.
    - Daarnaast wordt er gebruik gemaakt van een koppeling met SBV-Z/BRP. Hierbij worden een aantal gegevens automatisch opgehaald uit de Basisadministratie Personen, zoals het adres waar je bent ingeschreven, je geboortedatum en je geslacht. Deze gegevens zijn belangrijk om het verloop van de pandemie goed te kunnen volgen en te analyseren.
- Gegevens over de testuitslag die je meldt, zoals de testdatum, de uitslag en het type test dat is afgenomen.
- Gegevens die gebruikt kunnen worden om de bron van de besmetting vast te stellen. Bijvoorbeeld de datum waarop je de eerste gezondheidsklachten kreeg, de omgeving en waarin je mogelijk besmet bent geraakt en het tijdstip van besmetting. Bent je mogelijk in een omgeving besmet waar veel kans is dat ook anderen hier zijn besmet, zoals een vliegtuig of een woonvorm waar ook veel anderen wonen, dan kun je dit ook aangeven. Hetzelfde geldt als je een beroep hebt waarin je veel met anderen te maken hebt, zoals in de zorg of in het onderwijs.
- Gegevens om het risico te kunnen bepalen dat je loopt. Dit is bijvoorbeeld informatie over je gezondheid of over zwangerschap, of over je vaccinatiestatus.
- Gegevens over je contacten in de besmettelijke periode. Hierdoor kunnen zij worden gewaarschuwd en een advies krijgen dat is toegesneden op het risico dat zij lopen.
- Je e-mailadres en/of telefoonnummer, om je op een snelle manier te kunnen bereiken als de GGD n.a.v. van de door jou ingevulde gegevens graag contact met je wil opnemen.

Omdat met het Portaal gebruik wordt gemaakt van het internet zal ook je IP-adres verwerkt worden. Het IP-adres wordt enkel verwerkt voor beheers- en beveiligingsdoeleinden.

Gezien de aard van de verwerking in Webportaal ZelfBCO hebben alle verwerkte gegevens direct of indirect betrekking op de gezondheid van een persoon.

Een volledig overzicht van de gegevens die Webportaal ZelfBCO verwerkt wordt is opgenomen in **Bijlage 1**. In **Bijlage 2** zijn alle vragen opgenomen zoals deze gesteld worden in het Webportaal ZelfBCO.

Labels
Alle meldingen die in de Portalen worden gedaan worden tijdelijk opgeslagen in GGD Contact. Deze zijn alleen zichtbaar voor medewerkers die binnen de GGD'en de rol van werkverdeler hebben. Deze medewerkers hebben o.a. tot taak het uitvoeren van triage over de door hen ontvangen meldingen. Om dit ook bij grote meldingsaantallen te kunnen doen, worden meldingen op basis van de in het portaal ingevoerde gegevens een label toegevoegd. Een overzicht van de gestelde vragen en het label dat op basis daarvan aan een case wordt toegekend is opgenomen in **Bijlage 2**.

De in de Webportalen gebruikte labels zijn een subset van de labels die in GGD Contact handmatig aan een case kunnen worden toegevoegd. Hieraan is één extra label toegevoegd, namelijk "gezondheidsindicatie". Doel hiervan is om het voor de GGD'en mogelijk te maken om deze specifieke groep apart te benaderen.

3. Gegevensverwerkingen

In en rondom het Webportaal ZelfBCO vinden de volgende verwerkingen plaats:

1. Verwijzing naar Webportaal ZelfBCO
   Een index ontvangt een verwijzing naar het ZelfBCO Webportaal via: (a) bulkmail, (b) verwijzing vanuit Meldportaal Zelftest, (c) verwijzing vanuit coronatest.nl.
2. Identificatie met DigiD.
   Index logt in met DigiD, waardoor gewaarborgd wordt dat de vragenlijst voor de juiste persoon wordt ingevuld (resultaat = BSN).
3. SBV-Z: na succesvolle inlog via DigiD wordt via de SBV-Z koppeling (of BRP bij uitval SBV-Z) met een lookup Postcode 3, geboortedatum en gender en een pseudoBSN teruggegeven en wordt BSN weggegooid.
4. Invullen triage vragenlijst
   De index doorloopt de vragenlijst van 13 vragen (een verkorte Osiris-vragenlijst).

5. Index ontvangt advies en handelingsperspectief
   Index ontvangt direct na afronding vragenlijst (isolatie) advies en handelingsperspectief m.b.t. informeren contacten.
6. Doorzetten gegevens naar GGD voor BCO en RIVM voor statistieken
   Intakevragenlijst worden automatisch gekoppeld aan cases indien deze al in GGD Contact staan. Een case kan ook met behulp van de BCO sync extensie worden overgezet naar het BCO-portaal, waarna de informatie uit de intakevragenlijst hier automatisch ingeladen wordt. Dit zorgt ervoor dat BCO sneller kan worden afgehandeld.

4. Verwerkingsdoeleinden

Het goed kunnen uitvoeren van BCO is van belang voor de gehele keten van infectieziektebestrijding. Zonder actuele en relevante data ontbreekt het aan het benodigde inzicht om de pandemie te kunnen volgen en bestrijden. Het BCO is daarin van cruciaal belang, zo wordt ook in diverse OMT-adviezen onderschreven. Het Webportaal ZelfBCO kan daarin een grote bijdrage leveren om BCO te kunnen uitvoeren, dit te versnellen en efficiënter te kunnen uitoefenen. Ook is BCO van belang om de index en zijn contacten te voorzien van relevantie informatie over het handelingsperspectief.

Bij grote aantallen nieuwe besmettingen is het mogelijk dat de testcapaciteit bij de GGD'en tekortschiet. Als gevolg hiervan worden dan niet meer alle besmettingen bij de GGD geregistreerd, waardoor door de gehele keten van infectieziektebestrijding aan informatie ontbreekt, wat een onwenselijke situatie. Hoofdoel van Webportaal ZelfBCO is het bedienen van de keten van infectieziektebestrijding om informatie over COVID-19 besmettingen te verzamelen en de index en contacten van noodzakelijke informatie te voorzien ten aanzien van de besmetting.

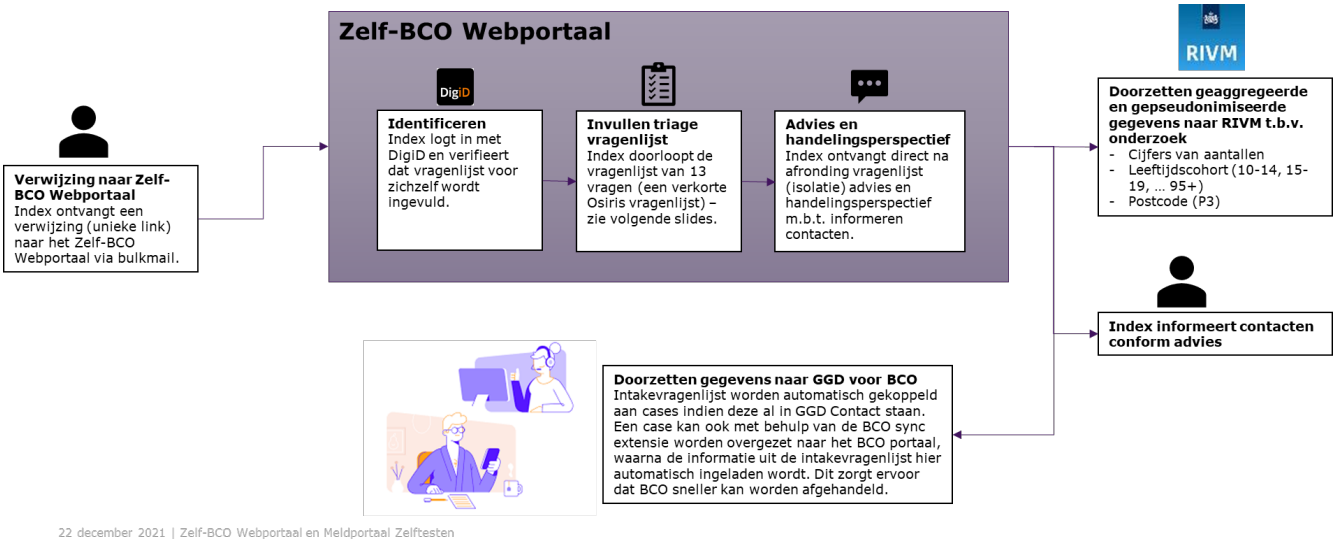
Op basis van de verzamelde informatie kan een GGD tevens besluiten in gevallen met een hoog (besmettings)risico alsnog gericht BCO door een medewerker te laten uitvoeren.

Gerelateerd aan de in paragraaf 3 benoemde verwerkingen zijn de volgende verwerkingsdoelen te benoemen:

1	Verwijzing naar Zelf-BCO portaal	• Toeleiding van indexen naar het Webportaal ZelfBCO
2	Identificatie met DigiD.	• Vaststellen identiteit van degene die inlogt, zodat verstrekte gegevens aan een uniek identificeerbare persoon kunnen worden gekoppeld. • Voorkomen van grote hoeveelheden onjuiste meldingen
3	Koppeling aan SBV-Z	• Ophalen van gegevens van degene die inlogt uit de BRP
4	Invullen triage vragenlijst	• Verzamelen van informatie die nodig is om de index een juist advies te geven en om de noodzakelijke gegevens te verzamelen ten behoeve van het volgen van de pandemie op basis van door GGD/RIVM vastgestelde OSIRIS-vragenlijst
5	Index ontvangt advies en handelingsperspectief	• Index helpen bij het bepalen van de juiste leefregels tijden de besmettelijke periode
6	Doorzetten gegevens naar GGD voor BCO en RIVM voor statistieken	• Verwerken van ontvangen informatie ten behoeve van BCO door de GGD • Verwerken van ontvangen informatie ten behoeve van onderzoek door het RIVM • Voldoen aan de wettelijke meldplicht van de GGD'en aan het RIVM

5. Betrokken partijen

Onderstaand schema geeft aan welke partijen bij de verwerking van gegevens in het Webportaal ZelfBCO betrokken zijn.



Welke rol de hierboven beschreven partijen hebben ten aanzien van de gegevensverwerking binnen Webportaal ZelfBCO wordt bepaald door de feitelijke omstandigheden van de verwerking. De wijze waarop het contractueel is geregeld is daarin niet doorslaggevend er moet gekeken worden naar de praktijk. De daadwerkelijke mate van autonomie en de beslissingsbevoegdheid ten aanzien van de essentiële elementen van de verwerking is doorslaggevend.[3] In de hierna beschreven AVG-rollen zijn de onderstaande factoren meegenomen in de overweging.

Factoren die wijzen op verwerkingsverantwoordelijkheid, zijn onder meer welke partij:	
I	het initiatief heeft genomen om de persoonsgegevens te verzamelen en te verwerken;
II	heeft besloten wat het doel/de gewenste uitkomst van het verwerken is;
III	het contract is aangegaan op basis waarvan de persoonsgegevens verwerkt dienen te worden;
IV	heeft besloten welke typen persoonsgegevens nodig zijn en van welke personen; en/of
V	een directe relatie heeft met de betrokkenen.[4]
Factoren die wijzen op het zijn van verwerker, zijn onder meer:	
VI	het volgen van instructies van een andere partij ten aanzien van de verwerking;
VII	het hebben verkregen van persoonsgegevens van een andere partij (of instructies hebben ontvangen welke persoonsgegevens verzameld dienen te worden); en/of
III	het niet kunnen beslissen over het doel en de grondslag van de verwerking en het eventueel verstrekken daarvan aan andere partijen van de verwerking.

Verwerkingsverantwoordelijke
Het initiatief tot het bouwen van Webportaal ZelfBCO komt voort uit het OMT-advies en de opdracht van de minister VWS. VWS heeft het portaal gebouwd en stelt het ter beschikking aan de GGD'en. Het gaat nadrukkelijk niet om het nemen van het initiatief tot het verzamelen en verwerken van (nieuwe) gegevens, maar om het faciliteren van de BCO-taak van de GGD'en.

De verantwoordelijkheid voor het uitvoeren van BCO ligt op basis van artikel 6 lid 1 sub c Wpg bij de GGD'en. De gegevens die in het Webportaal ZelfBCO verwerkt zijn onderdeel van dit proces. De gegevens zijn gebaseerd op de door GGD en RIVM gezamenlijk vastgestelde Osiris-vragenlijst. Het ontwerp van het ZelfBCO Webportaal is gebaseerd op die Osiris-vragenlijst en de door GGD'en gestelde ontwerpeisen voor GGD Contact waar BCO in wordt uitgevoerd.

[3] EPBP, Guidelines 07/2020 on the concepts of controller and processor in the GDPR, 2 September 2020.
[4] ICO, via: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/key-definitions/controllers-and-processors/.

Ondanks dat het initiatief tot het bouwen van Webportaal ZelfBCO bij het ministerie van VWS en OMT-advies ligt, bepalen de GGD'en (doordat het gebaseerd is op hun bestaande werkwijzen en ontwerpeisen) hoe en waarvoor het gebruikt wordt, ten behoeve van hun wettelijke taak.

Het is geheel aan de GGD en zij is vrij om de keus te maken om Webportaal ZelfBCO in te zetten in haar BCO-proces.

Gegevens die in het Webportaal ZelfBCO worden ingevoerd worden vier weken opgeslagen in GGD Contact. Wordt binnen deze periode in GGD Contact voor dezelfde index een case aangemaakt, dan worden de in het Webportaal ZelfBCO ingevoerde gegevens tevens onderdeel van de GGD Contact case. Ook voor deze verwerking hebben de GGD'en de rol van verwerkingsverantwoordelijke (zie hiervoor DPIA GGD Contact).

De door de index het Webportaal ZelfBCO gegeven antwoorden worden in gepseudonimiseerde vorm gedeeld met het RIVM. Het delen van deze gegevens valt onder de verantwoordelijkheid van de GGD'en in verband met de wettelijke plicht die op hen rust om de gegevens onverwijld door te geven [artikelen toevoegen]. Voor de verwerking door het RIVM nadat de gegevens gedeeld zijn, is het RIVM zelf verwerkingsverantwoordelijke.

Conclusie: Voor de verwerkingen binnen ZelfBCO zijn GGD'en verwerkingsverantwoordelijke in de zin van de AVG.

(Sub-)verwerkers
Zowel het Webportaal ZelfBCO als het portaal Zelftestmelden worden ontwikkeld door VWS (RDO), en van daaruit beschikbaar gesteld aan de GGD'en. Bij ingebruikname van beide portalen, heeft de minister geen rol bij de verwerking van de gegevens binnen Webportaal ZelfBCO. VWS hosten en beheert de portalen ten behoeve van de GGD'en. Dit betekent dat VWS de rol van verwerker heeft in de zin van de AVG [artikelen toevoegen].

Tussen de GGD'en en VWS is ten behoeve van GGD Contact een dienstverleningsovereenkomst gesloten, waar het gebruik van Webportaal ZelfBCO onderdeel uit gaat maken van de daarin gemaakte afspraken.

De hosting van de portalen is door VWS belegd bij een hostingpartij, die de rol van subverwerker heeft. Voor de aanvullende dienstverlening m.b.t. de portalen zal middels een addendum of een separate (verwerkers)overeenkomst de reeds gemaakte afspraken schriftelijk worden vastgelegd.

Overige betrokken partijen
Bij het inloggen van een index met DigiD wordt op basis koppeling aan de BRP een aantal gegevens van de index opgehaald. Hierbij wordt gebruik gemaakt van de een zogenaamde SBV-Z koppeling waarover iedere GGD beschikt. Deze wordt beheerd door het CIBG.

In het geval de SBV-Z koppeling tijdelijk niet beschikbaar is, kan Webportaal ZelfBCO gebruik maken van een alternatieve koppeling met de BRP. Hiervoor wordt de RIVG-koppeling van de Regio Rotterdam-Rijnmond gebruikt.

6. Belangen bij de gegevensverwerking

Zie onder 4 doeleinden.

Bij grote aantallen nieuwe besmettingen is het mogelijk dat de testcapaciteit bij de GGD'en tekort schiet. Als gevolg hiervan worden dan niet meer alle besmettingen bij de GGD geregistreerd, waardoor door de GGD informatie gemist wordt die van belang is voor het volgen van de pandemie. Omdat tevens niet meer alle besmettingen bij de GGD bekend zijn, zal dan bij een deel van de besmettingen geen BCO worden uitgevoerd en geen advies meer worden gegeven over de te volgen leefregels.

Deze zorg is bevestigd in het OMT-advies van 18 december 2021. Hierin schetst het OMT een zorgwekkend beeld, mede omdat de omikronvariant zich veel sneller verspreidt dan de deltavariant, de bescherming door

eerdere besmetting of vaccinatie beperkter lijkt en de ziektelast nog onduidelijk is.[5] Het OMT heeft naar aanleiding van deze zorg aandacht onder meer gevraagd voor het inrichten en beschikbaar stellen van elektronische systemen voor het uitvoeren een intake door de index zelf in het kader van BCO door de GGD'en.

Om ook in deze situatie het overzicht te behouden en besmette personen een passend advies te geven, is het Webportaal ZelfBCOontwikkeld. Op basis van de verzamelde informatie kan een GGD tevens besluiten in gevallen met een hoog (besmettings)risico alsnog gericht BCO door een medewerker te laten uitvoeren.

Onderstaand overzicht geeft weer welke groepen belang hebben bij het gebruik van de Portalen en hoe deze belangen eruit zien.

Regionale GGD'en	• Snelle en efficiënte verwerking nieuwe besmettingen • Bron van informatie m.b.t. nieuwe besmettingen zonder dat hiervoor persoonlijk contact met de index nodig is • Mogelijkheid om beschikbare BCO-capaciteit efficiënt en risico gestuurd in te zetten • Mogelijkheid om reeds opgehaalde informatie te gebruiken in GGD Contact • Gestructureerde invoer in lijn met structuur GGD Contact • Kunnen voldoen aan wettelijke taken binnen keten van infectieziektebestrijding
Indexen	• Snel en gemakkelijk kunnen aanleveren van informatie die voor de GGD van belang is voor het uitvoeren van BCO • Direct na het invullen van de vragenlijst een persoonlijk advies en contacten snel kunnen informeren.
Minister van VWS	• Beschikbaarheid van informatie binnen de keten van infectieziektebestrijding die nodig is om zicht te houden op de pandemie en om beleid op te baseren
RIVM	• Beschikbaarheid van informatie die nodig is om zicht te houden op de pandemie en onderzoek te kunnen uitvoeren

7. Verwerkingslocaties

Alle gegevensverwerkingen m.b.t. het Webportaal ZelfBCO vinden binnen Nederland plaats.

8. Techniek en methode van gegevensverwerking

Het Webportaal ZelfBCO is bedoeld om informatie over besmettingen te kunnen verzamelen zonder dat elke index hiervoor persoonlijk benaderd hoeft te worden vanuit de GGD. Er vindt een digitale intake plaats ten behoeve van het BCO door de GGD. Op basis van de digitaal verzamelde informatie kan dan besloten worden voor een aantal geselecteerde indexen alsnog verder BCO uit te voeren door contact op te nemen.

Het verzamelen van de intake-informatie is onderdeel van bestaande processen binnen de GGD en RIVM binnen hun wettelijke taken. Via het ZelfBCO Webportaal wordt een deel van de vragen die anders telefonisch worden gesteld, nu via een portaal binnengehaald. Er is daarom geen sprake van (semi-) geautomatiseerde besluitvorming of profilering in de zin van de AVG.

Gebruikers van beide portalen loggen in met DigiD, zodat hun identiteit uniek kan worden vastgesteld. Dit maakt het tevens mogelijk om herhaald melden door eenzelfde persoon te signaleren en het aantal meldingen dat iemand kan doen te beperken.

Verzamelde gegevens worden tijdelijk (vier weken) opgeslagen in GGD Contact. Ingeval dat hierin een case wordt aangemaakt van een index van wie op basis van een Portaalmelding een vragenlijst beschikbaar is, worden de eerder uitgevraagde gegevens aan de case in GGD Contact toegevoegd.

[5] Zie: Advies VWS n.a.v. OMT 134 met aanpassing, bijlage bij Kamerstuk 25 295, nr. 1672.

De in de portalen uitgevraagde gegevens worden dagelijks in gepseudonimiseerde vorm aan het RIVM ter beschikking gesteld. De te delen data met het RIVM wordt geaggregeerd gedeeld voorzien van een uniek-ID (niet herleidbaar voor RIVM) om later (bij aanvulling op OSIRIS-melding van GGD Contact de data te kunnen ontdubbelen.

In Bijlage 3 is een overzicht opgenomen van de wijze waarop gegevensstromen lopen bij het gebruik van ZelfBCO Webportaal.

9. Juridisch en beleidsmatig kader

De GGD heeft als taak binnen de infectieziektebestrijding om o.a. meldingen van artsen te ontvangen, bron- en contact onderzoek uit te voeren en informatie door te geven aan het RIVM. De activiteiten die plaatsvinden binnen Webportaal ZelfBCO vallen binnen dit kader van uitvoering geven aan publieke taken bij wet bepaald.

Op basis van de registratie van de positieve testuitslag (conform de geldende regelingen) in CoronIT ontvangt een index een beveiligde e-mail met een uitnodiging om in het Webportaal ZelfBCO de vragenlijst in te vullen.[6] Het door de index invullen van de op de OSIRIS-vragenlijst gebaseerde set aan vragen wordt gezien als de intake voor het BCO dat door de GGD wordt uitgevoerd. De Webportaal ZelfBCO-vragenlijst is daarmee een uitvraag ten behoeve van het BCO omdat die informatie ook in het BCO-wordt uitgevraag, maar op digitale manier wordt verkregen. De uitvoering van BCO door de GGD op basis van een gevalideerde melding heeft als grondslag artikel 6 lid 1 sub c Wpg.

Besluit de GGD op gebruik te maken van Webportaal ZelfBCO dan wordt op basis van de testuitslag in CoronIT een case aangemaakt in GGD Contact. Blijkt hierbij dat voor dezelfde index kort daarvoor een melding is gedaan in het Webportaal ZelfBCO, dan wordt dit door het systeem gesignaleerd, waarna de in het portaal ingevoerde gegevens ook in het dossier in GGD Contact worden opgenomen. Hiermee wordt voorkomen dat de index bij het BCO dezelfde vragen krijgt als die in het portaal reeds beantwoord zijn.

Artsen (waaronder GGD-artsen) zijn op grond van artikel 22 en 24 Wpg verplicht om besmettingen te melden bij de GGD. In artikel 24 lid 1 Wpg is gespecificeerd welke gegevens de melding moet bevatten:

- de naam, het adres, het geslacht, de geboortedatum, het burgerservicenummer en de verblijfplaats van de betrokken persoon,
- de infectieziekte dan wel een beschrijving van het ziektebeeld, de eerste ziektedag, de vaccinatietoestand, het gebruik van chemoprofylaxe, de vermoedelijke infectiebron, de datum van vermoeden of vaststelling van infectie, de wijze van vaststelling van die infectieziekte, en
- indien nodig, of de betrokken persoon dan wel een persoon in zijn directe omgeving beroeps- of bedrijfsmatig betrokken is bij de behandeling van eet- of drinkwaren of bij de behandeling, verpleging of verzorging van andere personen.

Naast de meldplicht van de arts aan de GGD, bestaat er een meldplicht van de GGD aan het RIVM. Artikel 28 lid 3 Wpg geeft een opsomming van de gegevens die onderdeel van deze doorgifte zijn:

- 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, alsmede de eerste drie cijfers van de postcode van diens adres, en
- de uitslag van het nader onderzoek (als bedoeld in artikel 25 lid 5 Wpg).[7]

Het RIVM gebruikt deze gegevens voor onderzoek en voor het monitoren van het landelijke beeld. Naast de gegevens uit deze melding, worden door de GGD'en tevens een aantal andere voor het RIVM relevante gegevens met hen gedeeld. Deze gegevens worden door de GGD voor het RIVM uitgevraagd met behulp van de

[6] Zie voor de vragen die onderdeel zijn van deze vragenlijst Bijlage 2.
[7] Eventueel ontvangt het RIVM ook bestanden met aantallen, omdat dit om geanonimiseerde gegevens gaat valt dit buiten de scope van deze DPIA.

Osiris-vragenlijst. Vindt dit uitvragen plaats via het Webportaal ZelfBCO, dan wordt hiervan een subset gebruikt. De wettelijke basis hiervoor is de grondslag voor het BCO (artikel 6 lid 1 sub c Wpg en artikel 11 lid 1 Besluit publieke gezondheid (Bpg) of in de algemene grondslag voor bestrijding van infectieziekten door de GGD (artikel 6 lid 1 Wpg).

10. Bewaartermijnen

De gegevens die in het Portaal ZelfBCO wordt bewaard voor een periode die gelijk is aan de epidemiologische relevante periode. Op dit moment is die periode 28 dagen. Wordt voor dezelfde besmetting binnen deze periode tevens een case aangemaakt in GGD Contact (het systeem van de GGD voor BCO), dan worden de ingevoerde gegevens in dit systeem hergebruikt. Op dossiers in GGD Contact is een bewaartermijn van vijf jaar van toepassing, waarbij na één jaar pseudonimisering plaatsvindt.

B. Beoordeling rechtmatigheid gegevensverwerkingen

11. Rechtsgrond

De wettelijke grondslag waarop de verwerkingen van persoonsgegevens in de portalen gebaseerd is, is de vervulling van een taak van algemeen belang door de GGD'en (artikel 6 lid 1 sub e AVG). De basis voor de ontwikkeling en het gebruik van het ZelfBCO Webportaal is gelegen in de taak die de GGD'en hebben op basis van infectieziektebestrijding, de rechtsgrond hiervoor is artikel 6 lid 1 Wpg. Daarnaast worden de verwerkingen gebaseerd op een aantal specifieke grondslagen die uiteen zijn gezet in de Wpg.

Op grond van artikel 6, eerste lid, onderdeel c, Wpg jo. artikel 14 Wpg heeft de GGD de wettelijke taak om de BCO uit te voeren. Het ZelfBCO Webportaal functioneert niet als BCO dat zelfstandig wordt uitgevoerd door de index, maar een uitvraag ten behoeve van de uitvoering van de wettelijke taak van de GGD'en. Het ZelfBCO Webportaal vormt een intake (en heeft daarmee slechts een ondersteunende functie) voor het BCO dat de GGD'en uitvoeren na een melding van een besmetting met corona.

Een arts maakt op basis van een positieve test een case aan in CoronIT, dit gebeurt op basis van de WGBO (buiten scope van deze DPIA). Wat wel binnen scope van deze DPIA is, is het melden van de besmetting door de arts aan de GGD. De rechtsgrond voor het doorgeven van deze melding is gelegen in artikel 22 en 24 Wpg. Dit betreft een in de wet vastgestelde set aan persoonsgegevens. Zoals uit Bijlage 1 volgt wordt er in dit kader een aanvullende set aan persoonsgegevens verwerkt, gelijk aan het huidige BCO-proces zonder dat gebruik wordt gemaakt van Webportaal ZelfBCO. Deze gegevens zijn nodig voor de GGD'en om het BCO correct uit te voeren en de grondslag hiervoor is daarmee artikel 6 lid 1 sub c Wpg.

Vervolgens wordt er ook een melding gemaakt aan het RIVM. Dit gebeurt op basis van artikel 28 lid 3 Wpg. De gegevens die het RIVM ontvangt zijn gepseudonimiseerd, en daarmee voor het RIVM niet te herleiden tot een individu. Voor aanvullende gegevens die gedeeld worden met het RIVM geldt dat de grondslag hiervoor wordt gevonden in de algemene grondslag voor bestrijding van infectieziekten door de GGD (artikel 6 lid 1 Wpg).

Waar het bijzondere persoonsgegevens betreft die worden verwerkt kunnen de GGD'en gebruik maken van de doorbrekingsgrond uit artikel 9, tweede lid, aanhef en onder i, AVG.

12. Bijzondere persoonsgegevens

Gezien de aard van de verwerking zeggen alle verwerkte gegevens iets over de gezondheid van de index. Het verbod op de verwerking van bijzondere persoonsgegevens wordt opgeheven door de uitzondering van artikel 9 lid 2 sub i AVG (algemeen belang op het gebied van volksgezondheid).

Onderdeel van de gegevens die verwerkt worden is ook het BSN van de besmette persoon. Bij een melding in het portaal ZelfBCO, dus naar aanleiding van een positieve test conform de geldende regelgeving, ligt de wettelijke basis hiervoor in artikel 24 Wpg. Hierin staat het BSN benoemd als onderdeel van de verplchte melding die een arts aan de GGD moet doen.

Het BSN wordt tevens verwerkt bij het inloggen op het portaal met DigiD en voor het aanmaken van een unieke gebruikerscode. De grondslag hiervoor ligt in artikel 10 Wet algemene bepalingen burgerservicenummer (Wabb).

13. Doelbinding

De verwerkingsdoelen zijn uitgewerkt in paragraaf 4 van deze DPIA. Er worden geen gegevens gebruikt voor andere doelen dan waarvoor de oorspronkelijk zijn verzameld.

14. Noodzaak en evenredigheid

Proportionaliteit

In bijlage 1 is een overzicht opgenomen van de gegevens die in het kader van de Webportaal ZelfBCO en het Webportaal Zelftestmelden verwerkt worden. Hierbij is tevens aangeven voor welk doel dit noodzakelijk is. Deze vragenlijst en de bijbehorende keuzemogelijkheden zijn een extract van de OSIRIS-vragenlijst. De OSIRIS-vragenlijst wordt vastgesteld in overleg tussen de GGD en het RIVM. In dat overleg worden de grondslagen, doelbinding, noodzakelijkheid en proportionaliteit van iedere vraag in de lijst afgewogen. In deze DPIA wordt daarom niet verder ingegaan op de afweging van de noodzakelijkheid nu deze door de GGD en RIVM in gezamenlijk overleg daar wordt vastgesteld. De noodzakelijkheid en proportionaliteit van de vragenlijst en antwoorden ten behoeve van BCO wordt daarmee aangenomen.

Naast de wettelijk verplichte gegevens uit de melding van de arts aan de GGD en van de GGD aan het RIVM, worden aanvullende gegevens verwerkt om de identiteit te kunnen vaststellen binnen Webportaal ZelfBCO, wat noodzakelijk is om te kunnen vaststellen wie de vragenlijst invoert.

Subsidiariteit

- Het gebruik van webportalen voor de verwerking van informatie over besmettingen wordt op verzoek van de minister mogelijk gemaakt om te voorkomen dat we in een situatie van een ondercapaciteit bij de GGD'en het zicht op de pandemie verliezen. De onderbouwing van deze keuze is te vinden in de Kamerbrief van 18 december 2021. De inzet van webportalen is daarmee een politieke en beleidsmatige keuze en is daarmee buiten scope van deze DPIA. Het is aan de GGD of zij gebruik wil maken van Webportaal ZelfBCO. Het verkrijgen van de antwoorden is op vrijwillige basis. De belangen van de betrokkene worden daardoor door de betrokkene zelf ingevuld. De subsidiariteitsafweging of de GGD aan haar wettelijke taken invullingen kan geven op een andere wijze dan via Webportaal ZelfBCO is aan de GGD.

15. Rechten van de betrokkene

Personen die gebruik hebben gemaakt van het Webportaal ZelfBCO kunnen in de privacyverklaring vinden hoe zij gebruik kunnen maken van de in de AVG opgenomen rechten van betrokkenen. Deelname aan Webportaal ZelfBCO is vrijwillig. De betrokkene wordt hier nadrukkelijk op gewezen in de flow van het Webportaal. Het tweede scherm dat de betrokkene ziet bevat ook een directe verwijzing naar de privacyverklaring. [screenshot invoegen]

Indien er geen redenen zijn om een verzoek niet (geheel) in te willigen, kan op korte termijn aan een verzoek worden voldaan. Indien er een case wordt aangemaakt binnen GGD Contact kan daar gebruik worden gemaakt van de Compliance Officer-rol die AVG-verzoeken daar kan uitoefenen. (nog verder uit te werken)

C. Beschrijving en beoordeling risico's voor de betrokkenen

Voor de technische en organisatorische maatregelen bij de organisatie van GGD'en ten aanzien van de toegang tot case-data wordt aangesloten bij de DPIA GGD Contact en de daar bepaalde risico's en maatregelen.

Risico 1 – Onbevoegden hebben toegang tot persoonsgegevens in Webportaal ZelfBCO

Risico zonder maatregelen
In Webportaal ZelfBCO worden gezondheidsgegevens verwerkt van een (potentieel) grote hoeveelheid personen die een besmetting hebben gemeld. Dit maakt de portalen tot een interessant doelwit. Onbevoegde toegang kan leiden tot verlies van de beschikbaarheid, de integriteit en de vertrouwelijkheid van de gegevens. De impact hiervan op betrokkenen en op de GGD'en zou zeer groot zijn. In het hypothetische geval dat de portalen zonder beveiligingsmaatregelen operationeel zou zijn, zou de kans op een cyber-aanval groot zijn.

Maatregelen
Vanwege de gevoeligheid en de grote hoeveelheid data die in de portalen verwerkt wordt is het systeem vanaf het begin ontworpen met Security by Design en Privacy by Design als uitgangspunten.

Een overzicht van de genomen security-maatregelen is opgenomen in onderdeel D van deze DPIA.

Restrisico
Met bovenstaande maatregelen is het kans dat onbevoegden toegang krijgen tot het Webportaal ZelfBCO klein. Vanwege directe versleuteling van de verstuurde informatie wordt met de genomen maatregelen de impact van een hack voor betrokkene op laag ingeschat. De impact van een poging tot toegang verschaffen waarbij alleen versleutelde data betrokken zijn wordt ingeschat op laag voor wat betreft het dataverlies en op midden voor wat betreft het reputatierisico.

Risico 2 – Bij de externe hosting provider vindt een datalek plaats

Risico zonder maatregelen

Voor de hosting van de portalen wordt gebruik gemaakt van de diensten van Prolocation B.V. Dit is een subverwerker van het ministerie van VWS. Zonder controlemaatregelen vanuit VWS kan niet worden vastgesteld of het niveau van de beveiliging bij Prolocation aan de hiervoor geldende eisen voldoet. Vaststaat dat indien zich bij Prolocation een datalek van enige omvang zou voordoen, de impact hiervan groot is. In de eerst plaats omdat in de portalen een grote hoeveelheid vertrouwelijke gegevens is opgeslagen. Daarnaast doordat een datalek in één van de webportalen het vertrouwen van het publiek in de corona-aanpak van de regering sterk kan aantasten.

Maatregelen
Prolocation voldoet tevens aan de eisen uit ISO 27001 en NEN 7510. Met Prolocation is een verwerkersovereenkomst afgesloten, waarin dit beveiligingsniveau is vastgelegd.

Restrisico
Met alle genomen beheersmaatregelen is de kans op security incidenten klein. Vanwege de toegepaste encryptie is de impact van incident op de betrokkene klein. Het reputatierisico voor VWS en de GGD'en maakt dat de impact van een datalek op midden wordt ingeschat.

D. Beschrijving voorgenomen maatregelen

17. Maatregelen

Privacy by design

- Grondslag en doelbinding: verwerking van persoonsgegevens is op basis van wettelijke verplichtingen en publieke taak infectieziektebestrijding. Het invullen van de vragenlijst is op vrijwillige basis.
- Dataminimalisatie: alleen meest relevante gegevens uit de Osiris-vragenlijst zijn in de vragenlijst in het portaal opgenomen
- Dataset RIVM voor het RIVM niet te herleiden tot individuele personen. Waar combinatie van PC3 en regio te kleine dataset oplevert worden geen postcodegegevens in de dataset verwerkt.
- Foutief melden zelftesten: beperken op aantal (positieve) zelftesten door koppeling DigiD inlog.
- Bescherming gevoelige persoonsgegevens: anonimisering en pseudonimisering waar mogelijk, alleen herleidbare (bijzondere) persoonsgegevens als het essentieel is voor uitvoering van taken.
- Kwetsbaarheden in de keten: sterke scheiding tussen vragenlijst, bronbestand en doelsystemen (GGD Contact, RIVM).
- Bescherming tegen DDoS-aanvallen en grote aantallen gebruikers.

Security by design

- Voldoet aan NEN 7510
- Risicoanalyse conform FMEA
- Specifieke maatregelen publiek gedeelte: geen local storage in browser, directe encryptie invoer van velden, TLS versleuteling conform NCSC richtlijnen, datasluis (gelijk aan mobiele apps)
- Specifieke maatregelen BCO portaal: nieuwe cases alleen zichtbaar voor werkverdeler. Alleen herkende dossiers worden gekoppeld.

Privacy by design in relatie tot security

- Publiek gedeelte: duidelijke toelichting voor gebruik van meldportaal.

Publiek gedeelte en beschikbaarheid

- Aparte domeinnamen per portaal
- PKI-Overheidscertificaat
- Internet.nl score 100% op zowel websites als mailservers
- Responsible disclosure en security.txt
- NaWas aansluiting
- Dubbele uitvoer bevraging persoonsregistraties om eventuele uitval op te vangen: via SVB-Z en BRP.
- Logging conform NEN 7513, maar zonder bijzondere persoonsgegevens.

Autorisatie

- Link via bulkmail met GGD regio en Samplenummer (tijdelijke koppeling totdat CoronIT koppeling gereed is.
- DigiD inlog via aparte DigiD aansluiting, afhandeling via aparte DigiD broker. Maakt gebruik van zelfde systeem CoronaCheck).
- PseudoBSN (soort hash) op basis van SVB-Z koppeling. Maakt gebruik van zelfde systeem GGD Contact.
- Monitoring door RDO voor infrastructuur, monitoring GGD Contact door hoster.

Datadeling

- NTA 7516-compliant mailuitwisseling via SMTP gecertificeerde leverancier (tijdelijke oplossing totdat er een mailportaal beschikbaar is via GGD Contact - reeds ingepland).
- Gepseudonimiseerde dataset naar RIVM.

- Koppeling met Indexdossiers op basis van pseudoBSN (soort hash).

Overig

- Codereview conform secure software development
- Pentesten zijn en worden uitgevoerd. Portaal gaat niet live met medium of high bevindingen

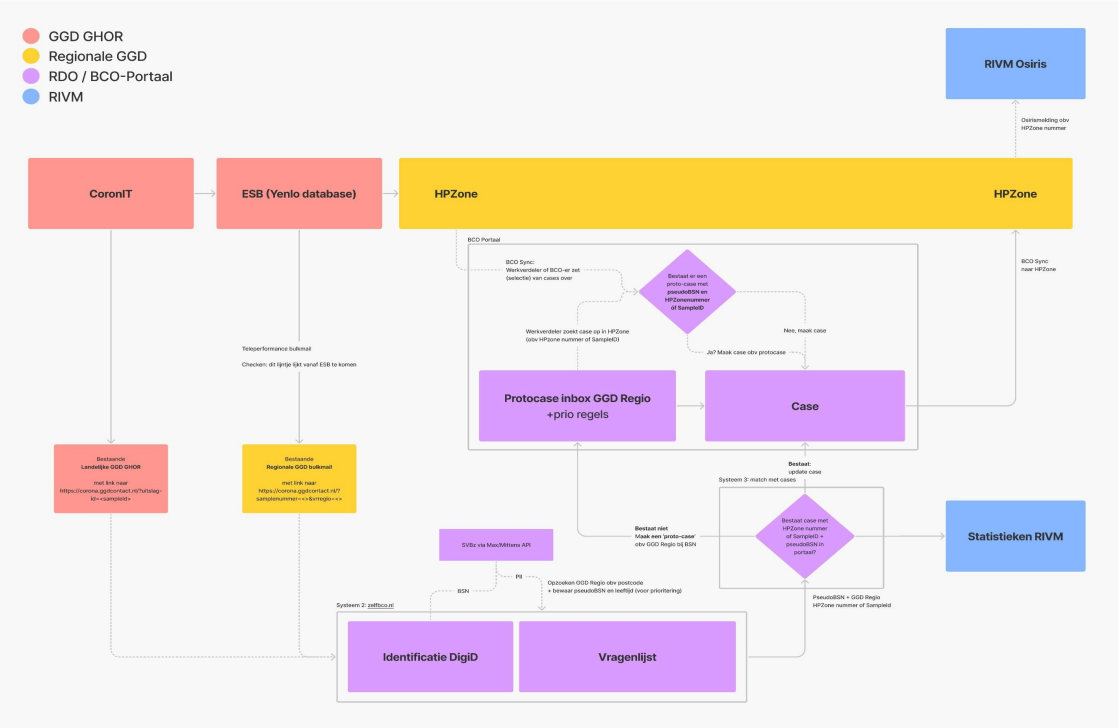
Bijlage 1: Datavelden, grondslagen en doelbinding

Veldnaam	Beschrijving	Waarde in Webportaal ZelfBCO	Naar RIVM?	Doelbinding	Grondslag voor verwerking door GGD	Grondslag voor delen met RIVM	Bron / vraag
rivmIdentifier2	Gegenereerde id, niet herleidbaar tot andere databronnen	ja	ja	unieke identificatie van de case (niet herleidbaar naar persoon)	6 lid 1 Wpg	6 lid 1 Wpg	Gegenereerd
reportDate	Datum en uur van indienen vragenlijst	YYYY-MM-DD HH24	ja	vastleggen metadata melding t.b.v. onderzoek / analyse	6 lid 1 Wpg	6 lid 1 Wpg	Metadata
ggdRegio	GGD-regio	wordt niet gedeeld i.c.m. PC3			6 lid 1 Wpg		Hyperlink index
bco.reason	Indicator die aangeeft of het een zelfTest of zelfBCO is	confirmedCase	ja	vastleggen metadata melding t.b.v. onderzoek / analyse	6 lid 1 Wpg	6 lid 1 Wpg	Metadata
bco.actor	Zelfmelding (vermoeden) of melding door van gevalideerde test (index)	index	ja	vastleggen metadata melding t.b.v. onderzoek / analyse	6 lid 1 Wpg	6 lid 1 Wpg	Metadata
meta.pc3	Postcode van de index, gepseudonimiseerd	pc3	ja	vastleggen locatiegegevens t.b.v. onderzoek / analyse	24 lid 1 Wpg	28 lid 3 Wpg	BRP via SBV-Z-koppeling
index.gender	Geslacht van de index	gender	ja	vastleggen geslacht t.b.v. onderzoek / analyse	24 lid 1 Wpg	28 lid 3 Wpg	BRP via SBV-Z-koppeling
index.dateOfBirth	Geboortedatum van de index, gepseudonimiseerd	YYYY-MM	gepseudonimiseerd	vastleggen leeftijdscohort t.b.v. onderzoek / analyse	24 lid 1 Wpg	28 lid 3 Wpg	BRP via SBV-Z-koppeling
test.dateOfTest	De datum van de eerste positieve test waaruit corona bleek	YYYY-MM-DD	ja	vaststellen besmettelijke periode t.b.v advies	24 lid 1 Wpg	28 lid 3 Wpg	Wanneer was de eerste test waaruit bleek dat je nu corona hebt?
test.InfectionIndicator	Het type test dat gebruikt is bij deze eerste positieve test		ja	vastleggen metadata melding t.b.v. onderzoek / analyse	6 lid 1 Wpg	6 lid 1 Wpg	Dit was een:
symptoms.hasSymptoms	Indicator voor symptomen		ja	vastleggen ziektebeeld t.b.v. onderzoek / analyse	24 lid 1 Wpg	28 lid 3 Wpg	Heb of had je klachten die passen bij corona?
symptoms.symptoms	Lijst van symptomen	zie lijst, geen vrije tekst	ja	vastleggen ziektebeeld t.b.v. onderzoek / analyse	24 lid 1 Wpg	28 lid 3 Wpg	Welke klachten heb je (gehad)?
symptoms.dateOfSymptomOnset	Datum waarop klachten begonnen	YYYY-MM-DD	ja	vaststellen besmettelijke periode t.b.v advies	24 lid 1 Wpg	28 lid 3 Wpg	Op welke dag begonnen je klachten?
underlyingSuffering.hasUnderlyingSuffering	Indicator voor kwetsbare gezondheid		ja	inschatten gezondheidsrisico voor index	6 lid 1 Wpg	6 lid 1 Wpg	Heb je een kwetsbare gezondheid?
underlyingSuffering.items	Lijst van aspecten van kwetsbare gezondheid	zie lijst, geen vrije tekst	ja	inschatten gezondheidsrisico t.b.v. advies en prioritering	6 lid 1 Wpg	6 lid 1 Wpg	Geef aan wat op jou van toepassing is
Pregnancy.isPregnant	Indicator voor zwangerschap		ja	inschatten gezondheidsrisico t.b.v. advies en prioritering	6 lid 1 Wpg	6 lid 1 Wpg	Ben je op dit moment zwanger?
Pregnancy.dueDate	De geschatte uitgerekende datum, gepseudonimiseerd naar trimester		gepseudonimiseerd naar trimester	inschatten gezondheidsrisico t.b.v. advies en prioritering	6 lid 1 Wpg	6 lid 1 Wpg	(Geschatte) uitgerekende datum
RecentBirth.hasRecentlyGivenBirth	Indicator voor recentelijke bevalling	binnen 6 weken	ja	inschatten gezondheidsrisico t.b.v. advies en prioritering	6 lid 1 Wpg	6 lid 1 Wpg	Ben je in de afgelopen 6 weken bevallen?
Vaccination.isVaccinated	Indicator voor vaccinatie		ja	inschatten gezondheidsrisico t.b.v. advies en prioritering	24 lid 1 Wpg	28 lid 3 Wpg	Ben je gevaccineerd tegen corona?
Vaccination.vaccineInjections[VaccineInjection]	De lijst van vaccinaties	All	ja	inschatten gezondheidsrisico t.b.v. advies en prioritering	24 lid 1 Wpg	28 lid 3 Wpg	
VaccineInjection.injectionDate	De datum van een vaccinatie, voor zelfTest gepseudonimiseerd	YYYY-MM-DD	gepseudonimiseerd	inschatten gezondheidsrisico t.b.v. advies en prioritering, input voor onderzoek/analyse	24 lid 1 Wpg	28 lid 3 Wpg	(Geschatte) datum {eerste/tweede...} prik
VaccineInjection.Vaccine	Het type vaccin bij een vaccinatie	All	ja	input voor onderzoek/analyse	24 lid 1 Wpg	28 lid 3 Wpg	Welk vaccin?
Test.isReinfection	Indicator voor herinfectie		ja	input voor prioritering	6 lid 1 Wpg	6 lid 1 Wpg	Heb je eerder corona gehad?
Test.previousInfectionDateOfSymptom	De geschatte datum van de vorige besmetting, voor zelfTest gepseudonimiseerd	YYYY-MM-DD	ja	input voor prioritering	6 lid 1 Wpg	6 lid 1 Wpg	(Geschatte) datum vorige besmetting
Abroad.wasAbroad	Indicator voor buitenland		ja	inschatten besmettingsrisico, input voor prioritering	6 lid 1 Wpg	6 lid 1 Wpg	Ben je tussen {beginBronperiode} en {eindBronperiode} in het buitenland geweest?
Abroad.Trips[Trip]	De lijst van reizen		ja	inschatten besmettingsrisico, input voor prioritering	6 lid 1 Wpg	6 lid 1 Wpg	Over je reis
Trip.returnDate	Datum van terugkeer, gepseudonomiseerd	YYYY-MM-DD	gepseudonimiseerd	input voor bron- en contactonderzoek	6 lid 1 Wpg	6 lid 1 Wpg	Datum terugkeer
Trip.countries	De lijst van landen		ja	inschatten besmettingsrisico, input voor prioritering	6 lid 1 Wpg	6 lid 1 Wpg	Bezochte land(en)?
Tasks	Broncontacten (max 1 voor nu)		ja	input voor bron- en contactonderzoek	24 lid 1 Wpg	28 lid 3 Wpg	
Task.General.isSource	Indicator voor broncontact		ja	input voor bron- en contactonderzoek	24 lid 1 Wpg	28 lid 3 Wpg	Ken je mensen met corona die jou misschien besmet hebben?
Task.General.reference	Nummer van het bron- en contactonderzoek van de bron		ja	input voor bron- en contactonderzoek	24 lid 1 Wpg	28 lid 3 Wpg	Nummer van het bron- en contactonderzoek
SourceEnvironments.hasLikelySourceEnvironments	Waarschijnlijke besmettingsbron		ja	input voor bron- en contactonderzoek	24 lid 1 Wpg	28 lid 3 Wpg	Heb je een idee in welke situatie je besmet bent?
SourceEnvironments.likelySourceEnvironments	Waarschijnlijke besmettingsbron	zie lijst, geen vrije tekst	ja	input voor bron- en contactonderzoek / clusteranalyse en prioritering	24 lid 1 Wpg	28 lid 3 Wpg	Geef aan waar je waarschijnlijk besmet bent:
Job.wasAtJob	Aanwezigheid werk, studie of school		ja	input voor bron- en contactonderzoek / clusteranalyse en prioritering	24 lid 1 Wpg i.c.m. 6 lid 1 Wpg	6 lid 1 Wpg	Ben je tussen {startBronPeriode} en vandaag naar je school, studie of werk geweest?
Job.sectors	Type werk, studie of school	zie lijst, geen vrije tekst	ja	input voor bron- en contactonderzoek / clusteranalyse en prioritering	24 lid 1 Wpg i.c.m. 6 lid 1 Wpg	6 lid 1 Wpg	Geef aan waar je voor je werk, studie of school bent geweest:
Housemates.hasHouseMates	Aanwezigheid huisgenoten		ja	input voor leefstijladvies	6 lid 1 Wpg	6 lid 1 Wpg	Heb je huisgenoten?
meta.cat1Count	Aantal huisgenoten		ja	input voor leefstijladvies	6 lid 1 Wpg	6 lid 1 Wpg	Aantal huisgenoten
Housemates.canStrictlyIsolate	Mogelijkheid om afstand te houden tot huisgenoten		ja	input voor leefstijladvies	6 lid 1 Wpg	6 lid 1 Wpg	Lukt het om afstand te houden van je huisgenoten?
meta.estimatedCat2Count	Aantal nauwe contacten		ja	inschatten besmettingsrisico, input voor prioritering	6 lid 1 Wpg	6 lid 1 Wpg	Met hoeveel mensen heb je tussen {startBesmettelijkePeriode} en vandaag nauw contact gehad?
Contact.phone	Telefoonnummer index		nee	contact kunnen opnemen met index	24 lid 1 Wpg (in de geest van)	n.v.t.	Hoe kunnen we je bereiken?
Contact.email	E-mailadres index		nee	contact kunnen opnemen met index	24 lid 1 Wpg (in de geest van)	n.v.t.	Hoe kunnen we je bereiken?

Bijlage 2: Overzicht vragen Webportaal ZelfBCO en labels

Vraag	Mogelijkheden	Waarde	Label
Vaststellen EZD/besmettelijke periode			
Eerste test waaruit bleek dat je corona hebt	Datum	Datum	
Soort test	Zelftest/test bij GGD/test op andere plek	Zelftest	
		Test bij GGD	
		Test op andere plek	
Heb/had je klachten die passen bij corona	Ja (+opties voor klachten)/Nee	Alle klachten	
		Nee	
Op welke dag begonnen de klachten	Datum	Datum	
Medische gegevens			
Heb je een kwetsbare gezondheid?	Ja (+ opties verminderde afweer)/Nee/Weet ik niet	Ja	Gezondheidsindicatie
		Nee	
		Weet ik niet of Zeg ik liever niet	Onvolledige gegevens
Ben je op dit moment zwanger	Ja (+ uitgerekende datum)/Nee/Weet ik niet	Ja	
		Nee	
		Weet ik niet	
Ben je in de afgelopen 6 weken bevallen?	Ja (+ datum bevallen)/Nee/Weet ik niet	Ja	
		Nee	
		Weet ik niet	
Ben je gevaccineerd tegen corona?	Ja (+ data/merk prikken)/Nee	Ja	
		Nee	
Heb je eerder corona gehad?	Ja (+ datum vorige besmetting)/Nee	Ja, > 8 weken geleden	Herhaaluitslag
		Nee	
Vragen over (mogelijke) bron			
Ben je tussen xx en xx in het buitenland geweest?	Ja (+ datum terugkeer en land)/Nee	Ja	Buitenland
		Nee	
Ken je mensen met corona die jou misschien besmet hebben?	Ja (+nummer BCO)/Nee	Ja	
		Nee	
Heb je een idee in welke situatie je besmet bent?	Ja (+ meest waarschijnlijke plek)/Nee	Ja, basisschool	School
		Ja, hele lijstje onderwijs & kinderopvang	School
		Ja, schip of haven	Scheepvaart opvarende
		Ja, vliegtuig of vliegveld	Vluchten
		Ja, hele lijstje langdurige zorg	Zorg
		Ja, hele lijstje ziekenhuis en medische praktijk	Zorg
Ben je tussen xx en xx naar school, studie of werk geweest?	Ja (+ waar)/Nee	Ja, hele lijstje in de zorg	Medewerker zorg
		Ja, hele lijstje Onderwijs & kinderopvang	School
		Ja, mantelzorg	Medewerker zorg
		Nee	
Vragen over verspreidingsrisico (contactonderzoek)			
Heb je huisgenoten?	Ja (+ aantal & afstand houden wel/niet)/Nee	Ja	
		Nee	
Met hoeveel mensen heb je tussen xx en vandaag nauw contact gehad?	Aantal mensen	Aantal	
Adviezen per email ontvangen	Ja/Nee	Ja	
		Nee	

Bijlage 3: overzicht systemen ZelfBCO Webportaal



DPIA: GGD CONTACT

12 april 2021

Data Protection Impact Assessment (DPIA) GGD Contact ter ondersteuning BCO

- Landelijke referentie DPIA voor GGD'en -

DPIA: GGD Contact **1**
Versiegeschiedenis 3
Definities **5**
Inleiding **7**
A. Beschrijving kenmerken proces gegevensverwerkingen **11**
1. Voorstel 11
2. Persoonsgegevens 11
3. Betrokken partijen en rolverdeling 17
4. Gegevensverwerking 22
5. Verwerkingsdoeleinden 29
6. Belangen bij gegevensverwerking 30
7. Verwerkingslocaties 32
8. Techniek en methode van gegevensverwerking 32
9. Juridisch en beleidsmatig kader 33
10. Bewaartermijn 34
B. Beoordeling rechtmatigheid gegevensverwerkingen **37**
12. Doelbinding 40
13. Noodzaak en evenredigheid 40
14. Rechten van betrokkenen 42
C. Beschrijving en beoordeling risico's voor de betrokkenen **45**
15. Risico's 45
D. Beschrijving voorgenomen maatregelen **67**
16. Maatregelen 67
E. Bijlagen **76**
Volledige BCO vragenlijst index **Epic-naam: volledige vragenlijst inclusief contacten** 77
Gestandaardiseerde zoekfunctie locaties/contexten **Epic-naam: Contexten** 78
Beknopte vragenlijst huisgenoten en nauwe contacten **Epic-naam: volledige vragenlijst inclusief contacten** 78
Cases die niet zijn afgerond aan anderen kunnen toewijzen **Epic-naam: nvt** 78
GGD Contact app met Zelf BCO mogelijkheid **Epic-naam: ZelfBCO App** 78
Bijlage 2 - Procesflow GGD Contact 80
4– Achtergrond risiconiveaus 83
Bijlage 4 – Logging 85
Bijlage 5 – Advies Functionaris Gegevensbescherming (FG) GGD Hart voor Brabant 86

Versiegeschiedenis

Versie	Auteur	Verspreiding bij	Activiteiten
0.1	[redacted] (Cuccibu)	- [redacted] (Regio Twente) - [redacted] (GGD West-Brabant) - [redacted] (Regio Gooi & Vecht) - [redacted] (GGD Zuid – Limburg) - [redacted] (VWS) - [redacted] (VWS) - [redacted] (VWS) - [redacted] - [redacted] (GGD GHOR Nederland) - CISO GGD GHOR	- Inzage & advies tussenversie DPIA
0.2	[redacted]	- FG GGD GHOR Nederland	- FG advies opvragen
0.3	[redacted]	- [redacted] (Cuccibu)	- Aanpassingen naar aanleiding FG advies & review
0.4	[redacted]	- [redacted] (VWS) - [redacted]n (VWS) - [redacted] (VWS) - [redacted] - [redacted] (GGD GHOR Nederland) - CISO GGD GHOR - [redacted] (VWS)	- Delen concept versie DPIA ter review VWS
0.5	[redacted]	- [redacted] (Pels Rijcken) - [redacted] (Pels Rijcken)	- Review DPIA (op hoofdlijnen)
0.6	[redacted]	- [redacted] (Pels Rijcken) - [redacted] (Pels Rijcken)	- Tekstvoorstel betrokken partijen en rolverdeling
0.7	[redacted]	- [redacted] (Pels Rijcken)	- Tekstvoorstel Telecommunicatiewet

		- [redacted] (Pels Rijcken)	
1.0	[redacted]	- [redacted] (Pels Rijcken) - [redacted] (Pels Rijcken) - [redacted] (Regio Twente) - [redacted] (GGD West-Brabant) - [redacted] (Regio Gooi & Vecht) - [redacted] (GGD Zuid – Limburg) - [redacted] (VWS) - [redacted] (VWS) - [redacted] (VWS) - [redacted] (Joan Knecht) - [redacted] (GGD GHOR Nederland) - CISO GGD GHOR Nederland - FG GGD GHOR Nederland - [redacted] (Cuccibu)	- Definitieve versie referentie DPIA - FG advies opvragen praktijkregio's + FG GGD GHOR Nederland
1.1	[redacted]		Aanpassingen naar aanleiding van FG Advies, begeleidingscommissie advies en FG advies GGD'en
1.1.1	[redacted]	- [redacted] (VWS)	Samenvoeging referentie DPIA 1.0 met Addenda: Zelf-BCO, BCO Vragenlijst + Osiris Vragenlijst, Evaluatie GGD Contact
1.1.2	[redacted]	- [redacted] (GGD GHOR Nederland) - 25 FG's v.d. 25 GGD'en	Wijziging naar scope 'Release 1.1' Review ten behoeve van FG-advies

Definities

Bron – en contactopsporing (BCO)	Een wettelijke taak van de GGD zoals bedoeld in artikel 6 lid 1 sub c Wet publieke gezondheid ten behoeve van infectieziektebestrijding. Het doel van BCO is om contacten te identificeren, hen te informeren over de blootstelling en het risico op besmetting, hen te wijzen op maatregelen die genomen moeten worden om verdere verspreiding te voorkomen en hen hierin te begeleiden. Door middel van BCO wordt tevens mogelijk om locaties of situaties waarin mensen besmet zijn geraakt te monitoren, om eventuele verheffingen of lokale risico's te signaleren en zo mogelijk extra maatregelen te implementeren.
BCO-medewerker	Medewerker die BCO uitvoert. Dit kan een medewerker van de GGD zelf betreffen, maar kan ook een medewerker betreffen die vanuit de landelijke schil wordt ingezet.
BCO-portaal	Het webportaal dat de BCO-portaal Gebruiker gebruikt om BCO uit te voeren
BCO-portaal Gebruiker	Iedere gebruiker van het BCO-portaal, waaronder de BCO-medewerker, de werkverdeler (en in latere releases van het BCO-portaal ook andere functies).
Contactgegevens	Gegevens die de GGD kan gebruiken om een persoon te benaderen, zoals een telefoonnummer of e-mailadres.
GGD Contact	Het deel van het BCO-proces dat gebruik maakt van de functionaliteiten binnen GGD Contact, dit bevat de verwerkingen binnen de App en het BCO-portaal.
GGD Contact App	De App die de index downloadt en gebruikt voor het aanleveren van zijn contacten en/of uitvoeren van zelf-BCO.
GGD GHOR	GGD GHOR Nederland
VWS	Ministerie van Volksgezondheid, Welzijn en Sport

Inleiding

Ten behoeve van infectieziektebestrijding hebben GGD'en op basis van Wet publieke gezondheid (hierna: Wpg) de taak gekregen om BCO uit te voeren.[1] GGD'en hebben voor BCO een werkbaar proces voor wat betreft infecties die zich op kleine schaal voordoen. Het reguliere proces van BCO is lastig uitvoerbaar bij een pandemie zoals bij COVID-19 het geval is. Ter ondersteuning van het BCO Proces COVID-19 gaan GGD'en in Nederland gebruik gaan maken van een BCO-ondersteunende app met het bijbehorende webportaal: GGD Contact.

Doel document: Referentie DPIA GGD Contact

Dit document is opgesteld in nauwe samenwerking tussen de GGD'en, GGD-GHOR en VWS. Dit document dient als referentie-document voor iedere GGD afzonderlijk. In dit document wordt de conform de AVG verplichte gegevensbeschermingseffectbeoordeling (DPIA) op GGD Contact vastgelegd. Iedere GGD kan dit document gebruiken om deze om te zetten en aan te passen op haar eigen interne processen. Het model gegevensbeschermingseffectbeoordeling Rijksdienst (PIA) is gebruikt als uitgangspunt voor het opstellen deze DPIA-rapportage.

Noodzaak tot DPIA

Op de gegevensverwerkingen in GGD Contact is de AVG van toepassing. Autoriteit Persoonsgegevens heeft een lijst gepubliceerd van soorten verwerkingen waarvoor een DPIA als bedoeld in artikel 35 van de AVG verplicht is.[2] In deze lijst wordt gesteld dat voor grootschalige verwerkingen van gezondheidsgegevens een DPIA dient te worden uitgevoerd. Hoewel in de applicatie geen sprake is van opname van informatie over het ziektebeeld en het welbevinden van de index of diens contacten, zegt de opname van de persoonsgegevens in BCO-portaal iets over de gezondheid van de index en over het ziekterisico dat zijn contacten lopen. Daarmee is er sprake van verwerking van gegevens over de gezondheid en deels bijzondere persoonsgegevens.[3] Het doel en noodzaak van GGD Contact impliceert grootschalige gegevensverwerking, nu het potentieel gaat een groot gedeelte van de Nederlandse bevolking. In het geval van een infectieziekte zoals COVID-19 is de grootschalige gegevensverwerking (grote hoeveelheden betrokkenen (index en contacten) en hun (contact)gegevens) een gegeven.

Ontwikkelingen in functionaliteit GGD Contact

- Oorspronkelijke functionaliteit
  Sinds maart 2020 heeft Nederland te maken met de infectieziekte COVID-19. Gelet op de grootschaligheid van deze infectieziekte en de noodzaak van het snel en efficiënt handelen ter voorkoming of beperking van de verspreiding ervan is door de 'Begeleidingscommissie Digitale Ondersteuning Bestrijding Covid-19' van VWS gekeken naar digitale verbetermogelijkheden die ondersteunend hiervoor kunnen zijn. Medio april 2020 heeft

[1] Artikel 6 lid 1 sub c Wpg.
[2] https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/stcrt-2019-64418.pdf
[3] Artikel 9 lid 1 AVG en de daarop van toepassing zijnde overweging 35 AVG.

VWS ten aanzien van de digitale mogelijkheden ter bestrijding van COVID-19 een marktconsultatie gedaan. Vanuit de wens van GGD'en heeft de brancheorganisatie GGD GHOR Nederland VWS gevraagd om ondersteuning te bieden in de realisatie van GGD Contact, waarbij de minister een wettelijke verantwoordelijkheid heeft met betrekking tot het bestrijden van infectieziektebestrijding. De realisatie van GGD Contact (release 1.0) heeft plaatsgevonden binnen het VWS-programma Realisatie Digitale Ondersteuning (RDO).

- In opdracht van de minister van VWS dient HPZone vervangen te worden.[4] Op 12 februari 2021 heeft de DPG-raad besloten om HPZone Lite te vervangen op korte termijn. Het gekozen scenario voor de vervanging op korte termijn en de functionaliteiten die deze bevat wordt aangemerkt als release 1.1. De keuze en afweging voor GGD Contact is nader in de daarvoor uitgewerkte beslisnotities uitgewerkt.

Scope

Met GGD Contact kan de GGD sneller en met de aanwezigheid van minder fouten relevante contactgegevens verzamelen die nodig zijn voor BCO. Dit gebeurt doordat de index via de App de contactgegevens van de personen met wie hij in aanraking is gekomen deelt met de BCO-medewerker in plaats van een volledige inventarisatie door de BCO-medewerker.

De scope van de referentie DPIA omvat de gegevensverwerkingen binnen GGD Contact ten behoeve van de ondersteuning van het BCO-proces.

- De applicatie GGD Contact met daarin zelfBCO door de index. De index selecteert in de app welke corona-gerelateerde klachten hij had/heeft en op welke dag deze klachten zijn begonnen.
- De sluis, betreffende een API[5] tussen GGD Contact en het webportaal waarmee de BCO-medewerker gaat werken.[6]
- Het webportaal van GGD Contact waarmee de BCO-medewerker gaat werken.

Voor de nadere uitwerking van die scope is aansluiting gezocht bij de doelen die GGD Contact heeft ten aanzien van infectieziektebestrijding:

- Het BCO-proces – bedoeld om (verdere) transmissie van de infectieziekte te voorkomen dan wel te beperken – te ondersteunen door sneller relevante contacten in beeld te krijgen. Wanneer deze contacten sneller in beeld zijn, kan het handelingsperspectief eerder gedeeld worden door de BCO-medewerker met de betreffende contacten. Indien nodig, kan tijdig quarantaine of thuisisolatie op basis van eigen initiatief van het contact, gestart worden.
- Het aantal uur dat GGD per index besteedt aan BCO verminderen, waardoor GGD voor meer indexen BCO kan uitvoeren.

[4] Stand van zakenbrief digitale ondersteuning pandemiebestrijding 12 februari 2021
[5] Application Programming Interface waardoor GGD Contact met het BCO webportaal kan communiceren.
[6] De sluis kan worden gezien als een doorgeefluik waar de gegevens tijdelijk staan opgeslagen totdat deze vanuit GGD Contact aan het BCO webportaal worden doorgegeven.

De ondersteuning van het BCO-proces door middel van inzet GGD Contact beoogt te resulteren in:

- Tijdsbesparing van de BCO-medewerker doordat dubbele administratie wordt voorkomen; handmatig overnemen van gegevens is niet meer nodig vanwege het webportaal dat voor GGD Contact wordt ontwikkeld en eraan gekoppeld is. In de beoogde toekomstige release wordt ook de koppeling naar een bronsysteem als functionaliteit toegevoegd.

- Een verbetering van de kwaliteit van de gegevens in relatie tot het reguliere BCO-proces. De juistheid en volledigheid van digitaal aangeleverde gegevens is naar verwachting beter dan wanneer deze mondeling worden doorgegeven. Hierdoor kan een BCO-medewerker sneller de juiste contacten bereiken. Voor de kwaliteit van de data is deze mede afhankelijk van de kwaliteit van het adresboek in de mobiele telefoon van de index.

De scope van de DPIA omvat **niet**:

- Het 'reguliere' BCO proces zoals wordt gevolgd bij géén gebruik van GGD Contact of het proces waar GGD Contact onderdeel van is;
  Lokale aanvulling: Voor het BCO proces is een aparte DPIA uitgevoerd. Deze ligt ter beoordeling bij de FG voor.
- Het proces rondom het informeren van de contacten vanuit GGD contact (mail, sms etc.);
- De verwerking van persoonsgegevens in en naar HP Zone Lite van infectieziektes van de GGD, HPZone, HPZone Lite;
- In het BCO-portaal is de volledige BCO-vragenlijst opgenomen en tevens de Osirisvragenlijsten. In deze fase van de DPIA is geen privacy-analyse gedaan op de noodzakelijkheid van de vragen in deze lijst.

Ontwikkeling GGD Contact

GGD Contact wordt ontwikkeld door VWS in samenwerking met GGD GHOR en de GGD'en. BCO-portaal zal op termijn HPZone Lite vervangen. Voor de tweede release versie (release 1.1) van GGD Contact is dit nog niet het geval.

Privacy & Security: Definition of done/ready

GGD Contact wordt Agile ontwikkelt. De scope van de releases wordt beschreven aan de hand van **epics** die door de product owners van de GGD'en vastgesteld worden. Iedere functionaliteit wordt met als uitgangspunt de beschrijving in de epic getoetst aan privacy en security vereisten. In de ontwerp- en bouwfase is afstemming tussen development en privacy en security-adviseurs om GGD Contact te laten voldoen aan de privacy- en security vereisten. Bij de bouw van de epics door het ontwikkelteam worden deze getoetst aan een definition of ready en definition of done voor privacy en security. In de ontwikkeling wordt ook getest aan de hand van deze beschrijvingen. Uitgangspunt daarbij is de geldende norm voor gegevensuitwisseling in de zorg: de NEN7510 en onderliggende normen. De DPIA en beschrijving van de security-/privacy maatregelen zijn onderdeel van de oplevering van deze en toekomstige releases van GGD Contact.

Releases:

Release 1.0 Praktijktestregio's 10 december 2020

Release 1.0 is de release die de initieel beoogde functionaliteit bevat voor ondersteuning en efficiëntere inrichting van het BCO. Uitgerold onder de praktijktestregio's.

Release 1.1 Release voorbereidend op vervanging HP-Zone Lite [datum] (Bijlage 1: Beschrijving Releases)

Release 1.1 is de beoogde landelijke uitrol van de volgende functionaliteiten:

- Volledige BCO vragenlijst index (epic-naam: Volledige vragenlijst inclusief contacten)
- Gestandaardiseerde zoekfunctie locaties/contexten (epic-naam: Contexten)
- Beknopte vragenlijst huisgenoten en nauwe contacten (epic-naam: volledige vragenlijst inclusief contacten
- GGD Contact app met Zelf-BCO mogelijkheid (epic-naam:zelfBCO app)

Beheer

De beheertaken ten aanzien van GGD Contact worden door of in opdracht van VWS en GGD GHOR vervuld. Globaal zijn deze taken onder te verdelen over:

- Ontwikkeling GGDContact omgeving ligt bij VWS-Ontwikkelteam en blijft daar voorlopig liggen.
- Hosting GGDContact omgeving door Intermax onder aansturing van VWS
- Applicatie en Functioneel beheer GGDContact ligt tot nader order bij VWS
- Change Management is verantwoordelijkheid VWS

Op termijn zal het volledige beheer van de applicatie worden toegewezen door de GGD'en aan een andere partij.

- GGD GHOR richt de Service Desk in (alleen voor info en incidenten)
- Incident Management is verantwoordelijkheid GGD GHOR

A. Beschrijving kenmerken proces gegevensverwerkingen

1. Voorstel

Het voorstel voor deze DPIA betreft de gegevensverwerkingen die plaatsvinden in:

- De applicatie GGD Contact is bedoeld voor de besmette persoon; de index. Om het BCO-proces voor de BCO-medewerker te ondersteunen stelt GGD Contact de indexen zelf in staat om digitaal de besmettingsperiode te bepalen en het aanleveren van hun contacten aan de GGD. De applicatie GGD Contact is ook te gebruiken door een index wanneer de GGD van zijn regio de App nog niet gebruikt voor doorgeven van informatie vanuit het zelf-BCO.
- Het BCO-portaal van GGD Contact is bedoeld voor de BCO-medewerker. Hierin legt de BCO-medewerker een en ander klaar voor de index zodat deze in GGD Contact eenvoudig zijn contacten kan selecteren en doorsturen naar de BCO-medewerker.
  Daarnaast kan de BCO-medewerker het BCO-portaal ook gebruiken indien de index de app niet gebruikt. In het BCO-portaal is de gehele vragenlijst voor het uitvoeren van het bron- en contactonderzoek opgenomen evenals de Osiris-vragenlijst.
- De sluis tussen GGD Contact en het BCO webportaal. De sluis kan worden gezien als een doorgeefluik waar de gegevens tijdelijk staan opgeslagen totdat deze vanuit GGD Contact aan het BCO webportaal worden doorgegeven.

Op verschillende momenten kan een persoon te maken hebben met GGD Contact:

1. De persoon heeft zich aangemeld voor een test, wacht op een testresultaat of heeft een positief testresultaat ontvangen (index) en krijgt een advies om GGD Contact te installeren en te gebruiken.
2. De persoon downloadt GGD Contact uit een App store op eigen initiatief.

2. Persoonsgegevens

Binnen GGD Contact, de sluis en het BCO webportaal van de BCO-medewerker worden onderstaande persoonsgegevens verwerkt. De velden die de index in GGD Contact kan invullen zijn optioneel.

Er bestaat geen verplichting om de gegevens aan te leveren. Het is dus ook mogelijk dat de index ervoor kiest geen enkel gegeven in te vullen of wel in te vullen maar niet te verzenden. Bij het delen van de gegevens met de GGD krijgt de index wel een herinnering dat niet alle velden zijn ingevuld. Deze melding kan worden genegeerd door de index. Er is bewust gekozen om de gegevens als optioneel aan te merken in de GGD Contact app zodat de data niet wordt ‘tegengehouden’ indien aan de kant van de index data niet compleet is. De index uploadt de gegevens namelijk niet een voor een, maar als een batch. Hierdoor kan het voorkomen dat de index contact A wel reeds heeft aangeleverd met een telefoonnummer, maar van contact B alleen

nog maar een naam heeft. Door de gegevens als optioneel aan te merken kan het BCO wel reeds gestart worden met de data die door de index wordt aangeleverd en kunnen in het gesprek worden aangevuld. Daarnaast kan het per situatie verschillen welke gegevens als minimaal noodzakelijk aangemerkt dienen te worden. Zo is het denkbaar dat er gevallen zijn waarbij de IZB arts aan de hand van alleen de naam en de kennis dat het bijvoorbeeld om een 'broer' gaat, het voldoende informatie is om de betreffende persoon op te zoeken in bestaande data uit HPZone. Indien de index een upload wil uitvoeren waarbij niet minimaal een e-mailadres of telefoonnummer is ingevuld, dan vraagt de App aan de index om nog eens te kijken of voor die contacten er contactgegevens beschikbaar zijn. Uitgangspunt bij de ontwikkeling van de App het niet verplicht maken van specifieke velden om ervoor te zorgen dat het delen van de gegevens nooit geblokkeerd kan worden door het missen van een veld. Dit betekent dat een inrichting met verplichte velden technisch wel mogelijk is om in te richten, maar dit een bewuste afweging is geweest om het niet te doen om de aanlevering van gegevens vanuit de Index niet te belemmeren.

In onderstaande tabel is per persoonsgegeven weergegeven om wat voor type persoonsgegeven (gewone, bijzondere of wettelijk identificerende) het gaat. Hoewel in de applicatie geen sprake is van opname van informatie over het ziektebeeld en het welbevinden van de index of diens contacten, zegt de opname van de persoonsgegevens in GGD Contact wel iets over de gezondheid van de index (index is besmet) en over het ziekterisico dat zijn contacten lopen. De context waarin

de persoonsgegevens worden verwerkt maakt dat er sprake is van verwerking van gegevens over de gezondheid en dus bijzondere persoonsgegevens.[7]

Hieronder wordt nader ingegaan op de noodzaak van het opvragen van deze persoonsgegevens.

Persoonsgegeven	**Gewoon persoonsgegeven**	**Bijzonder persoonsgegeven**	**Index en/of contact**	**Toelichting noodzaak**
Voor- en achternaam	Ja	Ja, zie toelichting hierboven.	Contact/Index	A
Telefoonnummer	Ja	Ja, zie toelichting hierboven.	Contact/Index	A
E-mailadres	Ja	Ja, zie toelichting hierboven.	Contact	A
Datum laatste contactmoment	Ja	Ja, zie toelichting hierboven.	Contact/Index	E
Risicoclassificatie[8]	Ja	Ja, zie toelichting hierboven.	Contact	B
Aandachtspunten[9]	Ja	Ja, zie toelichting hierboven.	Contact	C
Vrij opmerkingsveld	Ja	Ja, zie toelichting hierboven.	Contact	F
Contacttype	Ja	Ja, zie toelichting hierboven.	Contact	H (b)
Index heeft het contact zelf al geïnformeerd (ja/nee).	Ja	Ja, zie toelichting hierboven.	Index	D
Dag van aanvang van de symptomen	Ja	Ja, zie toelichting hierboven.	Index	G

[7] Artikel 9 lid 1 AVG en de daarop van toepassing zijnde overweging 35 AVG.
[8] Risicoclassificatie betreft een drietal vragen om de classificatie te beoordelen. De vragen betreffen of de index in hetzelfde huis woont of langer dan 12 uur op dezelfde plek is geweest. Hoe lang de index en het contact bij elkaar waren en of de index en het contact binnen 1,5m van elkaar zijn geweest. Er zijn 4 mogelijke uitkomsten: 1) Huisgenoten, 2a) Overige nauwe contacten, 2b) Overige nauwe contacten, 3) Overige (niet nauwe) contacten. Indien de BCO-medewerker de risicoclassificatie niet al bij het telefoongesprek met index heeft vastgesteld, moet index deze bepalen a.h.v. een drietal vragen. Indien de BCO-medewerker de risicoclassificatie al heeft vastgesteld, wordt dit in het BCO webportaal opgeslagen en niet meer naar GGD Contact gestuurd.
[9] Er wordt een meerkeuzevraag gesteld of één of meer van de opgenoemde punten van toepassing zijn. Keuze uit: Student, 70 jaar of ouder, gezondheidsklachten of extra gezondheidsrisico's, woont in een asielzoekerscentrum, spreekt slecht of geen Nederlands en werkt in de zorg. Hierop kan dan met een "Ja" of "Nee, denk het niet" op geantwoord worden.

Label	Ja	Ja, zie toelichting hierboven.	Contact	H (a)
Context	Ja	Ja, zie toelichting hierboven.	Contact	H (b)
Bron (contact handmatig of per GGD Contact toegevoegd)	Ja	Ja, zie toelichting hierboven.	Index	H (c)
Type	Ja	Ja, zie toelichting hierboven.	Contact	H (d)
Uniek ID	Ja	Ja, zie toelichting hierboven.	Index	H (e)

A. Instelbare vragen[10] **om contact op te kunnen nemen met het contact van de index,** waaronder vragen over voornaam, achternaam, telefoonnummer en e-mailadres.

B. Instelbare vragen[11] **om het risico van besmetting van het contact van de index in te schatten** om tot een risicoclassificatie te komen. De risicoclassificatie is noodzakelijk om te bepalen welk handelingsperspectief een contact moet krijgen. Omdat de index de contacten zelf kan informeren is het noodzakelijk dat de index aan de hand van de risicoclassificatie een juist handelingsperspectief in GGD Contact ziet. Het verstrekken van verkeerde adviezen aan de contacten draagt namelijk niet aan een effectieve indamming van een infectieziekte. In principe wordt de risicoclassificatie door de BCO-medewerker ingevuld tijdens het opmaken van het eerste lijstje. Omdat het ook mogelijk is voor de index om zelf contacten toe te voegen, is het echter noodzakelijk dat er vragen gesteld worden om de risicoclassificatie en daarmee de relevantie van het contact voor BCO te bepalen en de gegevens met de GGD te delen. De vragen die leiden tot de risicoclassificatie zijn afhankelijk van de door het RIVM opgestelde LCI- richtlijnen.

C. Instelbare vraag **om te identificeren of het contact tot een risicogroep behoort**, om in GGD Contact de keuze te geven of het contact via de index zelf of via de GGD benaderd moet worden. GGD Contact vraagt niet tot *welke* risicogroep iemand behoort, maar enkel of één of meer risicogroepen van toepassing zijn op het contact. De definitie van wat een risico- of prioriteit contact is, is afhankelijk van de laatste inzichten over de infectieziekte[12].

D. Antwoord op de vraag of de index het contact zelf al heeft geïnformeerd (ja/nee). Er zit geen functionaliteit in GGD Contact om de contacten zelf te informeren. Wel ondersteunt

[10] Het betreft instelbare vragen omdat de vragen die in de GGD Contact worden gesteld, (centraal door GGD GHOR Nederland) configureerbaar zijn. Aanpassen van de gevraagde gegevens moet altijd in overleg met FG i.v.m. mogelijke impact.
[11] De wijze van het beoordelen van de risicoclassificatie berust op de LCI-richtlijn bron- en contactonderzoek: https://whimsical.com/8SzFoAMZD5AC14b8g6uLN6
[12] Tijdens het schrijven van deze DPIA-rapportage hebben wij in Nederland nog steeds te maken met COVID-19.

GGD Contact bij het aangeven of de index mogelijk al een contact heeft geïnformeerd. De index kan in de App aangegeven of hij het contact zelf al heeft geïnformeerd.

E. De **datum van het laatste contactmoment** tussen index en het contact: in geval een contact in quarantaine moet, bepaalt dit laatste contactmoment tot wanneer de quarantaine moet duren. Zonder de laatste contactdatum kan door de GGD niet een juist handelingsperspectief worden verstrekt. Het is noodzakelijk dit aan de index te vragen omdat a) dit het handelingsadvies voor het contact bepaalt en b) de index het recht heeft anoniem te blijven tegenover het contact, waardoor datum van laatste contact niet aan het contact kan worden gevraagd.

F. Vrij opmerkingsveld bedoeld voor de index om eventuele opmerkingen toe te voegen waarvan hij inschat dat dit voor de GGD relevant is om te benoemen over het contact.

Met betrekking tot de gegevens die de GGD naar GGD Contact stuurt, geldt:

G. De **dag van aanvang symptomen**. Dit heeft de index nodig om te bepalen of contacten die hij/zij zelf nog toevoegt relevant zijn voor het BCO.

H. Een lijst van 'taken' die de index moet vervullen. Elke taak is een uitvraag naar contactgegevens. Per taak wordt doorgegeven:

a. Een **label**, aan de hand waarvan de index weet om wie het gaat. Het label kan zijn 'Jan Eric', 'Moeder', al naar gelang wat de GGD invult.

b. Een **context**, bijv. 'voetbaltrainer'. Dit heeft de index nodig om te herinneren om welk contact het gaat en onder welke omstandigheden contact heeft plaatsgevonden.
   Het label en de context tezamen beschrijven het contacttype van de index zonder dat de BCO-medewerker tijdens het gesprek de volledige naam hoeft uit te vragen. Dit maakt de relatie tussen de index en het contact duidelijker, voor zowel de index als de BCO-medewerker, en helpt daarmee persoonsverwisseling te voorkomen.

c. De **bron**. Een technisch veldje waarmee wordt bijgehouden of het contact initieel door de BCO-medewerker is opgegeven of door de index handmatig is toegevoegd. In het geval dat het contact door de index in GGD Contact is toegevoegd, is dit in het BCO webportaal van de BCO-medewerker zichtbaar, zodat de BCO-medewerker weet dat bijvoorbeeld de inschatting van de risicocategorie die door de index is gedaan, nog gevalideerd moet worden. Het gaat hier niet om een persoon/mogelijke bron van besmetting.

d. Een **type**. Een veld dat aangeeft dat de taak om het invullen van een contactpersoon gaat. In de toekomst kunnen in dit veld ook taken van heel andere aard worden gegeven (locaties, zelfrapportage). Voorlopig staat hier altijd 'contact' in.

e. Een **uniek ID** van de taak, zodat als de index de gegevens verstuurt het antwoord aan de juiste taak gekoppeld kan worden. Elke taak krijgt een uniek ID, die enkel door GGD Contact en het BCO webportaal wordt gebruikt. De plek waar de taak

ontstaat, dit kan het BCO webportaal zijn of de telefoon voor handmatig toegevoegde contacten, genereert een uniek ID.

Een deel van de bovengenoemde persoonsgegevens wordt reeds door de BCO-medewerker in het webportaal ingevuld. Indien de index telefonisch met de BCO-medewerker enkele contacten doorgeeft met wie hij in contact is geweest noteert de BCO-medewerker in het BCO webportaal:

- Label
- Context
- De bron
- Risicoclassificatie
- Datum laatste contactmoment
- Aandachtspunten
- Dag van aanvang van de symptomen
- Type
- Uniek ID (gebeurt automatisch, dit hoeft de BCO-medewerker niet in te voeren)

Indien de index zelf zijn contactgegevens aanlevert via de GGD Contact-app dan kan de index de volgende velden invullen:

- Naam + achternaam
- Telefoonnummer
- E-mailadres
- Datum laatste contactmoment (indien het een nieuw contact is en de BCO-medewerker dit nog niet heeft ingevuld)
- Risicoclassificatie (indien het een nieuw contact is en de BCO-medewerker dit nog niet heeft ingevuld)
- Aandachtspunten
- Vrij opmerkingsveld
- Contacttype (indien het een nieuw contact is en de BCO-medewerker dit nog niet heeft ingevuld)
- Of de index het contact zelf al heeft geïnformeerd
- Dag van aanvang van de symptomen (indien het een nieuw contact is en de BCO-medewerker dit nog niet heeft ingevuld)

Zelf-BCO door de Index

Wanneer de index door middel van Zelf-BCO in de App zelf zijn besmettelijke periode bepaalt, dient de index klachten te selecteren door middel van het aanvinken van checkboxen. Het is ook mogelijk dat een index geen klachten heeft. Bij geen klachten geldt de testdatum als eerste ziektedag en kan dat worden ingevuld.

Wanneer de index de eerste ziektedag niet wil invullen kan je de app niet gebruiken. Hiervoor is gekozen omdat zonder inzicht in de besmettelijke periode het verzamelen van de contacten niet nuttig/mogelijk is. Indien er vooraf contact is geweest met de GGD en de informatie omtrent de eerste ziektedag reeds bekend is, dan wordt deze vraag niet opnieuw in de GGD Contact-app gesteld.

Voor het verzenden van de klachten van app naar portal geldt: De te verwerken gegevens in functionaliteit zelf-BCO worden ook in het reguliere BCO-proces (d.w.z. zonder gebruikmaking van GGD Contact) uitgevraagd en vastgelegd. De noodzakelijkheid van het verzamelen van klachten moet in de DPIA van het reguliere BCO-proces worden onderbouwd. Buiten de scope van deze DPIA valt de beoordeling of de verwerking van klachten noodzakelijk is voor het BCO. Bij het opstellen van deze DPIA is hiervan uitgegaan dat het verwerken van klachten noodzakelijk is voor het BCO.

BCO Vragenlijst en Osirisis Vragenlijsten

Met de toevoeging van de functionaliteit BCO- en Osiris vragenlijst wordt de vastlegging van het uitvraagproces binnen het reguliere BCO proces verplaatst naar het BCO-portaal. De toevoeging

van deze functionaliteit zorgt niet voor de vastlegging van nieuwe (persoonsgegevens) ten opzichte van het huidige BCO-proces. De uitvraag van de informatie door middel van deze vragenlijsten zijn landelijk door de GGD'en vastgesteld in de werkinstructie voor BCO-medewerkers. Met het verzoek van de GGD'en om het BCO te ondersteunen, geven zij opdracht deze gegevens nu in het BCO-portaal te verwerken.

De aanvullende gegevens ten behoeve van RIVM (Osiris) zijn niet tot een persoon te herleiden.

De toevoeging betreft concreet:

1. Toevoeging van gegevens aan het BCO-portaal:
    a. Vragen van het volledige BCO-gesprek conform de landelijke werkinstructie
    b. Vragen ten behoeve van de informatieverstrekking aan RIVM ten behoeve van de onderzoeken die RIVM uitvoert t.a.v. COVID-19 pandemie (ook wel 'Osiris-vragenlijst' genoemd)
2. Uitbreiding gebruik voor alle indexen:
    a. Alle gegevens in het portaal zijn bewerkbaar en invulbaar door de BCO-medewerker in een portaal.

De noodzakelijkheid van het verzamelen van de gegevens voor het volledige BCO-gesprek en de Osirisvragenlijst moet in de DPIA van het reguliere BCO-proces worden onderbouwd. Voor de 'Referentie DPIA GGD Contact' is deze buiten scope van deze DPIA.

3. Betrokken partijen en rolverdeling

In het onderstaande wordt achtereenvolgens de rol besproken van de GGD, de minister van VWS, en GGD GHOR, bij de ontwikkeling (hierna ook aangeduid als: realisatiefase), en het gebruik (hierna ook aangeduid als: praktijkfase), van de GGD Contact-app.

GGD'en

Op grond van artikel 6, eerste lid, onderdeel c, Wpg jo. artikel 14 Wpg heeft de GGD de wettelijke taak om de BCO uit te voeren.

Naar aanleiding van de druk op de BCO tijdens de Corona-crisis hebben de GGD'en er gezamenlijk toe besloten om met behulp van digitale middelen de BCO te ondersteunen. Dat gezamenlijk besluit heeft geresulteerd in de opdracht om de GGD Contact-app te ontwikkelen die kan worden gebruikt ter ondersteuning van de BCO. Daarbij wordt benadrukt dat de app zich niet beperkt tot de BCO in het kader van COVID-19.

De opdracht tot het doen ontwikkelen van de GGD Contact-app past dan ook in de wettelijke taak van de GGD'en.

De verwerking van persoonsgegevens aan de hand van de GGD Contact-app gebeurt daarom ook ten behoeve van de vervulling van de taak van algemeen belang van de GGD'en (als bedoeld in artikel 6, eerste lid, aanhef en onder e, AVG jo. artikel 6, eerste lid, onderdeel c jo. artikel 14 Wpg)

Voor zover bijzondere persoonsgegevens worden verwerkt kunnen de GGD'en gebruik maken van de doorbrekingsgrond uit artikel 9, tweede lid, aanhef en onder i, AVG.

VWS
Naast de wettelijke taak van de GGD'en tot het uitvoeren van de BCO, heeft de minister van VWS op basis van artikel 3, eerste lid, Wpg de taak om de kwaliteit en doelmatigheid van de publieke gezondheidszorg te bevorderen, en zorg te dragen voor de instandhouding en verbetering van de landelijke ondersteuningsstructuur. Daarbij geeft de minister van VWS op basis van artikel 7, eerste lid, Wpg leiding aan de bestrijding van infectieziekten, waaronder COVID-19.

Bij de ontwikkeling van de GGD Contact-app is VWS met name stelselverantwoordelijk voor de inrichting en ontwikkeling van de app, en het informeren van de gebruikers over de werking van de app. Daarbij is VWS ook verantwoordelijk voor de (tijdelijke) hosting van de GGD Contact-app.

De minister van VWS heeft opdracht gegeven tot de vervanging van HPZone, waarbij door de DPG-raad is gekozen voor GGD Contact. De minister van VWS is samen met de GGD'en ook eindverantwoordelijk voor de verschillende stappen bij de realisatie van de GGD Contact-app. De uitwerking daarvan wordt op dit moment vastgelegd in een nieuwe governancestructuur.

Voor zover persoonsgegevens worden verwerkt bij de ontwikkeling van de GGD Contact-app heeft de minister daarvoor een verwerkingsgrondslag op basis van de vervulling van zijn taak van algemeen belang (artikel 6, eerste lid, aanhef en onder e, AVG jo. artikel 3, eerste lid jo. artikel 7, eerste lid Wpg).

In het geval bijzondere persoonsgegevens worden verwerkt kan de minister van VWS gebruik maken van de doorbrekingsgrond artikel 9, tweede lid, aanhef en onder i, AVG.

*Gezamenlijke verwerkingsverantwoordelijkheid GGD'en en VWS (**realisatiefase)***
Uit het voorgaande blijkt dat het doel van de verwerking van persoonsgegevens bij de ontwikkeling, en de inzet van de GGD Contact-app, is bepaald door de GGD'en, in het verlengde van hun wettelijke taak.

Uit het voorgaande blijkt ook dat de minister van VWS, naast de GGD'en, tijdens de realisatiefase eindverantwoordelijk is voor bepaalde belangrijke deelelementen die bepalend zijn voor het functioneren van de GGD Contact-app.

Conclusie
Om die reden moeten de GGD'en en de minister van VWS worden aangemerkt als gezamenlijk verwerkingsverantwoordelijk voor zover tijdens de ontwikkeling van de GGD Contact-app sprake is van de verwerking van (bijzondere) persoonsgegevens.

Zelfstandige verwerkingsverantwoordelijkheid GGD'en & Verwerkerschap VWS ***(praktijkfase)***
Na het afronden van de realisatiefase, en de ingebruikname van de GGD Contact-app, verliest de minister van VWS de zeggenschap die hij had tijdens de ontwikkelingsfase.

De minister van VWS oefent tijdens de praktijkfase dan ook geen zeggenschap uit over het middel, de GGD Contact-app, waarmee persoonsgegevens worden verwerkt. De GGD'en behouden daarentegen wel zeggenschap over de werking en inrichting van de GGD Contact-app tijdens de praktijkfase. Om die reden kunnen de GGD'en en de minister van VWS tijdens de praktijkfase niet als gezamenlijk verwerkingsverantwoordelijk worden aangemerkt.

Conclusie
Vanwege het behouden van de zeggenschap over de GGD Contact-app, en het bepalen van het doel van de verwerking van (bijzondere) persoonsgegevens aan de hand van de GGD Contact-app, zijn de GGD'en tijdens de praktijkfase als zelfstandig verwerkingsverantwoordelijken aan te merken voor de betreffende verwerkingen.

Voor de minister van VWS geldt dat hij tijdens de praktijkfase aan te merken is als verwerker. Dit omdat, hij tijdens de praktijkfase enkel zorgdraagt voor de (tijdelijke) hosting van de GGD Contact-app in opdracht van de GGD'en en geen zeggenschap heeft over het doel en de middelen van gegevensverwerking

Verwerkerschap GGD GHOR Nederland (realisatiefase)
Ten behoeve van de realisatie van de GGD Contact-app is de minister van VWS (als opdrachtgever) met GGD GHOR (als opdrachtnemer) overeengekomen dat GGD GHOR ondersteunende diensten verricht in het kader van de ontwikkeling van de GGD Contact-app.

Uit artikel 1.1 van de Dienstverleningsovereenkomst ARVODI-2018 Opdracht aan GGD GHOR voor het realiseren van digitale randvoorwaarden ten behoeve van de bestrijding van COVID-19 (hierna: DVO digitale randvoorwaarden) blijkt dat de ondersteunende diensten van GGD GHOR Nederland (voor zover relevant) bestaan uit:

- Het realiseren van een koppeling tussen de GGD Contact en de reeds aanwezige bedrijfssystemen van Opdrachtnemer en een gebruikersportaal voor bron- en contactonderzoekers. Daarnaast wordt de integratie van de Thuisrapportage App met HPZone uitgevoerd.

- Het landelijk centraliseren van het beheer van HPZone, waarbij ook HPZoneLite wordt uitgerold ten behoeve van de landelijke schil aan medewerkers voor bron- en contactonderzoek.
- Het bijbehorende programmamanagement.

Zie: artikel 1.1 DVO digitale randvoorwaarden.

Voor de ontwikkeling van de GGD Contact-app is eveneens een samenwerkingsverband opgericht waar GGD GHOR Nederland deel van uitmaakt. Dat samenwerkingsverband wordt aangeduid als Stuurgroep Oplossing 2 (IZB) (hierna: de Stuurgroep). De Stuurgroep bestaat uit vertegenwoordigers van zowel GGD'en, de minister van VWS, als GGD GHOR Nederland, en moet worden getypeerd als overlegorgaan.

Zoals blijkt uit het Plan van Aanpak ligt de formeel juridische eindverantwoordelijkheid, en daarmee zeggenschap, bij de GGD'en en de minister van VWS afzonderlijk (zie daarover randnr.0), en niet bij GGD GHOR Nederland. Om zeker te stellen dat de feitelijke zeggenschap niet afwijkt van de formeel-juridische regeling kan het nuttig zijn om daarover nadere afspraken te maken.

Naast dat GGD GHOR Nederland onderdeel vormt van de Stuurgroep, vervult GGD GHOR Nederland ook een rol bij het implementeren van de GGD Contact-app, en draagt hij zorg voor de koppeling met het GGD-systeem HPzone (zie randnr.0).

Conclusie
Gelet op het voorgaande blijft de rol van GGD GHOR Nederland tijdens de realisatiefase beperkt tot zijn rol binnen de Stuurgroep, en de implementatie en koppeling van de GGD Contact-app. Daarmee oefent GGD GHOR Nederland **geen zeggenschap** uit over het doel en de middelen van de verwerking van (bijzondere) persoonsgegevens tijdens de ontwikkeling van de GGD Contact-app. Om die reden is GGD GHOR Nederland tijdens de realisatiefase dan ook niet aan te merken als (gezamenlijk) verwerkingsverantwoordelijke.

Voor zover GGD GHOR Nederland zorgdraagt voor de implementatie van de GGD Contact-app en de koppeling met HPzone, en daarbij persoonsgegevens worden verwerkt, moet GGD GHOR Nederland worden aangemerkt als verwerker in de zin van artikel 4, onderdeel 8, AVG jo. artikel 28 AVG.

Verwerkerschap GGD GHOR (praktijkfase)
Voor zover de implementatie van de GGD Contact-app, en (het beheren van) de koppeling met HPzone voortduurt, en daarbij door GGD GHOR Nederland (bijzondere) persoonsgegevens worden verwerkt, is GGD GHOR Nederland ook tijdens de praktijkfase aan te merken als verwerker in de zin van artikel 4, onderdeel 8, AVG jo. artikel 28 AVG.

Intermax – verwerker

GGD Contact, de datasluis en het BCO webportaal worden vooralsnog gehost bij Intermax. Intermax wordt door VWS ingeschakeld. Op den duur zal de hosting bij GGD GHOR Nederland op het platform van Mendix plaatsvinden. Momenteel is dit niet aan de orde en maakt Mendix om die reden dan ook geen onderdeel uit van deze DPIA.

VWS heeft voor het ontwikkelen van GGD Contact en de bijbehorende onderdelen Egeniq ingeschakeld. Deze partij ontwikkelt slechts de software en heeft behalve het ontwikkelen geen rol bij de verwerking van persoonsgegevens. Derhalve komt aan deze partij geen rol toe vanuit de AVG.

Tussen VWS en Intermax is een hostingovereenkomst gesloten en tussen VWS en de GGD'en zal een verwerkersovereenkomst worden gesloten, waarbij Intermax wordt aangemerkt als subverwerker. Gelet op toekomstige brede inzet van GGD Contact voor andere infectieziekten dan COVID-19, de bedoeling van partijen om GGD Contact in de toekomst op het platform van Mendix te plaatsen, maar vooral de rol van GGD GHOR Nederland in het geheel, is het niet alleen voor de hand liggend dat GGD GHOR Nederland samen met de GGD'en de contractpartij is voor de hosting bij Intermax, maar is vanuit het oogpunt van het snel handelen bij bijvoorbeeld beveiligingsincidenten van enorm belang.

Index – betrokkene

De index is de verstrekker van de contactgegevens van zijn contacten aan de GGD in het kader van BCO. Daarnaast worden de gegevens van de index in GGD Contact verwerkt, waardoor de index als betrokkene wordt gekwalificeerd. Dat de index zelf gegevens van andere betrokkenen aan de GGD verstrekt, impliceert niet dat de index als verwerkingsverantwoordelijke in de zin van de AVG moet worden aangemerkt. Allereerst past deze verwerking door de index niet binnen het materieel toepassingsgebied van de AVG.[13] Daarnaast stelt de index het doel en de middelen van de verwerking niet vast. De index heeft de keuze uit de aangereikte middelen van de GGD om deel te nemen aan BCO en ten behoeve hiervan verstrekt de gegevens aan de GGD.

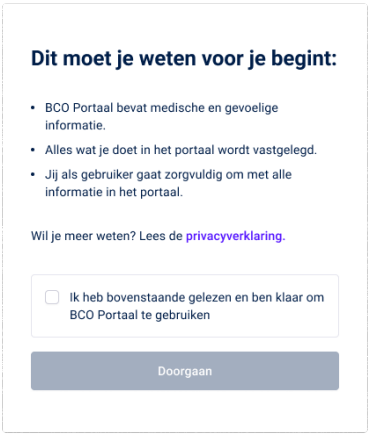
Contacten *(betrokkene)*

De contacten waarvan persoonsgegevens worden verwerkt zijn evenals de index aan te merken als een betrokkene van wie de persoonsgegevens in GGD Contact en de bijbehorende datasluis en het BCO webportaal worden verwerkt. In deze situatie kan het contact van de index gezien worden als een indirecte betrokkene en de index zelf als direct betrokkene. Het verschil met de index is dat het contact niet de verstrekker is van zijn eigen persoonsgegevens, maar dat deze in het kader van BCO door de index aan de GGD wordt verstrekt.

[13] Artikel 2 AVG.

BCO-portaal Gebruiker (*betrokkene*)

Van de BCO-medewerkers worden gegevens vastgelegd ten behoeve van het (rechtmatige) gebruik van GGD Contact. De logging van deze gegevens bevat ook persoonsgegevens. In deze situatie is de BCO-portaal Gebruiker aan te merken als direct betrokkene. Deze logging van deze persoonsgegevens over de BCO-medewerkers worden verwerkt in het kader van de veldnormen voor gegevensverwerking in zorg, die volgen uit de NEN7513. De BCO-portaal Gebruiker wordt over deze logging geïnformeerd bij het eerste gebruik:



4. Gegevensverwerking

Het gebruik van GGD Contact doorloopt de volgende processen, gebaseerd op de procesflow (**Bijlage 2**):

Stap	Uitwerking
1	**Verificatie identiteit index**
	Het BCO is aan de orde vanaf het moment dat er een melding van infectieziekte is gedaan.[14] Het BCO-proces begint bij de BCO-medewerker die telefonisch contact opneemt met de index.[15]
2	**Verzoek om GGD Contact te downloaden**
	Ten tijde van het telefonisch contact met de index vraagt de BCO-medewerker aan de index of hij bereid is om GGD Contact te downloaden. a) Indien de index ervoor kiest GGD Contact niet te downloaden, wordt het reguliere BCO-proces gevolgd. Doordat de volledige BCO-vragenlijst is opgenomen in het BCO-portaal kan de BCO-medewerker het BCO-portaal zowel bij gebruiken bij een index die de App wel gebruikt als bij een index die de App niet gebruikt.

[14] Het doen van deze melding na vaststelling van een ziekte als COVID-19 is bij wet verplicht, artikel 22 Wpg.
[15] Hierbij wordt de identiteit van de index geverifieerd. Dit gebeurt door middel van naam, geboortedatum en telefoonnummer.

	b) Indien de index ervoor kiest om GGD Contact wel te downloaden, dan volgt stap 3. De index kan ook op eigen initiatief de GGD Contact app reeds hebben gedownload vóór het telefonisch contact met de BCO-medewerker.
3	**Index downloadt GGD Contact**
	Indien de index instemt met digitaal versturen van de contactgegevens, kan de index GGD Contact in de Appstore (Apple) of playstore (Android) downloaden. GGD Contact is beschikbaar voor IOS vanaf versie 11 en voor Android vanaf versie 5.[16]
4	**Privacyverklaring wordt getoond**
	De index krijgt voordat hij akkoord gaat met het gebruik van GGD Contact een privacyverklaring te zien. Deze privacyverklaring is tevens te allen tijde binnen GGD Contact gemakkelijk terug te vinden en kan zo worden teruggelezen door de index. Zo is in GGD Contact de tekst opgenomen: 'Help bij het bron- en contactonderzoek. Gegevens blijven op jouw telefoon totdat je ze deelt met de GGD. Lees meer in de privacyverklaring'. Met hierbij een link naar de privacyverklaring. In de tekst op de GGD-website die verwijst naar het bestaan van de app is ook opgenomen dat het gebruik van GGD Contact vrijwillig is. Ook in de werkinstructie en e-learning voor BCO-medewerkers is opgenomen te benadrukken dat het gebruik van GGD Contact vrijwillig is.
5	**Zelf-BCO door de Index**
	• Indien de index op eigen initiatief de App heeft gedownload start het gebruik van de App met het zelf-BCO. • De index selecteert zijn klachten uit een lijst met COVID-19 gerelateerde klachten en voert de datum in dat de klachten zijn begonnen. Op basis hiervan wordt de besmettelijke periode vastgesteld. • Indien er geen klachten zijn, voert de index de testdatum in. • Wanneer de index de eerste ziektedag niet wil invullen kan je de app niet gebruiken. Hiervoor is gekozen omdat zonder inzicht in de besmettelijke periode het verzamelen van de contacten niet nuttig/mogelijk is. Indien er vooraf contact is geweest met de GGD en de informatie omtrent de eerste ziektedag reeds bekend is, dan wordt deze vraag niet opnieuw in de GGD Contact-app gesteld. • Zelf-BCO is ook te doorlopen indien de GGD die het BCO niet met behulp van de GGD Contact app uitvoert. Dan kan het worden gebruikt in de voorbereiding op het BCO-gesprek met de BCO-medewerker en stopt het proces bij deze stap. De gegevens worden dan handmatig ingevoerd.
6	**BCO-medewerker vult contactenlijst in het BCO webportaal**
	Tijdens het telefoongesprek tussen de index en de BCO-medewerker maakt de BCO-medewerker een eerste contactenlijst op in het BCO-portaal. Hierbij wordt niet ingegaan

[16] Er is gekozen voor een zo grote mogelijke dekking zodat GGD Contact ook werkt op oudere telefoontoestellen. Het gebruik van oudere versies wordt echter gestaakt zodra er geen beveiligingspatches meer voor worden gemaakt. Dit heeft geleid tot de keuze van versie 11 voor IOS en versie 5 voor Android.

	op de specifieke contactgegevens van het contact van een index, maar wordt door middel van herkenbare woorden ofwel labels aangegeven met wie de index in contact is geweest. Bijvoorbeeld 'oma of broertje'. Hierdoor weet de index op het moment dat hij dit terug ziet in GGD Contact van wie hij de contactgegevens moet toevoegen. De BCO-medewerker maakt een nieuwe case aan indien de index niet reeds bekend is en noteert: • Naam index • Telefoonnummer index • Casenummer De BCO-medewerker maakt een eerste aanzet voor de contactenlijst van de index en noteert: • Eerste ziektedag index • Label • Context • Bron • Type • Risicocategorie Indien de index door middel van zelf-BCO zelf de besmettelijke periode heeft bepaald, kan de BCO-medewerker in het telefoongesprek de informatie verifiëren en eventueel aanpassen.
7	**BCO-medewerker registreert BCO-vragenlijst + Osiris Vragenlijst**
	Separaat aan het registeren van de informatie van de contacten registreert de BCO-medewerker het volledig BCO uitvraagscript in het BCO-portaal. Voor de BCO-medewerker is het hierdoor niet van belang of de index wel of niet de App gebruikt. De BCO-medewerker doorloopt de volledige vragenlijst in het portaal incl. de vragen die nodig afkomstig zijn uit de Osiris vragenlijst. Indien de index de App wel gebruikt volgt stap 8 en wordt het voorbereide contactlijstje uit stap 7 gedeeld met de index middels een activatiecode.
8	**Activatiecode wordt verstuurd**
	Tijdens het telefoongesprek verstrekt de BCO-medewerker een activatiecode aan de index. De BCO-medewerker vraagt aan de index deze code op te schrijven, zodat deze na het telefoongesprek kan worden ingevuld in GGD Contact. Deze activatiecode is nodig om het door de BCO-medewerker opgestelde contactpersonenlijstje op te halen in GGD Contact. De activatiecode is eenmalig te gebruiken door de index. Daarnaast is de activatiecode ook beperkt geldig. De code is gedurende 45 minuten bruikbaar. Deze 45 minuten geven de index voldoende tijd om het gesprek met de GGD af te ronden en na het gesprek de App te downloaden en te activeren.
9	**Invoer activatiecode door index**

	Tijdens of na het telefoongesprek kan de index de door de BCO-medewerker verstrekte activatiecode in GGD Contact invullen.
10	**Verificatie van de activatiecode**
	Er vindt een verificatie van de activatiecode plaats tussen GGD Contact en de backend.
11	**Contactenlijst wordt vanuit de backend opgehaald**
	De vooraf opgestelde contactenlijst wordt tijdens het telefoongesprek van de BCO-medewerker met de index vanuit de backend naar GGD Contact opgehaald.
12	**Ophalen contactenlijst door de index**
	Wanneer de index aangeeft dat hij de privacy verklaring heeft gelezen en begrijpt hoe GGD Contact zijn gegevens gebruikt kan de index de activatiecode invoeren en wordt de eerder opgestelde contactenlijst door de BCO-medewerker in GGD Contact geïmporteerd.
13	**Toestemming voor toegang tot contacten**
	De index krijgt in GGD Contact een pop-up scherm waarop om toestemming voor het ophalen van de contacten uit het adresboek van de telefoon van de index wordt gevraagd. De tekst in de pop-up luidt als volgt: "De app heeft zo toegang tot de contacten op je telefoon. Wil je dit niet? Dan kun je contactgegevens ook handmatig toevoegen." a) Wanneer de index toestemming geeft voor het ophalen van de contacten uit het adresboek van zijn telefoon, worden allen namen uit de telefoon uitgelezen om een match te maken in GGD Contact. b) Wanneer de index géén toestemming geeft voor het ophalen van het contact uit het adresboek van zijn telefoon, kunnen de contacten handmatig worden toegevoegd door de index in GGD Contact. Bij het ophalen van de contactgegevens uit het adresboek van de telefoon worden enkel de namen van de contactpersonen zichtbaar in GGD Contact. De gegevens worden alleen lokaal, op het gebruikte apparaat, verwerkt. Overige extra velden die index mogelijk in het adresboek heeft toegevoegd (bijvoorbeeld woonadres, geboortedatum en extra notities over het contact), worden niet zichtbaar.
14	**Aanvulling contacten door de index**
	Voor de index is aan de hand van de reeds opgehaalde contactenlijst inzichtelijk welke contactgegevens hij dient aan te vullen. Indien er toestemming is verleend voor het importeren van de contactenlijst uit het adresboek van de telefoon van de index, stelt GGD Contact aan de hand van het label in de contactenlijst in GGD Contact een suggestie voor. Dit voorgestelde contact is gebaseerd op het adresboek uit de telefoon van de index (bijv. het label 'Aziz F' wordt gekoppeld aan de relatie 'Aziz Firat' uit de telefoon). De index wordt gevraagd om de volgende gegevens in te vullen in GGD Contact: • Contactgegevens van het contact van de index

	• Soort contact →Hier worden vragen gesteld over de ontmoeting met het contact, waardoor het contacttype wordt bepaald. Dit wordt bepaald door de beantwoording van de vragen: o langer dan 12 uur op dezelfde plek als het contact geweest (Ja/Nee) o langer dan 15 minuten in dezelfde ruimte als het contact geweest (Ja/Nee) o dichter dan 1,5 meter bij het contact geweest (Ja/Nee) *Hierbij maakt het niet uit of het een kort of langdurig moment is geweest waarbij je dichter dan 1,5 meter bij het contact bent geweest.* [17] • Prioriteitsgroep → Of het contact ook tevens in een van de hieronder opgesomde prioriteitsgroep valt. Deze vraagstelling is breed waarbij ja of nee ingevuld dient te worden. Prioriteitsgroep indien: o Student o 70 jaar of ouder o Gezondheidsklachten of extra gezondheidsrisico's o Woont in een zorginstelling (bijvoorbeeld bejaardentehuis) of asielzoekerscentrum o Spreekt slecht of geen Nederlands o Werkt in de zorg, onderwijs of een contactberoep (bijvoorbeeld kapper).
15	**Aanlevering nieuwe contacten door index**
	Het is voor de index mogelijk om nieuwe contacten aan te leveren die nog niet door de BCO-medewerker in de contactenlijst zijn opgenomen. Dit is mogelijk op één van de hiervoor beschreven manier namelijk: ophalen uit het adresboek van de telefoon van index of handmatig invoeren.
16	**Risico-inschatting 'soort contact' door index**
	Wanneer de index een nieuw contact invoert in GGD Contact, dient de index een risico-inschatting te maken over wat voor een soort contact het is (risicoclassificatie) nadat alle gegevens over het contact zijn ingevuld. Dit is bedoeld zodat er leefregels/handelingsperspectief voor deze contactpersoon verschijnt. De risico-inschatting vindt plaats door het stellen van onderstaande vragen aan de index, welke hij in GGD Contact beantwoordt: 1. Woon je in hetzelfde huis of ben je langer dan 1 uur op dezelfde plek geweest? (Ja/Nee). 2. Hoe lang waren jullie waarschijnlijk bij elkaar in de buurt? Langer dan 15 minuten/korter dan 15 minuten. a. Bij het antwoord "korter dan 15 minuten" krijgt de index de vervolgvraag, namelijk: Is een of meerdere van deze dingen tijdens jullie ontmoeten gebeurd?

[17] Deze indicatie wordt aangepast aan de hand van de geldende LCI-richtlijn.

	- In je gezicht geniesd - Geknuffeld of gezoend - Ander lichamelijk contact Het antwoord kan zijn: Ja, één of meerdere dingen/Nee, denk het niet. 3. Zijn jullie binnen 1,5 meter van elkaar geweest? Het antwoord kan zijn: Ja, denk het wel/Nee, denk het niet. Wanneer was de laatste ontmoeting?
17	**Verschijnen van leefregels/handelingsperspectief**
	Wanneer de index alle informatie omtrent de persoon waarmee hij in contact is geweest, heeft ingevuld, verschijnen de leefregels – ook wel het handelingsperspectief – voor dit specifieke contact. Hierin kan bijvoorbeeld zijn opgenomen dat het betreffende contact wordt geadviseerd om nog 5 dagen in thuisisolatie te verblijven. De leefregels/handelingsperspectief zijn/is afhankelijk van risicoclassificatie (het soort contact). Zie het protocol van het RIVM[18] voor het handelingsperspectief per risicoclassificatie (huisgenoot/nauw contact/overig contact).
18	**Delen van de/het leefregels/handelingsperspectief door index**
	Wanneer de leefregels in GGD Contact verschijnen, heeft de index de mogelijkheid om deze leefregels te delen met het contact. Dit is mogelijk door op de knop 'kopieer leefregels' te drukken. Deze leefregels kunnen dan op een eigen gekozen manier door de index worden gedeeld met het contact.
19	**Controlevraag voor het informeren van het contact**
	Wanneer de index het contact heeft toegevoegd en de leefregels heeft ingezien en vervolgens een nieuw contact wil toevoegen, stelt GGD Contact eerst een controlevraag, namelijk: "Heb jij het contact geïnformeerd en de leefregels gedeeld?". Hierop kan de index antwoorden: - Ja; - Nee, doe ik later; - Nee. De keuze van de index op deze vraagstelling wordt opgeslagen in GGD Contact, zodat indien nodig de BCO-medewerker contact kan opnemen met het contact indien de index dit niet heeft gedaan.
20	**Opslag gegevens in de sluis**
	De sluis is een API tussen GGD Contact en het BCO-portaal. Het brengt communicatie tussen GGD Contact en het BCO-portaal teweeg en kan worden gezien als een doorgeefluik waar de gegevens tijdelijk staan opgeslagen totdat deze vanuit GGD Contact aan het BCO-portaal worden doorgegeven. De sluis zorgt voor de koppeling tussen het device van de index en het BCO-portaal van de BCO-medewerker.

[18] https://lci.rivm.nl/COVID-19-bco

	De data die door de sluis 'reist' is versleuteld, waarbij de sluis zelf de data niet kan 'lezen'. Eveneens is het voor de sluis niet bekend van wie de data afkomstig is. Door gebruik van een token is het voor GGD Contact en het BCO-portaal duidelijk bij welke case de data hoort. De sluis zelf kan de data in de sluis niet ontcijferen. Indien een kwaadwillende zich toegang tot de sluis verschaft, is het voor deze persoon niet te achterhalen welke data er door de sluis heengaat.
21	**Verzending contactenlijst naar BCO-portaal**
	Nadat de index de contactenlijst heeft ingevuld, kan hij op de 'ik ben klaar'-button/'verstuur gegevens naar GGD' drukken. De ingevulde contactenlijst wordt doorgestuurd naar het BCO-portaal van de BCO-medewerker. De index heeft 48 uur na het activeren van de activatiecode om de contactenlijst aan te vullen en naar het BCO-portaal te versturen. Bij het niet (volledig) invullen van de velden in GGD Contact, krijgt de index hiervan een melding. Zoals eerder aangegeven is het niet verplicht alle velden in te vullen daarom kan de index deze melding doorklikken.
22	**Verdeling casenummers onder BCO-medewerkers door werkverdeler**
	De werkverdeler van de GGD verdeelt de ontvangen contactenlijsten op basis van een casenummer onder de BCO-medewerkers.
23	**BCO-medewerker beoordeelt risicoclassificatie**
	Bij handmatige invoer van contacten door de index, checkt de BCO-medewerker of de risicoclassificatie juist is ingevuld.
24	**BCO-medewerker kan contact opnemen met contact van index**
	Wanneer de BCO-medewerker het nodig acht om bijvoorbeeld nog gegevens aan te vullen van een contact in het BCO-portaal, kan de BCO-medewerker contact opnemen met het betreffende contact. Tevens kan de BCO-medewerker een handelingsperspectief delen met het contact als hier aanleiding voor is.
25	**Nieuwe gegevensaanlevering door index**
	Het kan voorkomen dat de index zich op een later moment bedenkt dat hij tevens met nog een nieuw contact in contact is geweest gedurende de besmettingsperiode. In dat geval kan de index volgens het eerder beschreven proces eveneens een nieuw contact aanmaken. Deze gegevens kunnen dan opnieuw met de GGD worden gedeeld en toegevoegd aan de contactenlijst. Zoals in de scope van de DPIA eerder is aangegeven ziet deze DPIA op het gebruik van de App en het BCO-portaal van de BCO-medewerker.
26	**(Handmatige) koppeling gegevens aan HP Zone Lite GGD**
	De gegevens worden door de BCO-medewerker vanuit het BCO webportaal handmatig gekopieerd naar HP Zone Lite van de GGD, te weten HPZone. Voor de toekomstige versies van GGD Contact en het BCO webportaal bestaat de wens om een automatische koppeling met HPZone te realiseren. In deze DPIA wordt nog uitgegaan van een

	handmatige handeling, waarmee de aangeleverde gegevens door de GGD uit het BCO webportaal in HPZone worden gezet. Zoals eerder aangegeven ziet deze DPIA op het gebruik van GGD Contact en het BCO webportaal van de BCO-medewerker. Het proces van de gegevensverwerking naar en in HPZone valt buiten de scope van deze DPIA, aangezien het een reeds bestaande verwerking betreft in een systeem dat niet gekoppeld is aan GGD Contact

5. Verwerkingsdoeleinden

Voor infectieziektebestrijding is het noodzakelijk dat BCO wordt uitgevoerd. GGD Contact (met de bijbehorende sluis en het portal) is een digitaal hulpmiddel dat ter versnelling van het BCO-proces van de GGD rondom infectieziektebestrijding dient en waar momenteel COVID-19 de aanleiding voor is. De doelen van de gegevensverwerkingen rondom GGD Contact:

- Het doel van de app GGD Contact is om het aantal uur dat GGD per index besteedt aan BCO te verminderen, waardoor GGD voor meer indexen BCO kan uitvoeren.
- De verwerkingen binnen GGD Contact zijn bedoeld ter ondersteuning van het BCO-proces door middel van het aanleveren van de contacten van de index aan de GGD door de index zelf. Dit zorgt ervoor dat de GGD sneller in beeld heeft wie de mogelijke contacten van de index zijn, hen kan informeren over de blootstelling en het risico op besmetting, hen te wijzen op maatregelen die genomen moeten worden om verdere verspreiding te voorkomen en hen hierin te begeleiden. Aanvullend hierop betreft het monitoren van locaties of situaties waarin mensen besmet zijn geraakt, om eventuele verheffingen of lokale risico's te signaleren en zo mogelijk extra maatregelen te implementeren.
- De verwerkingen in de sluis zijn noodzakelijk om de gegevens van GGD Contact naar het BCO webportaal te verzenden.
- Daar waar GGD Contact (de applicatie zelf) voor de index is bedoeld, is het BCO webportaal voor de BCO-medewerkers bedoeld om contactenlijsten klaar te zetten voor de index. Hierdoor neemt de tijdsbesteding aan het BCO af, waardoor in tijden van grootschalige infectieziektebestrijding een BCO-medewerker meer werk aankan.

Door het geheel van de verwerkingen (in GGD Contact, sluis en BCO webportaal) neemt daarnaast de kwaliteit van BCO toe, doordat het digitaal aanleveren van contactgegevens vanuit de GGD Contact minder foutgevoelig is dan wanneer gegevens nadat ze mondeling worden verstrekt worden geregistreerd.

6. Belangen bij gegevensverwerking

De volgorde van de beschrijving van de diverse belangen zegt niets over de prioritering van de belangen.

Samenleving als geheel

De samenleving als geheel heeft een aantal belangen bij het gebruik van GGD Contact. Doordat het BCO-proces sneller en efficiënter kan worden uitgevoerd, resulteert dit in het effectiever terugdringen van de uitbraak van een infectieziekte die zich op grote schaal voordoet en snel verspreidt. Snelle infectieziektebestrijding is immers ter bescherming van de samenleving als geheel en is essentieel voor goede publieke gezondheid. Het digitale BCO-proces door GGD Contact zorgt voor een snelle en minder foutgevoelige BCO dat door middel van het regulier BCO-proces niet behaald kan worden.

Voor wat betreft het monitoren van BCO op basis van de gegevens in GGD Contact omtrent de inzichten van de verspreiding van een infectieziekte, is tevens van een groot belang voor de samenleving. Op basis van rapportages van deze monitoring kan namelijk inzicht worden verschaft in de verspreiding van de infectieziekte, waardoor effectief en gericht gestuurd kan worden op infectieziektebestrijding. Zoals eventuele verheffingen of lokale risico's die gesignaleerd kunnen worden en zo mogelijk extra maatregelen implementeren of juist afschalen van maatregelen. Het op een snelle, digitale wijze beoordelen van contactmomenten tussen de index en het contact en het vervolgens kunnen verstrekken van een handelingsperspectief, waardoor het contact weet of en welke eventuele maatregelen hij zelf moet nemen, zorgt voor beperking van de verspreiding van de infectieziekte. Uiteraard komt dit ten goede van de volksgezondheid, met de daarbij horende effecten voor een draaiende economie.

Contactpersonen index

Door de aanlevering van gegevens uit GGD Contact kan een contact van de index snel op de hoogte worden gebracht dat hij in contact is geweest met een persoon die positief is getest. Door het snel bieden van een handelingsperspectief aan de contactpersonen hetzij door de index, hetzij door de BCO-medewerker, weet het contact waar hij aan toe is en welke maatregelen hij wel of niet moet gaan nemen ter bescherming van zichzelf en anderen in zijn omgeving.

Ministerie van VWS

Op basis van diverse internationale regels heeft een ieder het recht op bescherming van de gezondheid.[19] Dit recht brengt met zich mee – en is expliciet in het internationaal recht opgenomen – dat de staat de verplichting heeft om maatregelen te nemen om dit recht te verwezenlijken. In

[19] Artikel 11 Europees Sociaal Handvest, artikel 12 lid 1 Internationaal Verdrag inzake economische, sociale en culturele rechten (IVESCR), maar ook lid 2 van artikelen 8, 9, 10 en 11 Europees Verdrag tot bescherming van de Rechten van de Mens en fundamentele vrijheden (EVRM) die de basis vormen voor het recht op bescherming van de gezondheid.

het geval van bestrijding van een infectieziekte zoals COVID-19 rust op de staat de plicht om maatregelen te nemen ter voorkoming, behandeling en bestrijding ervan.[20]

In Nederland heeft deze wettelijke verplichting uitwerking gevonden in de Wet publieke gezondheid. Daarin is onder andere bepaald dat het ministerie van VWS, vertegenwoordigd door de minister, verantwoordelijk is voor onder andere het coördineren van de bestrijding van epidemieën van infectieziekten behorend tot groep A (zoals COVID-19) en het toepassen van maatregelen kan opdragen.[21] Het ministerie (en de minister) heeft derhalve belang bij het op een zorgvuldige en efficiënte manier uitvoeren van BCO nu het bijdraagt aan het beperken van de verspreiding van een infectieziekte. De minister van VWS heeft opdracht gegeven tot de vervanging van HP Zone, waarvoor de DPG-raad GGD Contact en het bijbehorende webportaal heeft aangewezen.

Contactpersonen index
Door de aanlevering van gegevens uit GGD Contact kan een contact van de index snel op de hoogte worden gebracht dat hij in contact is geweest met een persoon die positief is getest. Door het snel bieden van een handelingsperspectief aan de contactpersonen hetzij door de index, hetzij door de BCO-medewerker, weet het contact waar hij aan toe is en welke maatregelen hij wel of niet moet gaan nemen ter bescherming van zichzelf en anderen in zijn omgeving.

GGD
Ten behoeve van infectieziektebestrijding hebben GGD'en op basis van Wpg de taak gekregen om BCO uit te voeren.[22] Het belang van de GGD bij het inzetten van GGD Contact het op een snelle wijze verkrijgen van de gegevens voor BCO waardoor efficiënter kan worden gewerkt. Dit bespaart de BCO-medewerkers tijd en vermindert de kans op fouten nu voor BCO relevante gegevens niet telefonisch hoeven te worden doorgegeven en vervolgens genoteerd. Het snel kunnen starten van BCO (door middel van GGD Contact) draagt bij aan infectieziektebestrijding wat weer een taak is van de GGD.[23]

GGD GHOR Nederland
GGD GHOR Nederland is de koepelorganisatie van de GGD'en en heeft op basis van de statuten onder andere het doel de publieke gezondheid, de fysieke en sociale veiligheid te bewaken, te beschermen en te bevorderen. Daarnaast heeft GGD GHOR Nederland het doel het inhoudelijk functioneren van de GGD'en te bevorderen, de belangen van de leden te behartigen en al hetgeen te doen dat "met één of ander rechtstreeks of zijdelings verband houdt of daartoe bevorderlijk kan zijn, alles in de ruimste zin des woords". [24] Met betrekking tot het BCO-proces draagt GGD GHORNederland bij aan het mede-coördineren van BCO op landelijke schaal met als hoger gelegen

[20] Artikel 12 lid 1 sub c IVESCR.
[21] Artikel 7 lid 1 Wpg.
[22] Artikel 6 lid 1 sub c Wpg.
[23] De uitvoering van algemene infectieziektebestrijding is wederom een taak van de GGD, artikel 6 lid 1 Wpg jo artikel 14 Wpg.
[24] Artikel 2 Statuten GGD GHOR Nederland.

doel tevens het ondersteunen van de infectieziektebestrijding door de GGD'en. Een goed functionerend BCO-proces is derhalve in het belang van GGD GHOR Nederland.

7. Verwerkingslocaties

Bij de verwerkingen die binnen de scope van deze DPIA vallen (verwerkingen binnen GGD Contact, de bijbehorende sluis en het BCO webportaal) worden buiten de Europese Unie of Europese Economische Ruimte geen persoonsgegevens verwerkt. Meer specifiek vinden de verwerkingen plaats in Nederland te Rotterdam nu GGD Contact, de sluis en het BCO webportaal wordt bij Intermax worden gehost.

8. Techniek en methode van gegevensverwerking

Toegang

- GGD Contact App

De toegang van de index tot de GGD Contact App komt tot stand door het te downloaden vanuit de Google Play appstore of Apples App Store.

- BCO-portaal

De toegang tot het BCO-portaal vindt plaats nadat een Gebruiker de autorisatie daartoe heeft vergekregen via de GGD waarvoor de Gebruiker werkzaam is. Het portaal is benaderbaar via een weblink. De autorisaties worden vergeven op basis van een autorisatiematrix. De autorisatiematrix is afgestemd met de product owners van de GGD'en.

Release 1.1:
Release 1.1 kent twee rolbeschrijvingen:
- Werkverdeler
- BCO-medewerker

Geen hoog-risico verwerkingen

Ten aanzien van de verwerkingen binnen GGD Contact wordt van geen van de onderstaande technieken gebruik gemaakt:

- Analyse van databestanden op persoonsniveau
- (Semi-)geautomatiseerde besluitvorming
- Profilering
- Big-dataverwerking

De vragen die gesteld worden voor het vaststellen van de risicoclassificatie van contacten zijn afkomstig van een aan de achterkant ingerichte beslisboom. Aan de hand van de antwoorden op de vragen wordt een risicocategorie getoond. Het bepalen van deze risicoclassificatie kan niet worden aangemerkt als een louter op geautomatiseerde verwerking gebaseerd besluit.[25] Door middel van een menselijk component, namelijk de BCO-medewerker die de antwoorden afkomstig uit de

[25] Overweging 91 AVG.

vragen gebaseerd op de beslisboom in het BCO webportaal binnenkrijgt, vindt er een extra controle plaats op de aangeleverde gegevens van de index. Het resultaat van de uitkomst van de risicoclassificatie betreft een bijpassend handelingsperspectief voor het contact van de index. Deze risicoclassificatie evenals het handelingsperspectief kan niet worden gezien als profilering ter beoordeling van de gezondheid omdat de enkele constatering van de index dat hij op een bepaalde wijze in contact is geweest met deze persoon niet hoeft te duiden op een beoordeling van de gezondheid van het contact. In het kader van de risicoclassificatie ten behoeve van BCO is het toewijzen van een categorie gebaseerd op een feitelijke handeling namelijk aan het soort contact dat er heeft plaatsgebonden, dit is niet gebaseerd op de gezondheid van de index noch van het contact.

In toekomstige versies van GGD Contact zou eventueel een beoordeling van de gezondheid van het contact kunnen plaatsvinden met als gevolg dat gezondheidsklachten worden geregistreerd. In dat geval zou sprake kunnen zijn van **profilering.** In de huidige versie van GGD Contact is dit echter niet aan de hand. Derhalve ziet deze DPIA niet toe op de toekomstige versies van GGD Contact.

In de huidige versie van GGD Contact is (nog) geen sprake van de big-dataverwerking en analyse van databestanden op persoonsniveau. Het is echter niet uit te sluiten dat dit in de latere versies wel kan plaatsvinden bijvoorbeeld voor wat betreft analyses door het RIVM. Derhalve ziet deze DPIA niet toe op de toekomstige versies van GGD Contact. In dat geval dient er een afzonderlijke risico-analyse plaats te vinden.

9. Juridisch en beleidsmatig kader

Voor de verwerkingen in GGD Contact is de volgende wet- en regelgeving van toepassing:

- Wet Publieke gezondheid (Wpg);
- Besluit publieke gezondheid;
- Algemene verordening Gegevensbescherming (AVG);
- Algemene wet bestuursrecht (Awb);
- Protocol bron- en contactonderzoek COVID-19
- Telecommunicatiewet (Tw)

Op grond van artikel 11.7a van de Telecommunicatiewet (hierna: Tw) is het via een elektronisch communicatienetwerk (zoals internet) plaatsen of uitlezen van informatie op een randapparaat, zoals een smartphone, ongeacht of er daarbij sprake is van persoonsgegevens, uitsluitend toegestaan op voorwaarde dat de gebruiker daarvoor toestemming heeft verleend, en is voorzien van duidelijke en volledige informatie.

Uit de Tw volgt dan ook, naast de plichten uit de AVG, een informatieplicht en een toestemmingsvereiste voor het opslaan van de GGD Contact-app op een smartphone. De betreffende informatieplicht en het toestemmingsvereiste gelden ongeacht of sprake is van de verwerking van persoonsgegevens.

Kortom: Uit artikel 11.7a Tw volgt informatieplicht en een toestemmingsvereiste voor het opslaan van de GGD Contact-app op een smartphone. De GGD Contact-app moet zodanig ingericht worden dat aan de voorgaande vereisten is voldaan.

Zo moet bij de installatie of het eerste gebruik van de GGD Contact-app op de smartphone van de gebruiker, de gebruiker worden geïnformeerd over het plaatsen van de app op de telefoon en het uitlezen van de betreffende gegevens daaruit, en moet daarvoor toestemming worden verkregen.

Dat deze toestemming in vrijheid kan worden gegeven volgt uit het feit dat personen die de GGD Contact-app niet gebruiken steeds terecht kunnen bij de GGD'en voor de reguliere (telefonische) bron- en contactopsporing.

10. Bewaartermijn

Ten aanzien van de bewaartermijn van de persoonsgegevens binnen GGD Contact, dient onderscheid te worden gemaakt tussen de gegevens die in de applicatie, de sluis en het BCO webportaal worden opgeslagen.

<u>Bewaartermijn applicatie GGD Contact</u>

In GGD Contact blijven de gegevens bewaard totdat de index ervoor kiest om de gegevens te wissen of de applicatie in zijn geheel te verwijderen. De omgang met de persoonsgegevens in de applicatie valt volledig onder de verantwoordelijkheid van de index. Hoewel de applicatie als persoonlijk gebruik kan worden gezien waardoor op de index de AVG niet van toepassing is, maakt de context waarin de applicatie is gedownload de verwerkingsverantwoordelijke verantwoordelijk om by design wel een houdbaarheidstermijn voor de gegevens in te regelen.

Dit wordt op de volgende manieren ingevuld:

- De gegevens worden automatisch gewist 14 dagen nadat gegevens voor het laatst zijn aangepast door de index of verzonden naar het BCO webportaal voor BCO-onderzoek.
- de index die gebruik maakt van de app wordt hier via de privacyverklaring op geattendeerd.

<u>Bewaartermijn datasluis</u>

De persoonsgegevens die encrypted in de sluis zijn opgeslagen worden bewaard tot het moment dat deze aan het portal worden doorgegeven. Dit betekent dat de gegevens hierin maximaal 2 dagen (48 uur) worden opgeslagen. Dit staat gelijk aan de periode waarbinnen de window om de contacten in te voeren, beschikbaar is.

<u>Bewaartermijn BCO webportaal</u>

De gegevens binnen het BCO webportaal zijn relevant zolang de index geïnfecteerd is. Uitgangspunt is dat HPzone Lite het bronbestand is. GGD Contact kent een tijdelijke opslag om het

dossier af te handelen voordat het naar HP Zone (handmatig) gekopieerd wordt. Persoonsgegevens moeten zo snel mogelijk worden verwijderd uit BCO-portaal.

De bewaartermijn is uitgewerkt is verschillende scenario's, nu de relevantie per case kan verschillen:

Scenario 1: Bewaartermijn open cases

1. BCO-er (landelijk of regionaal) krijgt case(nummer) toegewezen via bestaande route
2. BCO-er zoekt case op in HPZone
3. BCO-er maakt case aan in portaal (start dossier = T0)
    a. BCO-er doet BCO
    b. BCO-er vult vragenlijst in
    c. BCO-er geeft koppelcode door (window koppelen van 2 dagen)
4. Index geeft informatie door via GGD Contact app
5. BCO-er kopieert output BCO naar HPZone.
6. BCO-er sluit dossier af (dossier komt in lijst cases waarvan BCO is afgerond)
7. Dossier wordt na T+7dagen na start verwijderd

Scenario 2: BCO wordt niet afgerond

1. Trigger: BCO is niet afgerond aan het einde van de dag.
2. Cases waar einde dag / begin volgende dag bco-status niet op "afgerond" is gezet komen in werkvoorraad van werkverdeler.
3. De werkverdeler kent een case toe aan BCO-er
4. Terug naar scenario 1, stap 4.

Scenario 3: Index levert aanvullende informatie via app

1. Trigger: Index stuurt aanvullende informatie (na 1e verzending).
2. Index stuurt aanvullende informatie door via GGD Contact app (dossier wordt eenmalig verlengd met 5 dagen)
3. Dossier komt in werkvoorraad van werkverdeler als "Actief - nieuwe gegevens".
4. De werkverdeler kent een case toe aan BCO-er
5. Terug naar scenario 1, stap 4.

Met het overzetten van de gegevens uit het BCO webportaal naar de systemen van de GGD betekent niet dat de gegevens direct uit het BCO webportaal worden verwijderd. Deze blijven conform de hierboven beschreven scenario's bewaard. Wanneer de persoonsgegevens na het verstrijken van deze termijn worden verwijderd, kan de betrokkene geen beroep meer uitoefenen op zijn rechten. Dit is echter geen beperking van de rechten van de betrokkene aangezien het

verwijderen in lijn is met het beginsel van dataminimalisatie[26] en de betrokkene door middel van de privacyverklaring geïnformeerd is over deze bewaartermijnen.

De GGD Contact App en het BCO-portaal zij technisch zo ingeregeld dat deze de gegevens automatisch verwijderen na het verlopen van de hier beschreven bewaartermijnen.

[26] Artikel 5 AVG.

B. Beoordeling rechtmatigheid gegevensverwerkingen

11. Rechtsgrond

Verwerking van persoonsgegevens

Voor de toelichting van de rechtsgrond voor de gegevensverwerkingen binnen GGD Contact wordt niet op alle infectieziekten ingegaan maar slechts op COVID-19 en de daarvoor relevante wetsbepalingen.

De bestrijding van een infectieziekte zoals COVID-19 betreft de bestrijding van een infectie die behoort tot groep A[27] waarvoor de veiligheidsregio's verantwoordelijk zijn.[28] De uitvoering van BCO is vervolgens een wettelijke taak van de GGD'en.[29] De wettelijke taak om BCO uit te voeren betreft **niet d**e wettelijke plicht om persoonsgegevens te verwerken. Bij wet- regelgeving is immers niet bepaald hoe het BCO-proces dient te worden uitgevoerd en welke gegevensverwerking hiervoor nodig is.

Van de wettelijke mogelijkheid[30] om de concrete uitvoering van het BCO-proces bij algemene maatregel van bestuur (amvb) nader uit te werken, is geen gebruik gemaakt. Regeling publieke gezondheid regelt er immers niets over en de Nota van toelichting bij het Besluit publieke gezondheid zegt ten aanzien van BCO[31] dat deze "kerntaak" al in de Wpg is opgenomen. Met andere woorden: verdere uitwerking bij amvb is niet nodig omdat de taak stevig genoeg en voldoende duidelijk is geformuleerd. Dit betekent dat het BCO een belangrijke en een verplichte taak is voor de GGD'en.

Om BCO- taak uit te voeren zijn persoonsgegevens nodig. De gegevens die verwerkt worden zijn "noodzakelijk voor de vervulling van een taak van algemeen belang " zoals bedoeld bij artikel 6 lid 1 sub e AVG, en in dit geval voor BCO. De nadere uitwerking van het BCO-proces is gedaan in het BCO-protocol[32] waarin het doel van BCO duidelijk is gesteld. Deze betreft 1) contacten identificeren, 2) hen te informeren over de blootstelling en risico op besmetting, 3) hen te wijzen op maatregelen die genomen moeten worden om verdere verspreiding te voorkomen en 4) hen hierin te begeleiden. Hieruit kan geconcludeerd worden dat het BCO-proces ziet op het opvragen van gegevens van de contacten van de positief geteste persoon. Dit opvragen van persoonsgegevens door de GGD is geen wettelijke plicht, maar is noodzakelijk voor het vervullen van een taak van algemeen belang of een taak in het kader van de uitoefening van het openbaar

[27] Artikel 1 Regeling 2019-nCoV. Meldingsplichtige ziekten zijn verdeeld over de groepen A, B1, B2 en C. Deze indeling is gebaseerd op de mate waarin dwingende matregelen opgelegd kun worden om de bevolking te bescherming. Bij groep A zijn mogelijke wettelijke maatregelen: gedwongen opname tot isolatie of thuisisolatie, gedwongen onderzoek, gedwongen quarantaine (inclusief medisch toezicht), verbod van beroepsuitoefening. Zie: https://www.rivm.nl/meldingsplicht-infectieziekten/welke-infectieziekten-zijn-meldingsplichtig voor een recent overzicht van ziekten die onder groep A vallen.
[28] Artikel 6 lid 2 Wpg.
[29] Artikel 6 lid 1 sub c Wpg jo artikel 13 Wpg.
[30] Art 6 lid 5 Wpg: Bij algemene maatregel van bestuur kunnen de taken, bedoeld in het eerste, tweede, derde en vierde lid, nader worden uitgewerkt.
[31] Artikel 11 Nota van toelichting bij Besluit publieke gezondheid.
[32] https://lci.rivm.nl/COVID-19-BCO

gezag.[33] De verwerking van deze contactgegevens is namelijk nodig om de taak van BCO uit te voeren. Hiervoor is het noodzakelijk dat dit bij lidstatelijk recht geregeld is. In het geval van BCO is dit geregeld in artikel 6 lid 1 sub c Wpg.

HP Zone Lite waarin de verwerkingen in het kader van BCO plaatsvinden betreft geen medisch dossier als bedoeld bij Wgbo.[34] Er is tussen de index en de BCO-medewerker geen sprake van geneeskundige behandelingsovereenkomst als gevolg van "het verrichten van handelingen op het gebied van de geneeskunst, rechtstreeks betrekking hebbende op de persoon"[35] Er is slechts sprake van het opvragen van contacten van de positief geteste persoon ten behoeve van de uitvoering van BCO in het kader van infectieziekteziektebestrijding als zijnde een taak van publieke gezondheid. De geneeskundige behandeling ziet daarentegen op het genezen van het individu. Derhalve speelt Wgbo in het BCO-proces geen rol

Verwerking van bijzondere persoonsgegevens

De opname van de persoonsgegevens in GGD Contact zegt iets over de gezondheid van de index (index is besmet) en over het ziekterisico dat zijn contacten lopen. Daarnaast is het ook mogelijk voor de index om in de GGD Contact-app zijn klachten te registreren aan de hand waarvan de eerste ziektedag wordt bepaald. De context waarin de persoonsgegevens worden verwerkt en het invullen van de klachten in de app maakt dat er sprake is van verwerking van gegevens over de gezondheid en dus bijzondere persoonsgegevens.

In beginsel geldt er een verbod op het verwerken van bijzondere persoonsgegevens in de AVG. Het verbod op het verwerken van bijzondere persoonsgegevens kan worden doorbroken wanneer de verwerking onder andere "noodzakelijk is om redenen van algemeen belang op het gebied van de volksgezondheid, op grond van Unierecht of lidstatelijk recht waarin passende en specifieke maatregelen zijn opgenomen ter bescherming van de rechten en vrijheden van de betrokkene, met name van het beroepsgeheim."[36]

De uitzondering om bijzondere persoonsgegevens te mogen verwerken om redenen van algemeen belang op het gebied van de volksgezondheid kan zijn gelegen in sectorspecifieke wetgeving of in de Uitvoeringswet Algemene Verordening Gegevensbescherming (UAVG). De UAVG heeft artikel 9 lid 2 sub i AVG bewust niet verder uitgewerkt.[37] Wanneer er geen speciale wetgeving van toepassing is, moet een beroep worden gedaan op de lex generalis; de UAVG. De bestrijding van een infectieziekte zoals COVID-19, waarvoor BCO moet worden uitgevoerd, kan worden gezien als een verwerking die noodzakelijk is om redenen van algemeen belang op het gebied van de volksgezondheid. In Nederland is de bestrijding van infectieziekten in de nationale wetgeving

[33] Artikel 6 lid 1 sub e AVG.
[34] Artikel 7:454 Burgerlijk Wetboek (Wgbo)
[35] Artikel 7:446 lid 1 Burgerlijk Wetboek (Wgbo)
[36] Artikel 9 lid 2 sub i AVG: De verwerking is noodzakelijk om redenen van algemeen belang op het gebied van de volksgezondheid, zoals bescherming tegen ernstige grensoverschrijdende gevaren voor de gezondheid of het waarborgen van hoge normen inzake kwaliteit en veiligheid van de gezondheidszorg en van geneesmiddelen of medische hulpmiddelen.
[37] Kamerstukken II 2017/18, 34 851, nr. 3, p. 43 (MvT bij UAVG).

geregeld, te weten de Wpg (lex specialis). Omdat de UAVG een lex generalis betreft en Wpg een lex specialis, gaat lex specialis in de Nederlandse gelaagde rechtstructuur voor. Dit betekent dat het verbod op verwerking van bijzondere persoonsgegevens in het kader van BCO kan worden doorbroken met een beroep op artikel 9 lid 2 sub i AVG jo artikel 6 lid 1 sub c Wpg.

Passende en specifieke maatregelen (artikel 9 lid 2 sub i)
Om een beroep op artikel 9 lid 2 sub i AVG te kunnen doen, is het noodzakelijk dat bij lidstatelijk recht voor passende en specifieke maatregelen is gezorgd voor de desbetreffende verwerking.

In de Algemene wet bestuursrecht (Awb), de basiswet voor alle openbare lichamen en bestuursorganen, en de Ambtenarenwet 2017 waarin verplichtingen van ambtenaren geregeld staan. In het kader van infectieziektebestrijding - waaronder BCO, draagt het College van B&W zorg voor de uitvoering hiervan. Het College van B&W is in de rol van bestuursorgaan onderworpen aan o.a. de Awb. Hierin is geregeld dat: voor een ieder die betrokken is bij de uitvoering van de taak van een bestuursorgaan en daarbij de beschikking krijgt over gegevens met vertrouwelijk karakter, geldt een geheimhoudingsplicht. Deze plicht geldt ook voor degene die niet uit hoofde van ambt of beroep of wettelijk voorschrift aan geheimhouding zijn verbonden.[38]
Instellingen of daartoe behorende of daarvoor werkzame personen die door een bestuursorgaan worden betrokken bij de uitvoering van zijn taak én instellingen (incl. werkzame personen) die bij wet een taak hebben toegekend gekregen, zijn ook onderworpen aan deze geheimhoudingsplicht.[39] Hierdoor kan worden aangenomen dat de wettelijke geheimhoudingsplicht uit art. 2:5 Awb van toepassing is op eenieder die betrokken is bij de uitvoering van een overheidstaak. [40]

Taken van het College van B&W worden uitgevoerd door GGD'en.[41] die onderdeel gaan uitmaken van het door een gemeenschappelijke regeling opgericht openbaar lichaam.[42] De GGD'en zelf kunnen worden aangemerkt als een a-orgaan.[43] Indien er sprake is van een arbeidsovereenkomst bij een overheidswerkgever, zoals in bovengenoemd geval van toepassing is, is er sprake van een ambtenaar waarop de Ambtenarenwet 2017 van toepassing is.[44]

Ambtenaren leggen de eed af of doen de belofte[45] waardoor ambtenaren verplicht zijn tot geheimhouding van hetgeen hen in verband met hun functie ter kennis is gekomen.[46] Medewerkers van de GGD zijn ambtenaren die werkzaam zijn op basis van een arbeidsovereenkomst en omdat zij betrokken zijn bij de uitvoering van de GGD-taken, zijn zij gebonden aan de geheimhoudingsplicht uit artikelen 9 Ambtenarenwet 2017 én 2:5 Awb. Tevens geldt de

[38] Artikel 2:5 lid 1 Awb.
[39] Artikel 2:5 lid 2 Awb.
[40] Zie Toelichting Besluit Ambtenarenwet 2017
[41] Artikel 14 lid 1 en 2 Wpg.
[42] Zie toelichting bij artikel 2 Uitvoeringsbesluit Ambtenarenwet 2017.
[43] A-orgaan = een orgaan van een rechtspersoon die krachtens publieksrecht is ingesteld (art 1:2 lid 1 sub a Awb)
[44] Artikel 1 Ambtenarenwet 2017.
[45] Artikel 7 Ambtenarenwet 2017.
[46] Artikel 9 Ambtenarenwet 2017

contractuele geheimhouding die bij indiensttreding van de niet-artsen wordt afgesloten. Op deze manier is geheimhouding gewaarborgd.

Tot slot, daar waar de AVG verwijst naar Unierecht of lidstatelijk recht wordt hier niet noodzakelijkerwijs vereist dat er een door een parlement vastgestelde wetgevingshandeling nodig is.[47] Met andere woorden hoeft het lidstatelijk recht geen 'wet in formele zin' te betreffen. Vereist is dat een dergelijke maatregel duidelijk en nauwkeurig is en de rechtsgevolgen voor de betrokkenen voorspelbaar zijn.[48] Een maatregel die hieraan voldoet betreft het eerder genoemde BCO-protocol. Dit protocol vloeit voort uit lidstatelijk recht, is duidelijk en nauwkeurig opgesteld en wordt door de GGD'en gevolgd. In dit BCO-protocol zijn voldoende passende en specifieke maatregelen opgenomen ter bescherming van de rechten en vrijheden van betrokkenen. Bijvoorbeeld de expliciete aandacht voor verwerking van gegevens van kinderen en/of met een kinderopvang welke is opgenomen in het protocol.

Concluderend met betrekking tot de grondslag kan worden geoordeeld dat de GGD (bijzondere) persoonsgegevens mag verwerken voor BCO op basis van artikel 6 lid 1 sub e jo. 9 lid 2 sub i AVG.

12. Doelbinding

De verwerkingen die binnen GGD Contact, de datasluis en het BCO webportaal plaatsvinden, zijn bedoeld om het BCO-proces ten behoeve van infectieziektebestrijding, efficiënter en sneller te laten verlopen.

De persoonsgegevens worden daarnaast verwerkt ter analyse van GGD Contact en in hoeverre dit bijdraagt aan het doel van infectieziektebestrijding.

13. Noodzaak en evenredigheid

Bij het ontwikkelen van de GGD Contact is rekening gehouden met de beginselen proportionaliteit ('Staat het doel in verhouding tot de inbreuk?') en subsidiariteit ('Is dit de beste/minst ingrijpende manier om het doel te bereiken?').

Proportionaliteit: GGD Contact is opgebouwd om het BCO-proces te ondersteunen, te versnellen en het registreren van de gegevens van de contacten zorgvuldiger te laten verlopen. Daarnaast voldoet het huidige systeem dat gebruikt wordt voor de registratie van deze gegevens niet aan de vereiste gegevensbeschermende waarborgen. Dit is een van de reden om een alternatieve voorziening voor te bereid. Release 1.1. biedt op korte termijn de door de product owners gewenste functionaliteit en is daarnaast de voorbereidende release op de vervanging van HPZone Lite.

[47] Overweging 41 AVG.
[48] EHRM 26 april 1979, *NJ* 1980/146 (Sunday Times)

De BCO-medewerker kan, indien nodig, sneller contact opnemen met contacten van de index. Per stap is duidelijk vastgesteld welke persoonsgegevens gevraagd en geregistreerd worden. Per persoonsgegeven dat wordt gevraagd en verwerkt in GGD Contact is nagegaan of het vragen van het betreffende gegeven een evenredige verwerking oplevert voor het doel dat wordt nagestreefd. Oftewel de inbreuk die wordt gemaakt, wordt afgewogen ten opzichte van het beoogde doel. Voor de gehele verwerking voor BCO in GGD Contact is aan de hand van het doel nagegaan of de gegevensverwerking noodzakelijk is ten behoeve van BCO. De gegevens die gevraagd worden in GGD Contact zijn noodzakelijk om het BCO uit te kunnen voeren. Om de proportionaliteit aan te kunnen tonen, zal er een evaluatie moeten plaatsvinden van GGD Contact, waaruit dit zal moeten blijken. Op dit moment is ervoor gekozen om de evaluatie (en analyse in deze DPIA van de gegevens die ten behoeve van die verwerking benodigd zijn) niet in Release 1.1. mee te nemen vanwege de benodigde doorgifte van gegevens daarvoor en de te realiseren koppeling om dit mogelijk te maken.

Subsidiariteit: GGD Contact is ontwikkeld, omdat na marktconsultatie is gebleken dat er momenteel geen (digitale) oplossingen zijn om het BCO-proces te ondersteunen en te versnellen. Andere webapplicaties of apps ter ondersteuning van het BCO zijn door de ontwikkeling van GGD Contact overbodig gemaakt, waardoor een wildgroei aan lokale oplossingen wordt vermeden.

Het minder ingrijpende alternatief is het analoge BCO. Het analoge BCO kan echter enkel in die gevallen versneld uitgevoerd worden als extra grote groep BCO-medewerkers tegelijkertijd uitvraag doen. Hiermee zou de werkdruk voor de BCO-medewerker verlicht kunnen worden. Het is hierbij echter wel de vraag hoeveel extra fte hiervoor dient te worden ingezet om dit effect van verlichting op de werkdruk te bereiken. Een volgend alternatief zou nog kunnen zijn dat de index zelf al zijn contacten gaat informeren buiten het BCO-proces om, dus zonder inmenging van de BCO-medewerker. Het nadeel hiervan is dat registratie ontbreekt en de index foutieve informatie (bijvoorbeeld over de te nemen maatregelen) aan zijn contacten verstrekt. Dit kan negatieve gevolgen hebben voor infectieziektebestrijding wanneer contacten bijvoorbeeld doorkrijgen van de index dat zij niet in thuisisolatie hoeven, terwijl dit wel gewenst is.

De voorgesproken alternatieven dragen niet bij aan een goede BCO aangezien de beoogde winst gericht is op de kwaliteit van de informatie. Dat is moeilijk te realiseren door de inzet van meer personen door de GGD of wanneer de betrokkene zelf contacten gaat informeren.

De ondersteuning van het BCO door GGD Contact is een extra verwerking in het BCO-proces ten aanzien van het reguliere BCO-proces, namelijk door toevoeging van een digitaal component, GGD Contact en het BCO webportaal. Het ophalen van het gehele adresboek in GGD Contact resulteert daarbij in een verwerking die buiten de grenzen van BCO gaat. Bij BCO gaat het immers om de contactgegevens van de personen waarmee de index in contact is geweest en niet zijn gehele telefoonboek. Bij het geven van toestemming om het gehele adresboek weer te geven in de GGD Contact App worden dus ook contacten zichtbaar waarmee de index tijdens zijn besmettelijke

periode niet in contact is geweest. Dit is dientengevolge een risico waar passende maatregelen op dienen te worden genomen. Door toepassing van privacy-by-design wordt hier rekening mee gehouden doordat enkel de namen uit het telefoonboek zichtbaar worden en overige informatie uit het adresboek achterwege blijft. Overigens worden deze opgehaalde gegevens niet naar de GGD gestuurd, maar blijven deze gegevens lokaal opgeslagen op de telefoon.

Wanneer de index kiest voor 'gegevens delen met de GGD' worden enkel die gegevens van zijn contacten gedeeld die daadwerkelijk in GGD Contact zijn ingevoerd bij een specifiek contact. Het is ook mogelijk om een alternatief te kiezen: het handmatig invoeren van contactgegevens. De voorkeur wordt gegeven aan het automatisch inlezen van het contact, omdat deze daardoor minder foutgevoelig is voor overtyp-fouten. In de flow van het BCO-proces worden de ingeladen gegevens van het contact vervolgens ook nog nagelopen in het BCO-proces, wat een aanvullende waarborg is ten aanzien van de juistheid van de informatie.

Daarnaast wordt het recht op bescherming van persoonsgegevens geëerbiedigd tijdens de verwerkingen die gedaan worden in de Applicatie. Er worden passende en specifieke (technische) maatregelen getroffen ter bescherming van de grondrechten en fundamentele belangen van de betrokkene. De maatregelen die zijn of zullen worden getroffen, zijn opgenomen in onderdeel D.

14. Rechten van betrokkenen

De invulling van rechten van betrokkenen kan GGD specifiek zijn. Voor de meest actuele wijze waarop rechten van betrokkenen uitgevoerd kunnen worden, kan de GGD aanvulling geven op onderstaande werkwijze.

Doordat in GGD Contact persoonsgegevens worden verwerkt, komen de betrokkenen een aantal rechten toe, zoals bepaald in hoofdstuk III van de AVG.

De index kan zijn rechten geldend maken ten aanzien van de gegevens die worden verwerkt in het BCO webportaal. Ten aanzien van de gegevensverwerkingen in GGD Contact geldt dat de index de gegevens zelf kan verwijderen. De index kan zijn rechten tevens geldend maken wat betreft de verwerkingen in het BCO webportaal. De contacten van de index die ingevoerd zijn door de index kunnen hun rechten via de desbetreffende GGD'en geldend maken. Voor de gegevensverwerkingen is een privacyverklaring in de maak. De privacyverklaring is voor deze DPIA daarom niet beoordeeld. Het is in ieder geval de bedoeling dat de uitoefening van de onderstaande rechten, de wijze van uitoefening en bij wie deze rechten kunnen worden uitgevoerd, in de privacyverklaring worden toegelicht. Per GGD kan dan overeenkomstig eigen procedures omtrent de uitoefening van de rechten van betrokkenen, uitvoering geven aan de onderstaande rechten.

Recht op informatie (art. 13 AVG)

De betrokkene heeft het recht om informatie te ontvangen over de verwerking van zijn persoonsgegevens. Om deze informatie te verstrekken, wordt in GGD Contact toelichting gegeven bij de diverse velden. Tevens wordt er een privacyverklaring gedeeld bij het downloaden van GGD Contact. Daarnaast wordt er een privacyverklaring over de verwerking van gegevens in GGD

Contact op de website van GGD GHOR Nederland gepubliceerd, waarnaar via de website van de GGD'en kan worden verwezen.

Recht op inzage en afschrift (art. 15 AVG)
De betrokkene heeft het recht om zijn persoonsgegevens in te zien. De gegevens kunnen worden opgevraagd bij de betreffende GGD waar de gegevens van de index en/of het contact worden verwerkt die ook een afschrift van die gegevens kan verstrekken.

Recht op rectificatie (art. 16 AVG)
De betrokkene heeft het recht om gegevens die niet (langer) juist zijn, te laten rectificeren. Een aanvraag daartoe kan de betrokkene indienen bij de desbetreffende GGD waar de gegevens worden verwerkt. Het is in GGD Contact niet meer mogelijk om de gegevens aan te passen nadat deze naar het BCO webportaal (naar de GGD) zijn verstuurd. Wanneer de gegevens wel naar de GGD zijn gestuurd, kan hij dan wel een nieuw contact aanmaken in GGD Contact (dus opnieuw hetzelfde contact invoeren) zodat deze juiste gegevens worden verstuurd naar de GGD. Ofwel de index kan telefonisch contact opnemen met de GGD zodat de BCO-medewerker handmatig de wijziging door te voeren.

Recht op gegevenswissing (art. 17 AVG)
De betrokkene kan de GGD verzoeken persoonsgegevens te wissen. Gezien de situatie, waarbij persoonsgegevens worden verwerkt, namelijk in het kader van algemeen belang op het gebied van de volksgezondheid, kan de verwijdering enkel plaatsvinden als het gaat om de verwijdering van optionele gegevens, om gegevens die niet meer noodzakelijk zijn voor BCO of als de bewaartermijn is verstreken. Hierbij wordt aangesloten op het hiervoor opgestelde beleid door GGD GHOR waarin de gegevens die in aanmerking komen voor gegevenswissing nader zijn uitgewerkt.

Per concreet geval dient door de GGD te worden beoordeeld of de gegevens niet meer noodzakelijk zijn voor het doel waarvoor ze zijn verzameld (i.c. identificeren, informeren en adviseren van contacten ik het kader van BCO). In het BCO webportaal worden de gegevens automatisch gewist afhankelijk van het toepasselijke scenario.

Recht op beperking van de verwerking (art. 18 AVG)
De betrokkene kan in de door de wet bepaalde gevallen de GGD verzoeken om de verwerking van zijn gegevens te beperken. Dit is voornamelijk het geval indien:

- De gegevens mogelijk onjuist zijn. Een voorbeeld hiervan betreft het doorgeven van contactgegevens van een contact door de index, maar waarvan later blijkt dat het contactmoment buiten de besmettingsperiode is geweest. De index kan bij de voor hem van toepassing zijnde GGD informeren hoe zijn gegevensverwerking beperkt kan worden. Dit kan per GGD verschillen, het is advies om hiervoor op de website van de desbetreffende GGD te kijken.
- De gegevens zijn niet meer nodig. Dit dient beoordeeld te worden door de GGD van geval tot geval.

- Er is bezwaar gemaakt tegen de gegevensverwerking. De wijze van bezwaar maken kan per GGD verschillen, geadviseerd wordt om de informatievoorziening van de desbetreffende GGD hiervoor te raadplegen.

Recht op overdraagbaarheid van de gegevens (art. 20 AVG)
De betrokkene kan bij de GGD waar hij getest is verzoeken om zijn gegevens over te dragen naar bijvoorbeeld een andere GGD in een gangbare vorm. Ondanks dat dit recht niet van rechtswege van toepassing is (aangezien toestemming of overe enkomst niet de grondslag is van de verwerking) zal de GGD dit direct kan doorsturen naar de gewenste ontvanger, en zal dit worden verzorgd. Indien dit niet mogelijk is, zal de GGD de gegevens in een technisch gangbaar formaat aan de betrokkene overhandigen.

Indien betrokkene een verzoek op het recht van overdraagbaarheid van de gegevens wil uitvoeren, kan hiervoor de informatievoorziening van de GGD worden geraadpleegd. De wijze van verstrekking kan per GGD verschillen.

Recht van bezwaar (art. 21 AVG)
De betrokkene heeft het recht om in de wet bepaalde gevallen bezwaar te maken tegen de verwerking van persoonsgegevens, wanneer de individuele omstandigheden van het geval dit rechtvaardigen. Het bezwaar kan worden ingediend bij de GGD waar de betrokkene is getest. De GGD zal het verzoek vervolgen in behandeling nemen.

Recht om niet te worden onderworpen aan geautomatiseerde individuele besluitvorming (art. 22 AVG)
Er is geen sprake van geautomatiseerde besluitvorming overeenkomstig art. 22 AVG binnen de verwerkingen van GGD Contact ten behoeve van het BCO-proces. Zie hiervoor de toelichting bij paragraaf 8 ‘Techniek en methode van gegevensverwerking’.

C. Beschrijving en beoordeling risico's voor de betrokkenen

15. Risico's

Uit bovenstaande analyse van de voorgestelde verwerking van persoonsgegevens zijn enkele risico's gedestilleerd. Hieronder is per risico kort uiteengezet wat het risico voor betrokkenen is en hoe dit risico gekwalificeerd dient te worden. Hierbij wordt uitgegaan van een intrinsiek risicobegrip. Dit houdt in dat de kans en impact van het risico wordt beoordeeld zonder daarbij reeds genomen maatregelen in mee te nemen. De schaal waarmee gewerkt wordt, betreft: "Laag" (L), "middel(hoog)" (M), "hoog" (H). In **Bijlage 3** is een uitgebreide omschrijving opgenomen van de berekening en de definities van kans, impact en risiconiveaus. Hieronder is aangegeven hoe de uiteindelijke risicocalculatie plaatsvindt.

Risicocalculatie

De kans en impact wordt gebruikt om het niveau van het risico te bepalen, op basis van de beschreven aspecten:

- De kans (K) dat een risico effectueert; en
- De impact (I) op de organisatie of de Betrokkene als het risico is geëffectueerd.

Het risiconiveau wordt toegekend door een vooraf vastgestelde matrix die het belang van mitigerende maatregelen aangeeft. De combinaties van kans en impact zijn gegroepeerd in hoog (H, rood), midden (M, geel) en laag (L, groen). De matrix toont hoe de risico's zijn geclassificeerd gebaseerd op de impact en kans.

Kans → / Impact ↓	Laag	Middel	Hoog
Laag	Laag	Laag	Middel
Midden	Laag	Middel	Hoog
Hoog	Middel	Hoog	Hoog

Op basis van de risiconiveaus uit de matrix staat in de tabel hieronder beschreven welke maatregelen verwacht worden.

Risico Niveau	Risico Beschrijving en te verwachten maatregel
Hoog	Als een waarneming of bevinding wordt geëvalueerd als een hoog risico, is er sterke behoefte aan corrigerende maatregelen. Een bestaand systeem kan blijven werken, maar een beveiligingsplan of

	andere risico-beperkende maatregel moet zo snel mogelijk worden geïmplementeerd.
Midden	Als een waarneming wordt beoordeeld als gemiddeld risico, moeten eventuele corrigerende maatregelen worden overwogen.
Laag	Als een waarneming wordt beschreven als een laag risico, kunnen corrigerende maatregelen nog steeds nodig zijn of kan het risico worden geaccepteerd.

***Aanvulling lokale GGD**:*

Per risico is beoordeeld of de beschreven maatregelen door de lokale GGD of door de GGD GHOR en/of VWS genomen moeten worden. De maatregelen die door de lokale GGD opgepakt worden/zijn, zijn hieronder vet gedrukt.

1. Misbruik van de identificatiecode

Er zijn twee verschillende risico's met betrekking tot misbruik van de identificatiecode.

a) Misbruik doordat de index de code onbeschermd noteert en deze wordt gezien/opgevangen door een kwaadwillende. Deze kwaadwillende kan de code vervolgens zelf gebruiken en daarmee mogelijk toegang krijgen tot – door de BCO-medewerker op basis van het telefoongesprek klaargezette – contactgegevens.
   - De kans dat dit risico zich manifesteert zonder maatregelen is laag. De betrokkene krijgt telefonisch de code en zal deze hoogstwaarschijnlijk direct na of nog tijdens het telefoongesprek met de BCO-medewerker invoeren. Daarnaast is de index positief getest en verblijft hij waarschijnlijk in thuisisolatie waardoor inzage op de overgeschreven code door kwaadwillende ook minder aannemelijk is.
   - De impact van dit risico zonder maatregelen is Hoog. Indien de identificatie van betrokkene wordt misbruikt kan dit leiden tot o.a. identiteitsfraude dan wel het aanleveren van mogelijk onjuiste gegevens door kwaadwillende waardoor foutief opgegeven contacten kunnen worden beperkt in hun vrijheden.

   Geadviseerd wordt om de volgende maatregelen te nemen:
   - Geldigheidsduur van de code kort in te stellen, maximaal 45 minuten;
   - **De index informeren over de geldigheidsduur van de code en – de wijze van – gebruik hiervan; actie GGD Hart voor Brabant: nagaan of dit verwerkt staat in de werkinstructies.**
   - De code voor eenmalig gebruik in te stellen;
   - Unieke code doorgeven
     - Door middel van een algoritme voor het genereren van een code;
     - Review op dit algoritme.

- Monitoring (SIEM/SOC) van verdacht gedrag (bijvoorbeeld benadering vanuit het buitenland) op gebruik identificatiecode.

Risico voor Betrokkene (voor maatregelen)	Middel
Risico voor Betrokkene (na maatregelen)	Laag

b) De Activatie- en casecode (zowel de code als de grote sleutel) is niet lang genoeg en vatbaar voor hacking. Dat heeft eveneens toegang door een kwaadwillende tot gevolg.

- De kans dat dit risico zich manifesteert zonder maatregelen is Middel. Door de gevoeligheid van de gegevens en de interesse van buitenaf in de gegevens, is het aannemelijk dat er hack-pogingen gedaan zullen gaan worden, namelijk door het 'raden'/ van de activatiecode of door het omzeilen van de activatiecode door het zoeken naar kwetsbaarheden in de beveiliging rondom de activatiecode. De hacker moet dan de bijbehorende activatiecode binnen de daarvoor gestelde 45 minuten 'raden/hacken' en tevens op de hoogte zijn wanneer de activatiecode wordt vrijgegeven/aangemaakt.
- De impact van dit risico zonder maatregelen is hoog. De kwaadwillende hacker kan de gegevens namelijk openbaar maken of misbruiken.

Geadviseerd wordt om de volgende maatregelen te nemen:

- Code review op de activatie- en casecode;
- Gebruik van een lange code, welke minder gemakkelijk te hacken is;
- Geldigheidsduur van de code kort instellen, maximaal 45 minuten;
- De code voor eenmalig gebruik instellen;
- Vermijden van eenvoudig verwisselbare karakters bij het telefonisch doorgeven van de sleutel (bijvoorbeeld "O" versus "0" (nul)).
- Monitoring (SIEM/SOC) van verdacht gedrag (bijvoorbeeld benadering vanuit het buitenland) op gebruik identificatiecode.
- Ghost responses: door gebruik te maken van ghost responses is het voor een hacker niet inzichtelijk of hij met een achterhaalde key daadwerkelijk succes heeft.

Risico voor Betrokkene (voor maatregelen)	Hoog
Risico voor Betrokkene (na maatregelen)	Laag

2. <u>Opslag in onvoldoende beveiligde systemen</u>

Opslag van (bijzondere) persoonsgegevens vindt plaats op onvoldoende beveiligde systemen (systemen die niet voldoen aan de IB-standaarden zoals NEN7510/BIO) binnen de procesketen met mogelijke inbreuken tot gevolg.

- De kans dat dit risico zich manifesteert zonder maatregelen is Middel. Betrouwbare en bekende partijen worden ingeschakeld om de opslag van de GGD Contact en de bijbehorende systemen te verzorgen op basis van eisen aan certificering, en ze worden bevraagd op inrichting van (passende) beveiligingsmaatregelen.
- De impact van dit risico zonder maatregelen is Hoog. Inbreuken waarbij toegang tot de gegevens in de systemen wordt bereikt, kan leiden tot kwaadwillenden die de gegevens openbaar maken of misbruiken.

Geadviseerd wordt om de volgende maatregelen te nemen:

- Leveranciers kiezen die aantoonbaar informatiebeveiliging op orde hebben. Borgen door middel van:
    - Vastlegging contractuele afspraken met leveranciers van de systemen omtrent voldoen aan informatiebeveiligingstandaarden zoals NEN7510/BIO.
    - Periodieke verantwoording door leverancier op nader overeen te komen KPI's op het vlak van informatiebeveiliging op basis van rapportages (bijvoorbeeld SLR, waarvan effectiviteit van beveiligingsmaatregelen onderdeel is)
    - Overleggen van SOC 2 type 2 assurancerapportage ten aanzien van de aspecten "Security, Availability, Processing Integrity, Confidentiality en Privacy"
    - In bezit van NEN7510/ISO 27001/BIO certificering.
- Certificaten en/of uitgever van het certificaat vastleggen in de applicatie.

Risico voor Betrokkene (voor maatregelen)	Hoog
Risico voor Betrokkene (na maatregelen)	Laag

3. <u>Verwerking van meer gegevens dan noodzakelijk</u>

GGD Contact krijgt toegang tot volledige contactenlijst van de index. Tevens kan de index in de open tekstvelden niet-noodzakelijke informatie/gegevens vrij invullen.

- De kans dat dit risico zich manifesteert zonder maatregel is Hoog. Momenteel is als standaardinstelling opgenomen dat bij het verstrekken van toestemming de gehele contactenlijst wordt ingeladen. Open velden blijven tevens beschikbaar voor de index om vrij naar eigen invulling in te vullen.
- De impact van dit risico zonder maatregelen is Hoog, afhankelijk van de persoonsgegevens die hierbij betrokken zijn. Indien in het open tekstveld medische of gevoelige gegevens worden opgenomen, kan dit tegenstrijdig zijn aan het vereiste van dataminimalisatie of doelbinding.

Geadviseerd wordt om de volgende maatregelen te nemen:

- Opvolgen van het advies van het privacy-team om de mogelijkheid voor het ophalen van de gehele contactenlijst uit GGD Contact te verwijderen. Enkel het zelf selecteren van de contacten mogelijk maken.
- Aangeven hoe om te gaan met een vrij veld (wat wordt precies verwacht van een toevoeging in een vrij veld). Of;
- Vrije velden verwijderen, indien de informatie niet noodzakelijk is in het vrije veld deze optie uit GGD Contact halen. Oftewel beoordeling van de noodzakelijkheid van het vrije veld.
    - Eventueel vrije veld vervangen door een keuzeveld met informatie die noodzakelijk is.
- Beperken van het aantal vrije invulvelden tot een minimum, en duidelijk aangeven aan de index wat er wel/niet verwacht wordt dat er dan ingevuld mag worden. Verder zoveel mogelijk gebruik maken van vooraf gedefinieerde pop-up mogelijkheden.

Risico voor Betrokkene (voor maatregelen)	Hoog
Risico voor Betrokkene (na maatregelen)	Laag

4. *Gebrekkig inzicht beveiliging(sissues)*

Gebrekkig inzicht in beveiliging(sissues) (oudere) versies Android en iOS leidt tot datalekken en inbreuken.

- De kans dat dit risico zich manifesteert zonder maatregel is Laag. Hiervoor dient de index een oude versie te hebben draaien op de telefoon én dient in die oude versie een exploitable vulnerability aanwezig te zijn.
- De impact van dit risico zonder maatregelen is Middel. Inbreuk in de gegevens kan leiden tot openbaarmaking of misbruik van de gegevens. Dit heeft alleen betrekking op de index die gebruik maakt van een oude versie, niet op alle indexen.

Geadviseerd wordt om de volgende maatregelen te nemen:

- Het gebruik van oudere versies wordt gestaakt zodra er geen beveiligingspatches meer voor worden gemaakt (of wanneer de versie van OS of browser niet up-to-date is).
- BCO-medewerker aan de index te laten vragen om te updaten.

Risico voor Betrokkene (voor maatregelen)	Laag
Risico voor Betrokkene (na maatregelen)	Laag

5. Phishing

Phishing (e-mail en sms en voice phishing) met link naar fake-code BCO, waardoor gegevens op straat komen te liggen of misbruik van kan worden gemaakt.

- De kans dat dit risico zich manifesteert zonder maatregelen is Hoog. Dit gebeurt momenteel ook bij Coronamelder en is zeer waarschijnlijk dat dit tevens bij GGD Contact zal gebeuren.
- De impact van dit risico zonder maatregelen is Hoog. Persoonsgegevens van een specifieke index bij wie de phishing plaatsvindt, kunnen door kwaadwillende openbaar gemaakt worden en misbruik worden gemaakt van de gegevens.

Geadviseerd wordt om de volgende maatregelen te nemen:

- Duidelijke informatieverstrekking vanuit Rijksoverheid/VWS, GGD'en en GGD GHOR Nederland in publiekscampagnes, op de website en in sociale media dat er géén e-mail of sms wordt verstuurd met verzoeken. Eveneens informatieverstrekking over het proces m.b.t. de activatiecode, namelijk dat deze enkel verstrekt wordt en nooit opgevraagd wordt. Enkel voor het verschaffen van toegang in GGD Contact wordt om de code expliciet gevraagd.
- **Duidelijke informatieverstrekking door de BCO-medewerker waarbij informatie wordt gegeven over het gebruik van de GGD Contact en werking van de code inclusief de geldigheidsduur. Inherent hieraan is het goed opleiden van de BCO-medewerkers om ervoor te zorgen dat eenduidige instructies worden gegeven. – actie GGD Hart voor Brabant**
- Actief volgen van App-stores op gelijksoortige Apps en actie nemen indien nodig om deze kwaadaardige App(s) te laten verwijderen.

Risico voor Betrokkene (voor maatregelen)	Hoog
Risico voor Betrokkene (na maatregelen)	Middel

Rest risico na genomen maatregelen i.v.m. mogelijkheid tot phishing. Dit in de verband met een reële kans die blijft bestaan dat een index vatbaar is na phishing ook na een duidelijke informatieverstrekking. Het uitsluiten van phishing-pogingen ligt buiten de invloedsfeer van de GGD'en, dit betreft acties van kwaadwillenden, welke mogelijkheid blijft bestaan.

6. Te lange bewaartermijnen

Persoonsgegevens worden onnodig lang bewaard door het niet naleven van bewaartermijnen.

- De kans dat dit risico zich manifesteert zonder maatregelen is Middel. Door de drukte bij GGD'en is het denkbaar dat gegevens langer dan nodig in het web portal vindbaar zijn. Tevens is het denkbaar dat de index de gegevens niet uit GGD Contact verwijdert.
- De impact van dit risico zonder maatregelen is Middel. De gegevens zijn reeds bekend bij de GGD'en er zullen geen nieuwe of andere beslissingen met betrekking tot de rechten en vrijheden van betrokkene worden genomen. Wel bestaat de kans op toegang door kwaadwillende indien de gegevens beschikbaar zijn.

Geadviseerd wordt om de volgende maatregelen te nemen:

- Technisch een maximale bewaartermijn in het BCO webportaal inregelen, maximaal 16 dagen, waarna gegevens automatisch verwijderd worden.
- **Duidelijke informatieverstrekking naar de index over het verwijderen van gegevens in GGD Contact wanneer niet meer nodig. Actie GGD Hart voor Brabant – privacyverklaring**
- By design mogelijkheden onderzoeken om gegevens voor een bepaalde termijn houdbaar te maken in GGD Contact, bijvoorbeeld tevens maximaal 16 dagen.

Risico voor Betrokkene (voor maatregelen)	Middel
Risico voor Betrokkene (na maatregelen)	Laag

7. Toegang tot gegevens na restore

De gegevens in GGD Contact staan in de back-up van de telefoon, wat kan leiden tot ongewenste personen die door middel van een inbreuk toegang hebben tot gegevens na een restore.

- De kans dat dit risico zich manifesteert zonder maatregelen is Laag. Het is denkbaar dat door kwaadwillende partijen een analyse plaatsvindt op alle gegevens die na een restore nog aanwezig zijn op de telefoon.
- De impact van dit risico zonder maatregelen is Middel. Dit kan leiden tot misbruik van persoonsgegevens of gegevens die openbaar worden gemaakt van een specifieke index.

Geadviseerd wordt om de volgende maatregelen te nemen:

- Duidelijke informatieverstrekking over het verwijderen van de gegevens uit GGD Contact indien BCO is afgelopen.

Versleuteling van de data op het device/ encryptie (at rest).
Alle data die zich in GGD Contact bevinden zijn encrypted, waarbij het aanleveren van de gegevens in GGD Contact enkel mogelijk is binnen 48 uur na invoer van de activatiecode. Bij restore van een eventuele backup zal GGD Contact niet te openen zijn, aangezien de activatiecode niet (meer) geldig is.

Risico voor Betrokkene (voor maatregelen)	Middel
Risico voor Betrokkene (na maatregelen)	Laag

8. *Belemmering uitoefenen rechten van betrokkenen*

Het is een risico dat de betrokkenen (zowel index als de contacten van de index) worden belemmerd in het uitoefenen van hun rechten omdat:

- Niet duidelijk voor betrokkenen is bij welke GGD ze hun rechten kunnen uitoefenen.
- Bij de GGD'en en GGD GHOR Nederland onduidelijkheid bestaat over bij welke GGD een index of contact hoort.

- De kans dat dit risico zich manifesteert zonder maatregelen is Middel. Door de hoeveelheid aan GGD'en en verschillende regio's is het denkbaar dat het onduidelijk is voor de betrokkene waar betrokkenen hun rechten kunnen uitoefenen.
- De impact van dit risico zonder maatregelen is Laag. Het kost meer tijd om bijvoorbeeld te achterhalen welke GGD van toepassing is en waar de gegevens van betrokkenen zijn, maar het blijft mogelijk om hun rechten uit te oefenen.

Geadviseerd wordt om de volgende maatregelen te nemen:

- **Duidelijke informatievoorziening over hoe de rechten van betrokkenen kunnen worden uitgeoefend en onder welke GGD-regio een index of contact valt, in de privacyverklaring en op de website van de GGD'en en in GGD Contact. – actie GGD Hart voor Brabant Privacyverklaring**
- Opzetten en implementeren van procedures en afspraken over verantwoordelijkheden (governance en compliance breed inrichten).
- Eén-op-één doorgeven van contractuele vereisten aan (sub)verwerkers, waardoor eenzelfde vereisten gelden voor alle betrokken partijen zoals leveranciers.

Risico voor Betrokkene (voor maatregelen)	Middel
Risico voor Betrokkene (na maatregelen)	Laag

9. Onjuiste koppeling van gegevens aan dossier

De door de index geüploade contactgegevens worden door een technische/procedurele oorzaak ten onrechte gekoppeld aan een dossier/BSN van een andere burger. Dit kan zijn door bijvoorbeeld een foutieve koppeling van GGD Contact, waardoor de gegevens onjuist of onveilig worden overgezet.

- De kans dat dit risico zich manifesteert zonder maatregelen is Middel. Een menselijke fout zoals het verkeerd intypen van een naam is mogelijk waardoor informatie in een verkeerd dossier wordt gezet of een verkeerde contactpersoon wordt gebeld.
- De impact van dit risico zonder maatregelen is Middel. Een contact kan onterecht gebeld worden, met als consequentie dat het contact tijdelijk in zijn vrijheden kan worden beperkt en gegevens ten onrechte worden opgenomen in een dossier.

Geadviseerd wordt de volgende maatregelen te nemen:

- **Duidelijke instructie voor de BCO-medewerker hoe de gegevens in het BCO webportaal te koppelen (zowel digitaal als handmatig) aan de index (via casenummer). Actie GGD Hart voor Brabant: landelijke werkinstructies**
- Voor het borgen van de technische aspecten zal onder meer gesteund dienen te worden op goede ontwikkel- en beheerprocessen en het testen hiervan
- Periodieke kwaliteitscontrole op (afwijkingen) van het dossier
    - Zoals bijvoorbeeld rapportering door BCO-medewerker bij opvallen foutieve koppeling.

Risico voor Betrokkene (voor maatregelen)	Middel
Risico voor Betrokkene (na maatregelen)	Laag

10. Leverancier(s) kom(t)(en) afspraken niet na

Afspraken uit (verwerkers)overeenkomsten en convenanten worden niet nagekomen en/of afspraken worden niet goed beheerd.

- De kans dat dit risico zich manifesteert zonder maatregelen is Middel. Door de hoeveelheid aan nieuwe projecten en leveranciers worden er externen ingehuurd waardoor het mogelijk is dat medewerkers langs elkaar heen werken en afspraken niet na worden gekomen door bijvoorbeeld miscommunicatie tussen de partijen.
- De impact van dit risico zonder maatregelen is Hoog. Privacy waarborgen kunnen gemist worden en/of zijn niet (volledig) in beeld. Eenzelfde geldt voor verantwoordelijkheden waarvan onduidelijk is wie deze op zich neemt.

Geadviseerd wordt om de volgende maatregelen te nemen:

- **Compliance borgen binnen de organisatie (zowel GGD GHOR Nederland als de GGD'en) d.m.v.het inrichten van een governance structuur. Zie volgende maatregel.**
- **Inrichten van Governancestructuur (leveranciersmanagement):**
    - **Inrichten stuurgroep tijdens ontwikkelfase**
    - **Controle en evaluatie op de nakoming van contractuele afspraken met betrekking op privacy en informatiebeveiliging in ontwikkel- en beheerfase met leveranciers. Actie GGD Hart voor Brabant**
- Contractuele afspraken met leveranciers en alle andere overige partijen.
- Periodieke verantwoording door leveranciers op nader overeen te komen KPI's op het vlak van informatiebeveiliging. Overleggen van SOC 2 type 2 assurancerapportage ten aanzien van de aspecten "Security, Availability, Processing Integrity, Confidentiality en Privacy".

- Leveranciers die betrokkenen zijn bij de systemen waarin (bijzondere) persoonsgegevens zijn opgenomen, dienen in het bezit te zijn van NEN7510, ISO27001 of soortgelijke certificering.
- Inrichten en afstemmen van periodieke evaluatie en sancties bij niet-nakomen.

Risico voor Betrokkene (voor maatregelen)	Hoog
Risico voor Betrokkene (na maatregelen)	Laag

11. <u>Onjuiste aanlevering van gegevens door Index</u>

De door de index gestuurde gegevens aan de GGD bevatten fouten (bewust/onbewust). Zoals het opgeven van contacten waarmee index niet in contact is geweest.

- De kans dat dit risico zich manifesteert zonder maatregelen is Hoog. Het is aannemelijk dat er interesse kan zijn om processen te verstoren.
- De impact van dit risico zonder maatregelen is Hoog. Contacten die niet in contact zijn geweest met de index kunnen toch een handelingsperspectief gedeeld krijgen waardoor zij onnodig in hun vrijheden worden beperkt.

Geadviseerd wordt om de volgende maatregelen te nemen:

- Verstrekken van informatie aan contacten van de index die vragen/onduidelijkheden hebben naar aanleiding van het krijgen van bijvoorbeeld een handelingsperspectief.
- Afdwingen authentiseren/verifiëren van de index voordat door BCO-medewerker gegevens in dossiers worden ingevoerd door middel van een koppeling van een casenummer op de achtergrond.
    - Invoer van gegevens op aangeven van de index is pas mogelijk na een positieve test. Bij deze test is de index reeds geverifieerd aan de hand van geldig ID-bewijs bij het doen van een coronatest.
- **Plausibiliteitschecks invoeren (bekende Nederlanders etc.). Bij twijfelt dient door de BCO-coördinator meegekeken te worden (werkinstructie), eventueel wordt de index nogmaals benaderd. Hiervoor dient een werkbare definitie te worden opgesteld, indien nog niet aanwezig ter voorkoming van dubbel werk voor de coördinator. Actie GGD Hart voor Brabant – werkinstructie**

Risico voor Betrokkene (voor maatregelen)	Hoog
Risico voor Betrokkene (na maatregelen)	Middel

Rest risico na genomen maatregelen i.v.m. onjuiste aanlevering van gegevens door Index. Dit in verband met de mogelijkheid die blijft bestaan dat de index bewust/onbewust onjuiste gegevens aanlevert. Indien er onbewust onjuiste gegevens worden aangeleverd kan indien de index zelf

contact opneemt met de BCO-medewerker de impact worden verlaagd door acteren van de BCO-medewerker (aanpassen van het handelingsperspectief) of de index die het contact zelf informeert.

12. Ongeautoriseerde inzage in het BCO webportaal

Ongeautoriseerde inzage van de indexgegevens en de contactenlijst door de BCO-medewerker of andere onbevoegden binnen de GGD(of samenwerkingspartners).

- De kans dat dit risico zich manifesteert zonder maatregelen is Hoog. In het verleden is bij andere dossiers omtrent Corona ook gebleken dat dit zich heeft voorgedaan.
- De impact van dit risico zonder maatregelen Hoog. Het netwerk van een index is hiermee inzichtelijk evenals kans op openbaarmaking.

Geadviseerd wordt om de volgende maatregelen te nemen:

- Uitgangspunt is onder meer het informatiebeveiligingsbeleid van GGD GHOR Nederland waarin onder meer aandacht wordt gegeven aan toereikende authenticatiemiddelen (MFA), gedragscodes en sanctiebeleid.
- **Inrichten autorisaties/autorisatiematrix. Actie GGD Hart voor Brabant**
- Dossiertoegang wordt gelogd. Periodiek (wekelijks) wordt een analyse uitgevoerd op onrechtmatige/ongeautoriseerde inzage in dossiers. Hierover wordt verslag uitgebracht aan directie. Bij geconstateerde overtredingen treedt sanctiebeleid in werking.
- **Training BCO-medewerkers m.b.t. juist en ethisch gebruik gegevens. Actie GGD Hart voor Brabant – inwerkbeleid**
- BCO-medewerker kan in het BCO portal alleen zoeken op aan hem/haar toegewezen dossiers en alleen op actieve BCO dossiers.
- **Antecedentenonderzoek nieuwe medewerkers (ook bij samenwerkingspartners) – Actie GGD Hart voor Brabant**

Risico voor Betrokkene (voor maatregelen)	Hoog
Risico voor Betrokkene (na maatregelen)	Laag

13. Sociaal maatschappelijk risico

Kwaadwillenden zijn geïnteresseerd in het netwerk dat de GGD in kaart brengt. Het is een database met mensen die elkaar kennen, opgebouwd door BCO.

- De kans dat dit risico zich manifesteert zonder maatregelen is Hoog. In analyses (dreigingsanalyse) is naar voren gekomen dat er interesse is in deze gegevens.
- De impact van dit risico zonder maatregelen is Hoog. Er kan misbruik of openbaarmaking van de gegevens plaatsvinden.

Geadviseerd wordt om de volgende maatregelen te nemen:

- Inrichten van Governance structuur (leveranciersmanagement):
    - Inrichten stuurgroep tijdens ontwikkelfase
    - Controle en evaluatie op de nakoming van contractuele afspraken in ontwikkel- en beheerfase
- Periodieke verantwoording door leveranciers op nader overeen te komen KPI's op het vlak van informatiebeveiliging
- Overleggen van SOC 2 type 2 Assurance rapportage ten aanzien van de aspecten "Security, Availability, Processing Integrity, Confidentiality en Privacy".
- Leveranciers die betrokkenen zijn bij de systemen waarin (bijzondere) persoonsgegevens worden verwerkt, dienen in het bezit te zijn van NEN7510/ISO 27001/BIO certificering
- Inzicht in technische kwetsbaarheden
    - Voorkomen: Beheerst ontwikkel- en beheerproces (zie ook volgend risico), en uitvoeren van (technische) securitytesten op de GGD Contact, de aansluitingen (koppelingen) en het BCO BCO webportaal.
    - Detecteren en analyseren: Inrichten van IDS/IPS, SIEM oplossingen voor tijdig detecteren en analyseren van aanvallen. Linking pin hierbij is een goed (security) incidentproces.
    - Acteren: Threat-hunting, inrichting CERT
    - Attack surface minimization: Een minimaal aantal API's aan de buitenkant van de sluis aanbieden die vanaf het internet beschikbaar zijn. Hierdoor is er geen mogelijkheid om vanaf het internet de "achterkant" van het systeem te benaderen.
    - Toepassing TLS: Transport versleuteling (TLS) op alle verbindingen.
    - Encryptie (at rest: Encryptie van de (gevoelige) velden voordat deze in de database terecht komen. Tevens at rest encryptie van secrets, data en logging. Hiermee wordt voorkomen dat er toegang tot de data mogelijk is.

Risico voor Betrokkene (voor maatregelen)	Hoog
Risico voor Betrokkene (na maatregelen)	Middel

Rest risico na genomen maatregelen i.v.m. sociaal maatschappelijk risico. Dit in de verband met de mogelijkheid die blijft bestaan kwaadwillenden interesse hebben in de gegevens en hier pogingen tot inbreuk voor zullen blijven doen, ook via de – mogelijk – beperkt beveiligde omgevingen van de index.

14. Niet op orde zijn van beheerprocedures

*(*deze wordt nog nader afgestemd met betrokkenen vanuit beheer)*

Beheerprocedures zijn niet voldoende op orde, waardoor risico ontstaat van misbruik/onrechtmatige verwerking zonder dat verantwoordelijke of verwerker daarvan op de hoogte is.

- De kans dat dit risico zich manifesteert zonder maatregelen is Middel. Door ontoereikend beheer worden incidenten niet tijd onderkend, opgepakt en opgelost.
- De impact van dit risico zonder maatregelen is Middel. De beschikbaarheid, integriteit en vertrouwelijkheid van de systemen kan worden aangetast, maar dit is niet per se het geval.

Geadviseerd wordt om de volgende maatregelen te nemen:

- Opzetten en implementeren van ICT-beheerprocessen. Gebaseerd op/aansluitend bij een door de directie geaccordeerd informatiebeveiligingsbeleid. Aansluiten bij binnen de markt bekende standaarden zoals ITIL, in combinatie met BIO/NEN 7510/ISO 27001. In ieder geval aandacht voor
  - Security management
  - Access management
  - Availability management
  - Change management
  - Incident management
  - Problem management
  - Patch management
  - Knowledge management
  - Supplier management
- Eisen ten aanzien van ICT-beheerprocessen 1-op-1 vertalen naar de contractuele afspraken met leveranciers ((sub-)verwerkers)
- Periodieke controle op naleving van beheerprocedures.
- Periodieke evaluatie op de beheerprocedures.

Risico voor Betrokkene (voor maatregelen)	Hoog
Risico voor Betrokkene (na maatregelen)	Laag

15. Data gaat verloren/is (tijdelijk) niet beschikbaar

Door kwaadwillende dan wel een onbewuste menselijke fout kan de data in zowel GGD Contact als in het BCO webportaal verloren gaan. Dan wel de continuïteit van de applicaties en de onderliggende data is niet gewaarborgd, zodat gegevens verloren gaan of (tijdelijk) niet beschikbaar zijn.

- De kans dat dit risico zich manifesteert zonder maatregelen is Hoog. De interesse in de data van buitenaf maakt het aannemelijk dat data verloren kan gaan door bijvoorbeeld het stelen en vervolgens vernietigen van de data. Ook een onbewuste menselijke fout door aanwezige werkdruk is denkbaar.
- De impact van dit risico zonder maatregelen is Hoog. Dit kan resulteren in een datalek met openbaarmaking van en/of misbruik van de gegevens.

Geadviseerd wordt om de volgende maatregelen te nemen:

- Inzicht in technische kwetsbaarheden
    - Voorkomen: Beheerst ontwikkel- en beheerproces (zie ook volgend risico), en uitvoeren van (technische) penetratietesten op GGD Contact, de aansluiting op en het BCO webportaal.
    - Detecteren en analyseren: Inrichten van IDS/IPS, SIEM oplossingen voor tijdig detecteren en analyseren van aanvallen. Linking pin hierbij is een goed (security) incidentproces.
    - Acteren: Threat-hunting, inrichting CERT
    - Toepassing TLS: Transport versleuteling (TLS) op alle verbindingen.
    - Encryptie (at rest: Encryptie van de (gevoelige) velden voordat deze in de database terecht komen. Tevens at rest encryptie van secrets, data en logging. Hiermee wordt voorkomen dat er toegang tot de data mogelijk is.

Risico voor Betrokkene (voor maatregelen)	Hoog
Risico voor Betrokkene (na maatregelen)	Laag

16. Geen of onduidelijk eigenaarschap

Het eigenaarschap van GGD Contact en het BCO webportaal is niet helder of geformaliseerd.

- De kans dat dit risico zich manifesteert zonder maatregelen is Hoog. De samenwerking door een grote hoeveelheid partijen en de verdeling in verantwoordelijkheid, maakt het aannemelijk dat niemand eigenaarschap neemt of deze verlegt bij een ander.
- De impact van dit risico zonder maatregelen is Hoog. Noodzakelijke verantwoordelijkheden komen niet of niet op de juiste plek te liggen.

Geadviseerd wordt om de volgende maatregelen te nemen:

- Concrete en duidelijke geformaliseerde afspraken over (gedeelde) verantwoordelijkheden ten aanzien van GGD Contact en het BCO webportaal.
- Inrichten van Governancestructuur (leveranciersmanagement):
    - Inrichten stuurgroep tijdens ontwikkelfase

- Periodieke controle en evaluatie op de nakoming van contractuele afspraken in ontwikkel- en beheerfase.
- Contractuele afspraken met betrekking tot samenwerkingsafspraken en de verantwoordelijkheden die hiermee samenhangen tussen de betrokken partijen.

Risico voor Betrokkene (voor maatregelen)	Hoog
Risico voor Betrokkene (na maatregelen)	Laag

17. Data index en contact niet beschikbaar

Een (tijdelijke) uitval van systemen zorgt ervoor dat data van de index en het contact niet beschikbaar is in de GGD Contact en/of het BCO webportaal.

- De kans dat dit risico zich manifesteert zonder maatregelen is Middel. Door bijvoorbeeld een bewuste of onbewuste technische oorzaak is het mogelijk dat er een uitval van systemen plaatsvindt of dat systemen (tijdelijk) niet aan de gevraagde capaciteit kunnen voldoen.
- De impact van dit risico zonder maatregelen is Middel. Het digitale BCO kan (tijdelijk) niet worden voortgezet, maar het reguliere BCO kan worden voortgezet waardoor het niet geheel onmogelijk is om BCO uit te voeren.

Geadviseerd wordt om de volgende maatregelen te nemen:

- Redundante uitvoering van essentiële systemen en infrastructuur voor de GGD'en.
- Voor het borgen van de technische aspecten zal onder meer gesteund dienen te worden op een goede juist ingerichte ontwikkel- en beheerprocessen waarin dergelijke scenario's zoals uitval van systemen zijn opgenomen en die bekend zijn bij de beheerders van GGD Contact en/of het BCO webportaal.
- Opleiding van de BCO-medewerker bij voordoen uitvalscenario's.

Risico voor Betrokkene (voor maatregelen)	Middel
Risico voor Betrokkene (na maatregelen)	Laag

18. Onvoldoende veilig ingerichte koppelingen

Koppelingen tussen systemen en applicaties zijn op een onvoldoende veilige manier ingericht.

- De kans dat dit risico zich manifesteert zonder maatregelen is Hoog. Indien voorbij wordt gegaan aan informatiebeveiligingsaspecten m.b.t. het transport van de data tussen systemen of wanneer derden zich toegang tot de koppeling en/of systemen kunnen verschaffen is het aannemelijk dat er onveilige koppeling zijn ingericht.

- De impact van dit risico zonder maatregelen is Hoog. Indien er transport van data plaatsvindt door onvoldoende veilige koppelingen is de koppeling hiermee vatbaar voor inbreuken van buitenaf, waardoor gegevens openbaar kunnen worden gemaakt en/of misbruik van de data plaats kan vinden.

Geadviseerd wordt om de volgende maatregelen te nemen:

- Bij de inrichting van systemen vereisten opstellen (voor leveranciers) waaraan minimaal voldaan dient te worden en testen van deze systemen.
- Opzetten en implementeren van ICT-beheerprocessen. Gebaseerd op een door de directie geaccordeerd informatiebeveiligingsbeleid. Aansluiten bij binnen de markt bekende standaarden zoals ITIL, in combinatie met BIO/NEN 7510/ISO 27001. In ieder geval aandacht voor
    - Security management
    - Access management
    - Availability management
    - Change management
    - Incident management
    - Problem management
    - Patch management
    - Knowledge management
    - Supplier management
- Eisen ten aanzien van ICT-beheerprocessen 1-op-1 vertalen naar de contractuele afspraken met leveranciers ((sub-)verwerkers)
- Goede contractuele afspraken
- Toepassing TLS: Transport versleuteling (TLS) op alle verbindingen.
- Encryptie (at rest: Encryptie van de (gevoelige) velden voordat deze in de database terecht komen. Tevens at rest encryptie van secrets, data en logging. Hiermee wordt voorkomen dat er toegang tot de data mogelijk is.

Risico voor Betrokkene (voor maatregelen)	Hoog
Risico voor Betrokkene (na maatregelen)	Laag

19. Verwerken persoonsgegevens indexen die buiten RIVM Protocol vallen

Bij het gebruik van GGD Contact wordt geen onderscheid gemaakt in groepen personen (zoals personen onder de 18 jaar)/functies (zoals contactberoepen). Er wordt in het kader van BCO gevraagd door de GGD'en om gegevens aan te leveren van personen met wie de index in contact is

geweest, terwijl in het RIVM-protocol specifieke afspraken zijn opgenomen voor bijvoorbeeld contactberoepen, scholen, kinderopvang en/of kinderen onder de 18. Deze personen behoren niet in dit BCO-onderzoek als index te worden aangemerkt en daarvan zouden geen gegevens verwerkt moeten worden in dit portaal.

- De kans dat dit risico zich manifesteert zonder maatregelen is Hoog. Momenteel lijkt het erop dat met de richtlijnen voor specifieke personen (zoals kinderen) of specifieke beroepen (zoals contactberoepen) in het RIVM-protocol hiermee geen rekening is gehouden in de ontwikkeling van GGD Contact.
- De impact van dit risico zonder maatregelen is Hoog. Hierdoor komt een index in de positie dat gevraagd wordt om gegevens te delen van personen waardoor zij onterecht (tijdelijk) in hun vrijheden worden beperkt. Bijvoorbeeld de situatie waarin de index een leidster is op de kinderopvang waarbij zij alle kinderen met wie zij in contact is geweest dient in te vullen in GGD Contact. Hierover zijn andere specifieke richtlijnen opgenomen in het RIVM-protocol. Dit kan afwijken van de handelingsperspectieven die in GGD Contact worden getoond.

Geadviseerd wordt om de volgende maatregelen te nemen:

- Zorgen voor afstemming tussen het RIVM-protocol en het proces van GGD Contact.

Risico voor Betrokkene (voor maatregelen)	Hoog
Risico voor Betrokkene (na maatregelen)	Laag

20. <u>Ontbreken verwerkersovereenkomsten</u>

Met alle betrokken partijen die aangemerkt kunnen worden als verwerker dient een verwerkersovereenkomst te worden gesloten tussen GGD'en(mogelijk met GGD GHOR Nederland als facilitator) en de verwerkers. Dit betreft de hostingpartij Intermax.

- De kans dat dit risico zich manifesteert zonder maatregelen is Hoog. Momenteel is met nog niet alle partijen, zoals de hostingpartij, een verwerkersovereenkomst gesloten.
- De impact van dit risico zonder maatregelen is Hoog. Het ontbreken van verwerkersovereenkomsten zorgt voor een ongecontroleerde deling van gegevens met derden waardoor misbruik van gegevens mogelijk is. Tevens is het ontbreken van verwerkersovereenkomsten in strijd met de AVG

Geadviseerd wordt om de volgende maatregelen te nemen:

- Opstellen van contractuele afspraken met name verwerkersovereenkomsten indien er sprake is van een verwerkingsverantwoordelijke – verwerker rolverdeling.
- Inrichten van Governancestructuur (leveranciersmanagement):
    - Inrichten stuurgroep tijdens ontwikkelfase

- Controle en evaluatie op de nakoming van contractuele afspraken in ontwikkel- en beheerfase

Risico voor Betrokkene (voor maatregelen)	Hoog
Risico voor Betrokkene (na maatregelen)	Laag

21. Ontbreken vastlegging toestemming

De toestemmingsvraag in GGD Contact die aan de index wordt gesteld omtrent het ophalen van de adreslijst, wordt niet expliciet vastgelegd.

- De kans dat dit risico zich manifesteert zonder maatregelen is Hoog. Door de huidige instellingen in het ontwerp van GGD Contact wordt de keuze van het wel/niet gegeven van toestemming niet vastgelegd.
- De impact van dit risico zonder maatregelen is Hoog. Er wordt niet voldaan aan de verantwoordingsplicht in het kader van de AVG.

Geadviseerd wordt om de volgende maatregelen te nemen:

- Vastleggen en documenteren van wel/niet gegeven toestemming in GGD Contact op basis van een opt-in.

Risico voor Betrokkene (voor maatregelen)	Hoog
Risico voor Betrokkene (na maatregelen)	Laag

22. Toegang door derden in de GGD Contact

GGD Contact is niet met een wachtwoord beveiligd of anderszins beveiligd bij de toegang van de applicatie.

- De kans dat dit risico zich manifesteert zonder maatregelen is laag. Dit is een kans die zich voortdoet voortbouwend op een maatregel die een index zelf al treft op het toestel. Een groot aantal van de gebruikers van smartphones heeft zijn toestel beveiligd. In het geval dat het toestel niet beveiligd is, is aannemelijk dat de index zijn/haar telefoon niet gedurende de gehele dag bij zich draagt waardoor iemand anders dan de index toegang tot de telefoon en daarmee GGD Contact kan verschaffen.
- De impact van dit risico zonder maatregelen is Hoog. Een derde heeft inzicht in de gegevens die de index heeft ingevuld in GGD Contact en kan deze informatie voor kwaadwillende doeleinden gebruiken zoals openbaren.

Geadviseerd wordt om de volgende maatregelen te nemen:

- BCO-medewerker opleiden in het geven van advies omtrent het beveiligen van de telefoon zoals advies toevoegen de telefoon te beveiligen met een pincode, wachtwoord of biometrische kenmerken of;
- Toegang tot GGD Contact vooraf laten gaan door een zelf ingestelde pincode.

Risico voor Betrokkene (voor maatregelen)	Middel
Risico voor Betrokkene (na maatregelen)	Laag

23. <u>Gebruik van GGD Contact door landelijke partners</u>

Landelijke partners (zoals SOS en onderaannemer Yource), die momenteel ook BCO uitvoeren voor de GGD'en, gaan tevens met GGD Contact werken en hebben hiermee toegang tot het BCO webportaal. Er is door GGD GHOR een separate DPIA uitgevoerd op de landelijke schil, waarin risico's en maatregelen zijn benoemd.

- De kans dat dit risico zich manifesteert zonder Maatregelen is Hoog. Momenteel wordt er gekeken naar het inschakelen van deze landelijke partners bij de praktijktesten.
- De impact van dit risico zonder maatregelen is Hoog. Door de inzet van een flexibele schil medewerkers via ingehuurde callcenters is er minder zicht op gegevensverwerking en is misbruik en/of openbaarmaking van gegevens mogelijk.

Geadviseerd wordt om de volgende maatregelen te nemen:

- Vastleggen van contractuele afspraken met daarin o.a. afspraken over de verantwoordelijkheden, sub-verwerkers en eventuele datalekken.
- Uitgangspunt is onder meer het informatiebeveiligingsbeleid van GGD GHOR Nederland waarin onder meer aandacht wordt gegeven aan toereikende authenticatiemiddelen (MFA), gedragscodes en sanctiebeleid.
    - Waaronder 2FA gebruik op de identity Hub
- **In het autorisatiebeleid maatregelen opnemen waarin BCO-medewerkers vanuit landelijke schil tevens nieuwe autorisatie verkrijgen die past bij de GGD waar zij op dat moment werkzaamheden voor dienen te verrichten, evenals het verwijderen van autorisatie bij het verlaten van de betreffende GGD. Actie GGD Hart voor Brabant – autorisatiematrix**
- Dossiertoegang wordt gelogd. Periodiek wordt een analyse uitgevoerd op onrechtmatige/ongeautoriseerde inzage in dossiers. Hierover wordt verslag uitgebracht aan directie. Bij geconstateerde overtredingen treedt sanctiebeleid in werking.

Risico voor Betrokkene (voor maatregelen)	Hoog
Risico voor Betrokkene (na maatregelen)	Laag

24. Loggingsinformatie als gevolg van gebruik van GGD Contact en het uploaden van de informatie is te herleiden naar de index

(wordt waarschijnlijk niet meer gelogd in release 1.1, wordt nog geverifieerd)*

Bij logging op (onder meer) IP-adres is de loggingsinformatie herleidbaar naar een individu.

- De kans dat dit risico zich manifesteert zonder maatregelen is Hoog. Er is sprake van logging en indien hier geen afspraken over worden gemaakt is het aannemelijk dat de gevoelige informatie bij gebruik van logging van het IP-adres te herleiden is naar een individu.
- De impact van dit risico zonder maatregelen is Hoog. Door bijvoorbeeld de herleiding aan de hand van het IP-adres is herleidbaar wat hij/zij aan acties heeft verricht met behulp van de GGD Contact. Met als gevolg inzage en oneigenlijk gebruik.

Geadviseerd wordt om de volgende maatregelen te nemen:

- Vastleggen van contractuele afspraken over de wijze van logging en de documentatie hiervan met de betrokken partijen zoals de hostingpartij, leverancier BCO webportaal en de logging m.b.t. inzage in HPZone.
- Inrichten van Governance structuur (leveranciersmanagement):
    - Inrichten stuurgroep tijdens ontwikkelfase
    - Controle en evaluatie op de nakoming van contractuele afspraken in ontwikkel- en beheerfase
- Periodieke verantwoording door leveranciers op nader overeen te komen KPI's op het vlak van informatiebeveiliging.
- Overleggen van SOC 2 type 2 assurancerapportage ten aanzien van de aspecten "Security, Availability, Processing Integrity, Confidentiality en Privacy".

Risico voor Betrokkene (voor maatregelen)	Hoog
Risico voor Betrokkene (na maatregelen)	Laag

25. Onduidelijkheid omtrent beheerstaken GGD GHOR Nederland

Op het moment van schrijven van de DPIA is niet duidelijk welke beheertaken GGD GHOR Nederland op zich gaat nemen en hoe GGD GHOR Nederland deze taken gaat uitvoeren.

- De kans dat dit risico zich manifesteert zonder maatregelen is Hoog. Momenteel is niet duidelijk hoe de beheertaken door GGD GHOR Nederland uitgevoerd gaan worden.

- De impact van dit risico zonder maatregelen is Hoog. Doordat verantwoordelijkheden niet helder zijn kunnen o.a. privacy en informatiebeveiligingsvraagstukken omtrent het beheer blijven liggen of liggen deze elders waardoor er geen grip op is voor GGD GHOR Nederland en de GGD'en.

Geadviseerd wordt om de volgende maatregelen te nemen:

- Op de korte termijn verduidelijken en vastleggen van de beheertaken van GGD GHOR Nederland.
- Navolging van vastgestelde beheerstaken

Risico voor Betrokkene (voor maatregelen)	Hoog
Risico voor Betrokkene (na maatregelen)	Laag

26. <u>Ontbreken van afspraken omtrent rolverdeling en verantwoordelijkheden</u>

Ten tijde van schrijven van deze DPIA zijn er nog geen afspraken gemaakt tussen de partijen over de verdeling van hun verantwoordelijkheden ten aanzien van de uitoefening van de rechten van betrokkenen en maatregels als gevolg van inbreuken in verband met de beveiliging van persoonsgegevens (datalekken) .

- De kans dat dit risico zich manifesteert zonder maatregelen is Hoog. Momenteel zijn er nog geen bindende overeenkomsten afgesloten tussen de verantwoordelijken en de verwerkers.
- De impact van dit risico zonder maatregelen is Hoog. Verantwoordelijkheden zijn niet belegd of ontbreken bij de verantwoordelijke partijen.

Geadviseerd wordt om de volgende maatregelen te nemen:

- **Hetzij vanuit gezamenlijke verantwoordelijkheid één convenant opstellen tussen GGD'en enerzijds en VWS anderzijds waarin de rollen en verantwoordelijkheden van deze partijen zijn opgenomen. Hierin kan het stukje verwerkerschap omtrent hosting van VWS ook worden opgenomen. Een aparte verwerkersovereenkomst is hierbij niet noodzakelijk, maar kan wel. Tevens kan in dit convenant GGD GHOR Nederland ook partij zijn waarin de rol van GGD GHOR Nederland als facilitator op basis van de statuten wordt toegelicht. Verwerkersovereenkomst tussen GGD GHOR en GGD'en over het beheer van GGD contact, BCO webportaal en sluis. Actie GGD Hart voor Brabant – Governance**

Risico voor Betrokkene (voor maatregelen)	Hoog
Risico voor Betrokkene (na maatregelen)	Laag

27. <u>Strijd met het transparantiebeginsel, art 5.1 AVG</u>

Art. 13 AVG verplicht niet tot het verstrekken van een beschrijving van de functionaliteit, maar in de privacyverklaring as-is (zonder toevoeging functionaliteit Zelf-BCO) wordt wel een toelichting gegeven op functionaliteit as-is. Zonder een aanpassing van de privacyverklaring zou die toelichting niet compleet zijn. Dat is in strijd met het transparantiebeginsel van art. 5.1 AVG.

- De kans dat dit risico zich manifesteert is Laag. Vanuit het project GGD Contact is een functionaliteitswijziging in scope en daarmee tevens de aanpassing van de privacyverklaring.
- De impact van dit risico zonder maatregelen is Laag.

Geadviseerd wordt om de volgende maatregelen te nemen:

- **Aanpassing van de privacyverklaring n.a.v. toevoeging zelf-BCO in de GGD Contact-app. Actie GGD Hart voor Brabant – privacyverklaring**

Risico voor Betrokkene (voor maatregelen)	Laag
Risico voor Betrokkene (na maatregelen)	Laag

28. <u>Verwerking van klachten door GGD blijkt niet-noodzakelijk</u>

Door het niet onderbouwen van de noodzaak van de gegevens die vanuit het reguliere BCO worden uitgevraagd kan de noodzakelijkheid van het verwerken van de persoonsgegevens niet worden gewaarborgd.

- De kans dat dit risico zich manifesteert is hoog. Naar aanleiding van navraag bij de GGD'en blijkt er géén DPIA te zijn van het reguliere BCO-proces.
- De impact van dit risico zonder maatregelen is Hoog. Er dient een adequate risicoanalyse uitgevoerd te worden op het regulier BCO-proces om de noodzaak van de uitgevraagde persoonsgegevens in beeld te krijgen om een onrechtmatige verwerking van gegevens te voorkomen.

Geadviseerd wordt om de volgende maatregelen te nemen:

- **Uitvoeren DPIA regulier BCO/onderbouwing noodzaak van gegevens regulier BCO. Actie GGD Hart voor Brabant – DPIA is opgesteld, ligt voor bij de FG ter beoordeling.**

Risico voor Betrokkene (voor maatregelen)	Hoog
Risico voor Betrokkene (na maatregelen)	Laag

D. Beschrijving voorgenomen maatregelen

16. Maatregelen

Als uitvoerder van het BCO-proces heeft een GGD de verantwoordelijkheid om medische data adequaat te beveiligen. Een veilig middel is pas veilig, als het ook veilig gebruikt wordt. Het is daarom van belang dat de gehele keten van het BCO proces veilig is. Een groot gedeelte van de securitymaatregelen kunnen niet door een applicatie afgedekt kunnen worden, omdat de keten breder is dan alleen de technische oplossing. Een aantal voorbeelden van maatregelen die niet door de applicatie worden getroffen, maar wel horen bij een adequate beveiliging door een GGD:

- Information Security Management Systeem
- Organisatorische maatregelen
- Technische maatregelen in de Identitybroker (GGD-GHOR)
- Werkplekbeveiliging
- Bewustwording
- Join-Move-Leave proces
- Beheer AD/IDP
- Acceptable Use policy en gebruikersovereenkomsten
- Indienstreding (integriteitcontrole, geheimhoudings-overeenkomsten)
- Wachtwoordkluis voor gebruikers (vanuit de BIO)

Tijdens het ontwerp van GGD Contact zijn aandachtspunten/acties naar voren gekomen die betrekking hebben op veilig gebruik van een webapplicatie met medische informatie (BCO-portaal) en getroffen moeten worden door de GGD omdat ze de basis vormen voor de beveiliging van de keten (en daarmee de applicatie). **Het gaat om de volgende acties voor de GGD Hart voor Brabant:**

- **Hanteer eisen, pas maatregelen toe en richt toezicht in voor de beveiliging van de BCO werkplekken conform NEN 7510. Stel gebruikers op de hoogte hoe ze veilig kunnen werken.**
- **Richt auditlogging in voor de active directory (AD) of directory service, conform 7513.**
- **Controleer periodiek of alle toekomstige en huidige gebruikers voor het portaal een uniek AD gebruikersaccount hebben.**
- **Controleer periodiek of alle toekomstige en huidige gebruikers voor het portaal een VOG hebben.**
- **Controleer of alle toekomstige en huidige gebruikers voor het portaal een geheimhoudingsverklaring hebben getekend**

- **Houd het Join-Move-Leave proces bij: Elke wijziging aan rollen vertrekkende medewerkers (leave), medewerkers met een andere rol (move) en nieuwe medewerkers (join) moet direct worden verwerkt in de AD.**
- **Controleer periodiek of alle huidige gebruikers de juiste rollen hebben toebedeeld gekregen.**
- **Meld incidenten bij de helpdesk van GGD Contact.**
- **Registreer incidenten op het gebied van onrechtmatig gebruik van de corona gerelateerde applicaties.**

Maatregelen vanuit DPIA

Om de risico's zoals in dit document omschreven te beperken zijn verschillende maatregelen getroffen. Hieronder zijn de verschillende maatregelen opgenomen.

1. *Geheimhoudingsverklaringen BCO-medewerkers*

Geheimhoudingsverklaringen zijn ondertekend door personeel van GGD GHOR en externen die zijn ingehuurd door GGD GHOR Nederland voor het functioneel beheer.

2. *Autorisatiematrix*

Een autorisatiematrix is opgesteld waarin de rollen en rechten zijn bepaald voor de verschillende medewerkers die werken met het BCO webportaal. In de Identity Hub met bestaande GGD-accounts zijn aan de BCO-medewerkers specifieke rollen met rechten toegewezen. BCO-medewerkers hebben binnen het systeem alleen die toegang die ze nodig hebben.

3. *Overeenkomsten en/of convenanten*

Met de verschillende leveranciers en betrokken partijen zijn passende afspraken gemaakt over de verwerking van persoonsgegevens, zodat de gegevens niet onrechtmatig worden gebruikt. Daarnaast is, waar nodig, bepaald welke beveiligingsmaatregelen moeten worden genomen en door wie.

4. *Logging*

Er is sprake van logging (datasluis (GGD API en GGD webapplicatie, tezamen: het BCO webportaal) over bewegingen in het BCO webportaal en in systemen van leveranciers (vb. logging in de hosting door hostingpartij) die wordt vastgelegd en gecontroleerd (audittrails). In **Bijlage 4** is een nadere uitwerking te vinden van welke gegevens gelogd worden.

5. *Gebruik identificatie*

GGD Contact verstuurt geen gegevens naar GGD of verzamelde contacten zonder ontgrendeling met een code en uitdrukkelijke toestemming van de index om de gegevens te delen met de GGD. De gebruiker ontvangt die pas op het moment dat hij positief getest is of benaderd wordt als onderdeel van contactonderzoek.

6. *Security testen*

Meerdere security testen zijn er vooraf en worden er tijdens het gebruik van GGD Contact op zowel de Applicatie als op het BCO webportaal en de systemen die hiermee verbonden zijn uitgevoerd. Denk hierbij aan: pen-test op GGD Contact, de API's, het BCO webportaal en een code review. De software en de implementatie van de oplossing wordt inhoudelijk beoordeeld door partijen die hierin gespecialiseerd zijn.

7. *SSL Pinning*

Alle gegevens die verzonden worden van het BCO webportaal naar GGD Contact worden ondertekend met een digitale handtekening. De digitale handtekening laat aan de ontvanger (in dit geval de GGD Contact (de applicatie) zien dat de gegevens zonder tussenkomst van anderen afkomstig zijn van de zender (in dit geval het BCO webportaal).

8. *Duidelijke informatievoorziening richting BCO-medewerker dan wel richting betrokkenen*

Over essentiële en/of kritische processen/risico's dient een duidelijke informatievoorziening richting betrokkenen dan wel BCO-medewerker plaats te vinden in de vorm van werkinstructies en/of informatie pop-ups in GGD Contact/BCO webportaal.

9. *Gebruik sterke en beperkte code*

Het gebruik van een sterke (lange) code en een code die slechts gedurende een bepaalde tijd bruikbaar is maakt de code minder vatbaar voor kwaadwillende. Oftewel een one time code overdracht via het telefoon gesprek met de BCO-medewerker. Er wordt voor de koppeling met de GGD Contact-app een eenmalige kort geldige code via de telefoon doorgegeven. Dit gebeurt pas na het normale verificatieproces waarbij de BCO medewerker weet welke persoon men aan de telefoon spreekt. Door de tijd tussen het verstrekken van een code en het mogelijk gebruik van deze activatiecode kort te houden is misbruik vele malen moeilijker.

10. *Leveranciers kiezen die aantoonbaar informatiebeveiliging op orde hebben*

Door te kiezen voor leveranciers die voldoet aan IB-standaarden waarborg je o.a. de veiligheid van de informatie in de systemen van leveranciers waaronder beschikbaarheid, integriteit en vertrouwelijkheid. Leveranciers dienen in het bezit te zijn van NEN7510, ISO27001 of een vergelijkbare certificering.

11. *Controle en evaluatie op (beheer)procedures*

Door controle te houden op (beheer)procedures en hier ook evaluatie op te laten plaatsvinden blijven mogelijke risico's inzichtelijk en kan hierop geacteerd worden.

12. *Training BCO-medewerker*

Voorafgaande aan de training zit een screening van de BCO-medewerker. De BCO-medewerkers ontvangen alvorens zij starten diverse soorten trainingen en werkinstructies m.b.t. de verwerking van de persoonsgegevens in de systemen. Hierbij is speciale aandacht voor juistheid van gegevens, geheimhouding, vertrouwelijkheid en gedragsregels. Aanwezigheid van werkinstructies voor de BCO-medewerker.

13. Duidelijke informatieverstrekking op websites GGD'en en in de privacyverklaring

Over rechten van betrokken wordt een duidelijke informatievoorziening opgezet op de websites van de GGD'en en in de privacyverklaring van GGD Contact.

14. Bewaartermijnen technisch inregelen

Door het inregelen van een beperkte opslagperiode in het BCO webportaal worden gegevens niet langer bewaard dan noodzakelijk.

15. Gebruik van oudere versies op mobiele telefoon staken bij afwezigheid beveiligingspatches

Het gebruik van GGD Contact is niet mogelijk bij verouderde versies waarvoor geen beveiligingspatches meer beschikbaar zijn. Dit voorkomt inbreuken van buitenaf.
*** Check of dit niet is neergelegd bij risico van de gebruiker, dit zou tot effect hebben dat app een beperkte adoptie graad heeft.

16. Dataminimalisatie toepassen

Enkel de gegevens die bijdragen aan het doel worden uitgevraagd in GGD Contact.

17. Unieke code

Doorgifte van een unieke code. Een algoritme voor generen unieke code, dit laten ondersteunen en review op algoritme.

18. Vermijden verwisselbare karakters

Vermijden van eenvoudig verwisselbare karakters bij het telefonisch doorgegeven van de sleutel (bijvoorbeeld "O" versus "0" (nul)).

19. Informatieverstrekking vanuit Rijksoverheid/VWS

Duidelijke informatieverstrekking vanuit Rijksoverheid/VWS.

20. Procedures rechten van betrokkenen

Opzetten en implementeren van procedures om invulling te geven aan rechten van betrokkenen.

21. Doorgifte vereisten (sub)verwerkers

Eén-op-één doorgegeven van (contractuele) vereisten aan (sub)verwerkers.

22. Borgen technische aspecten

Het borgen van de technische aspecten zal onder meer gesteund dienen te worden op een goede ontwikkel- en beheerprocessen.

23. Inrichten van de Governancestructuur

Het inrichten van de Governancestructuur (leveranciermanagement) omvat:

- Het inrichten van een stuurgroep tijdens de ontwikkelfase;
- Controle en evaluatie op de nakoming van contractuele afspraken in ontwikkel- en beheerfase.

24. Vastlegging contractuele afspraken

Goede contractuele afspraken met alle betrokken partijen in de keten.

25. Periodieke verantwoording door leveranciers

Periodieke verantwoording door leveranciers op nader overeen te komen KPI's op het vlak van informatiebeveiliging. Overleggen van SOC 2 type 2 Assurance rapportage ten aanzien van de aspecten "Security, Availability, Processing Integrity, Confidentiality en Privacy".

26. NEN7510, ISO27001 of soortgelijke certificering

Leveranciers dienen in het bezit te zijn van NEN7510, ISO27001 of soortgelijke certificering

27. Authentiseren/verifiëren van de index

Afdwingen authentiseren/verifiëren van de index voordat door BCO-medewerker gegevens in dossiers worden ingevoerd.
Invoer van gegevens op aangeven van de index is pas mogelijk na een positieve test. Bij deze test is de index reeds geverifieerd aan de hand van geldig ID-bewijs.

28. Plausibiliteitschecks

Plausibiliteitschecks invoeren in de werkinstructie (bekende Nederlander, etc.). Bij twijfel dient door de BCO-coördinator meegekeken te worden (werkinstructie), eventueel wordt de index nogmaals benaderd.

29. Informatiebeveiligingsbeleid GGD GHOR Nederland

Uitgangspunt is onder meer het informatiebeveiligingsbeleid van GGD GHOR Nederland waarin onder meer aandacht wordt gegeven aan toereikende authenticatiemiddelen (MFA), gedragscodes en sanctiebeleid van GGD'en.

30. Dossiertoegang loggen

Periodiek wordt een analyse uitgevoerd op onrechtmatige/ongeautoriseerde inzage in dossiers. Hierover wordt verslag uitgebracht aan directie. Bij geconstateerde overtredingen treedt sanctiebeleid van de GGD in werking.

31. Inzicht in technische kwetsbaarheden

Voorkomen: Beheerst ontwikkel- en beheerproces en uitvoeren van (technische) penetratietesten op GGD Contact, de sluis en het BCO webportaal.

b. Detecteren en analyseren: Inrichten van IDS/IPS, SIEM oplossingen voor tijdig detecteren en analyseren van aanvallen. Linking pin hierbij is een (security) incident proces.
c. Acteren: Threat hunting, inrichting CERT
   Threat-hunting: Het proactief en iteratief zoeken in netwerken om geavanceerde bedreigingen te detecteren die bestaande beveiligingsoplossingen (proberen) te omzeilen en deze dreigingen succesvol te isoleren. Dit wordt gedaan door middel van hypothesegericht onderzoek en onderzoek op basis van bekende aanvalsindicatoren.
   Web application firewall met throtting: inkomende verbindingen worden gemonitord, met automatisch ingrijpen wanneer teveel (pogingen tot een) verbindingen worden opgezet door een andere computer op het internet.

32. Opzetten en implementeren van ICT-beheersprocessen

Opzetten en implementeren van ICT-beheerprocessen. De beheerorganisatie hiervoor wordt op dit moment uitgewerkt in afstemming tussen VWS en GGD GHOR.

33. Eisen ICT-beheerprocessen

Eisen ten aanzien van ICT-beheerprocessen 1-op-1 vertalen naar de contractuele afspraken met leveranciers ((sub-)verwerkers)

34. Afspraken over (gedeelde) verantwoordelijkheden

Concrete en duidelijke geformaliseerde afspraken over (gedeelde) verantwoordelijkheden ten aanzien van GGD Contact en het BCO webportaal.

35. Redundante uitvoering

Redundante uitvoering van essentiële systemen voor de GGD

36. Afstemming met RIVM protocol

Zorgen voor afstemming tussen het RIVM protocol en het proces van GGD Contact.

37. DPIA opstellen/vaststellen

Het periodiek en bij aanpassingen functionaliteit GGD Contact uitvoeren en vaststellen van een DPIA.

38. Vastlegging toestemming

Het vastleggen en documenteren van de wel/niet gegeven toestemming in GGD Contact.

39. Actief volgen van gelijksoortige Apps

Actief volgen van App-stores op gelijksoortige Apps en actie nemen indien nodig om deze kwaadaardige App te laten verwijderen.

40. Monitoring van verdacht gedrag

Monitoring (SIEM/SOC) van verdacht gedrag (bijvoorbeeld bij benaderingen vanuit het buitenland) op het gebruik identificatiecode.

41. Uitvoeren juridische checks

Door middel van het uitvoeren van juridische check(s) op o.a. de toepasselijkheid van EER wetgeving vs niet toepasselijkheid van EER-wetgeving (zoals American Cloudact e.a.) Eveneens juridische check(s) met betrekking tot het vaststellen of het een bedrijf uit de EER betreft.

42. Toelichting omtrent gebruik/toepassing vrije velden

Aan te geven in GGD Contact hoe om te gaan met een vrij veld (wat wordt precies verwacht van een toevoeging in een vrij veld of informatie omtrent het invullen van een vrij veld opnemen in de instructies die de BCO-medewerker telefonisch verstrekt aan de index.

43. Vrije velden verwijderen

Indien de informatie niet noodzakelijk is die wordt ingevuld in de vrije velden is een logische gevolgtrekking om de optie voor een vrij veld te verwijderen uit GGD Contact. Oftewel een beoordeling laten plaatsvinden van de noodzakelijkheid van de vrije velden en indien de noodzakelijkheid ontbreekt hierop acteren door het verwijderen van de vrije velden.
Een optie is het vrije veld vervangen door een keuzeveld met informatie die noodzakelijk is om te registreren in het kader van BCO.

44. Monitoring van verdacht gedrag

Monitoring (SIEM/SOC) van verdacht gedrag (bijvoorbeeld benadering vanuit het buitenland) op gebruik identificatiecode. Tevens het Implementeren van firewalls, inbraakdetectiesystemen (IDS), malware-sandbox en SIEM-systemen, welke doorgaans identificeren op basis van uitgevoerd onderzoek nadat er een waarschuwing is geweest voor een mogelijke bedreiging.

45. *Contracteren met partijen binnen EER*

Geen partijen contracteren die niet binnen de EER gevestigd zijn met hun hoofdkantoor en die geen maatregelen hebben getroffen om te voorkomen dat de data naar niet-EER landen gaan/verwerkt worden.

46. *Technische maatregelen databehoud binnen EER*

Technische maatregelen treffen om te voorkomen dat buitenlandse mogendheden en entiteiten bij de data kunnen.

47. *Bewaartermijn by design inrichten*

By design mogelijkheden onderzoeken om gegevens voor een bepaalde termijn houdbaar te maken in GGD Contact.

48. *Periodieke kwaliteitscontrole op (afwijkingen) van het dossier*

Zoals bijvoorbeeld rapportering door BCO-medewerker bij opvallen foutieve koppeling

49. *Instellen pincode voorafgaande toegang GGD Contact*

Toegang tot GGD Contact vooraf laten gaan door een zelf ingestelde pincode van de index.

50. *Rolverdeling VWS*

Vanuit gezamenlijke verantwoordelijkheid een convenant opstellen met de rol en verantwoordelijkheden van VWS daarin opgenomen.

51. *Versleuteling van data op het device*

Op het device van de index (telefoon/tablet) zal de data die de index heeft ingevoerd versleuteld worden opgeslagen waarbij gebruik gemaakt wordt van de beste versleutelingsmogelijkheden die het apparaat biedt. Dit betekent dat andere apps op het apparaat niet bij de gegevens kunnen komen en kunnen uitlezen wat er opgeslagen of verzonden is. Er is sprake van End-To-End versleuteling van de data in de GGD Contact-app waarbij de decryptie in het webportaal pas plaatsvindt. Tevens is het hierdoor niet mogelijk dat de aan het internet aangesloten ontvangende server (de sluis) informatie kan ontlenen aan de verzonden informatie.

52. *Attack surface minimization*

Een minimaal aantal API's aan de buitenkant van de sluis aanbieden die vanaf het internet beschikbaar zijn. Hierdoor is er geen mogelijkheid om vanaf het internet de "achterkant" van het systeem te benaderen.

53. *Toepassing TLS*

Transport versleuteling (TLS) op alle verbindingen. Waarbij wordt versleuteld conform de meest veilige standaard/stand van techniek.
Tevens een TLS pinning in de apps.

54. Certificaten vastleggen in applicatie

De gebruikte certificaten en/of de uitgever van het certificaat worden vastgelegd in de applicatie.

55. 2FA Identity Hub

Door middel van 2 factor authenticatie op de identity hub login is het zeker dat een medewerker niet alleen een username en password weet, maar tevens een geactiveerd device in het bezit heeft.

56. Ghost responses

Door gebruik te maken van ghost responses is het voor een hacker niet inzichtelijk of hij met een achterhaalde key succes heeft. Door gebruik te maken van niet van echt te onderscheiden antwoorden kan bij een niet-echte gebruiker (hacker) die een verzoek doet voor informatie wel een antwoord worden teruggegeven. Hierdoor is op het passief netwerk niveau niet te ontdekken of dit correcte data is.

57. Encryptie (at rest)

Encryptie van de (gevoelige) velden voordat deze in de database terecht komen. In de applicatie worden (privacygevoelige) velden versleuteld opgeslagen (zie hiervoor ook versleuteling van data op het device).
Tevens at rest encryptie van secrets, data en logging. Hiermee wordt voorkomen dat er toegang tot de data mogelijk is.

58. Aanvulling van de privacyverklaring n.a.v. nieuwe functionaliteiten

De privacyverklaring moet worden aangevuld met een toelichting op de Functionaliteit Zelf-BCO.

59. *Vaststelling DPIA/noodzakelijkheid regulier BCO*

In de referentie DPIA v1.1 wordt uitgegaan van een privacy risicoanalyse die gedaan is op het reguliere BCO-proces. Deze risicoanalyse is nodig om de noodzaak van de uitgevraagde gegevens te toetsen. Als blijkt dat de noodzaak niet kan worden onderbouwd, moet de functionaliteit gewijzigd worden.

E. Bijlagen

Bijlage 1 – Beschrijving Releases

Release 1.1

Wat doet de eerste release van het BCO Portaal?

(beschrijving van 12 april 2021)

Volledige BCO vragenlijst index

Epic-naam: volledige vragenlijst inclusief contacten

Een volledige gespreksondersteunende BCO vragenlijst. De vragenlijst volgt de opbouw van het indexgesprek. In de vragenlijst zijn de vragen voor de verslaglegging bij de GGD en de Osiris melding voor het RIVM gecombineerd. De vragenlijst bestaat uit de volgende onderdelen:

- **Over de index**
  - Index/dossiergegevens (naam + HPZone nummer, testdatum)
  - Contactgegevens index
  - Contactgegevens alternatief contact
  - Voorkeurstaal communicatie
  - Opmerkingen/bijzonderheden BCO gesprek
- **Medische gegevens**
  (op basis van antwoorden op deze vragen worden besmettelijke periode, bronperiode en (minimale) isolatieperiode uitgerekend en getoond in een kalender die in hele dossier zichtbaar is)
  - COVID19 symptomen, ziekteverloop
  - Eerste ziektedag en test, aanleiding testen, herbesmetting
  - Vaccinatie
  - Gegevens evt ziekenhuisopname
  - Onderliggend lijden, zwangerschap, post-partum
  - Medicijnen en/of immuunrisico
  - Vastleggen gegevens huisarts
- **Woon & werkgegevens**
  - Alternatief verblijfadres
  - Index woont in instelling / AZC of andere risicolocatie
  - Mogelijkheid tot thuisisolatie
  - Werkgegevens (bedrijfsnaam, sector, vervolgvragen als index in besmettelijke periode gewerkt heeft)
  - School, kinderdagverblijf, gastouder incl hint om aan te maken als context
- **Brononderzoek**
  - Vastleggen van positief geteste bronpersonen (incl hpzone nummer), bronpersonen met coronagerelateerde klachten en aangeven welke een waarschijnlijke bron is.
  - Vastleggen broncontexten + bezoekdata, relatie tot context en of context waarschijnlijke besmettlingslocatie is.
  - Vastleggen settings die meestal geen context zijn (thuissituatie / bezoek, etc).
  - Buitenlandreizen (datums, landen, vervoermiddelen)
- **Contactonderzoek**
  - Link naar CoronaMelder portaal
  - Vastleggen contacten binnen besmettelijke periode
  - Schatting aantal categorie 3 contacten
  - Vastleggen contexten binnen besmettelijke periode
  - Link naar meldportaal GGD Kennemerland voor vliegreizen in besmettelijke periode

- **Afronden & status**

- Overzicht van alle verzamelde contacten en contexten
- HPZone: Voor-ingevulde tabellen voor diagnostic notes en events index
- HPZone: Voor-ingevulde tabellen voor contexten en contacten
- De voor-ingevulde tabellen kunnen door de BCO-er naar het dossier van de index in HPZone worden gekopieerd.

Gestandaardiseerde zoekfunctie locaties/contexten

Epic-naam: Contexten

- Voor het vastleggen van contexten in bron- en besmettelijke periode maken we gebruik van een door VWS ontwikkelde schil om Google Maps en BAG voor het toevoegen van nieuwe ad-hoc contexten. Die zijn daarmee altijd voorzien van een uniforme naamgeving en actuele adresgegevens.
- Contexten in het BCO portaal zijn gestructureerd tot op afdelingsniveau. Bezoek datums en tijden worden gestructureerd vastgelegd.

Beknopte vragenlijst huisgenoten en nauwe contacten

Epic-naam: volledige vragenlijst inclusief contacten

- Vastleggen persoonsgegevens, aanvullen contactgegevens
- Vastleggen wie een contact informeert (GGD/Index)
- Verslag contactgesprek (klachten, vaccinatie, coronatest gedaan ja/nee)
- Vastleggen of een contact geïnformeerd is.

Cases die niet zijn afgerond aan anderen kunnen toewijzen

Epic-naam: nvt

- Gebruikers met de rol werkverdeler hebben een overzicht van cases waarvan het bco nog niet is afgerond en die op dit moment niet aan een specifieke medewerker zijn toegewezen. Deze cases kunnen worden toegewezen aan een medewerker.
- Gebruikers met de rol werkverdeler kunnen zien welke medewerkers met welke cases bezig zijn. Mochten ze daarin een medewerker tegenkomen die vandaag niet werkt, dan kunnen ze de case toewijzen aan een andere medewerker.

GGD Contact app met Zelf BCO mogelijkheid

Epic-naam: ZelfBCO App

Voor indexen is de GGD contact app beschikbaar. Die kan op twee manieren gebruikt worden.

1. Voorafgaand aan het BCO gesprek. De index download de app direct na het vernemen van de positieve testuitslag. In de app wordt met behulp van een aantal vragen de besmettelijke periode vastgesteld (EZD of testdatum bij geen symptomen) en met behulp van een aantal geheugensteuntjes een reconstructie gemaakt van ontmoetingen in de besmettelijke periode. De gevonden contacten worden met behulp van een beslisboom gecategoriseerd in de juiste categorie (1,2a/2b/3a/3b) en per contact is obv de laatste contactdatum meteen het juiste advies zichtbaar. De index kan dit contact telefonisch doorgeven aan het contact, of via een zelfgekozen digitaal kanaal (copy/paste -- we mogen dit niet vanuit de app faciliteren).

   De EZD, symptomen en verzamelde contacten zijn tijdens het BCO gesprek met een GGD-er die het portaal gebruikt eenvoudig en veilig over te zetten naar het BCO portaal, en kunnen daar meteen verder verwerkt worden.

2. Na afloop van het eerste BCO gesprek. De index kan de tijdens het BCO gesprek geïnventariseerde contacten bekijken, contactgegevens aanvullen en deze gebruiken om het contact a) zelf te informeren of b) de gegevens met de GGD te delen. Deze functionaliteit is bruikbaar in alle fases van het BCO waarin GGD samen met index de contactinventarisatie doet. In fase 1/2a zijn de door de index aangeleverde gegevens bovendien te gebruiken om contact op te nemen met huisgenoten/nauwe contacten.

Bijlage 2 - Procesflow GGD Contact

Het proces voor deze DPIA start op het moment dat de index de GGD Contact-app gaat downloaden voor de volledigheid is ook het proces van de index voorafgaand aan het downloaden van de GGD Contact-app weergegeven. De voorgaande stappen hebben betrekking op de index die wacht op zijn of haar testresultaat naar aanleiding van een coronatest.
Met betrekking tot onderstaande procesflow wordt per aangegeven stap het volgende toegelicht:

- App downloaden

De index wordt door de BCO-medewerker gevraagd om GGD Contact te downloaden. Dit kan na het verkrijgen van een positief testresultaat en/of tijdens het eerste BCO-gesprek.

- Eerste BCO-gesprek/ Tijdlijn creëren / Contacten inventariseren

In het eerste telefoongesprek met de BCO-medewerker wordt een eerste inventarisatie gemaakt van de personen met wie de index in contact is geweest. De tijdlijn wordt gecreëerd wanneer de klachten van de index zijn begonnen en met wie hij in deze periode in contact is geweest.

- Contacten classificeren

Door de BCO-medewerker vindt een eerste risicoclassificatie plaats ten aanzien van de contacten van de index. Aan de hand van hoelang en wat voor een soort contact de index met het contact heeft gehad wordt bepaald of het contact een huisgenoot, nauw contact of overig contact is. Dit bepaalt op een later moment welk handelingsperspectief er met het contact gedeeld dient te worden.

- Contactgegevens inventariseren in de app

Vervolgens vraagt de BCO-medewerker aan de index of hij de reeds opgestelde contactenlijst verder kan aanvullen in de app. Door middel van de activatiecode die de index door de BCO-medewerker verkrijgt is de contactenlijst zichtbaar in de GGD Contact-app bij de Index.

- Monitoren status contactgegevens en informeren

De BCO-medewerker kan vanaf het moment dat de contactenlijst naar de index is gestuurd tot aan het moment de index de gegevens heeft aangeleverd in het webportaal zien of de index gegevens al reeds heeft gedeeld met de GGD of niet. De BCO-medewerker kan niet zien welke gegevens de index wel of niet heeft ingevuld, dit is pas mogelijk op het moment dat de index in de GGD Contact-app op de knop 'gegevens delen met GGD' klikt. In de tussentijd ziet de BCO-medewerker enkel een status staan zoals 'in behandeling'.

- Contactpersonen informeren

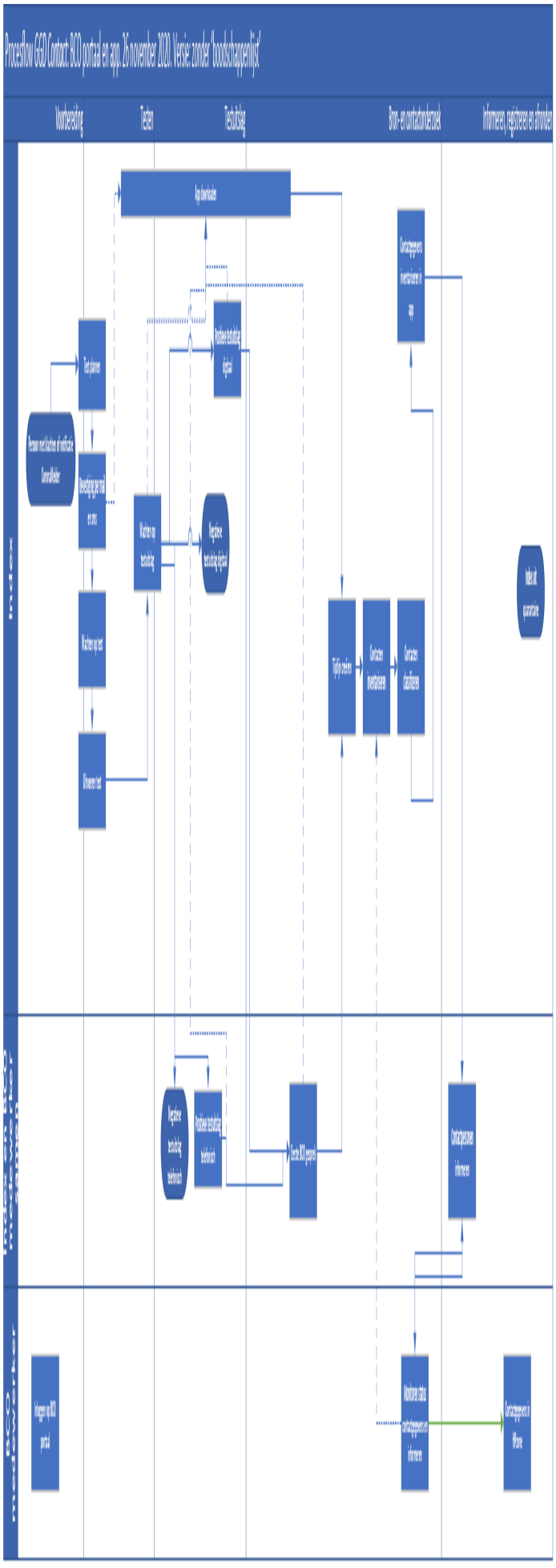
Indien de gegevens zijn aangeleverd door de index kan de BCO-medewerker een inventarisatie maken welke contacten geïnformeerd dienen te worden. Deze contactpersonen zullen worden geïnformeerd dat zij in contact zijn geweest met iemand die positief getest is op COVID-19 en nadere informatie krijgen in de vorm van een handelingsperspectief.

- Contactgegevens in HPZone

Wanneer de contactenlijst volledig is ingevuld in de GGD Contact-app kan de BCO-medewerker deze lijst vanuit het webportaal kopiëren naar HPzone. Hier wordt het dossier van de index bijgehouden.

- Index uit quarantaine

Tenslotte zal de index uit quarantaine of thuisisolatie gaan.



* Release 1.1 zonder RPA

4– Achtergrond risiconiveaus

In deze bijlage is opgenomen hoe het risiconiveau van de omschreven risico's is bepaald.

Kans

Bij het bepalen van de kans (K) dat een risico zich voordoet worden de volgende factoren in acht genomen:

- Het bestaan van gemotiveerde en bekwame actoren met bijbehorend hun motivaties en vaardigheden;
- Aard van het risico; en
- Aanwezig zijn van mitigerende maatregelen en hun effectiviteit.

De kans dat een risico voor Betrokkene zich voordoet wordt omschreven als hoog, midden, of laag. De onderstaande tabel beschrijft deze drie lagen.

Kans	Kans beschrijving
Hoog	Het risico voor Betrokkene zal zich zeker manifesteren indien: • Een kwaadwillende minimale inzet doet hiertoe; of • Een medewerker onbewust nalatig handelt of een fout maakt; of • Het inherent is aan het risico dat deze zich manifesteert.
Midden	Het risico voor Betrokkene zal zich wellicht manifesteren indien: • Een kwaadwillende voldoende middelen inzet; of • Een medewerker bewust nalatig is of opzettelijk handelt; of • Het zeer waarschijnlijk is vanwege de aard van het risico
Laag	Het risico voor Betrokkene zal zich enkel manifesteren indien: • Een kwaadwillende buiten proportionele middelen inzet; of • Een medewerker bewust zeer nalatig of opzettelijk handelt; of

Impact

De impact van een geëffectueerd risico wordt beschreven in termen van de mogelijke schadelijke gevolgen die de Betrokkene kan ondervinden.

Impact niveau	Impact Beschrijving
Hoog	1. Kan de reputatie of belang van de Betrokkene significant schaden, compromitteren of belemmeren; 2. Kan resulteren in sterfte of ernstig letsel; 3. Kan een grote inbreuk opleveren in de fundamentele rechten en vrijheid van Betrokkene
Midden	1. Kan de reputatie of belang van de Betrokkene schaden, compromitteren of belemmeren; 2. Kan resulteren in persoonlijk letsel;

	3. Kan een inbreuk opleveren in de fundamentele rechten en vrijheid van Betrokkene
Laag	1. Kan resulteren in beperkte materiële schade; 2. Kan de reputatie of belang van de Betrokkene schaden 3. Kan een kleine inbreuk opleveren in de fundamentele rechten en vrijheid van Betrokkene

Vervolgens vindt er een risico-calculatie plaats, waarna op basis van de risiconiveaus wordt bekeken welke soort maatregelen verwacht worden per niveau. Dit is reeds eerder beschreven in de DPIA.

Bijlage 4 – Logging

Logging van BCO-portaal zal plaatsvinden conform de vereisten en doeleinden van de NEN 7510 e.v.

Meer specifiek bevat dit de volgende persoonsgegevens:

- Accountgegevens
- Gegevens om de Gebruiker te identificeren;
- Systeemactiviteiten van de Gebruiker;
- Data, tijdstippen en details van belangrijke gebeurtenissen, bijv. in- en uitloggen;
- Identiteit of indien mogelijk de locatie van de apparatuur en de systeemidentificatie;
- Registratie van geslaagde en geweigerde pogingen om toegang te verkrijgen tot het systeem;
- Registratie van goedgekeurde en geweigerde gegevens en overige pogingen om toegang te verkrijgen tot bronnen van informatie.
- Systeemconfiguratieveranderingen;
- Gebruik van speciale bevoegdheden;
- Gebruik van systeemhulpmiddelen en -toepassingen;
- Bestanden die zijn geopend en het type toegang dat is verkregen;
- Netwerkadressen en -protocollen;
- Alarmen die worden afgegeven door het toegangsbeveiligingssysteem;
- Activering en de-activering van beschermingssystemen, zoals antivirussystemen en inbraakdetectiesystemen;
- Verslaglegging van transacties die door gebruikers in toepassingen zijn uitgevoerd.
- Case regio
- Regio BCO-Portaal Gebruiker
- Rol BCO-Portaal Gebruiker
- IP-adres BCO-portaal gebruiker

Van de App-gebruiker wordt een unieke ID gegenereerd bij het uploaden naar het BCO-portaal en deze unieke ID wordt gelogd.

Bijlage 5 – Advies Functionaris Gegevensbescherming (FG) GGD Hart voor Brabant

GGD GHOR Nederland heeft een referentie DPIA uitgevoerd op de gegevensverwerkingen in GGD Contact Zie voor de aanleiding de inleiding in onderhavige DPIA-rapport.

De Functionaris Gegevensbescherming is op tijd betrokkenen bij het DPIA-proces. Er vindt periodiek overleg plaats met GGD GHOR, VWS en alle FG's van de GGD'en. In de eerdere sessies is aandacht besteed aan de deelonderwerpen: governance, AVG-rollen, grondslag en doelbinding, securitymaatregelen en de scope van de 1.1 release.

De DPIA GGD Contact 1.1 is gebaseerd op de DPIA GGD Contact 1.0 + addenda, die reeds door de FG's van de praktijktestregio's zijn gereviewd en is in samenwerking met de landsadvocaat tot stand gekomen. De reviews van die FG's zijn verwerkt in de DPIA 1.1 (huidige versie). Vervolgens is het concept DPIA-rapport 1.1. aan de GGD'en in het land voorgelegd, waarop de FG heeft gereageerd. Deze tussentijdse adviezen de FG's van de GGD'en zijn in het DPIA-proces opgepakt en in het DPIA-rapport bijgesteld.

De Functionaris Gegevensbescherming is ervan overtuigd dat deze DPIA en daarmee de gegevensverwerking in GGD Contact met uiterste zorg is voorbereid en passende maatregelen zijn genomen om met betrekking tot gegevensverwerking te voldoen aan de vereisten van de AVG. De Functionaris Gegevensbescherming ziet daarom ook geen bezwaren om de verwerking in GGD Contact overeenkomstig deze DPIA uit te voeren en onderschrijft het DPIA-rapport en de daarin voorgestelde maatregelen.

<u>De Functionaris Gegevensbescherming adviseert de verwerkingsverantwoordelijke als volgt:</u>

- Compliance borgen binnen de organisatie d.m.v. het inrichten van een governancestructuur (leveranciersmanagement). Opzetten en implementeren van procedures en afspraken over verantwoordelijkheden -> governance en compliance breed inrichten. Op de korte termijn verduidelijken en vastleggen van de beheertaken van GGD GHOR Nederland.
- Nagaan of alle overeenkomsten m.b.t. GGD Contact zijn ondertekend en gearchiveerd.
- FG adviseert op de website een duidelijk privacy statement GGD Contact op te nemen, zodat aan de informatieplicht vanuit de AVG wordt voldaan. Belangrijk is dat in het statement is opgenomen dat het gebruik van GGD Contact vrijwillig is.
- De toegang tot het BCO-portaal vindt plaats nadat een Gebruiker de autorisatie daartoe heeft vergekregen via de GGD waarvoor de Gebruiker werkzaam is. Het portaal is benaderbaar via een weblink. De autorisaties worden vergeven op basis van een autorisatiematrix. De autorisatiematrix is afgestemd met de product owners van de GGD'en. FG adviseert het inrichting van een autorisatiematrix en de controle op deze matrix bij door- en uitstroom van medewerkers.
- Gelet op de aard en omvang van de verwerking is het belangrijk dat de GGD passende technische en organisatorische maatregelen neemt. FG adviseert om de beschreven

maatregelen in de DPIA strikt na te leven. Hieronder volgt een samenvatting van de belangrijkste maatregelen voor de GGD Hart voor Brabant:

- Duidelijke informatieverstrekking door de BCO-medewerker waarbij informatie wordt gegeven over het gebruik van de GGD Contact en werking van de code inclusief de geldigheidsduur. Inherent hieraan is het goed opleiden van de BCO-medewerkers om ervoor te zorgen dat eenduidige instructies
- Duidelijke instructie voor de BCO-medewerker hoe de gegevens in het BCO webportaal te koppelen (zowel digitaal als handmatig) aan de index (via casenummer).
- Plausibiliteitschecks invoeren (bekende Nederlanders etc.). Bij twijfelt dient door de BCO-coördinator meegekeken te worden (werkinstructie), eventueel wordt de index nogmaals benaderd. Hiervoor dient een werkbare definitie te worden opgesteld, indien nog niet aanwezig ter voorkoming van dubbel werk voor de coördinator.
- Training BCO-medewerkers m.b.t. juist en ethisch gebruik gegevens.
- Antecedentenonderzoek nieuwe medewerkers (ook bij samenwerkingspartners)

Tijdens het ontwerp van GGD Contact zijn aandachtspunten/acties naar voren gekomen die betrekking hebben op veilig gebruik van een webapplicatie met medische informatie (BCO-portaal) en getroffen moeten worden door de GGD omdat ze de basis vormen voor de beveiliging van de keten (en daarmee de applicatie). Het gaat om de volgende acties:

- Hanteer eisen, pas maatregelen toe en richt toezicht in voor de beveiliging van de BCO werkplekken conform NEN 7510. Stel gebruikers op de hoogte hoe ze veilig kunnen werken.
- Richt auditlogging in voor de active directory (AD) of directory service, conform 7513.
- Controleer periodiek of alle toekomstige en huidige gebruikers voor het portaal een uniek AD gebruikersaccount hebben.
- Controleer periodiek of alle toekomstige en huidige gebruikers voor het portaal een VOG hebben.
- Controleer of alle toekomstige en huidige gebruikers voor het portaal een geheimhoudingsverklaring hebben getekend
- Houd het Join-Move-Leave proces bij: Elke wijziging aan rollen vertrekkende medewerkers (leave), medewerkers met een andere rol (move) en nieuwe medewerkers (join) moet direct worden verwerkt in de AD.
- Controleer periodiek of alle huidige gebruikers de juiste rollen hebben toebedeeld gekregen.
- Meld incidenten bij de helpdesk van GGD Contact.
- Registreer incidenten op het gebied van onrechtmatig gebruik van de corona gerelateerde applicaties.

Wob-verzoek SOLV/ICAM datalek 2021 coronasysteem

11.0 Tekst Wob-verzoek en register documenten

Tekst verzoek (xii)

Informatie over de overname van het beheer van HPZone (Lite) door GGD GHOR

Register

Geen documenten aanwezig.

Wob-verzoek SOLV/ICAM datalek 2021 coronasysteem

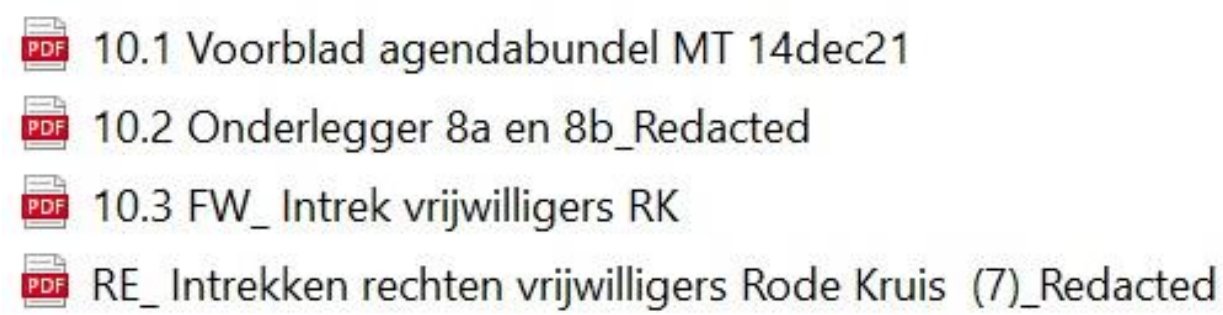
10.0 Tekst Wob-verzoek en register documenten

Tekst verzoek (x)

Informatie over signaleringen van gebreken of kwetsbaarheden in de (informatie)-beveiliging in het kader van het testen, vaccineren en bron- en contactonderzoek, en de wijze waarop daarop is gereageerd en welke maatregelen daarop zijn genomen, waaronder signaleringen van (externe) GGD-medewerkers en van medewerkers van VWS, zoals mevrouw Lieke de Reus, en van externe experts.

Register

Een screenshot van de verkennerpagina van map 10:



xxx

Bundel van de MT GGD WEST BRABANT van 14 december 2021

Agenda bijlagen

agenda MT GGD WB 14 december 2021.docx

1 Opening

2 Mededelingen

- agenda MT GGD WB 21 december 2021.docx
- 2. Verslag MT WB 20211123.docx
- 2.1 Aanvulling op het Strategisch Overleg vorige week dinsdagmorgen 20211123.docx

3 Verlenging contracten Astorium ([redacted] & [redacted]
[redacted]

- 3. 202112147 Aanbiedingsformulier MT GGD WB_verlenging inzet [redacted] (DEF).docx

4 Werkbegroting 2022 2e sessie
[redacted]

- 4. Aanbiedingsformulier MT werkbegroting 2022 14dec.docx
- 4.1 bijlage MT aanbiedingsformulier.xlsx

5 Directiebeoordeling (ca. 30 minuten)
[redacted]

- 5. Besluitenlijst directiebeoordeling 2021 (002)_[redacted].docx
- 5.1 Verslag Directiebeoordeling 2021.docx
- 5.2 2021 Onderlegger 4, Klanttevredenheid en klantfeedback.docx
- 5.3 2021 Onderlegger 8, AVG en informatiebeveiliging.docx
- 5.4 Factsheet directiebeoordeling 2021.pdf

6 Afspraken CNS vs. reguliere GGD
[redacted]

7 Rondvraag en sluiting

Onderlegger 8a. Algemene Verordening Informatiebeveiliging (AVG)

Opsteller: [redacted]

Onderwerp *De voortgang wordt vastgelegd aan de hand 12 punten op basis van het stappenplan van de Autoriteit Persoonsgegevens*	**Uitkomst/resultaten analyses** *Wat zijn de belangrijkste uitkomsten?*	**Verklaring en beoordeling uitkomsten/resultaten** *Hoe is het te verklaren en wat vinden we ervan (afgezet aan beleid en strategie GGD West Brabant?*	**Maatregelen** *Welke verbetering voeren we door?*
1. Informeren / transparantie / informatieplicht	De AVG kent een informatieplicht richting betrokkenen. Bij nieuwe verwerkingen wordt de website vaak aangevuld met nieuwe informatie. De GGD raakt meer afhankelijk van landelijke bronnen.	GGD collega's zijn meer gewend aan het principe van het (schriftelijk) informeren van mensen als er iets over hun wordt verwerkt. Soms worden ze nog getipt door de [redacted] en [redacted]	1.1 Beleg deze verantwoordelijkheid van het actualiseren of aanvullen van informatie op de website over verwerkingsactiviteiten bij de betrokken portefeuillehouder van het team. Voer een risicoanalyse (DPIA) uit of stel een reeds opgestelde risicoanalyse bij. → doorlopende activiteit.
2. Overzicht verwerking en wettelijke grondslag (datamanagement) - **Waaronder bestaande contracten / verwerkersovereenkomsten / leveranciers management**	Mede als gevolg van Corona zijn er veel nieuwe ontwikkelingen en verwerkingen bij gekomen (bijv. team infectieziekte bestrijding en team onderzoek). Het zogenaamde 'register van verwerkingsactiviteiten' dat moet zorgen voor een overzicht van welke persoonsgegevens er binnen de GGD worden verwerkt, wordt niet (consequent) geactualiseerd. De verwerkersovereenkomst met GGD Amsterdam m.b.t. Formatus is nog niet bekrachtigd. De (concept) samen werkersovereenkomst m.b.t. Formatus tussen de GGD'en Zeeland, HvB en WB is nog niet bekrachtigd.	Het register van verwerkingsactiviteiten betreft een Excel bestand bestaande uit verschillende tabbladen (voorstellende de teams). Het register van verwerkingsactiviteiten wordt niet regelmatig geactualiseerd; - niet duidelijk is welke functionaris binnen het team met deze taak belast is - Excelbestand is gevoelig voor vervuiling Hierdoor raakt de GGD het zicht kwijt op 'wat voor data we allemaal in huis hebben' en of de verwerkingen wel rechtmatig zijn.	2.1 Registreer nieuwe, significante onderzoeksprojecten, die kwalificeren als verwerking van persoonsgegevens, structureel in het register van verwerkingsactiviteiten van het team. → doorlopende activiteit. 2.2 Beleg deze verantwoordelijkheid van het actualiseren van het register van verwerkingsactiviteiten (de 'data boekhouding') bij de betrokken functionaris van het team. Dit kan als 'brengplicht' (zie ook 1.1), d.w.z. de portefeuillehouder geeft zelf een seintje als er iets wijzigt en wat er wijzigt. De [redacted] kan eventueel samen met de portefeuillehouder de aanpassingen doorspreken en doorvoeren. → nog niet in gang gezet, nog op zoek naar PMS. We werken nu met excelbestanden en dat is erg foutgevoelig.

		Bij een eventuele controle kan de GGD geen actueel overzicht van verwerkingen overleggen Door drukte en andere prioriteitstelling worden overeenkomsten niet altijd geactualiseerd of afgesloten.	2.3 Neem een bescheiden werkproces op in het kwaliteitshandboek dat ziet op het actualiseren van het register van verwerkingsactiviteiten door het team. → nog niet in gang gezet, nog op zoek naar PMS. We werken nu met excelbestanden en dat is erg foutgevoelig. 2.4. Bekrachtig de verwerkersovereenkomst tussen de GGD WB en GGD Amsterdam. → is opgesteld maar nog niet bekrachtigd door MT. 2.5. Bekrachtig de verwerkersovereenkomst tussen de GGD WB en GGD Zeeland en HvB. → is opgesteld maar nog niet bekrachtigd door MT.
3. Rechten van betrokkenen	Betrokkenen maken gebruik van hun rechten. Met name het recht op inzage en het recht op verwijdering van hun (medische) gegevens. Het betreft hier vooral verzoeken n.a.v. Corona. Processen en procedures zijn opgesteld en geïmplementeerd.	A.g.v. grote datalekken begin 2021 binnen de GGD'en heeft een groot aantal burgers gebruik gemaakt van haar rechten. Dit heeft er mede in geresulteerd dat een [redacted] zijn aangetrokken waardoor de [redacted] (Functionaris Gegevensbescherming) zijn onafhankelijke en toezichthoudende rol kan vervullen.	3.1. Rechten van betrokkenen kunnen ook worden uitgeoefend op de reguliere zorg. Er bestaat geen inzicht in hoeveelheid van aanvragen, behandeling en wijze van opvolging. Stel een proces en procedure zodat er inzicht en transparantie is m.b.t. verzoeken. Neem tevens op de mandatering c.q. autorisatie bij vervanging. → heeft prioriteit irt maatschappelijke kritische houding.
4. Privacy by design en privacy by default - **DPIA (Risico's)** - **Communicatie, privacyverklaring en cookies**	Het uitgangspunt is dat de verwerkingsverantwoordelijke verplicht is een DPIA uit te voeren voordat met de verwerking van persoonsgegevens wordt begonnen in het geval dat er sprake is van: gevoelige gegevens of gegevens van zeer persoonlijke aard, op grote	Er is nog te weinig kennis en bekendheid over het fenomeen 'DPIA'. De organisatie heeft de uitvoering van de DPIA nog niet 'in de vingers'. Teams worden op praktische	4.1 Stel vast van welke verwerkingen er op welk moment een DPIA moet zijn uitgevoerd. 4.2. Betrek in het voortraject (voornemen tot onderzoek / aanschaf applicatie e.d.) de

	schaal verwerkte gegevens, matching of samenvoeging van datasets, gegevens met betrekking tot kwetsbare betrokkenen DPIA uitgevoerd voor Formatus, Gezondheidsmonitor, Mynvea, Wijkgericht werken	wijze ondersteund door de [redacted]	[redacted] → dit moet afgestemd worden met inkoop.
5. [redacted] / Governance	Een [redacted] en een [redacted] zijn aangesteld (tijdelijke basis)	De [redacted] ondersteunt bij het opstellen van verwerkersovereenkomsten, uitvoeren van DPIA (risico analyse) en het creëren van awareness.	5.1. Neem een besluit rondom de wijze waarop de rol van [redacted] & [redacted] structureel wordt geborgd: • Samen met andere GGD'en roulerend • Vast contract / vast aantal uren voor [redacted] / [redacted]
6. Meldplicht datalekken	Icm MIC, archivering melding autoriteit (archivering) Inbreuk in verband met persoonsgegevens, zeker daar waar het kinderen betreft worden gemeld bij de autoriteit persoonsgegevens.	In de periode januari / september 2021 zijn er 9 datalekken opgetekend.	6.1. Zorg voor één centraal punt in de organisatie vanwaar de meldingen aan de Autoriteit Persoonsgegevens geschiedt (b.v. beleg deze taak bij de [redacted] 6.2. Bewaak transparatie en opvolging van de melding en genomen maatregelen.
7. Toestemming	Loopt, continue proces.	De GGD ontleent haar rechtsgrondslag voor verwerking van persoonsgegevens in de meeste gevallen op basis van haar wettelijke taken.	n.v.t.
8. Privacy beleid	Privacybeleid is in 2021 herschreven. Dit dient nog wel vastgesteld te worden.	A.g.v. het oude beleid heeft het nieuwe privacybeleid meer handvatten op e.e.a. aan te sturen in de organisatie	8.1. Communiceer het beleid en draag het verder uit. 8.2. Plaats het thema Privacy structureel op de MT-agenda.
Onderwerp	**Hoe tevreden ben je over de opzet en uitvoering? Brengt het ons voldoende?**	**Welke risico's en welke verbeterkansen zie je en wat is daarvoor nodig?**	

Overall conclusie proces/systeem: opzet en uitvoering van AVG beleid	Er gaat veel goed, het is een organisatie in ontwikkeling. 1. De hoogste prioriteit heeft de ontvlechting van Kidos (splitsing applicatie door BC). 2. Het verwerkingsregister dient volledig, actueel en betrouwbaar te zijn. 3. Het datalekregister dient volledig, actueel en betrouwbaar te zijn en maatregelen dienen opgevolgd te worden.	- Het is niet ingebed in de teams en er is geen aanspreekcultuur, dit maakt het onderwerp niet aantrekkelijk. - We hebben veel gevoelige informatie over kwetsbaarheid. Dat maakt het extra belangrijk. 1. Groot datalek, met veel betrokkenen en kwetsbare personen. 2. Je voldoet niet aan de wetgeving -> grote kans op hoge boete 3. Je voldoet niet aan de wetgeving -> grote kans op hoge boete

Onderlegger 8b. Informatiebeveiliging

Opsteller: [redacted]

Onderwerp	**Uitkomst/resultaten analyses** *Wat zijn de belangrijkste uitkomsten?*	**Verklaring en beoordeling uitkomsten/resultaten** *Hoe is het te verklaren en wat vinden we ervan (afgezet aan beleid en strategie GGD West Brabant?*	**Maatregelen** *Welke verbetering voeren we door?*
1 Risicobeheersing	(+) O.a. door datalekken en daaropvolgende maatregelen is er zowel landelijk, regionaal en binnen GGD WB meer aandacht voor informatiebeveiligingsrisico's. (-) Vastlegging van risico's is nog versnipperd en beoordeling + verbeterplannen zijn nog niet afgerond. (+) Begin gemaakt met het beoordelen van risico's voor kritische applicaties (KPMG project + GGD Ghor NL) (-) Te weinig voortgang in mitigeren van risico's (-) Beoordeling van informatiebeveiligingsrisico's geen vast onderdeel van projecten / wijzigingsbeheer	(+) Zeer veel riscio's geïnventariseerd (-) Nog geen expliciete keuzes gemaakt m.b.t. prioriteit van behandelen. Teveel risico's die een klein beetje aandacht krijgen. (-) Te weinig capaciteit en financiële middelen om risico's te behandelen. (-) Geen formeel change proces en geen projectaanpak waarin aandacht voor IB is geborgd.	1.1 Formaliseer en standaardiseer wijzigingsbeheerproces en project-aanpak en borg aandacht voor informatiebeveiliging en privacy hierin. 1.2 Budgeteer structureel meer middelen voor het inventariseren, beoordelen en behandelen van risico's. Hou rekening met onzekerheid c.q. onverwachte risico's die (direct) actie vereisen. 1.3 Stel middelen beschikbaar en plan deadline voor het implementeren van een managementsysteem voor informatiebeveiliging (ISMS) en het implementeren van de NEN 7510 beheersmaatregelen. 1.4 Implementeer software voor risicomanagement (onderdeel oplossing voor managementsysteem). 1.5 Beleg portefeuillehoudersrol m.b.t. informatiebeveiliging in de teams. Zorg voor voldoende kennis en tijd om er ook echt aandacht aan te besteden.

2 Bewustwording	(+) Door (tijdelijke) uitbreiding van het team PIM met [redacted] / [redacted] en projectleider is meer aandacht voor het onderwerp (+) Begin gemaakt met communicatie-site in Sharepoint m.b.t. informatiebeveiliging. (-) Nog beperkt aandacht voor meetbaar maken en vergroten awareness bij alle medewerkers.	Maken van aantrekkelijke en effectieve content / tests is tijdrovend. Awareness campagne vanuit GGD Ghor NL (#SamenZeker) waarop GGD WB heeft ingeschreven is er niet gekomen.	2.1 Schaf (samen met andere GGD'en) een toolkit (online platform + content) aan voor het trainen van medewerkers (nieuw en bestaand) en het toetsen van kennis / houding / gedrag. Door dit samen met andere GGD'en te doen gaan kosten omlaag en kwaliteit omhoog. Periodiek actuele content toevoegen. Verschillende tools inzetten afhankelijk van niveau en functie van medewerkers. 2.2 Maak van informatiebeveiliging en privacy een terugkerende agenda onderwerp op alle niveaus in de organisatie.
3 Kritische leveranciersbeheer	(+) Veel aandacht voor risico's en maatregelen m.b.t. landelijke systemen en hun leveranciers binnen GGD Ghor NL. Kennis gedeeld in [redacted] spreekuur (+) Team van specialisten (SOC) die landelijke systemen en omgeving monitoren en actie ondernemen in geval van verdacht gedrag. (-) Verantwoordelijkheidsverdeling tussen leverancier en GGD, GGD GHOR NL op het gebied van beheer van (nieuwe) applicaties niet altijd schep en niet op schrift.	(-) Te weinig capaciteit bij applicatiebeheer om voldoende aandacht te besteden aan taken op het gebied van informatiebeveiliging.	3.1 Schriftelijke afspraken maken met (kritische) leveranciers en, of GGD GHOR NL over verantwoordelijkheidsverdeling op het vlak van beheer, datagebruik, informatiebeveiliging en privacy 3.2 Beoordelen en waar nodig proberen bij te stellen van contractuele afspraken op het gebied van informatiebeveiliging met leveranciers van kritische (zorg)applicaties. 3.3 Plannen en uitvoeren leveranciers-beoordelingen op het gebied van informatiebeveiliging (o.a. opvragen en beoordelen certificaten / eventueel gebruik maken van auditrecht)

	(-) Nog geen periodieke beoordeling van prestaties van leveranciers op het gebied van informatiebeveiliging.		3.4 Zorg structureel voor voldoende capaciteit (applicatiebeheer / [redacted] / [redacted] voor het uitvoeren van taken op het gebied van informatiebeveiliging en privacy O.a. leveranciersbeoordeling, controle logging, en controle toegangsrechten.
4 Interne audits informatieveiligheid	(+) Nulmeting NEN 7510 uitgevoerd door [redacted] en NEN 7510 self assessment binnen KPMG project. (+) Onafhankelijke [redacted] + [redacted] + [redacted] (-) Geen periodieke interne audits op het gebied van informatiebeveiliging (verplichting NEN 7510 en BIO).	(-) Interne auditors zijn niet geschoold om te auditen op risico's op het gebied van informatiebeveiliging.	4.1 Stel interne auditplanning op voor informatiebeveiliging voor 2022 e.v. 4.2 Kies om te beginnen voor inhuur van onafhankelijke interne auditor (2022) 4.3 Bespreek met andere GGD'en en HSC de mogelijkheid om interne audits bij elkaar uit te voeren
5 Beleid informatiebeveiliging	(-) Er ontbreekt een (strategische en tactisch) informatiebeveiligingsbeleid		5.1 Opstellen en laten vaststellen informatiebeveiligingsbeleid. Voorbeelden van het HSC en andere GGD'en beschikbaar.
6 Governance	(+) Portefeuillehouder IB & Privacy benoemd. (+) Specialisten ingehuurd voor [redacted] en projectleidersrollen. (+) Onafhankelijke [redacted] (+) Bewaking landelijke systemen door GGD Ghor NL / SOC (+) Periodiek IBMF weer gestart	(-) Adhoc / reactief aandacht voor het onderwerp in het MT (-) Te weinig tijd / middelen om alle ambities / doelstellingen te realiseren en te voldoen aan alle behoeften van alle stakeholders. Er zullen explicietere keuzes moeten worden gemaakt.	5.1 Explicieter vaststellen en documenteren taken, verantwoordelijkheden en bevoegdheden op het gebied van informatiebeveiliging. 5.2 Portefeuillehouder laten deelnemen aan informatiebeveiligings-managementforum (IBMF) 5.3 Vaststellen ambitieniveau / risicobereidheid van organisatie op het gebied van informatiebeveiliging. In lijn

	(-) Nog onvoldoende helderheid m.b.t. ambitie / risicobereidheid van het MT / Bestuur op het gebied van informatie-beveiliging.		met ambitie en beschikbare middelen besluiten welke risico's wel en welke niet te behandelen. 5.4 Implementeer ondersteunende software voor het inrichten, gebruiken en continue verbeteren van het managementsysteem voor informatiebeveiliging (ISMS), indien mogelijk samen met kwaliteit. Hierdoor meer grip op doelstellingen, risico's, controles, afwijkingen, verbetermaatregelen.
Onderwerp	**Hoe tevreden ben je over de opzet en uitvoering?** **Brengt het ons voldoende?**	**Welke risico's en welke verbeterkansen zie je en wat is daarvoor nodig?**	
Overall conclusie proces/systeem: opzet en uitvoering van informatiebeveiliging	(+) Er is veel meer aandacht voor het onderwerp informatiebeveiliging. Voldoende specialisme beschikbaar (landelijk, bij HSC en binnen GGD WB) (-) Informatiebeveiliging is nog te veel een onderwerp dat aandacht krijgt binnen team PIM. (-) Informatiebeveiliging nog geen onderdeel van dagelijkse praktijk / bedrijfsvoering	Stel structureel meer budget beschikbaar om aandacht te besteden aan informatiebeveiliging op alle niveaus. Gebruik NEN 7510 als gereedschapskist om aantoonbaar risico's te inventariseren, maatregelen te treffen en de effectiviteit van deze maatregelen periodiek te toetsen en waar nodig actie te ondernemen. Implementeer een oplossing waarin (op termijn) een geïntegreerd managementsysteem kan worden gerealiseerd (Kwaliteit / P&C / Informatiebeveiliging / Privacy(. Zorg voor voldoende bezetting in team PIM en portefeuillehouders om ook in 2022 het onderwerp serieus te blijven oppakken en te zorgen dat informatiebeveiliging en privacy meer ingebed worden in alle processen. Informatiebeveiliging is van iedereen en niet iets van alleen team PIM. Ontwikkel een informatieveilige cultuur (o.a. elkaar aanspreken bij afwijkend / onveilig gedrag.	

		Vanwege het niet voldoen aan wet- en regelgeving en het grote aantal informatiebeveiligingsrisico's en de voorgevallen incidenten is informatiebeveiliging zeker een risico 4.

Archived: donderdag 12 mei 2022 11:49:58
From: [redacted]
Sent: maandag 8 februari 2021 13:17:30
To: [redacted]
Subject: FW: Intrekken rechten vrijwilligers Rode Kruis
Importance: Normal
Sensitivity: None
Attachments:
Outlook-hq2pnnp5.png;

Kunnen jullie dit???

Grtjs [redacted]

Met vriendelijke groet,

[redacted]

[redacted]

GGD West-Brabant	Doornboslaan 225-227, Breda Postbus 3024, 5003 DA Tilburg www.ggdwestbrabant.nl	T: [redacted] E; [redacted] Aanwezig op: ma-di-wo

---

Van: [redacted]
Verzonden: maandag 8 februari 2021 12:39
CC: [redacted]
Onderwerp: Intrekken rechten vrijwilligers Rode Kruis

Dag allen,

Tot voor kort stuurde het Rode Kruis naar de GGD-en waarvoor zij werkten op dagelijkse basis een lijst met vrijwilligers die voor hen aan de slag gingen. De GGD in kwestie zorgde dan voor toegang van de personen op de lijst en verwijderde rechten voor overige vrijwilligers.

De praktijk leerde echter dat rechten (bijna) nooit zijn verwijderd omdat dit veel tijd kost. Gevolg is dat er bij GGD-en nog vrijwilligers staan aangemeld die niet meer werkzaam zijn of hebben vrijwilligers soms op meerdere GGD-en rechten terwijl ze daarvoor niet meer werken. De procedure is toen gewijzigd. Het Rode Kruis stuurde alleen nog de namen van nieuwe vrijwilligers aan wie rechten verleend moesten worden.

Gezien de actuele situatie in het kader van de datadiefstal is dit niet langer een acceptabele situatie.

Daarom vragen we jullie in dat kader om op de kortst mogelijke termijn alle vrijwilligers van het Rode Kruis uit de Active Directory te verwijderen.

Voor die GGD-en die momenteel met vrijwilligers van het Rode Kruis werken geldt dat een actuele lijst met vrijwilligers in het bezit is.

Verder nog een aanvullende check: Zouden jullie willen toetsten of er in het licht van de AVG in jullie testomgeving alleen sprake is van fictieve casussen en deze omgeving dus geen data van actuele personen bevat? Ook dit is iets dat we afgelopen weken tegen zijn gekomen en dit mag niet. De testomgeving is alleen bedoeld voor fictieve casussen.

Alvast bedankt!

Groeten,

[redacted]

[redacted] GGD GHOR

Zwarte Woud 2
3524 SJ Utrecht
Mobiel: [redacted]

Website : www.ggdghor.nl
Twitter : @GGDGHORNL

De uitbraak van het nieuwe Coronavirus vraagt dat ook wij, in lijn met de maatregelen van de Rijksoverheid, zoveel mogelijk thuiswerken. U kunt mij goed bereiken via e-mail of via mijn mobiele telefoon.

Archived: donderdag 12 mei 2022 11:50:24
From: [redacted]
Sent: maandag 8 februari 2021 13:20:25
To: [redacted]
Cc: [redacted]
Subject: RE: Intrekken rechten vrijwilligers Rode Kruis
Importance: Normal
Sensitivity: None

There are a total of 2917 Partner Organisation Users with access to your Unit

ANWB: 7 Users

Eurocross: 4 Users

SOS International: 2904 Users

VHD: 2 Users

Niiemand van Rode kruis heeft nog toegang op dit moment.

Vandaag wordt er een inventarisatie gemaakt door Yource met SOS samen welke werknemers van de 2904 sos international geen toegang meer nodig hebben. Krijgen hier vandaag/morgen een overzicht van.

[redacted]

Van: [redacted]
Verzonden: maandag 8 februari 2021 13:10
Aan: [redacted]
CC: [redacted]
Onderwerp: RE: Intrekken rechten vrijwilligers Rode Kruis

Hoi [redacted]

Ik zal dit oppakken; heb HRCorona een actueel overzicht gevraagd van RodeKruis medewerkers die door GGDWestbrabant worden ingezet.

Met vriendelijke groet,

[redacted]

[redacted]

GGD West-Brabant

E [redacted]

GGD West-Brabant

Doornboslaan 225-227, Breda

www.ggdwestbrabant.nl

www.brabantscan.nl

[redacted]

Aanwezig op: ma-di-wo-do-vr

Benieuwd naar de gezondheid van West-Brabanders? Bezoek dan de Brabantscan!

Van: [redacted]
Verzonden: maandag 8 februari 2021 12:52
Aan: [redacted]
Onderwerp: Fwd: Intrekken rechten vrijwilligers Rode Kruis

Goedemiddag

Pakken jullie dit verzoek op?

Dank

Mgr [redacted]

Begin doorgestuurd bericht:

> **Van:** [redacted]
> **Datum:** 8 februari 2021 om 12:39:04 CET
> **Kopie:** [redacted]
> **Onderwerp: Intrekken rechten vrijwilligers Rode Kruis**
>
> Dag allen,
>
> Tot voor kort stuurde het Rode Kruis naar de GGD-en waarvoor zij werkten op dagelijkse basis een lijst met vrijwilligers die voor hen aan de slag gingen. De GGD in kwestie zorgde dan voor toegang van de personen op de lijst en verwijderde rechten voor overige vrijwilligers.
>
> De praktijk leerde echter dat rechten (bijna) nooit zijn verwijderd omdat dit veel tijd kost. Gevolg is dat er bij GGD-en nog vrijwilligers staan aangemeld die niet meer werkzaam zijn of hebben vrijwilligers soms op meerdere GGD-en rechten terwijl ze daarvoor niet meer werken. De procedure is toen gewijzigd. Het Rode Kruis stuurde alleen nog de namen van nieuwe vrijwilligers aan wie rechten verleend moesten worden.

Gezien de actuele situatie in het kader van de datadiefstal is dit niet langer een acceptabele situatie.

Daarom vragen we jullie in dat kader om op de kortst mogelijke termijn alle vrijwilligers van het Rode Kruis uit de Active Directory te verwijderen.

Voor die GGD-en die momenteel met vrijwilligers van het Rode Kruis werken geldt dat een actuele lijst met vrijwilligers in het bezit is.

Verder nog een aanvullende check: Zouden jullie willen toetsten of er in het licht van de AVG in jullie testomgeving alleen sprake is van fictieve casussen en deze omgeving dus geen data van actuele personen bevat? Ook dit is iets dat we afgelopen weken tegen zijn gekomen en dit mag niet. De testomgeving is alleen bedoeld voor fictieve casussen.

Alvast bedankt!

Groeten,

[redacted]

[redacted]

Zwarte Woud 2
3524 SJ Utrecht
Mobiel: 06 - 13 31 26 25

Website : www.ggdghor.nl
Twitter : @GGDGHORNL

De uitbraak van het nieuwe Coronavirus vraagt dat ook wij, in lijn met de maatregelen van de Rijksoverheid, zoveel mogelijk thuiswerken. U kunt mij goed bereiken via e-mail of via mijn mobiele telefoon.

Wob-verzoek SOLV/ICAM datalek 2021 coronasysteem

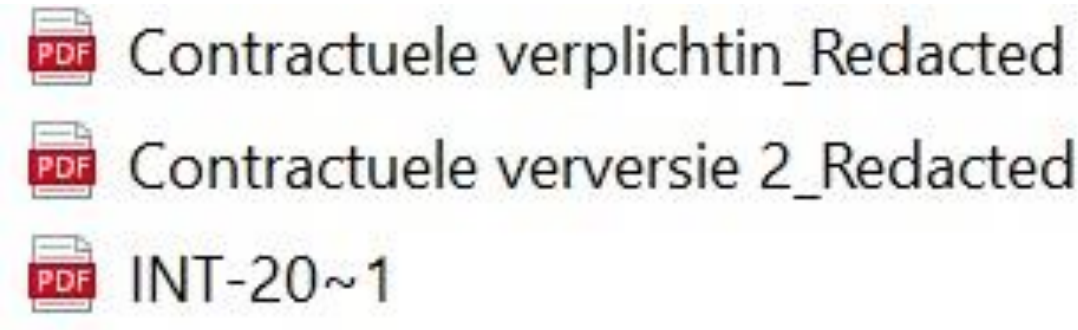
13.0 Tekst Wob-verzoek en register documenten

Tekst verzoek (xiii)

Overeenkomsten met GGD medewerkers en externen die gebruik maken en hebben gemaakt van CoronIT, HPZone en/of HPZone Lite, waaronder maar niet beperkt tot arbeidsovereenkomsten, opdrachtovereenkomst en/of geheimhoudingsovereenkomsten

Register

Een screenshot van de verkennerpagina van map 13:



Welkom bij de GGD West-Brabant!

Bij de GGD West-Brabant (‘GGD’) doe je belangrijk werk. Je draagt bij aan de bevordering, bescherming en bewaking van de gezondheid van alle inwoners van West-Brabant.

Tijdens het werk bij de GGD kom je in aanraking met gevoelige persoonsgegevens over de gezondheid van mensen. We willen dat je hier zorgvuldig mee omgaat en bewust bent van het feit welke verantwoordelijkheden dit met zich meedraagt.

Daarom vragen we jou om deze ‘integriteits- en geheimhoudingsverklaring’ door te lezen en te ondertekenen. Door ondertekening ga je een overeenkomst met ons aan waarbij je je verplicht tot het naleven van de beschreven bepalingen.

Zo draag ook jij bij aan een goede bescherming en beveiliging van de gezondheidsgegevens van alle inwoners van West-Brabant!

Veel succes en hartelijke groet,

[redacted]

Je hebt de integriteits- en geheimhoudingsverklaring ontvangen en moet deze ondertekenen. In de verklaring staan de wetsartikelen waar je je aan te houden hebt. Dit hoort erbij omdat we verplicht zijn om je goed en juridisch correct te informeren.

Wat staat er eigenlijk?

De gegevensverwerking (dit is ook het raadplegen HP-Zone, Coron-IT, Kidos of de BRP, direct of via een andere applicatie) is noodzakelijk voor de goede vervulling van een publiekrechtelijke taak en in het belang van betrokkene. Heb je de gegevens niet nodig, dan mag je ze ook niet raadplegen. Dit betekent ook dat je van een klant niet meer opvraagt, dan je voor je werk nodig hebt. We noemen dit ook wel "Need-to-Know". In de meeste applicaties is het toegangsbeheer per groep geregeld. Je hebt dus dezelfde rechten als je collega's, maar je hebt geen recht om gegevens te bekijken van een patiënt van een collega.

Als je niet kunt uitleggen waarom je iets opvraagt, handel je waarschijnlijk in strijd met de bepalingen uit onder andere de AVG (Algemene Verordening Gegevensbescherming).
Je weet dat alle opvragingen vastgelegd worden (logging) en dat dit regelmatig wordt gecontroleerd. Ook deze controle is een wettelijke verplichting.

Geheimhouding betekent ook dat je deze informatie niet met anderen deelt, behalve als je daar wettelijk toe verplicht bent. Concreet komt dit neer op de z.g. Clean Desk Policy (geen vertrouwelijke informatie open en bloot laten liggen, ook niet op het scherm van je computer) en niet over klanten/burgers praten als dit niet nodig is. Moet dat wel, dan zorg je ervoor dat anderen niet kunnen meeluisteren. Is dat niet mogelijk, doe het dan zo dat niet herkenbaar is over wie (geen namen of adressen noemen) het gaat.

De wetgever neemt geheimhouding serieus. Zo staat, in artikel 272 van het Wetboek van Strafrecht, aangegeven dat overtreding van deze regels wordt gezien als een misdrijf van de 4e categorie. Hiervoor kan een gevangenisstraf van maximaal 1 jaar of een geldboeten van de vierde categorie (per 01-12-2012 € 19.500 worden opgelegd. In minder ernstige gevallen neemt de werkgever disciplinaire maatregelen, die kunnen variëren van een waarschuwing tot ontslag.

Wat betekent dat voor jou?

Zie het als de bepalingen in een contract. We vertrouwen elkaar, zijn integer en houden ons aan de afspraken en de gedragscode. Na ondertekening kijk je niet meer naar het contract. Alleen voor de hoge uitzondering waarin het mis gaat, moet je alles wel goed geregeld hebben.

INTEGRITEITS-EN GEHEIMHOUDINGSVERKLARING GGD West-Brabant

Achternaam, voornaam en voorletters

Geboortedatum

Geboorteplaats

Functie

verklaart het volgende

1. Geheimhouding

- Ik verklaar geheim te houden alle informatie die mij gedurende mijn werkzame periode ter kennis komt, waarvan ik weet of vermoed dat deze vertrouwelijk is.
- Medische gegevens, persoonsgegevens, financiële gegevens, (interne) bedrijfsgegevens, klantgegevens, aanbestedingsgegevens en contractgegevens beschouw ik in ieder geval als vertrouwelijk.
- Ik verstrek deze informatie niet aan anderen, ook niet binnen de GGD, tenzij dit strikt noodzakelijk is voor de uitoefening van mijn taak of ik daartoe wettelijk verplicht ben.
- Bij twijfel neem ik contact op met de opdrachtgever van de GGD.

Ook niet-schriftelijke informatie kan een vertrouwelijk karakter hebben, zoals interne uitspraken van het management, discussies of verschillen van mening.

2. Toegang tot gebouwen

- Ik gebruik de hulpmiddelen voor toegang tot locaties, apparatuur en ruimten van de GGD uitsluitend voor het doel waarvoor deze aan mij ter beschikking zijn gesteld.
- Ik probeer niet om onbevoegd toegang te krijgen tot locaties van de GGD.
- Voor mij bestemde toegangsmiddelen behoud ik voor mijzelf en geef ik niet aan collega's of derden, tenzij daarover afspraken zijn gemaakt met de opdrachtgever en dit past in de bedrijfsvoering.
- Bij vermissing, ontvreemding, misbruik of ander onrechtmatig gebruik van de mij verstrekte toegangspas, sleutels, tags, toegangscodes, apparatuur of software stel ik de daartoe aangewezen personen binnen het organisatieonderdeel waar ik werkzaam ben onmiddellijk daarvan in kennis.
- Ik houd mij aan de regels die per locatie van de GGD zijn gesteld ten aanzien van het ontvangen en begeleiden van bezoekers.

Toegangsmiddelen zijn bijvoorbeeld toegangspassen, sleutels, tags, toegangscodes, passwords, apparatuur en software. Voorbeelden van extra kwetsbare ruimten zijn: computer-en netwerkruimten, ruimten met communicatieapparatuur zoals telefooncentrales, archiefruimten, ruimten met toegang tot bedrijfsvoeringsgegevens, ruimten waarin zich kluizen bevinden, werkplaatsen waar kostbare apparatuur aanwezig is.

3. Omgang informatie

- Ik laat geen stukken onbeheerd achter, ook niet op mijn bureau, in de ruimte of (thuis) werkplek waar ik werk, waarvan ik weet of zou kunnen weten dat deze vertrouwelijk zijn.
- Ik houd mij op mijn (thuis)werkplek aan de regels voor de beveiliging van informatie.
- Als ik vermoed dat er een inbreuk wordt gemaakt op de informatieveiligheid dan doe ik daarvan een melding aan mijn leidinggevende en aan de informatiebeveiligingsadviseur.
- Documenten, e-mails, en overige zaken die niet voor mij bestemd zijn, zend ik onmiddellijk door aan het juiste adres of ik retourneer deze aan de afzender. Is het juiste adres noch de afzender bekend, dan vernietig ik ze.
- Ik beloof vertrouwelijke gegevens niet in mijn persoonlijk bezit te bewaren
- Ik beloof mijn persoonlijke inlogaccount niet aan derden te verstrekken
- Ik beperk de inzage en/of het gebruik van vertrouwelijke gegevens tot wat nodig is voor de vervulling van mijn werkzaamheden (Need-to-Know principe).

Zoals onder het kopje 'Geheimhouding' al is aangegeven worden in ieder geval als vertrouwelijk beschouwd persoonsgegevens, financiële gegevens, klantgegevens, interne (bedrijfsgegevens), aanbestedingsgegevens en contractgegevens. Voorbeelden van mogelijke beveiligingsmaatregelen zijn: clean desk, afsluiten kasten, aanzetten schermbeveiliging tijdens afwezigheid, regelmatig wijzigen van wachtwoorden, niet uitlenen van apparatuur of gegevensdragers aan derden.

4. Omgang bedrijfsmiddelen

- Ik ga zorgvuldig om met alle mij ter beschikking gestelde bedrijfsmiddelen, zowel op mijn werkplek als elders waar ik bedrijfsmiddelen gebruik.
- Ik houd mij aan de geldende regels voor internet en e-mail gebruik en de huisregels van het organisatieonderdeel.
- Ik laat geen waardevolle bedrijfsmiddelen onbeheerd achter op mijn werkplek of elders waar ik bedrijfsmiddelen gebruik
- Bij verlies of diefstal van mobiele apparatuur of bij beschadiging maak ik direct melding bij mijn werkgever.

Voorbeelden van bedrijfsmiddelen zijn: computers, (mobiele) telefoons, kantoorbehoeften, laptops, beamers, vervoermiddelen zoals dienstauto of dienstfiets.
Voorbeelden van ongewenst gebruik van inter-/intranet en e-mail zijn het surfen naar dubieuze websites, het openen van e-mail van totaal onbekende afzenders dan wel e-mail met een vreemde bijlage, het downloaden van muziekbestanden of software zonder licentie, etc.

5. Integriteit

- Ik gedraag mij integer, wat in ieder geval inhoudt dat ik mij houd aan de interne regels over integriteit en de huisregels van mijn organisatieonderdeel.
- Als ik een misstand constateer, meld ik deze in eerste bij mijn opdrachtgever of diens superieur.
- Als ik anoniem wil blijven, zal ik gebruik maken van de 'Klokkenluiderregeling' en meld ik een geconstateerde misstand bij de vertrouwenspersoon integriteit bij mijn organisatieonderdeel.
- Bij twijfel raadpleeg ik de coördinator integriteit of de centrale vertrouwenspersoon integriteit.

6. Omgangsvormen

- Ik houd mij aan correcte omgangsvormen en ik houd mij aan de interne regels over ongewenst gedrag, omgangsvormen en de huisregels van mijn organisatieonderdeel.
- Krijg ik te maken met ongewenste omgangsvormen dan kan ik mijn opdrachtgever raadplegen, dan wel de vertrouwenspersoon ongewenste omgangsvormen bij mijn organisatieonderdeel of de vertrouwenspersoon. Wordt het probleem niet opgelost dan kan ik een klacht indienen bij de klachtenfunctionaris.

Ik verklaar verder in kennis te zijn gesteld van de inhoud van dit formulier en:

- mij te zullen houden aan alle in dit formulier genoemde (spel)regels;
- bekend te zijn met de verplichting melding te doen van elke schending van de geheimhoudingsplicht.
- Dit onverminderd hetgeen is bepaald in artikel 162 van het Wetboek van Strafvordering(geldend op 17 november 2015);
- kennis te hebben genomen van de bepalingen in het Wetboek van Strafrecht inzake geheimhouding (geldend op 20 april 2016), te weten de artikelen 2 tot en met 8, 23, 272 en 273(snelkoppelingen te vinden op internet);
- dat ik de betekenis en het belang van die bepalingen heb begrepen.

Ondertekening medewerker

Datum	Plaats	Handtekening

Gezien GGD

Datum	Plaats	Handtekening

Welkom bij de GGD West-Brabant!

Bij de GGD West-Brabant (‘GGD’) doe je belangrijk werk. Je draagt bij aan de bevordering, bescherming en bewaking van de gezondheid van alle inwoners van West-Brabant.

Tijdens het werk bij de GGD kom je in aanraking met gevoelige persoonsgegevens over de gezondheid van mensen. We willen dat je hier zorgvuldig mee omgaat en bewust bent van het feit welke verantwoordelijkheden dit met zich meedraagt.

Daarom vragen we jou om deze ‘integriteits- en geheimhoudingsverklaring’ door te lezen en te ondertekenen. Door ondertekening ga je een overeenkomst met ons aan waarbij je je verplicht tot het naleven van de beschreven bepalingen.

Zo draag ook jij bij aan een goede bescherming en beveiliging van de gezondheidsgegevens van alle inwoners van West-Brabant!

Veel succes en hartelijke groet,

[redacted]

Je hebt de integriteits- en geheimhoudingsverklaring ontvangen en moet deze ondertekenen. We leggen je kort uit wat er in deze verklaring staat zodat je weet wat je ondertekent, hoe belangrijk geheimhouding is en aan welke regels je je dient te houden. In de verklaring staan de wetsartikelen waar je je aan te houden hebt. Dit hoort erbij omdat we verplicht zijn om je goed en juridisch correct te informeren. Indien er iets onduidelijk is, vraag dit dan aan jouw contactpersoon bij de GGD.

Wat staat er eigenlijk?

De gegevensverwerking (dit is ook het raadplegen HP-Zone, Coron-IT, Kidos of de BRP, direct of via een andere applicatie) is noodzakelijk voor de goede vervulling van een publiekrechtelijke taak en in het belang van betrokkene. Heb je de gegevens niet nodig voor de uitvoering van jouw werkzaamheden, dan mag je ze ook niet raadplegen. Dit betekent ook dat je van een klant niet meer opvraagt, dan je voor je werk nodig hebt. We noemen dit ook wel "Need-to-Know". In de meeste applicaties is het toegangsbeheer per groep geregeld. Je hebt dus dezelfde rechten als je collega's, maar je hebt geen recht om gegevens te bekijken van een patiënt van een collega.

Geheimhouding betekent ook dat je deze informatie niet met anderen deelt, behalve als je daar wettelijk toe verplicht bent. Concreet komt dit neer op de z.g. Clean Desk Policy (geen vertrouwelijke informatie open en bloot laten liggen, ook niet op het scherm van je computer) en niet over klanten/burgers praten als dit niet nodig is. Moet dat wel, dan zorg je ervoor dat anderen niet kunnen meeluisteren. Is dat niet mogelijk, doe het dan zo dat niet herkenbaar is over wie (geen namen of adressen noemen) het gaat.

De wetgever neemt geheimhouding serieus. Zo staat, in artikel 272 van het Wetboek van Strafrecht, aangegeven dat overtreding van deze regels wordt gezien als een misdrijf van de 4e categorie. Hiervoor kan een gevangenisstraf van maximaal 1 jaar of een geldboeten van de vierde categorie (per 01-12-2012) € 19.500 worden opgelegd. In minder ernstige gevallen neemt de werkgever disciplinaire maatregelen, die kunnen variëren van een waarschuwing tot ontslag.

Wat betekent dat voor jou?

Zie het als de bepalingen in een contract. We vertrouwen elkaar, zijn integer en houden ons aan de afspraken en de gedragscode.

INTEGRITEITS-EN GEHEIMHOUDINGSVERKLARING GGD West-Brabant

Achternaam, voornaam en voorletters

Geboortedatum

Geboorteplaats

Functie

verklaart het volgende

1. Geheimhouding

- Ik verklaar geheim te houden alle informatie die mij gedurende mijn werkzame periode ter kennis komt, waarvan ik weet of vermoed of redelijkerwijs zou moeten weten dat deze vertrouwelijk is. Deze geheimhouding blijft ook van kracht nadat mijn werk voor de GGD is geëindigd.
- Ik ben mij ervan bewust dat ik voor de uitoefening van mijn werkzaamheden toegang heb tot vertrouwelijke en zeer gevoelige informatie waaronder Mmedische gegevens, persoonsgegevens, financiële gegevens, (interne) bedrijfsgegevens, klantgegevens, aanbestedingsgegevens en contractgegevens. Deze informatie beschouw ik in ieder geval als vertrouwelijk.
- Ik verstrek deze informatie niet aan anderen, ook niet binnen de GGD, tenzij dit strikt noodzakelijk is voor de uitoefening van mijn taak of ik daartoe wettelijk verplicht ben.
- Bij twijfel neem ik direct contact op met de opdrachtgever van de GGD.

Ook niet-schriftelijke informatie kan een vertrouwelijk karakter hebben, zoals informatie die jou telefonisch wordt verteld (door collega's, patiënten of derden), interne uitspraken van het management, discussies of verschillen van mening.

2. Omgang informatie

- Ik laat geen stukken onbeheerd achter, ook niet op mijn bureau, in de ruimte of (thuis) werkplek waar ik werk, waarvan ik weet of zou kunnen weten dat deze vertrouwelijk zijn.
- Ik houd mij op mijn (thuis)werkplek aan de regels voor de beveiliging van informatie.
- Als ik vermoed dat er een inbreuk wordt gemaakt op de informatieveiligheid dan doe ik daarvan een melding aan mijn leidinggevende en aan de informatiebeveiligingsadviseur.
- Documenten, e-mails, en overige zaken die niet voor mij bestemd zijn, zend ik onmiddellijk door aan het juiste adres of ik retourneer deze aan de afzender. Is het juiste adres noch de afzender bekend, dan vernietig ik ze.
- Ik beloof bewaar vertrouwelijke gegevens niet in mijn persoonlijk bezit te bewaren.
- Ik beloof verstrek mijn persoonlijke inlogaccount niet aan derden te verstrekken.
- Ik beperk de inzage en/of het gebruik van vertrouwelijke gegevens tot wat nodig is voor de vervulling van mijn werkzaamheden (Need-to-Know principe).
- Als ik toch (al dan niet per ongeluk) vertrouwelijke gegevens verwerk in strijd met deze verklaring dan meld ik dat direct aan mijn leidinggevende en aan de informatiebeveiligingsadviseur.

Mogelijke beveiligingsmaatregelen zijn: clean desk, afsluiten kasten, aanzetten schermbeveiliging tijdens afwezigheid, regelmatig wijzigen van wachtwoorden, niet uitlenen van apparatuur of gegevensdragers aan derden.
Voorbeelden van ongewenst gebruik van inter-/intranet en e-mail zijn het surfen naar dubieuze websites, het openen van e-mail van totaal onbekende afzenders dan wel e-mail met een vreemde bijlage, het downloaden van muziekbestanden of software zonder licentie, etc.

3. Integriteit

- Ik gedraag mij integer, wat in ieder geval inhoudt dat ik mij houd aan de interne regels over integriteit en de huisregels van mijn organisatieonderdeel .
- Als ik een misstand constateer of vermoed, meld ik deze meteen en in eerste instantie? bij mijn opdrachtgever of diens superieur.
- Als ik anoniem wil blijven, zal ik gebruik maken van de 'Klokkenluiderregeling' en meld ik een geconstateerde misstand bij de vertrouwenspersoon integriteit bij mijn organisatieonderdeel.
- Bij twijfel raadpleeg ik de coördinator integriteit of de centrale vertrouwenspersoon integriteit .

4. Omgangsvormen

- Ik houd mij aan correcte omgangsvormen en ik houd mij aan de interne regels over ongewenst gedrag, omgangsvormen en de huisregels van mijn organisatieonderdeel.
- Krijg ik te maken met ongewenste omgangsvormen dan kan ik mijn opdrachtgever raadplegen, dan wel de vertrouwenspersoon ongewenste omgangsvormen bij mijn organisatieonderdeel of de vertrouwenspersoon. Wordt het probleem niet opgelost dan kan ik een klacht indienen bij de klachtenfunctionaris.

Ik verklaar verder in kennis te zijn gesteld van de inhoud van dit formulier en:

- mij te zullen houden aan alle in dit formulier genoemde (spel)regels en verplichtingen;
- bekend te zijn met de verplichting melding te doen van elke schending van de geheimhoudingsplicht.
- Dit onverminderd hetgeen is bepaald in artikel 162 van het Wetboek van Strafvordering (geldend op 17 november 2015);
- kennis te hebben genomen van de bepalingen in het Wetboek van Strafrecht inzake geheimhouding (geldend op 20 april 2016), te weten de artikelen 2 tot en met 8, 23, 272 en 273 (snelkoppelingen te vinden op internet);
- dat ik de betekenis en het belang van die bepalingen heb begrepen.

Ondertekening medewerker

Datum	Plaats	Handtekening

Gezien GGD

Datum	Plaats	Handtekening

Overeenkomst gebruik ter beschikking gestelde bedrijfsapparatuur

De Naam betreffende GGD/RAV *(*verder te noemen *"De werkgever")* stelt aan haar medewerker bedrijfsapparatuur inclusief toebehoren in bruikleen ter beschikking:

de heer/mevrouw : Naam en voorletters medewerker/-ster (verder te noemen *"De medewerker"*)
Personeelsnummer : Personeelsnummer

1. Looptijd bruikleenovereenkomst

- *"De werkgever"* stelt de apparatuur ter beschikking voor de periode vanaf de datum van ondertekening van ontvangst van de ter beschikking gestelde apparatuur tot het einde of wijziging van het dienstverband (zie artikel 5);
- of wanneer op basis van artikel 6 van deze overeenkomst sprake is van opzegging om andere redenen door *"De werkgever"*.

2. Eigendom

De verstrekte apparatuur is en blijft eigendom van *"De werkgever"*. Vanaf het moment van ingebruikname is *"De medewerker"* verantwoordelijk voor de ter beschikking gestelde apparatuur.

3. Gebruik algemeen

- *"De medewerker"* gebruikt alleen het door de werkgever beschikbaar gestelde gebruikersaccount in de ter beschikking gestelde apparatuur;
- *"De medewerker"* stelt de apparatuur niet aan derden ter beschikking;
- *"De medewerker"* is verantwoordelijk voor het in goede staat houden van de apparatuur;
- *"De medewerker"* neemt de nodige zorgvuldigheid in acht ter voorkoming van diefstal, verlies of beschadiging van de apparatuur;
- De apparatuur is persoonsgebonden en niet overdraagbaar;
- *"De medewerker"* meldt verlies, diefstal, beschadiging of gebreken van de apparatuur zo snel mogelijk aan de Servicedesk HSC. De medewerker volgt de vervolgens door de Servicedesk te geven aanwijzingen op;
- *"De medewerker"* zal de benodigde zorgvuldigheid en privacy in acht nemen ter zake van vertrouwelijke gegevens van medewerkers, cliënten en relaties van *"De werkgever"*.

4. Kosten, sancties en aansprakelijkheid

- De kosten van gebruik, onderhoud en eventuele reparatie van de verstrekte apparatuur komen voor rekening van *"De werkgever"*;
- *"De werkgever"* kan sancties treffen als het gebruik van de apparatuur afwijkt van de met *"De medewerker"* gemaakte afspraken. Onder sancties wordt in dit kader verstaan het beperken van de gebruiksmogelijkheden of het innemen van de apparatuur;

- *"De werkgever"* kan *"De medewerker"* aansprakelijk stellen voor:
  - Schade aan de apparatuur, ontstaan door verwijtbare nalatigheid of onachtzaamheid;
  - De kosten die gemaakt zijn met niet tijdig geblokkeerde apparatuur.
- *"De werkgever"* is niet aansprakelijk voor schade als gevolg van het gebruik van de apparatuur.

5. Beëindiging overeenkomst en functiewijziging

Indien *"De medewerker"* uit dienst treedt of van functie wijzigt, wordt de apparatuur door *"De medewerker"* vóór de datum uitdiensttreding of datum functiewijziging ingeleverd bij *"De werkgever"*.
De apparatuur dient, behoudens normale slijtage, compleet incl. accessoires en zonder schade, te worden ingeleverd. Onder verwijzing naar artikel 4 van deze overeenkomst behoudt *"De werkgever"* zich het recht voor eventuele schade aan de apparatuur op *"De medewerker"* te verhalen.

6. Inname wegens andere redenen

- *"De werkgever"* behoudt het recht het gebruik van de apparatuur door de medewerker te beëindigen (ook in het geval het gebruik van de ter beschikking gestelde apparatuur door *"De medewerker"* naar oordeel van *"De werkgever"* niet langer noodzakelijk is voor een behoorlijke vervulling van de dienstbetrekking);
- *"De werkgever"* behoudt het recht om bij een tijdelijke afwezigheid van drie maanden of meer (bijvoorbeeld wegens arbeidsongeschiktheid dan wel zwangerschaps- of anderszins betaald of onbetaald verlof) de ter beschikking gestelde apparatuur in te nemen;
- Op verzoek van de *"De werkgever"* zal *"De medewerker"* de bruikleenzaken weer direct ter beschikking stellen aan *"De werkgever"*.

7. Gedragsregels

- Samen met deze 'Overeenkomst gebruik ter beschikking gestelde bedrijfsapparatuur' ontvangt de medewerker de "Gedragsregels gebruik door bedrijf verstrekte apparatuur".
- De medewerker verplicht zich regelmatig kennis te nemen van nieuwe of gewijzigde regels en bepalingen ten aanzien van o.a. het gebruik apparatuur, van internet en e-mail en conform deze regels te handelen.

Gedragsregels gebruik van bedrijfsapparatuur

I. Begrippen

Met bedrijfsapparatuur wordt in deze gedragsregels zowel gedoeld op draagbare computers zoals bijv. laptops, tablets, mobiele telefoons als niet draagbare apparatuur.
Voor zover van toepassing gelden deze regels ook voor andere (rand)apparatuur zoals pc's, printers, camera's, opnameapparatuur e.d.

II. Algemeen

1. Reikwijdte

Deze gedragsregels zijn van toepassing op iedereen die in het kader van zijn werk gebruik maakt van apparaten die eigendom zijn van en ter beschikking gesteld worden door de GGD Hart voor Brabant, de GGD West-Brabant, de GGD Noord- en Oost-Gelderland, de RAV Brabant Midden-West-Noord en Hét Service Centrum.
Waar verder in deze notitie gesproken wordt van *"De werkgever"* wordt daarmee de van toepassing zijnde organisatie bedoeld.

2. Algemene regels ten aanzien van het gebruik van apparatuur.

Van medewerkers die werken met door "De werkgever" verstrekte apparaten wordt verwacht dat ze bij het gebruik daarvan de algemene maatschappelijke normen en waarden respecteren en zich aan het integriteitsbeleid en de algemene gedragsregels van "De werkgever" houden.

- Het gebruik van apparaten moet binnen de grenzen van de wet plaatsvinden[1];
- Het gebruik ervan evenals dat van overige bedrijfsfaciliteiten moet in lijn zijn met de bedrijfsdoelstellingen of de bedrijfsvoering;
- Het gebruik mag niet ten koste gaan van primaire processen en of de bedrijfsvoering van *"De werkgever"*;
- Het ophalen en verspreiden van discriminerende en of kwetsende uitingen op of met behulp van mobiele apparaten is niet toegestaan;
- Het installeren van niet legale toepassingen is ten strengste verboden.

De apparatuur is en blijft eigendom van *"De werkgever"*. In voorkomende gevallen zoals crisissituaties kan men worden verzocht deze (tijdelijk) ter beschikking te stellen.
Dit kan consequenties hebben voor geïnstalleerde eigen (betaalde) apps en privé-email en -gegevens die verloren zouden kunnen gaan.
Ook bij verlies of diefstal kan apparatuur op afstand worden geblokkeerd en gewist. *"De werkgever"* is niet aansprakelijk voor het verloren gaan van privégegevens of apps.

[1] In het bijzonder zijn diefstal, fraude, ongeautoriseerd binnendringen in computersystemen van derden, schending van auteursrechten en valsheid in geschrifte verboden.

3. Controle

Er worden controles van de bedrijfssystemen uitgevoerd. In dat kader kan alle netwerk- en telefonieverkeer worden gemonitord. Doel van deze controles is het afdichten van mogelijke beveiligingsrisico's alsmede het detecteren van afwijkingen op het gebruik.

III. Gedragsregels

1. Gebruik apparatuur

Gebruikers hebben toegang tot de ICT-voorzieningen van *"De werkgever"*. Dit is op basis van de toegekende gebruikersnaam en een zelf gekozen sterk wachtwoord.

2. Gedragsregels

De inloggegevens zijn strikt persoonlijk en mogen dan ook niet aan derden worden verstrekt.
Wachtwoorden dienen periodiek gewijzigd te worden.
Aanwijzingen van medewerkers van de beheersorganisatie o.a. ten aanzien van virusbestrijding en het beheer dienen te worden gevolgd.

Het is niet toegestaan:

- Inloggegevens te gebruiken die op niet-reglementaire wijze verkregen zijn;
- Zich ongeoorloofd toegang te verschaffen tot gegevens van andere gebruikers.

"De werkgever" heeft het recht, als de continuïteit van de bedrijfsvoering in gevaar komt, zich toegang te verschaffen tot de zakelijke mailbox van de medewerker. Dit kan alleen onder specifieke voorwaarden:

- *De continuïteit van de bedrijfsvoering moet dusdanig in gevaar komen dat inzage in mail noodzakelijk is, of voor het instellen van een afwezigheidsassistent;*
- *Medewerker geeft toestemming voor inzage. Indien dit niet mogelijk is, is overtuigend bewijs noodzakelijk dat continuïteit van de bedrijfsvoering in gevaar komt;*
- *Bij inzage in de mailbox worden alleen de voor de bedrijfsvoering relevante mails geopend;*
- *Het vier-ogen-principe wordt gehanteerd.*

3. Gedragsregels e-mail

De voorzieningen om e-mail te ontvangen en te verzenden worden conform de voorschriften en of aanwijzingen van de organisatie gebruikt. Iedere gebruiker draagt er zorg voor dat zijn inloggegevens alleen voor eigen gebruik worden aangewend.
Medewerkers mogen het e-mailsysteem van laptop, tablet of smartphone gebruiken voor het ontvangen en versturen van persoonlijke e-mailberichten mits dit niet storend is voor de dagelijkse werkzaamheden en het computernetwerk.

Het is medewerkers **niet** toegestaan om alle inkomende bedrijfsmail automatisch door te sturen (forwarden) naar externe emailadressen.

4. Gedragsregels internet

Apparaten geven toegang tot het internet, dat kan bekabeld of via draadloze netwerken (wifi) of een telefoonverbinding. Maak echter zoveel mogelijk gebruik van het bekabelde netwerk op het werk of van aanwezige, veilige wifi-verbindingen (niet alleen op vestigingen van *"De werkgever"* maar ook thuis en op andere plaatsen). Pas goed op wanneer je gebruik maakt van openbare Wifi-netwerken.
Privégebruik van de apparatuur is niet verboden voor zover men zich aan de algemene regels houdt.

Het is niet toegestaan materiaal te downloaden met een discriminatoire of pornografische inhoud, dan wel met een zodanige inhoud dat de gebruiker redelijkerwijze kan begrijpen dat *"De werkgever"* zich hiermee niet kan verenigen en of betrokkenheid van de *"De werkgever"* bij dit materiaal de eer en goede naam van *"De werkgever"* schaadt.
Het is niet toegestaan software, gegevens en artikelen te downloaden of te kopiëren waarvoor auteursrechten gelden of licenties ontbreken.

5. Gedragsregels social media

Het is niet toegestaan tekst of materiaal te plaatsen met een discriminatoire of pornografische inhoud, dan wel met een zodanige inhoud dat de gebruiker redelijkerwijze kan begrijpen dat *"De werkgever"* zich hiermee niet kan verenigen en of betrokkenheid van de *"De werkgever"* bij dit materiaal de eer en goede naam van *"De werkgever"* schaadt.

IV. Sancties

Medewerkers waarvan geconstateerd is dat zij zich niet aan deze regeling houden worden door de eigen direct leidinggevende op hun gedrag aangesproken.
In uiterste gevallen kan worden overgegaan tot het nemen van (disciplinaire) maatregelen.

Door digitaal akkoord / ondertekening van deze overeenkomst verklaart de medewerker dat hij de gevolgen van deze overeenkomst heeft begrepen en zich daarmee akkoord verklaart en kennis heeft genomen van de bijbehorende gedragsregels.

Handtekening

Datum: __ / __ / ____

Wob-verzoek SOLV/ICAM datalek 2021 coronasysteem

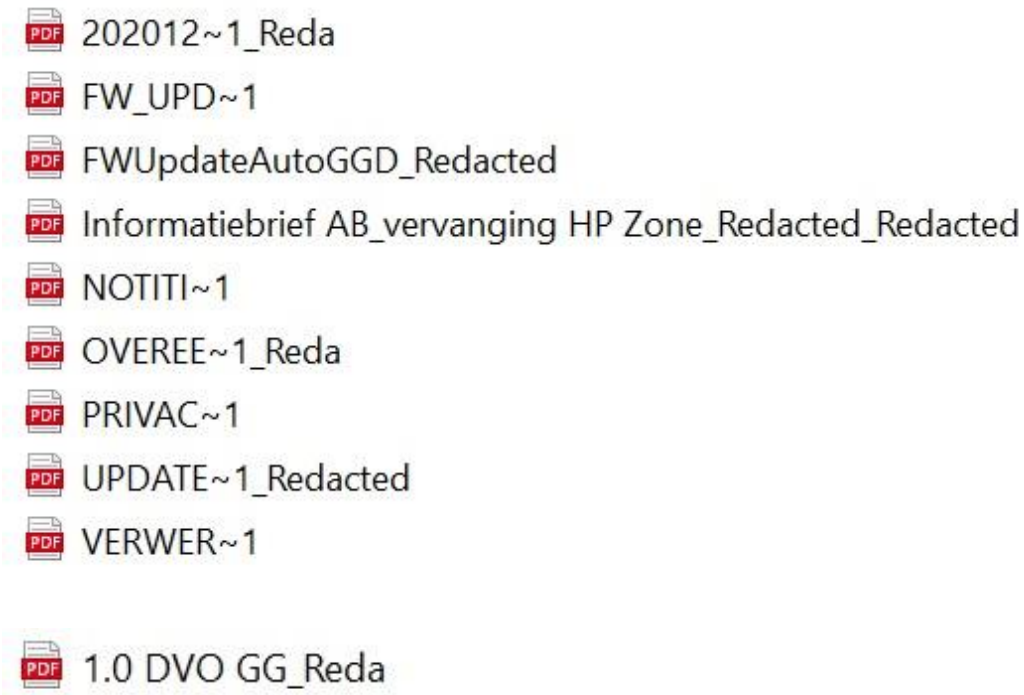
12.0 Tekst Wob-verzoek en register documenten

Tekst verzoek (xii)

Informatie over de overname van het beheer van HPZone (Lite) door GGD GHOR

Register

Een screenshot van de verkennerpagina van map 12:



Inhoud

Artikel 1. Begrippen 2
Artikel 2. Voorwerp van deze Verwerkersovereenkomst 3
Artikel 3. Inwerkingtreding en duur 3
Artikel 4. Omvang verwerkingsbevoegdheid Opdrachtnemer 3
Artikel 5. Beveiliging van de Verwerking 4
Artikel 6. Geheimhouding door Personeel van Opdrachtnemer 4
Artikel 7. Subverwerker 4
Artikel 8. Bijstand vanwege rechten van Betrokkene 5
Artikel 9. Inbreuk in verband met Persoonsgegevens 5
Artikel 10. Terugbezorgen of wissen Persoonsgegevens 5
Artikel 11. Informatieverplichting en audit 5
Bijlage 1. De Verwerking van Persoonsgegevens..... **Fout! Bladwijzer niet gedefinieerd.**
Bijlage 2. Passende technische en organisatorische maatregelen ..... **Fout! Bladwijzer niet gedefinieerd.**
Bijlage 3: Afspraken betreffende Inbreuken in verband met Persoonsgegevens 9

Verwerkersovereenkomst GGD Contact

De ondergetekenden:

1. De publiekrechtelijke rechtspersoon Gemeentelijke of Gemeenschappelijke Gezondheidsdienst West-Brabant, statutair gevestigd en kantoorhoudende te 4816 CZ, Breda te Doornboslaan 225, ingeschreven in het handelsregister van de Kamer van Koophandel onder nummer 20164916, hierbij vertegenwoordigd door [redacted] Publieke Gezondheid hierna te noemen: Opdrachtgever,

en

2. De Staat der Nederlanden, waarvan de zetel is gevestigd te Den Haag,
te dezen vertegenwoordigd door de Minister van Volksgezondheid, Welzijn en Sport,
namens deze, [redacted]
hierna te noemen: Opdrachtnemer,

hierna gezamenlijk te noemen: Partijen;

OVERWEGENDE DAT:

- voor zover Opdrachtnemer Persoonsgegevens Verwerkt ten behoeve van Opdrachtgever in het kader van de Overeenkomst, Opdrachtgever krachtens artikel 4, onderdeel 7 en onderdeel 8, van de Verordening kwalificeert als verwerkingsverantwoordelijke voor de Verwerking van Persoonsgegevens en Opdrachtnemer als verwerker;
- Partijen in deze Verwerkersovereenkomst, zoals bedoeld in artikel 28, derde lid, van de Verordening, hun afspraken over de Verwerking van Persoonsgegevens door Opdrachtnemer wensen vast te leggen.

KOMEN OVEREEN:

Artikel 1. Begrippen

In deze Verwerkersovereenkomst wordt een aantal begrippen met een beginhoofdletter gebruikt. Aan deze begrippen komt de betekenis toe die hieraan wordt gegeven in artikel 1 van de Algemene Rijksvoorwaarden voor het verstrekken van opdrachten tot het verrichten van Diensten 2018 (ARVODI-2018). In afwijking daarvan of in aanvulling daarop wordt onder de volgende begrippen in deze Verwerkersovereenkomst verstaan:

1.1 Betrokkene: degene op wie een Persoonsgegeven betrekking heeft.

1.2 Inbreuk in verband met Persoonsgegevens: een inbreuk op de beveiliging die per ongeluk of op onrechtmatige wijze leidt tot de vernietiging, het verlies, de wijziging of de ongeoorloofde verstrekking van of de ongeoorloofde toegang tot doorgezonden, opgeslagen of anderszins verwerkte gegevens.

1.3 Overeenkomst: de overeenkomst tussen Opdrachtgever en Opdrachtnemer OVEREENKOMST HOSTING EN BEHEER 'GGD CONTACT' van 14 december 2020.

1.4 Persoonsgegevens: alle informatie over een geïdentificeerde of identificeerbare natuurlijke persoon, die Opdrachtnemer in het kader van de Overeenkomst ten behoeve van Opdrachtgever verwerkt.

1.5 Verordening: Verordening (EU) 2016/679 van het Europees Parlement en de Raad van 27 april 2016 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens en tot intrekking van de Richtlijn 95/46/EG (algemene verordening gegevensbescherming).

1.6 Verwerkersovereenkomst: deze overeenkomst inclusief overwegingen en bijbehorende bijlagen.

1.7 Verwerking: een bewerking of een geheel van bewerkingen in het kader van de Overeenkomst met betrekking tot Persoonsgegevens, of een geheel van Persoonsgegevens, al dan niet uitgevoerd via geautomatiseerde procedés, zoals het verzamelen, vastleggen, ordenen, structureren, opslaan, bijwerken of wijzigen, opvragen, raadplegen, gebruiken, verstrekken door middel van doorzending, verspreiding of op andere wijze ter beschikking stellen, aligneren of combineren, afschermen, wissen of vernietigen.

Artikel 2. Voorwerp van deze Verwerkersovereenkomst

2.1 Deze Verwerkersovereenkomst regelt de Verwerking van Persoonsgegevens door Opdrachtnemer in het kader van de Overeenkomst.

2.2 De aard en het doel van de Verwerking, het soort Persoonsgegevens en de categorieën van Persoonsgegevens, Betrokkenen en ontvangers zijn in Bijlage 1 omschreven. Opdrachtgever garandeert dat de opdracht van de Verwerking in overeenstemming is met de door Opdrachtgever uitgevoerde data protection impact assessment (DPIA).

2.3 Opdrachtnemer garandeert de toepassing van passende technische en organisatorische maatregelen zoals bedoeld in Bijlage 2 , opdat de Verwerking aan de vereisten van de Verordening voldoet en de bescherming van de rechten van de Betrokkene is gewaarborgd.

2.4 Opdrachtnemer garandeert te voldoen aan de vereisten van de toepasselijke wet- en regelgeving betreffende de Verwerking van Persoonsgegevens zoals Opdrachtgever die heeft gecommuniceerd en vertaald zijn naar requirements.

Artikel 3. Inwerkingtreding en duur

3.1 Deze Verwerkersovereenkomst treedt in werking op het moment waarop deze door Partijen is ondertekend.

3.2 Deze Verwerkersovereenkomst eindigt nadat en voor zover Opdrachtnemer alle Persoonsgegevens overeenkomstig artikel 10 heeft gewist of terugbezorgd.

3.3 Geen van Partijen kan deze Verwerkersovereenkomst tussentijds opzeggen.

Artikel 4. Omvang verwerkingsbevoegdheid Opdrachtnemer

4.1 Opdrachtnemer Verwerkt de Persoonsgegevens uitsluitend in opdracht en op basis van schriftelijke instructies van Opdrachtgever behoudens afwijkende wettelijke voorschriften die op Opdrachtnemer van toepassing zijn.

4.2 Indien een instructie als bedoeld in het eerste lid naar het oordeel van Opdrachtnemer in strijd is met een wettelijk voorschrift inzake gegevensbescherming, stelt hij Opdrachtgever

daarvan voorafgaand aan de Verwerking in kennis, tenzij een wettelijk voorschrift deze kennisgeving verbiedt.

4.3 Indien Opdrachtnemer op grond van een wettelijk voorschrift Persoonsgegevens dient te verstrekken, informeert hij Opdrachtgever onmiddellijk, en zo mogelijk voorafgaand aan de verstrekking.

4.4 Opdrachtnemer heeft geen zeggenschap over het doel van en de middelen voor de Verwerking van Persoonsgegevens.

Artikel 5. Beveiliging van de Verwerking

5.1 In aanvulling op artikel 15 van de ARVODI-2018 en onverminderd artikel 2.3 treft Opdrachtnemer de technische en organisatorische beveiligingsmaatregelen zoals beschreven in Bijlage 2.

5.2 Partijen erkennen dat het waarborgen van een passend beveiligingsniveau voortdurend kan dwingen tot het treffen van aanvullende beveiligingsmaatregelen. Opdrachtgever garandeert Opdrachtnemer zo spoedig mogelijk op de hoogte te brengen van aanvullende of aangescherpte beveiligingseisen. Opdrachtnemer waarborgt een op het risico afgestemd beveiligingsniveau.

5.3 Indien en voor zover Opdrachtgever daarom uitdrukkelijk schriftelijk verzoekt, zal Opdrachtnemer aanvullende maatregelen treffen met het oog op de beveiliging van de Persoonsgegevens. Indien deze aanvullende maatregelen het beveiligingsniveau van Opdrachtnemer overstijgen en meerwerk oplevert dan komen de kosten voor deze aanvullende maatregelen voor rekening van Opdrachtgever.

5.4 Opdrachtnemer Verwerkt Persoonsgegevens niet buiten de Europese Unie, tenzij hij daarvoor uitdrukkelijk schriftelijk toestemming heeft verkregen van Opdrachtgever en behoudens afwijkende wettelijke verplichtingen.

5.5 Opdrachtnemer informeert Opdrachtgever zonder onredelijke vertraging zodra hij kennis heeft genomen van onrechtmatige Verwerkingen van Persoonsgegevens of inbreuken op beveiligingsmaatregelen zoals genoemd in het eerste en tweede lid.

5.6 Opdrachtnemer verleent Opdrachtgever bijstand bij het doen nakomen van de verplichtingen uit hoofde van de artikelen 32 tot en met 36 van de Verordening. De redelijke kosten die hierbij gemoeid zijn kunnen door Opdrachtnemer bij Opdrachtgever in rekening gebracht worden.

Artikel 6. Geheimhouding door Personeel van Opdrachtnemer

6.1 De Persoonsgegevens hebben een vertrouwelijk karakter als bedoeld in artikel 13.1 van de ARVODI-2018.

6.2 Opdrachtnemer toont op verzoek van Opdrachtgever aan dat zijn Personeel zich ertoe heeft verbonden vertrouwelijkheid in acht te nemen als bedoeld in artikel 13.2 van de ARVODI-2018.

Artikel 7. Subverwerker

Wanneer Opdrachtnemer, met inachtneming van het bepaalde in artikel 8 van de ARVODI-2018, een andere verwerker inschakelt om ten behoeve van Opdrachtgever verwerkingsactiviteiten te verrichten, worden aan deze andere verwerker bij een overeenkomst dezelfde verplichtingen inzake gegevensbescherming opgelegd als die welke in deze Verwerkersovereenkomst zijn opgenomen.

Artikel 8. Bijstand vanwege rechten van Betrokkene

Opdrachtnemer verleent Opdrachtgever bijstand bij het vervullen van diens plicht om verzoeken om uitoefening van de in hoofdstuk III van de Verordening vastgelegde rechten van de Betrokkene te beantwoorden. De redelijke kosten die hierbij gemoeid zijn worden door Opdrachtnemer bij Opdrachtgever in rekening gebracht.

Artikel 9. Inbreuk in verband met Persoonsgegevens

9.1 Opdrachtnemer informeert Opdrachtgever zonder onredelijke vertraging, zodra hij kennis heeft genomen van een Inbreuk in verband met Persoonsgegevens, overeenkomstig de afspraken zoals vastgelegd in Bijlage 3.

9.2 Opdrachtnemer informeert Opdrachtgever ook na een melding op grond van het eerste lid over ontwikkelingen betreffende de Inbreuk in verband met Persoonsgegevens.

9.3 Partijen dragen elk de door henzelf in verband met de melding aan de bevoegde toezichthoudende autoriteit en Betrokkene te maken kosten.

Artikel 10. Terugbezorgen of wissen Persoonsgegevens

10.1 Na afloop van de Overeenkomst draagt Opdrachtnemer, naar gelang de keuze van Opdrachtgever, zorg voor het terugbezorgen aan Opdrachtgever of het wissen van alle Persoonsgegevens. Opdrachtnemer verwijdert kopieën, behoudens afwijkende wettelijke voorschriften.

10.2 Zodra de Overeenkomst is beëindigd, zal Opdrachtnemer – naar keuze van Opdrachtgever – alle persoonsgegevens die bij haar aanwezig zijn in originele of kopievorm retourneren aan Opdrachtgever, en/of deze persoonsgegevens en eventuele kopieën daarvan verwijderen en/of vernietigen op instructie van Opdrachtgever.

Artikel 11. Informatieverplichting en audit

11.1 Opdrachtnemer stelt alle informatie ter beschikking die nodig is om aan te tonen dat de verplichtingen uit deze Verwerkersovereenkomst zijn en worden nagekomen.

11.2 Opdrachtnemer verleent op basis van nacalculatie alle benodigde medewerking aan audits. De bedoelde audit vindt plaatst nadat Opdrachtgever de bij Opdrachtnemer aanwezige soortgelijke auditrapportages heeft opgevraagd, beoordeeld en zij redelijke argumenten ziet om een audit te doen.

11.3 Opdrachtnemer verstrekt met een frequentie van eenmaal per jaar, uiterlijk op 1 maart aan Opdrachtgever een verklaring van een onafhankelijke externe deskundige, waarin deze een oordeel geeft over de genoemde naleving.

Artikel 12. Aansprakelijkheid

12.1 De totale aansprakelijkheid van Opdrachtnemer wegens een toerekenbare tekortkoming in de nakoming van de Verwerkersovereenkomst of de AVG, daaronder uitdrukkelijk ook begrepen iedere tekortkoming in de nakoming van een met Opdrachtgever overeengekomen garantieverplichting, is op jaarbasis beperkt tot maximaal € 500.000 (vijfhonderd duizend euro). Indien de schade samenhangt met fouten en/of tekortkomingen van derden c.q subverwerkers is Opdrachtnemer niet meer aansprakelijk dan zij bij die derden daadwerkelijk heeft verhaald.

12.2. De in dit artikel bedoelde uitsluitingen en beperkingen komen te vervallen indien en voor zover de schade het gevolg is van opzet of bewuste roekeloosheid van de bedrijfsleiding van Opdrachtnemer.

Aldus op de laatste van de twee hierna genoemde data overeengekomen en in tweevoud ondertekend,

Breda, datum: 14-12-20	Den Haag, datum: 15-12-2020
GGD WEST-BRABANT	DE MINISTER/STAATSSECRETARIS Volksgezondheid, Welzijn en Sport
namens deze,	

Bijlage 1. De Verwerking van Persoonsgegevens

In deze bijlage moet in ieder geval het volgende worden gespecificeerd:

Het onderwerp/aard en doel van de Verwerking	De verwerking door opdrachtnemer betreft het hosten van app, sluis en webportal van 'GGD Contact'. Het doel van de app GGD Contact is om het aantal uur dat GGD per index (besmet persoon) besteedt aan bron- en contactopsporing te verminderen, waardoor GGD voor meer indexen bron- en contactopsporing kan uitvoeren.
Het soort Persoonsgegevens	(1) bijzondere categorieën van gegevens als bedoeld in artikel 9 van de Verordening, (3) wettelijk voorgeschreven identificatienummers en (4) overige persoonsgegevens.
Beschrijving categorieën Persoonsgegevens	Gegevens die de GGD nodig heeft voor bron- en contactopsporing. Dit zijn gezondheidsgegevens. (Bijvoorbeeld: 'netwerk'/'relatie'-gegevens: gegevens over contacten van index; contactgegevens; besmettingsrisico; klachten; overige gegevens ingevuld door index in open veld)
Beschrijving categorieën Betrokkenen	Met infectieziekte besmette personen ('index') en diens contacten die mogelijk ook zijn besmet ('contacten')
Beschrijving categorieën ontvangers van Persoonsgegevens	-

Voor de inhoud van deze bijlage kan onder meer gebruik worden gemaakt van de registratie die de Verwerkingsverantwoordelijke op grond van artikel 30 van de Verordening dient aan te houden.

Bijlage 2. Passende technische en organisatorische maatregelen

In deze bijlage moeten de normen en maatregelen die Opdrachtnemer in het kader van de beveiliging van de Verwerking moet hanteren respectievelijk treffen worden gespecificeerd. Hiervoor kan worden verwezen naar documenten waarin normen en maatregelen zijn vastgelegd, zoals in voorkomend geval het programma van eisen of de offerteaanvraag.

ISO 27001
NEN 7510
Security Operations Center
Actieve Threat Hunting

Bijlage 3: Afspraken betreffende Inbreuken in verband met Persoonsgegevens

In deze bijlage moeten de afspraken over hoe Opdrachtnemer Opdrachtgever over Inbreuken in verband met Persoonsgegevens gaat informeren worden gespecificeerd.

Departementale procedure

Informatie die ten minste door Opdrachtnemer moet worden verstrekt

Aard van de Inbreuk in verband met Persoonsgegevens
De Persoonsgegevens en Betrokkene
Waarschijnlijke gevolgen van de Inbreuk in verband met Persoonsgegevens
Maatregelen die Opdrachtnemer heeft voorgesteld of genomen om de Inbreuk in verband met Persoonsgegevens aan te pakken, waaronder, in voorkomend geval, de maatregelen ter beperking van de eventuele nadelige gevolgen daarvan

Archived: donderdag 12 mei 2022 11:51:09
From: [redacted]
Sent: woensdag 10 maart 2021 11:52:43
To: [redacted]
Cc: [redacted]
Subject: FW: update vervanging HP Zone - inbreng IZ professionals [1]
Importance: Normal
Sensitivity: None
Attachments:
Interne nieuwsbericht - ontwikkeling nieuw ICT-systeem voor COVID-19-bestrijding.pdf;

GGD West-Brabant

[redacted]

\itap2M [redacted]
T [redacted]
E [redacted]
\itap2GGD West-Brabant
Doornboslaan 225-227
4816CZ Breda

\itap2www.ggdwestbrabant.nl/

Van: [redacted]
Verzonden: woensdag 10 maart 2021 10:19
Aan: [redacted]
Onderwerp: update vervanging HP Zone - inbreng IZ professionals [1]

Beste collega's,
Bijgevoegd aan deze email vind je het eerste nieuwsbericht over de vervanging van HPZone voor de COVID-19 bestrijding.
In deze begeleidende email willen we je uitleggen hoe de inbreng van de IZ-professionals (artsen, verpleegkundigen, epidemiologen) in de vervanging van HPZone is georganiseerd.
Dit is ook gepresenteerd in het LOI van 2 maart.
HPZone (voor de COVID-19 bestrijding) wordt op zo kort mogelijk termijn vervangen met een andere applicatie die uit 3 onderdelen bestaat:
1. een applicatie voor de uitvoering van bron- en contactonderzoek voor de COVID-19-bestrijding;
2. een voorziening voor data-analyse en uitbraakbestrijding;
3. een platform voor gegevensuitwisseling met het RIVM en de GGD'en.
Er is een landelijk programmaorganisatie opgericht om het nieuwe ICT-systeem te ontwikkelen en te implementeren. Artsen infectieziektebestrijding,
verpleegkundigen en epidemiologen van de verschillende GGD'en worden nauw betrokken bij de ontwikkeling van het nieuwe systeem, zodat het goed aansluit op de praktijk en behoeftes.
Onderdeel van deze projectorganisatie is het product-owner-overleg en bestaat uit vijf deelproceseigenaren en één product-owner. Dit zijn allemaal IZ professionals, die gekozen zijn op basis van hun kennis van het werkproces IZB.
Op dit moment wordt bepaald wat de minimale vereisten zijn voor het nieuwe ICT-systeem voor de COVID-19 bestrijding en dat voldoet aan alle eisen op het gebied van volledigheid, gebruiksvriendelijkheid en privacy.
Dit wordt het zgn. minimum viable product genoemd. Uiteindelijk levert dit een lijst (de backlog) op van benodigde functionaliteiten, die beschreven zijn in een korte tekst (user story) en vertaald worden naar "epics" die in "bouwerstaal" beschreven zijn.
Het ontwikkelteam gaat daarmee aan de slag in sprints van twee weken. In het product-owner-overleg wordt bepaald welke functionaliteit als eerste wordt ontwikkeld en wanneer de functionaliteit af is.

Het product-owner-overleg bestaat uit:

- Inhoudelijke IZB functionaliteit, [redacted]
- Proceseigenaar [redacted]
- Proceseigenaar [redacted]
- Proceseigenaar [redacted]
- Proceseigenaar [redacted]
- Proceseigenaar [redacted]

Per deelproces zijn er verder een aantal personen (arts, verpleegkundigen, epidemiologen (waaronder REC) aangehaakt als expert.
Je kunt in bovenstaande twee belangrijke besluiten zien:

- Wat is het minimum viable product?
- Wanneer is het minimum viable product af en klaar om geïmplementeerd te worden?

Over deze twee besluiten krijgt de COVID-19 Commissie van de DPG-raad advies van het zgn. afstemmingsoverleg. Dit overleg wordt voorgezeten door [redacted], arts M&G IZ, en bestaat uit:

- [redacted], arts M&G IZ, voorzitter HP Zone gebruikersgroep / GGD Brabant Zuid-Oost;
- [redacted], arts M&G IZ, RAC / GGD Zuid-Limburg;
- [redacted], arts M&G, RAC / GGD Amsterdam;
- [redacted], arts IZB, M&G i.o. / GGD Utrecht;
- [redacted], verpleegkundige M&G, LOVI / GGD Gelderland-Zuid;
- [redacted], arts M&G IZ, LCI RIVM;
- [redacted], arts M&G IZ, coördinator REC RIVM.

Het afstemmingsoverleg komt wekelijks bij elkaar en volgt de voortgang in het product owners-overleg op de voet zodat er proactief geadviseerd kan worden.
De programmaorganisatie wordt aangestuurd door een stuurgroep. [redacted] neemt, als voorzitter afstemmingsoverleg, deel namens de IZ-professionals.
De COVID-19 Commissie van de DPG-raad wordt geadviseerd door de voorzitter van de RAC [redacted] en voorzitter LOI [redacted].
We zijn van mening dat bovenstaande structuur goede inbreng van de IZ-professionals waarborgt en voorkomt dat door tijdsdruk of andere overwegingen de inhoudelijke kwaliteit van de applicatie onder druk komt te staan.
We informeren jullie over het vervolg via de nieuwsberichten, presentaties in het LOI, en waar nodig met een extra bericht zoals dit. Vragen en opmerkingen over bovenstaande kun je sturen aan medischadvies@ggdghor.nl.
Met vriendelijke groet,
[redacted]

Archived: donderdag 12 mei 2022 11:51:18
From: [redacted]
Sent: dinsdag 7 december 2021 12:07:58
To: [redacted]
Subject: FW: Update Autorisatiematrix GGD Contact en verzoek tot aanmaken AD groepen
Importance: Normal
Sensitivity: None
Attachments:
Rollenmatrix GGD Contact Nov 2021 GGD V1.8.pd[redacted]llenmatrix GGD Contact Nov 2021 Landelijk V1.8.p[redacted]11206 Beschrijving contextbeheer&dossierkwaliteit - GGD Contact[29].[redacted]

From: [redacted]
Sent: Monday, December 6, 2021 6:14 PM
To: [redacted]
Subject: Update Autorisatiematrix GGD Contact en verzoek tot aanmaken AD groepen

Beste [redacted]

Hieronder de mail die einde middag naar de TC's is gegaan t.b.v. de AD groepen.

Beste Transitie coördinatoren,

In deze mail treffen jullie informatie aan over nieuwe functionaliteit en bijhorende rollen t.b.v. het BCO-Portaal.

Hieronder sommen we de belangrijkste zaken op. Bijgevoegd treffen jullie nog 3 documenten aan te weten: Autorisatiematrix voor GGD'en, Autorisatiematrix voor landelijke partners (alleen ter informatie voor jullie) én een uitgebreide beschrijving van de rollen zoals hieronder vermeld in punt 1 en 2.

1. Aanmaken en toekennen rol Contextbeheer (per release 1.8)

Zoals in het laatste overleg (d.d. 1-12-2021) aangekondigd komt er op korte termijn functionaliteit beschikbaar voor context beheer, deze functionaliteit wordt in volgende releases verder uitgebreid. Deze functionaliteit is uitsluitend toegankelijk / te gebruiken voor collega's welke hiervoor de juiste rechten hebben. Hiervoor is een aparte AD rol noodzakelijk. De betreffende rol is Context beheerder. Deze staat opgenomen in de bijgevoegde autorisatiematrix. Aan jullie het verzoek om deze rol aan te (laten) maken en toe te kennen aan de juiste collega's binnen jullie organisatie. Een beknopte samenvatting van de betreffende rol is terug te vinden in de autorisatiematrix. Aanvullend tref je in deze mail een bijlage waarin een uitgebreide beschrijving is opgenomen van de rol contextbeheer. We willen jullie verzoeken deze beschrijving door te nemen met als doel hierna de AD rol aan juiste personen binnen jullie organisatie te kunnen toekennen. De rol van contextbeheerder mag worden toegekend aan collega's welke op dit moment ook een andere rol hebben in het BCO-Portaal.

2. Aanmaken en toekennen rol Medewerker dossierkwaliteit (waarschijnlijk per release 1.9)

Er wordt op dit moment hard gewerkt om functionaliteit beschikbaar te gaan maken t.b.v. kwaliteitschecks in een dossier. Deze functionaliteit komt waarschijnlijk in release 1.9 beschikbaar. Ook deze functionaliteit kan alleen worden gebruikt wanneer men beschikt over de bijbehorende AD rol. Net als voor de rol van contextbeheer is hiervoor ook een aparte AD rol beschikbaar.

Deze staat opgenomen in de bijgevoegde autorisatiematrix. Aan jullie het verzoek om deze rol aan te (laten) maken en toe te kennen aan de juiste collega's binnen jullie organisatie. Een beknopte samenvatting van de betreffende rol is terug te vinden in de autorisatiematrix. Aanvullend tref je in deze mail een bijlage waarin een uitgebreide beschrijving is opgenomen van de rol Medewerkers dossier kwaliteit. We willen jullie verzoeken deze beschrijving door te nemen met als doel hierna de AD rol aan juiste personen binnen jullie organisatie te kunnen toekennen. De rol van contextbeheerder mag worden toegekend aan collega's welke op dit moment ook een andere rol hebben in het BCO-Portaal.

3. Rollen aanmaken, maar nog niet toekennen: Medische supervisie en Gesprekscoach

In de autorisatiematrix staan nog twee andere nieuwe rollen toegekend, te herkennen aan een gele arcering. Ondanks dat er nog geen specifieke functionaliteit beschikbaar is voor deze rollen leek het ons belangrijk deze al in een vroeg stadium bij jullie onder de aandacht te brengen. Wanneer de rol van contextbeheerder wordt aangemaakt in jullie AD kan de afweging worden gemaakt om ook direct de andere rollen te (laten) aanmaken. Hierdoor reduceren we het aantal contactmomenten en kunnen dezelfde werkzaamheden direct na elkaar worden uitgevoerd. Wanneer de extra rollen al zijn aangemaakt kunnen deze in de toekomst snel(ler) worden toegekend. We zijn ons er van bewust dat dit laatste pas mogelijk is er meer informatie over de functionaliteit beschikbaar is. Hiervoor dienen we qua ontwikkeling nog verschillende stappen te maken. Later volgt er dan ook naar jullie toe een aanvullende beschrijving behorende bij de betreffende rollen.

4. DPIA aanpassingen

Afhankelijk van de exacte functionaliteit welke beschikbaar komt voor een bepaalde rol wordt bepaald of er aanpassing(en) noodzakelijk zijn aan de huidige DPIA. Dit heeft te maken met de mate van risico welke de functionaliteit met zich meebrengt. Dit invulling van de rol is daar dan onderdeel van, maar zeker niet het enige waar naar gekeken wordt. Voor de functionaliteit van clusterbeheer is de conclusie dat hiervoor geen apart addendum voor hoeft te worden opgesteld.

Voor de, in de bijgevoegde autorisatiematrix, aangegeven toekomstige rollen wordt er t.z.t. ook beoordeeld of hiervoor een addendum noodzakelijk is. Dit proces verloopt in overleg met de FG'en welke een periodieke afspraak met elkaar hebben. Pas wanneer de DPIA / het addendum hierop definitief is kan de functionaliteit in gebruik worden genomen. Voor vragen over de DPIA of mogelijke aanpassingen willen we jullie verzoeken om jullie eigen FG te consulteren.

5. Afsluitend nog over de autorisatiematrix zelf

In de autorisatiematrix tref je zowel de technische naamgeving aan, een korte beschrijving van de rol en welke mogelijkheden deze rol exact wel/niet heeft binnen de applicatie. De rechten en rollen zijn tot stand gekomen met behulp van collega's van regionale GGD-en en getoetst door experts van VWS en GGD GHOR op het vlak van security en privacy.

Alvast bedankt voor het aanmaken van de nieuwe rollen. Graag verneem ik wanneer de rollen zijn aangemaakt en de rollen Contextbeheerder en Medewerker Dossierkwaliteit ook zijn toegekend.

Voor vragen, onduidelijkheden ben ik via email bereikbaar.

Met vriendelijke groet,

[redacted]

[redacted]

GGD GHOR NEDERLAND

Zwarte Woud 2
3524 SJ Utrecht
Tel: [redacted]
Teams: [redacted]

E-mail : [redacted]
Website : www.ggdghor.nl
Twitter : @GGDGHORNL
Werkdagen : di, woe, do, vrij

West-Brabant

Aan: het algemeen
bestuur van de GGD
West-Brabant

Kenmerk: [redacted]293126616-9158 Datum: 15 februari 2021
Behandeld door: [redacted] E-mail: [redacted]
Onderwerp: Vervangen van ICT-systeem HP-Zone

Geachte leden van ons algemeen bestuur,

Graag wil ik u in vervolg op de eerdere berichtgeving rond de datadiefstal informeren. De datadiefstal, waarmee wij als GGD'en eind januari zijn geconfronteerd, heeft ook gevolgen voor de wijze van Coronabestrijding de komende periode.

Door deze diefstal zijn we op harde wijze geconfronteerd met kwetsbaarheden in onze ICT-systemen en de vergaande gevolgen hiervan. De impact van risico's die veelal eerder waren gesignaleerd, vragen om een daadkrachtige, snelle en eenduidige aanpak. Er zijn inmiddels aanzienlijke korte-termijn maatregelen genomen om gebleken risico's in de verwerking van persoonsgegevens te beperken. Daarboven wordt er hard gewerkt om de bescherming van persoonsgegevens verder te maximaliseren. Een belangrijk onderdeel hierin is de vervanging van HP-Zone.

Vervanging HP-Zone
Bij de GGD'en vormt HP-Zone het ICT-'hart' voor infectieziektebestrijding. Het systeem is bij vrijwel alle GGD'en al langere tijd in gebruik. Met de nodige aanpassingen is HP-Zone ingezet voor de bestrijding van de Corona-pandemie. Het systeem was voor het gebruik in zo'n grote omvang niet geschikt, maar een alternatief was helaas niet snel inzetbaar toen we als GGD-en onze activiteiten moesten opschalen. Om die reden werd de afgelopen maanden al gewerkt aan een vervangende applicatie 'GGD Contact'. De datadiefstal maakte nog meer zichtbaar dat HP-Zone niet kan worden aangepast tot een betrouwbaar en veilig systeem en zo spoedig mogelijk moet worden vervangen.

De genomen maatregelen om persoonsgegevens veilig te kunnen verwerken in HP-Zone hebben grote impact op het werkproces en vragen omslachtige maatregelen. Aanvullende externe analyses hebben nog dringender duidelijk gemaakt dat er onaanvaardbare risico's ontstaan, indien

wordt verder gewerkt met HP-zone. Deze risico's hebben betrekking op de operationele en inhoudelijke betrouwbaarheid van het systeem. Bovendien zijn binnen de architectuur van het systeem bestaande veiligheidsrisico's niet structureel te ondervangen.

Om het beëindigen van het gebruik van HP-Zone voor de Corona-bestrijding op korte termijn mogelijk te maken, zal een combinatie van applicaties worden ingezet: Dit betreft 'GGD-Contact' (BCO medewerkers-portaal en telefoon-app) voor uitvoering van Bron- en Contactonderzoek (BCO), een voorziening voor data-analyse, alsmede een voorziening voor het inhalen van gegevens door het RIVM. Daarmee wordt voorzien in de eisen ten aanzien van privacy, veiligheid en functionaliteit voor bestrijding van Covid-19.
Voor de vervanging van HP-Zone ten behoeve van de totale infectieziektebestrijding is meer tijd beschikbaar en daarvoor kan dan ook meer tijd worden genomen. Ook die stap blijkt noodzakelijk en bereiden we voor. De Minister van VWS treedt op als opdrachtgever voor het vervangingstraject, op zijn verzoek coördineert GGD GHOR landelijk de vervanging.

Besluit tot vervanging
De Directeuren Publieke Gezondheid hebben gezamenlijk derhalve besloten om de volgende stappen te ondernemen:
- Zo snel als mogelijk wordt 'GGD Contact' in combinatie met bovengenoemde voorzieningen bij alle 25 GGD'en geïmplementeerd en wordt daarmee HP-Zone niet meer gebruikt voor de Corona-bestrijding;
- In gezamenlijkheid bereiden GGD GHOR Nederland, de 25 GGD-en het RIVM voor de totale infectieziektebestrijding een spoedige vervanging van HP-Zone voor. Het is nog niet duidelijk hoe lang dit traject zal duren.

Beperking risico's
Overstappen naar een nieuw ICT systeem onder hoge tijdsdruk en tijdens een lopende operatie kent uiteraard risico's. Hierover zijn ook zorgen geuit door onder meer de artsen infectiebestrijding en het RIVM. Beide partijen zijn nauw betrokken bij aanvullende stappen om deze risico's te beperken. Daarboven worden binnen de afzonderlijke GGD'en inmiddels programmateams gevormd om de implementatie van GGD-Contact in combinatie met bovengenoemde voorzieningen in goede banen te leiden. Hierbij wordt in het bijzonder aandacht besteed aan:
- De ketensamenwerking in de bestrijding van Corona en andere infectieziekten (vooral de uitwisseling van gegevens).
- Het borgen van beschikbaarheid van historische data uit het HP-zone systeem
- De operationele betrouwbaarheid van de Corona-bestrijding
- De informatievoorziening aan gemeenten en andere ketenpartners.

Financiële risico's
De kosten voor de ontwikkeling en het gebruik van het nieuwe systeem GGD-Contact worden vrijwel geheel gedragen door het ministerie van VWS. De kosten voor ontwikkeling en uitvoering van een nieuw systeem voor de infectieziektebestrijding komen in principe ten laste van de begroting van de afzonderlijke GGD'en. Het is op dit moment nog niet aan te geven in hoeverre dit leidt tot structurele meerkosten in de gemeentelijke bijdrage. Zodra we hierover meer informatie hebben, kom ik hierop bij u terug.

Ik vertrouw erop dat we met deze aanpak een benodigde stap zetten om het vertrouwen in de ICT-systemen van de GGD-en te kunnen herstellen. Bij vragen kunt u contact opnemen met [redacted]

Met vriendelijke groet,

[redacted]
directeur publieke gezondheid

Notitie t.a.v. gebruik app voor burger naast BCO Portaal

Deze notitie bevat vanuit de inhoud geredeneerde voor- en nadelen bij het in gebruik nemen van de app GGD Contact die aanvullend zal werken bij BCO portaal.

Bij het schrijven van de notitie wordt er gekeken naar de huidige versie van de app (op 06-05-2021).

De voor- en nadelen

Voordelen	**Nadelen**
Burgers kunnen na het lezen van de uitslag via het uitslagenportaal makkelijker het BCO voorbereiden.	Enkel de burgers die de uitslag via het portaal krijgen zullen vooraf de app downloaden.
Wanneer burgers de app hebben gebruikt zal het BCO korter en naar waarschijnlijk effectiever zijn. Mits de huidige functionele issues verwerkt zijn.	Er zijn op moment van schrijven nog behoorlijk veel functionele issues die in de app verbeterd moeten worden.
Wanneer iemand heel veel contacten heeft, neemt de effectiviteit van de app toe en levert deze voor het BCO meer tijdswinst op.	De app heeft vooral vooraf toegevoegde waarde en het heeft veel minder waarde om de app tijdens of na het BCO nog te gebruiken.
Wanneer een index heel veel contacten heeft, kan het nog nuttig zijn om de app tijdens het BCO gesprek te downloaden (tijdswinst).	Er zijn twijfels over de draagkracht onder bewoners om de app te gaan gebruiken. Dit i.v.m. datadiefstal, een app moeten instaleren op je telefoon, enkel voor de mensen die via het portaal de uitslag inzien en de bereidheid om als burger van te voren werk te steken in het BCO.
De app maakt gebruik van cognitieve interview technieken in de wijze en volgorde van vragen stellen. Er is gebleken dat deze wijze resulteert in meer contacten identificeren gedurende het Contactonderzoek.	De app kan moeilijk in fases live. Wanneer op het uitslagenportaal staat dat je de app kunt downloaden dan moet iedere GGD het gebruik van de app ondersteunen (hier zijn mogelijk wel workarounds voor). Echter zal er ook rekening moeten worden gehouden met draagkracht wanneer het wel mogelijk is om de app in fases te implementeren. Als inwoners in Rotterdam er wel iets mee kunnen en Amsterdammers niet, ontstaat er in Amsterdam hoe langer die situatie voortduurt een lagere draagkracht.
Alle inwoners die gebruik maken van de app, krijgen dezelfde vragen. Dit levert kwalitatief betere data op voor epidemiologische analyse en clusters.	In de app worden bepaalde conclusies getrokken op wat inwoners invullen. Dus als ik denk dat ik wel 1,5 meter afstand hield en ik denk dat ik niet langer 15 minuten in dezelfde ruimte was met iemand concludeer ik samen met de app dat dit geen contact is. Mogelijk benoem ik dit daarom niet meer in het BCO, terwijl bij doorvragen mogelijk toch nauwer contact zou kunnen blijken.
Bij doorontwikkeling is er de mogelijkheid dat er voor bepaalde groepen een zelf-BCO uitgevoerd kan worden. Hierdoor kan de GGD haar energie vooral richten op de “special cases”, op clustermanagement en het	

volgen/analyseren van de epidemiologische trend in de regio.	

Als aanvulling op de voor/nadelen, kunnen we ook kijken naar de manier hoe we de app kunnen gebruiken en ook daar nog onderscheid in maken. Voor elk scenario zijn natuurlijk meer voor- en nadelen te bedenken.

Scenario 1: Uitrol Applicatie met volledige functionaliteit **inclusief** brede communicatie van de app bij positieve test (via coronatest.nl).
Consequenties:

1. Bij de communicatie moet aangegeven worden welke GGD'en met de APP werken en dat je de app alleen moet downloaden als je woonachtig bent in die GGD regio.
2. Zowel de regionale GGD als de Landelijke Partner moet met het Portaal werken, omdat anders Indexen bij landelijk terechtkomen met een ingevulde GGD Contact APP met informatie die ze niet kwijt kunnen.
3. Breder draagvlak en meeste functionaliteit

Scenario 2: Uitrol Applicatie met volledige functionaliteit **zonder** brede communicatie van de app bij positieve test (via coronatest.nl)

Consequenties:

1. Het gehele 'zelf-BCO' gedeelte vervalt
2. 2 andere functionaliteiten van GGD Contact APP blijven intact, zoals;
    a. Tijdens BCO met veel contacten kan er voor gekozen te worden om de Index tijdens het gesprek de app te laten downloaden en alle contacten via de APP aan te leveren. Gesprek wordt later opgepakt en de contacten worden gekoppeld. BCO'er kan vanuit daar weer verder met BCO. (vooral handig in fase 1a, 1b, 2 (hoog risico) met veel contacten die geïnventariseerd moeten worden.
    b. In lagere fases kan gekozen worden om samen met Index de contacten in beeld te brengen in het Portaal tijdens je BCO gesprek. Dus je vult alle contacten in met 'datum laatste blootstelling' en categorie contact. Aan het eind van het gesprek kan de index de GGD Contact APP downloaden en met de koppelcode krijgt de index alle informatie op zijn/haar telefoon. Vanuit daar kan de index iedereen zelf de de op maat gemaakte leefregels makkelijk versturen naar de contacten vanuit de APP.
    c. In dit scenario is het niet noodzakelijk dat de Landelijke Schil in het portaal werkt. Het voorstel om de app te gebruiken komt dan vanuit de BCO'er en kan alleen als hij/zij in het Portaal werkt.

3. **Scenario 3:** Uitrol 1.1 release zonder Applicatie
   Consequenties:
    1. De meerwaarde/tijdwinst van het Portaal wordt een stuk minder, waardoor minder draagvlak.

OVEREENKOMST HOSTING EN BEHEER 'GGD CONTACT'

1. De Staat der Nederlanden, waarvan de zetel is gevestigd te Den Haag, te dezen vertegenwoordigd door de Minister van Volksgezondheid, Welzijn en Sport, namens deze, [redacted], hierna te noemen: De Staat;

en

2. De publiekrechtelijke rechtspersoon Gemeentelijke of Gemeenschappelijke Gezondheidsdienst West-Brabant, statutair gevestigd en kantoorhoudende te 4816 CZ, Breda te Doornboslaan 225, ingeschreven in het handelsregister van de Kamer van Koophandel onder nummer 20164916, hierbij vertegenwoordigd door [redacted], [redacted] Publieke Gezondheid, hierna te noemen: GGD West-Brabant;

hierna gezamenlijk te noemen: Partijen;

komen overeen dat:

- De Staat ten behoeve van GGD West-Brabant het beheer en de hosting (zoals o.m. bedoeld in Plan van Aanpak realisatie GGD Contact-app, versie 0.955, 19 november 2020) verzorgt van 'GGD Contact', ofwel de applicatie die is bedoeld om door GGD'en te worden ingezet ter ondersteuning van de bron- en contactopsporing.

- GGD West-Brabant instemt met het inschakelen van Intermax Cloudsourcing BV door de Staat als zgn. subverwerker, voor het uitvoeren van het overeengekomen beheer en hosting. Tussen de Staat en Intermax Cloudsourcing BV is in dat kader een verwerkersovereenkomst gesloten (zie bijlage).

Bijlage: Verwerkersovereenkomst Staat - Intermax

Aldus op de laatste van de twee hierna genoemde data overeengekomen en in tweevoud ondertekend,

Plaats: Datum: De Minister van Volksgezondheid, Welzijn en Sport namens deze, [redacted] [redacted]	Plaats: Breda Datum: 14 december 2020 [redacted]

Privacyverklaring GGD Contact

Laatst bijgewerkt: 11 december 2020. Deze privacyverklaring kan worden gewijzigd.

Er zijn 25 GGD'en in Nederland. Welke GGD uw GGD is, is afhankelijk van uw woonplaats, zie: www.ggd.nl. Vijf GGD'en bieden het gebruik van 'GGD Contact' aan. Indien u in één van deze vijf regio's woont, kunt u 'GGD Contact' gebruiken. Met deze privacyverklaring informeert uw GGD u over hoe zij met uw gegevens omgaat bij het gebruik van 'GGD Contact'. Elke GGD is zelfstandig verantwoordelijk voor de gegevensverwerking via 'GGD Contact'. Het gaat om deze vijf GGD'en:

GGD West-Brabant: Doornboslaan 225-227, 4816CZ Breda, www.ggdwestbrabant.nl, [redacted]

GGD Zuid-Limburg: Het Overloon 2, 6411 TE Heerlen, www.ggdzl.nl, [redacted]

GGD Rotterdam-Rijnmond: Schiedamsedijk 95, 3011 EN Rotterdam, www.ggdrotterdamrijnmond.nl, (010) 433 9966, [redacted]

GGD Gooi- en Vechtstreek: Burgemeester de Bordesstraat 80, 1404 GZ Bussum, www.ggdgv.nl, [redacted]

GGD Twente: Nijverheidstraat 30, 7511 JM Enschede, www.ggdtwente.nl, [redacted]

De oplossing GGD Contact bestaat uit een app, datasluis en webportal. De app draait op uw smartphone. De datasluis en de webportal draaien op een server van een hostingpartij van uw GGD. Tijdens uw telefoongesprek met uw GGD krijgt u een activatiecode voor de app. Naar aanleiding van uw telefoongesprek met uw GGD maakt uw GGD een lijstje met nog in te vullen velden. Na activatie van de app verschijnt dit lijstje in de app op uw smartphone. Vanuit uw smartphone kunt u gegevens kopiëren naar de app. (Tip: Als u heel veel contacten heeft in uw smartphone, kunt gebruik maken van een extra functie in de app: op basis van de naam die uw GGD heeft ingevuld kan de app een suggestie doen uit contacten in uw smartphone en hoeft u niet te zoeken. Dit werkt alleen als u een kopie van alle namen uit uw telefoonboek in de app laat laden). U kunt de gegevens ook handmatig invullen en vervolgens naar uw GGD versturen. Verder is het mogelijk om nieuwe contacten aan het lijstje toe te voegen. Van deze contacten moet u dan zelf de risicocategorie bepalen aan de hand van een aantal vragen. Na het delen komen de gegevens via de datasluis (een doorgeefluik voor gegevens) in het webportal terecht. Tot 48 uur na activatie kunt u zo vaak gegevens delen als u wilt. Eenmaal verstuurde gegevens kunt u niet meer zelf terughalen. Via de webportal kan uw GGD uw gegevens inzien en bewerken. Vanuit de webportal worden de gegevens verplaatst naar de interne systemen van uw GGD. Deze privacyverklaring heeft alleen betrekking op gegevensverwerkingen met GGD Contact en niet op gegevensverwerkingen met de interne systemen van uw GGD.

Doel:

Het doel van de app 'GGD Contact' is om het aantal uur dat de GGD per besmet persoon besteedt aan bron- en contactopsporing te verminderen, waardoor GGD voor meer besmette personen bron- en contactopsporing kan uitvoeren. Door gebruik te maken van GGD Contact draagt u hieraan bij. Met GGD Contact kunt u gegevens over mensen die mogelijk door u zijn besmet verstrekken aan uw GGD. Het gaat om contactgegevens en besmettingsrisico.

Rechtsgrond:

De verwerking van persoonsgegevens via GGD Contact is noodzakelijk voor de vervulling van een taak van algemeen belang die aan uw GGD is opgedragen, namelijk het uitvoeren van bron- en contactopsporing. Deze verwerking is noodzakelijk om redenen van algemeen belang op het gebied van de volkgezondheid (artikel 6 lid 1 sub e jo. 9 lid 2 sub i Algemene verordening gegevensbescherming jo. artikel 6 lid 1 sub c Wet publieke gezondheid).

Ontvangers:

Uw GGD ontvangt de gegevens die u met GGD Contact verstuurt.

De hostingpartij van de datasluis en de webportal verwerkt uw gegevens. Alleen als dat nodig is om een probleem met de datasluis of webportal op te lossen, mag de hostingpartij gegevens bekijken. Uw gegevens zijn versleuteld, waardoor de hostingpartij deze niet kan zien.

De minister van VWS treedt op als contractspartij tussen uw GGD en de hostingpartij, maar heeft geen toegang tot de gegevens.

Bewaartermijnen:

De gegevens in de app op uw smartphone worden bewaard zolang u dat wilt. U kunt de gegevens zelf uit de app verwijderen. Als u de app verwijdert, verwijdert u daarmee ook alle gegevens.

De gegevens in de datasluis worden na 48 uur automatisch verwijderd.

De gegevens in het webportal worden na twee weken automatisch verwijderd.

Uw rechten:

U heeft het recht uw GGD te verzoeken om inzage van en rectificatie of wissing van de persoonsgegevens of beperking van de verwerking, alsmede het recht tegen de verwerking bezwaar te maken. De GGD zal niet altijd aan uw verzoeken kunnen voldoen, omdat de GGD een wettelijke taak heeft tot bron- en contactopsporing. Eenmaal verstuurde gegevens kunt u niet meer zelf terughalen. Uw GGD zal een verzoek alleen toewijzen als dat de bron- en contactopsporing niet belemmert.

U bent niet verplicht persoonsgegevens te verstrekken. Het verstrekken van gegevens gebeurt vrijwillig. Het verstrekken van gegevens is ook geen voorwaarde voor het sluiten van een overeenkomst. Zonder uw medewerking kan de GGD echter geen bron- en contactopsporing doen.

GGD Contact maakt geen gebruik van geautomatiseerde besluitvorming of profilering.

Klachten:

Bij vragen of klachten over GGD Contact kunt u contact opnemen met uw eigen GGD of diens Functionaris Gegevensbescherming.

U heeft ook altijd het recht een klacht in te dienen bij de Autoriteit Persoonsgegevens: www.autoriteitpersoonsgegevens.nl.

Archived: donderdag 12 mei 2022 11:51:14
From: [redacted]
Sent: Wed, 10 Mar 2021 09:18:51
To: [redacted]
Subject: update vervanging HP Zone - inbreng IZ professionals [1]
Importance: Normal
Sensitivity: None
Attachments:
Interne nieuwsbericht - ontwikkeling nieuw ICT-systeem voor COVID-19-bestrijding.pd[redacted]

Beste collega's,
Bijgevoegd aan deze email vind je het eerste nieuwsbericht over de vervanging van HPZone voor de COVID-19 bestrijding.
In deze begeleidende email willen we je uitleggen hoe de inbreng van de IZ-professionals (artsen, verpleegkundigen, epidemiologen) in de vervanging van HPZone is georganiseerd.
Dit is ook gepresenteerd in het LOI van 2 maart.
HPZone (voor de COVID-19 bestrijding) wordt op zo kort mogelijk termijn vervangen met een andere applicatie die uit 3 onderdelen bestaat:
1. een applicatie voor de uitvoering van bron- en contactonderzoek voor de COVID-19-bestrijding;
2. een voorziening voor data-analyse en uitbraakbestrijding;
3. een platform voor gegevensuitwisseling met het RIVM en de GGD'en.
Er is een landelijk programmaorganisatie opgericht om het nieuwe ICT-systeem te ontwikkelen en te implementeren. Artsen infectieziektebestrijding,
verpleegkundigen en epidemiologen van de verschillende GGD'en worden nauw betrokken bij de ontwikkeling van het nieuwe systeem, zodat het goed aansluit op de praktijk en behoeftes.
Onderdeel van deze projectorganisatie is het product-owner-overleg en bestaat uit vijf deelproceseigenaren en één product-owner. Dit zijn allemaal IZ professionals, die gekozen zijn op basis van hun kennis van het werkproces IZB.
Op dit moment wordt bepaald wat de minimale vereisten zijn voor het nieuwe ICT-systeem voor de COVID-19 bestrijding en dat voldoet aan alle eisen op het gebied van volledigheid, gebruiksvriendelijkheid en privacy.
Dit wordt het zgn. minimum viable product genoemd. Uiteindelijk levert dit een lijst (de backlog) op van benodigde functionaliteiten, die beschreven zijn in een korte tekst (user story) en vertaald worden naar "epics" die in "bouwerstaal" beschreven zijn.
Het ontwikkelteam gaat daarmee aan de slag in sprints van twee weken. In het product-owner-overleg wordt bepaald welke functionaliteit als eerste wordt ontwikkeld en wanneer de functionaliteit af is.
Het product-owner-overleg bestaat uit:

- Inhoudelijke IZB functionaliteit, arts-epidemioloog M&G IZB: [redacted]
- Proceseigenaar "basisproces BCO": [redacted]
- Proceseigenaar "coördinatie BCO": [redacted]
- Proceseigenaar "uitbraken in scholen en instellingen": [redacted]
- Proceseigenaar "epidemiologie & dashboarding": [redacted]
- Proceseigenaar "datastromen naar het RIVM": [redacted]

Per deelproces zijn er verder een aantal personen (arts, verpleegkundigen, epidemiologen (waaronder REC) aangehaakt als expert.
Je kunt in bovenstaande twee belangrijke besluiten zien:

- Wat is het minimum viable product?
- Wanneer is het minimum viable product af en klaar om geïmplementeerd te worden?

Over deze twee besluiten krijgt de COVID-19 Commissie van de DPG-raad advies van het zgn. afstemmingsoverleg. Dit

overleg wordt voorgezeten door [redacted], arts M&G IZ, en bestaat uit:

- [redacted]
- [redacted]
- [redacted]
- [redacted]
- [redacted]
- [redacted]
- [redacted]

Het afstemmingsoverleg komt wekelijks bij elkaar en volgt de voortgang in het product owners-overleg op de voet zodat er proactief geadviseerd kan worden.
De programmaorganisatie wordt aangestuurd door een stuurgroep. [redacted] neemt, als voorzitter afstemmingsoverleg, deel namens de IZ-professionals.
De COVID-19 Commissie van de DPG-raad wordt geadviseerd door de voorzitter van de RAC [redacted] en voorzitter LOI [redacted].
We zijn van mening dat bovenstaande structuur goede inbreng van de IZ-professionals waarborgt en voorkomt dat door tijdsdruk of andere overwegingen de inhoudelijke kwaliteit van de applicatie onder druk komt te staan.
We informeren jullie over het vervolg via de nieuwsberichten, presentaties in het LOI, en waar nodig met een extra bericht zoals dit. Vragen en opmerkingen over bovenstaande kun je sturen aan medischadvies@ggdghor.nl.
Met vriendelijke groet,
[redacted]

Inhoud

Artikel 1. Begrippen 2
Artikel 2. Voorwerp van deze Verwerkersovereenkomst 3
Artikel 3. Inwerkingtreding en duur 3
Artikel 4. Omvang verwerkingsbevoegdheid Opdrachtnemer 3
Artikel 5. Beveiliging van de Verwerking 4
Artikel 6. Geheimhouding door Personeel van Opdrachtnemer 4
Artikel 7. Subverwerker 4
Artikel 8. Bijstand vanwege rechten van Betrokkene 5
Artikel 9. Inbreuk in verband met Persoonsgegevens 5
Artikel 10. Terugbezorgen of wissen Persoonsgegevens 5
Artikel 11. Informatieverplichting en audit 5
Bijlage 1. De Verwerking van Persoonsgegevens..... **Fout! Bladwijzer niet gedefinieerd.**
Bijlage 2. Passende technische en organisatorische maatregelen ..... **Fout! Bladwijzer niet gedefinieerd.**
Bijlage 3: Afspraken betreffende Inbreuken in verband met Persoonsgegevens 9

Verwerkersovereenkomst GGD Contact

De ondergetekenden:

1. De publiekrechtelijke rechtspersoon Gemeentelijke of Gemeenschappelijke Gezondheidsdienst West-Brabant, statutair gevestigd en kantoorhoudende te 4816 CZ, Breda te Doornboslaan 225, ingeschreven in het handelsregister van de Kamer van Koophandel onder nummer 20164916, hierbij vertegenwoordigd door [redacted] Publieke Gezondheid hierna te noemen: Opdrachtgever,

en

2. De Staat der Nederlanden, waarvan de zetel is gevestigd te Den Haag,
te dezen vertegenwoordigd door de Minister van Volksgezondheid, Welzijn en Sport,
namens deze, [redacted]
hierna te noemen: Opdrachtnemer,

hierna gezamenlijk te noemen: Partijen;

OVERWEGENDE DAT:

- voor zover Opdrachtnemer Persoonsgegevens Verwerkt ten behoeve van Opdrachtgever in het kader van de Overeenkomst, Opdrachtgever krachtens artikel 4, onderdeel 7 en onderdeel 8, van de Verordening kwalificeert als verwerkingsverantwoordelijke voor de Verwerking van Persoonsgegevens en Opdrachtnemer als verwerker;
- Partijen in deze Verwerkersovereenkomst, zoals bedoeld in artikel 28, derde lid, van de Verordening, hun afspraken over de Verwerking van Persoonsgegevens door Opdrachtnemer wensen vast te leggen.

KOMEN OVEREEN:

Artikel 1. Begrippen

In deze Verwerkersovereenkomst wordt een aantal begrippen met een beginhoofdletter gebruikt. Aan deze begrippen komt de betekenis toe die hieraan wordt gegeven in artikel 1 van de Algemene Rijksvoorwaarden voor het verstrekken van opdrachten tot het verrichten van Diensten 2018 (ARVODI-2018). In afwijking daarvan of in aanvulling daarop wordt onder de volgende begrippen in deze Verwerkersovereenkomst verstaan:

1.1 Betrokkene: degene op wie een Persoonsgegeven betrekking heeft.

1.2 Inbreuk in verband met Persoonsgegevens: een inbreuk op de beveiliging die per ongeluk of op onrechtmatige wijze leidt tot de vernietiging, het verlies, de wijziging of de ongeoorloofde verstrekking van of de ongeoorloofde toegang tot doorgezonden, opgeslagen of anderszins verwerkte gegevens.

1.3 Overeenkomst: de overeenkomst tussen Opdrachtgever en Opdrachtnemer OVEREENKOMST HOSTING EN BEHEER 'GGD CONTACT' van 14 december 2020.

1.4 Persoonsgegevens: alle informatie over een geïdentificeerde of identificeerbare natuurlijke persoon, die Opdrachtnemer in het kader van de Overeenkomst ten behoeve van Opdrachtgever verwerkt.

1.5 Verordening: Verordening (EU) 2016/679 van het Europees Parlement en de Raad van 27 april 2016 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens en tot intrekking van de Richtlijn 95/46/EG (algemene verordening gegevensbescherming).

1.6 Verwerkersovereenkomst: deze overeenkomst inclusief overwegingen en bijbehorende bijlagen.

1.7 Verwerking: een bewerking of een geheel van bewerkingen in het kader van de Overeenkomst met betrekking tot Persoonsgegevens, of een geheel van Persoonsgegevens, al dan niet uitgevoerd via geautomatiseerde procedés, zoals het verzamelen, vastleggen, ordenen, structureren, opslaan, bijwerken of wijzigen, opvragen, raadplegen, gebruiken, verstrekken door middel van doorzending, verspreiding of op andere wijze ter beschikking stellen, aligneren of combineren, afschermen, wissen of vernietigen.

Artikel 2. Voorwerp van deze Verwerkersovereenkomst

2.1 Deze Verwerkersovereenkomst regelt de Verwerking van Persoonsgegevens door Opdrachtnemer in het kader van de Overeenkomst.

2.2 De aard en het doel van de Verwerking, het soort Persoonsgegevens en de categorieën van Persoonsgegevens, Betrokkenen en ontvangers zijn in Bijlage 1 omschreven. Opdrachtgever garandeert dat de opdracht van de Verwerking in overeenstemming is met de door Opdrachtgever uitgevoerde data protection impact assessment (DPIA).

2.3 Opdrachtnemer garandeert de toepassing van passende technische en organisatorische maatregelen zoals bedoeld in Bijlage 2 , opdat de Verwerking aan de vereisten van de Verordening voldoet en de bescherming van de rechten van de Betrokkene is gewaarborgd.

2.4 Opdrachtnemer garandeert te voldoen aan de vereisten van de toepasselijke wet- en regelgeving betreffende de Verwerking van Persoonsgegevens zoals Opdrachtgever die heeft gecommuniceerd en vertaald zijn naar requirements.

Artikel 3. Inwerkingtreding en duur

3.1 Deze Verwerkersovereenkomst treedt in werking op het moment waarop deze door Partijen is ondertekend.

3.2 Deze Verwerkersovereenkomst eindigt nadat en voor zover Opdrachtnemer alle Persoonsgegevens overeenkomstig artikel 10 heeft gewist of terugbezorgd.

3.3 Geen van Partijen kan deze Verwerkersovereenkomst tussentijds opzeggen.

Artikel 4. Omvang verwerkingsbevoegdheid Opdrachtnemer

4.1 Opdrachtnemer Verwerkt de Persoonsgegevens uitsluitend in opdracht en op basis van schriftelijke instructies van Opdrachtgever behoudens afwijkende wettelijke voorschriften die op Opdrachtnemer van toepassing zijn.

4.2 Indien een instructie als bedoeld in het eerste lid naar het oordeel van Opdrachtnemer in strijd is met een wettelijk voorschrift inzake gegevensbescherming, stelt hij Opdrachtgever

daarvan voorafgaand aan de Verwerking in kennis, tenzij een wettelijk voorschrift deze kennisgeving verbiedt.

4.3 Indien Opdrachtnemer op grond van een wettelijk voorschrift Persoonsgegevens dient te verstrekken, informeert hij Opdrachtgever onmiddellijk, en zo mogelijk voorafgaand aan de verstrekking.

4.4 Opdrachtnemer heeft geen zeggenschap over het doel van en de middelen voor de Verwerking van Persoonsgegevens.

Artikel 5. Beveiliging van de Verwerking

5.1 In aanvulling op artikel 15 van de ARVODI-2018 en onverminderd artikel 2.3 treft Opdrachtnemer de technische en organisatorische beveiligingsmaatregelen zoals beschreven in Bijlage 2.

5.2 Partijen erkennen dat het waarborgen van een passend beveiligingsniveau voortdurend kan dwingen tot het treffen van aanvullende beveiligingsmaatregelen. Opdrachtgever garandeert Opdrachtnemer zo spoedig mogelijk op de hoogte te brengen van aanvullende of aangescherpte beveiligingseisen. Opdrachtnemer waarborgt een op het risico afgestemd beveiligingsniveau.

5.3 Indien en voor zover Opdrachtgever daarom uitdrukkelijk schriftelijk verzoekt, zal Opdrachtnemer aanvullende maatregelen treffen met het oog op de beveiliging van de Persoonsgegevens. Indien deze aanvullende maatregelen het beveiligingsniveau van Opdrachtnemer overstijgen en meerwerk oplevert dan komen de kosten voor deze aanvullende maatregelen voor rekening van Opdrachtgever.

5.4 Opdrachtnemer Verwerkt Persoonsgegevens niet buiten de Europese Unie, tenzij hij daarvoor uitdrukkelijk schriftelijk toestemming heeft verkregen van Opdrachtgever en behoudens afwijkende wettelijke verplichtingen.

5.5 Opdrachtnemer informeert Opdrachtgever zonder onredelijke vertraging zodra hij kennis heeft genomen van onrechtmatige Verwerkingen van Persoonsgegevens of inbreuken op beveiligingsmaatregelen zoals genoemd in het eerste en tweede lid.

5.6 Opdrachtnemer verleent Opdrachtgever bijstand bij het doen nakomen van de verplichtingen uit hoofde van de artikelen 32 tot en met 36 van de Verordening. De redelijke kosten die hierbij gemoeid zijn kunnen door Opdrachtnemer bij Opdrachtgever in rekening gebracht worden.

Artikel 6. Geheimhouding door Personeel van Opdrachtnemer

6.1 De Persoonsgegevens hebben een vertrouwelijk karakter als bedoeld in artikel 13.1 van de ARVODI-2018.

6.2 Opdrachtnemer toont op verzoek van Opdrachtgever aan dat zijn Personeel zich ertoe heeft verbonden vertrouwelijkheid in acht te nemen als bedoeld in artikel 13.2 van de ARVODI-2018.

Artikel 7. Subverwerker

Wanneer Opdrachtnemer, met inachtneming van het bepaalde in artikel 8 van de ARVODI-2018, een andere verwerker inschakelt om ten behoeve van Opdrachtgever verwerkingsactiviteiten te verrichten, worden aan deze andere verwerker bij een overeenkomst dezelfde verplichtingen inzake gegevensbescherming opgelegd als die welke in deze Verwerkersovereenkomst zijn opgenomen.

Artikel 8. Bijstand vanwege rechten van Betrokkene

Opdrachtnemer verleent Opdrachtgever bijstand bij het vervullen van diens plicht om verzoeken om uitoefening van de in hoofdstuk III van de Verordening vastgelegde rechten van de Betrokkene te beantwoorden. De redelijke kosten die hierbij gemoeid zijn worden door Opdrachtnemer bij Opdrachtgever in rekening gebracht.

Artikel 9. Inbreuk in verband met Persoonsgegevens

9.1 Opdrachtnemer informeert Opdrachtgever zonder onredelijke vertraging, zodra hij kennis heeft genomen van een Inbreuk in verband met Persoonsgegevens, overeenkomstig de afspraken zoals vastgelegd in Bijlage 3.

9.2 Opdrachtnemer informeert Opdrachtgever ook na een melding op grond van het eerste lid over ontwikkelingen betreffende de Inbreuk in verband met Persoonsgegevens.

9.3 Partijen dragen elk de door henzelf in verband met de melding aan de bevoegde toezichthoudende autoriteit en Betrokkene te maken kosten.

Artikel 10. Terugbezorgen of wissen Persoonsgegevens

10.1 Na afloop van de Overeenkomst draagt Opdrachtnemer, naar gelang de keuze van Opdrachtgever, zorg voor het terugbezorgen aan Opdrachtgever of het wissen van alle Persoonsgegevens. Opdrachtnemer verwijdert kopieën, behoudens afwijkende wettelijke voorschriften.

10.2 Zodra de Overeenkomst is beëindigd, zal Opdrachtnemer – naar keuze van Opdrachtgever – alle persoonsgegevens die bij haar aanwezig zijn in originele of kopievorm retourneren aan Opdrachtgever, en/of deze persoonsgegevens en eventuele kopieën daarvan verwijderen en/of vernietigen op instructie van Opdrachtgever.

Artikel 11. Informatieverplichting en audit

11.1 Opdrachtnemer stelt alle informatie ter beschikking die nodig is om aan te tonen dat de verplichtingen uit deze Verwerkersovereenkomst zijn en worden nagekomen.

11.2 Opdrachtnemer verleent op basis van nacalculatie alle benodigde medewerking aan audits. De bedoelde audit vindt plaatst nadat Opdrachtgever de bij Opdrachtnemer aanwezige soortgelijke auditrapportages heeft opgevraagd, beoordeeld en zij redelijke argumenten ziet om een audit te doen.

11.3 Opdrachtnemer verstrekt met een frequentie van eenmaal per jaar, uiterlijk op 1 maart aan Opdrachtgever een verklaring van een onafhankelijke externe deskundige, waarin deze een oordeel geeft over de genoemde naleving.

Artikel 12. Aansprakelijkheid

12.1 De totale aansprakelijkheid van Opdrachtnemer wegens een toerekenbare tekortkoming in de nakoming van de Verwerkersovereenkomst of de AVG, daaronder uitdrukkelijk ook begrepen iedere tekortkoming in de nakoming van een met Opdrachtgever overeengekomen garantieverplichting, is op jaarbasis beperkt tot maximaal € 500.000 (vijfhonderd duizend euro). Indien de schade samenhangt met fouten en/of tekortkomingen van derden c.q subverwerkers is Opdrachtnemer niet meer aansprakelijk dan zij bij die derden daadwerkelijk heeft verhaald.

12.2. De in dit artikel bedoelde uitsluitingen en beperkingen komen te vervallen indien en voor zover de schade het gevolg is van opzet of bewuste roekeloosheid van de bedrijfsleiding van Opdrachtnemer.

Aldus op de laatste van de twee hierna genoemde data overeengekomen en in tweevoud ondertekend,

Breda, datum: 14-12-20 GGD WEST-BRABANT namens deze, [redacted]	Den Haag, datum: DE MINISTER/STAATSSECRETARIS Volksgezondheid, Welzijn en Sport namens deze, [redacted]

Bijlage 1. De Verwerking van Persoonsgegevens

In deze bijlage moet in ieder geval het volgende worden gespecificeerd:

Het onderwerp/aard en doel van de Verwerking	De verwerking door opdrachtnemer betreft het hosten van app, sluis en webportal van 'GGD Contact'. Het doel van de app GGD Contact is om het aantal uur dat GGD per index (besmet persoon) besteedt aan bron- en contactopsporing te verminderen, waardoor GGD voor meer indexen bron- en contactopsporing kan uitvoeren.
Het soort Persoonsgegevens	(1) bijzondere categorieën van gegevens als bedoeld in artikel 9 van de Verordening, (3) wettelijk voorgeschreven identificatienummers en (4) overige persoonsgegevens.
Beschrijving categorieën Persoonsgegevens	Gegevens die de GGD nodig heeft voor bron- en contactopsporing. Dit zijn gezondheidsgegevens. (Bijvoorbeeld: 'netwerk'/'relatie'-gegevens: gegevens over contacten van index; contactgegevens; besmettingsrisico; klachten; overige gegevens ingevuld door index in open veld)
Beschrijving categorieën Betrokkenen	Met infectieziekte besmette personen ('index') en diens contacten die mogelijk ook zijn besmet ('contacten')
Beschrijving categorieën ontvangers van Persoonsgegevens	-

Voor de inhoud van deze bijlage kan onder meer gebruik worden gemaakt van de registratie die de Verwerkingsverantwoordelijke op grond van artikel 30 van de Verordening dient aan te houden.

Bijlage 2. Passende technische en organisatorische maatregelen

In deze bijlage moeten de normen en maatregelen die Opdrachtnemer in het kader van de beveiliging van de Verwerking moet hanteren respectievelijk treffen worden gespecificeerd. Hiervoor kan worden verwezen naar documenten waarin normen en maatregelen zijn vastgelegd, zoals in voorkomend geval het programma van eisen of de offerteaanvraag.

ISO 27001
NEN 7510
Security Operations Center
Actieve Threat Hunting

Bijlage 3: Afspraken betreffende Inbreuken in verband met Persoonsgegevens

In deze bijlage moeten de afspraken over hoe Opdrachtnemer Opdrachtgever over Inbreuken in verband met Persoonsgegevens gaat informeren worden gespecificeerd.

Departementale procedure

Informatie die ten minste door Opdrachtnemer moet worden verstrekt

Aard van de Inbreuk in verband met Persoonsgegevens
De Persoonsgegevens en Betrokkene
Waarschijnlijke gevolgen van de Inbreuk in verband met Persoonsgegevens
Maatregelen die Opdrachtnemer heeft voorgesteld of genomen om de Inbreuk in verband met Persoonsgegevens aan te pakken, waaronder, in voorkomend geval, de maatregelen ter beperking van de eventuele nadelige gevolgen daarvan

Dienstverleningsovereenkomst Ministerie van Volksgezondheid, Welzijn en Sport en GGD West-Brabant

Betreft: Dienstverlening GGD Contact

Datum: 23 08 2021
Status: Definitief

Colofon

Afzendgegevens: [redacted]
Postbus 20350
2500 EJ Den Haag

Contactpersoon: [redacted]

Inhoudsopgave

Versiebeheer 5
1 Algemeen 6
1.1 Dienstverlening 6
1.2 Looptijd 6
1.3 Wijzigingen document 6
1.4 Gerelateerde documenten 6
1.5 Beëindiging 6
2 Dienstverlening 7
2.1 Algemene beschrijving dienstverlening 7
2.2 Niveau van dienstverlening 7
A. Rolverdeling AVG 7
B. Bereikbaarheid 7
C. Beschikbaarheid 7
D. Correctief onderhoud 8
E. Incidentmanagement 8
F. Change- en releasemanagement 9
G. Continuïteitsmanagement 9
3 Beveiliging 11
3.1 Van toepassing zijnde kaders 11
3.2 Logging en monitoring 11
3.3 Beveiliging afnemer 11
4 Verantwoordelijkheden 12
4.1 Verantwoordelijkheden VWS 12
4.2 Verantwoordelijkheden GGD 12
5 Communicatie 13
5.1 Rapporteren 13
5.2 Overlegvormen 13
6 Tekenblad 14

De ondergetekenden

1. de publiekrechtelijke rechtspersoon: **de Staat der Nederlanden (Ministerie van Volksgezondheid, Welzijn en Sport)**, hierna te noemen: VWS,

en

2. 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 bij deze dienstverleningsovereenkomst ("**DVO**") worden hierna gezamenlijk ook aangeduid als "**de Partijen**" en ieder als een "**Partij**".

Versiebeheer

Versie	Datum	Auteur	Omschrijving
0.1	26-05-2021	[redacted]	Initiële versie
0.2	28-05-2021		Eerste review RDO verwerkt
0.3	04-06-2021		Aanvullingen en review verwerkt
0.4	09-06-2021		Aanvullingen en review van GGD GHOR verwerkt
0.5	14-06-2021		Aanvullingen en review [redacted] verwerkt
0.6	15-06-2021		Review
0.9	15-06-2021		Review verwerkt
0.99	23-06-2021		Review Stuurgroep verwerkt
1.0	23-06-2021		Final Review

1 Algemeen

In deze Dienstverleningsovereenkomst (DVO) komen VWS en GGD de mate van dienstverlening van GGD Contact overeen.

1.1 Dienstverlening

Het doel van de dienstverlening is de GGD te ondersteunen in het Bron- en Contact Onderzoek (BCO) met het leveren, beheren en door ontwikkelen van de applicatie GGD Contact. Dit is de voorziening die het Bron- en Contact Onderzoek voor COVID-19 gerelateerd ondersteunt.

1.2 Looptijd

Deze DVO treedt in werking op 23 augustus 2021 en wordt aangegaan voor onbepaalde tijd.

1.3 Wijzigingen document

Het actueel houden van dit document is belegd bij de directie RDO van het ministerie VWS. Bij partijen kan de wens ontstaan om dit document te wijzigen. In gezamenlijk overleg wordt de wijziging vervolgens bepaald.

- Overeengekomen wijzigingen worden vastgelegd in een wijzigingsblad;
- Dit wijzigingsblad wordt door beide partijen formeel ondertekend en als addendum toegevoegd;
- De in het addendum opgenomen afspraken worden in de eerstvolgende geactualiseerde versie van de DVO opgenomen.
- De bijlagen in dit document kunnen na en in onderling overleg tussentijds worden geactualiseerd. Het tast de rechtmatigheid van de afspraken in dit document niet aan.

1.4 Gerelateerde documenten

De volgende documenten zijn gerelateerd aan deze DVO:

- Procedurebeschrijving beheer GGD Contact (bijlage 1)
- Verwerkersovereenkomst VWS – GGD (bijlage 2)
- Beveiliging GGD Contact release X (bijlage x) wordt vertrouwelijk gedeeld onder TLP:Amber classificatie (need to know basis).
- Landelijke Referentie DPIA GGD Contact
- Lijst Overeenkomsten GGD Contact

Van de gerelateerde documenten kunnen in de loop van de tijd nieuwe versies bestaan. Sommige documenten worden zelfs elke release geüpdatet. Dit heeft geen gevolgen voor de geldigheid van deze DVO.

1.5 Beëindiging

Het verzoek van een van de partijen om de DVO te beëindigen vindt schriftelijk plaats met opgave van de reden. Partijen hanteren een opzegtermijn van drie maanden en treden met elkaar in overleg over de wijze van beëindiging.

2 Dienstverlening

2.1 Algemene beschrijving dienstverlening

De te leveren dienstverlening omvat GGD Contact: het leveren, doorontwikkelen en beheren van de voorziening die de behandeling voor COVID-19 gerelateerd Bron- en Contact Onderzoek (BCO) ondersteunt.

2.2 Niveau van dienstverlening

Deze paragraaf beschrijft de specifieke afspraken voor de dienstverlening die door het ministerie wordt geleverd aan de GGD. Voor de dienstverlening levert het ministerie Applicatie- en Technisch beheer.

Aangezien de omvang en inzet van het Bron- en Contact Onderzoek (BCO) varieert op basis van het aantal COVID-19 besmettingen, kan de gewenste dienstverlening ook fluctueren. VWS zal driemaandelijks beoordelen of de dienstverlening nog past bij het gebruik van de applicatie en waar opportuun een voorstel doen voor aanpassing van de dienstverlening om zo kosteneffectief GGD Contact aan te kunnen bieden.

A. Rolverdeling AVG

De feitelijke rolverdeling tussen GGD en VWS is bepalend voor de verantwoordelijkheden van GGD en VWS zoals die volgen uit de Algemene Verordening Gegevensbescherming (AVG). De rolverdeling is vastgesteld in de referentie DPIA GGD Contact behorend bij de release. De referentie DPIA is afgestemd met de GGD en VWS.

GGD stemt in met alle (sub)verwerkers die VWS voor haar dienstverlening inschakelt, waarbij VWS zorgdraagt voor de verwerkersovereenkomsten. De lijst met (sub)verwerkers is beschreven in Lijst Overeenkomsten GGD Contact. Deze is opgenomen als bijlage bij deze DVO.

B. Bereikbaarheid

De servicedesk GGD GHOR is het centrale loket voor alle verzoeken en meldingen rondom GGD Contact. De GGD sluit een overeenkomst die ingaat op het moment van ingebruikname van GGD Contact.

C. Beschikbaarheid

Beschikbaarheid is de tijd dat de dienstverlening onder verantwoordelijkheid van VWS, voor eindgebruikers beschikbaar is. Gepland onderhoud valt buiten de berekening van de gerealiseerde beschikbaarheid. Ook de uitval van een tussenliggende component die niet onder verantwoordelijkheid van VWS valt, zoals generieke ICT-diensten geleverd door GGD (o.a. IdentityHub en een VPN - verbinding), waardoor de systemen voor gebruikers niet beschikbaar zijn, valt hierbuiten.

Per incident (dat leidt tot onbeschikbaarheid) gelden bovendien maximale hersteltijden. Deze zijn opgenomen onder de paragraaf incidentmanagement.

Onderwerp	Toelichting	Norm
Beschikbaarheid	De mate waarin de eindgebruikers GGD Contact functioneel kunnen gebruiken binnen het servicevenster. Onbeschikbaarheid wordt gemeten vanaf het moment van melden door servicedesk aan de Incidentmanager VWS.	Minimaal 99,8% binnen het servicevenster

D. Correctief onderhoud

Correctief onderhoud aan GGD Contact (geplande onbeschikbaarheid) wordt enkel uitgevoerd buiten het servicevenster als opgenomen in paragraaf E van deze DVO. Correctief onderhoud wordt bij voorkeur drie weken van tevoren en uiterlijk drie dagen van tevoren gemeld aan de servicedesk. De servicedesk is vervolgens verantwoordelijk voor de communicatie naar de eindgebruikers en afnemers toe. Bij een dreigende verstoring moet er soms direct ingegrepen worden, daarvoor geldt onderstaande norm.

Onderwerp	Toelichting	Norm
Onderhoud	Het benodigde onderhoud om de beschikbaarheid te kunnen garanderen.	90% buiten het Servicevenster

E. Incidentmanagement

Het incidentmanagementproces heeft als doel het zo snel mogelijk verhelpen van incidenten. De doelstelling is het terugbrengen van de dienstverlening naar het normale niveau, met zo min mogelijk gevolgen in de vorm van impact, benodigde mensen, middelen (financieel & materieel) en tijd. Het incidentmanagementproces staat uitgebreid beschreven in Bijlage 1 Procedurebeschrijving beheer GGD Contact. Onderstaand een overzicht van de gehanteerde normen.

Onderwerp	Toelichting	Norm[1]
Incidentmelding (storing)	De afhandeling van aangemelde verstoringen tijdens het servicevenster. Toewijzing prioriteit vindt plaats op basis van de prioriteitenmatrix (zie hiervoor de procedurebeschrijving). NB Responstijd en doorlooptijd 1ste lijn zijn onderdeel van de afspraken GGD GHOR SD met de GGD.De hersteltijd 2e lijn start na ontvangst van het incident van de Servicedesk door de tweede lijn	P1 Hersteltijd 2e lijn: 4 uur Servicevenster: 7*16u**
		P2 Hersteltijd 2e lijn: 1 dag Servicevenster: 7*16u**
		P3 Hersteltijd 2e lijn: 1 week Servicevenster: 7*16u**
		P4 Hersteltijd 2e lijn: 2 weken Servicevenster: 7*16**

[1] Dit is conform de standaardnormen van de GGD GHOR servicedesk

	Afhandeling buiten servicevenster	Alleen bij P1

** Ten tijde van een hoge infectiedruk wordt het servicewindow opgerekt van 5 x 9 (8.00 – 17.00 uur) naar 7 x 16 (7.00 – 23.00 uur).

Prioriteitenmatrix

Tijdens het aannemen van een incidentmelding door de servicedesk, wordt met de aanmelder een inschatting van de ernst (impact en urgentie) van het incident gemaakt. Op basis daarvan wordt door de servicedeskmedewerker de prioriteit vastgesteld, geregistreerd en afgehandeld.

In de Procedurebeschrijving beheer GGD Contact (bijlage 1) is de prioriteitenmatrix opgenomen.

F. Change- en releasemanagement

Change- en releasemanagement is het proces rondom het gecontroleerd afhandelen van verzoeken tot wijziging van de functionele of technische werking van GGD Contact. Het proces van change- en releasemanagement is uitvoerig beschreven in Bijlage 1 Procedurebeschrijving beheer GGD Contact.

Onderwerp	Toelichting	Norm
Afhandelen wijzigingsverzoeken	De afhandeling van geaccordeerde wijzigingen	Minimaal 95% van de goedgekeurde wijzigingen wordt gerealiseerd conform afspraak
Implementeren releases	Afhandelen van een verzameling van wijzigingen in een release voor GGD Contact	Minimaal 95% van de releases wordt gerealiseerd op de overeengekomen implementatiedatum

G. Continuïteitsmanagement

Continuïteitsmanagement is het proces dat zorgt voor afdoende technische voorzieningen om de continuïteit van de dienstverlening te borgen. De borging van de continuïteit wordt gerealiseerd conform onderstaande normen.

Onderwerp	Toelichting	Norm
Back-up en restore	Het veiligstellen van mail en volledig herstel GGD Contact (inclusief database) op de productieomgeving en het terugzetten hiervan.	- 24x per uur, RPO[2] maximaal 1 uur, RTO[3] maximaal 2 uur. Reactietijd: 15 minuten (met best effort voor sneller binnen kantooruren) - 30 x per maand[4], RPO maximaal 1 dag, RTO maximaal 4 uur.

[2] Recovery Point Objective of herstelpuntdoelstelling
[3] Recovery Time Objective of hersteltijddoelstelling
[4] Voor de back-ups die tot 1 maand teruggaan, is de RTO alleen haalbaar op basis van disaster recovery. Dat betekent dat alle databases van een omgeving in één keer terug worden gezet. Bij een lagere RPO en lagere RTO (bijv. bij back-ups die verder dan 1 maand teruggaan) wordt de data in een geïsoleerde omgeving (sandbox) beschikbaar gesteld waar een extract van wordt gemaakt.

		- 12 x per jaar, RPO maximaal 1 maand, RTO maximaal 2 (werk)dagen
Bewaartermijn	Periode dat de veiliggestelde gegevens worden bewaard.	Retentie van 7 jaar
Uitwijk	De mogelijkheid om, na een calamiteit, de dienstverlening te hervatten op een andere wijze of andere locatie.	Het datacentrum van de hostingpartij is dubbel uitgevoerd. Uitwijk bij uitval van het datacenter zal automatisch plaatsvinden. Specifieke uitval wordt opgepakt binnen incidentproces, waarbij back-up en uitrolplan van de specifieke release leidend zijn.

3 Beveiliging

In GGD Contact wordt gevoelige informatie verwerkt zoals medische gegevens (bijzondere persoonsgegevens en informatie over de persoonlijke levenssfeer (o.a. persoonlijke contacten). Informatiebeveiliging is daarmee een belangrijke randvoorwaarde voor een goede en vooral betrouwbare dienstverlening. De ontwikkeling van GGD Contact en het beheer gebeurt conform hoge informatiebeveiligings- en privacybeschermingseisen.

3.1 Van toepassing zijnde kaders

Aan de basis van de inrichting, bestendiging en verbetering van beveiliging liggen primair de volgende kader stellende documenten.

- AVG
- NEN 7510-1 en NEN 7510-2 voor zover relevant voor de ontwikkeling van de applicatie.
- NEN 7512 – als subset van beheersmaatregelen uit de NEN 7510-2 voor de vertrouwensbasis voor gegevensuitwisseling.
- NEN 7513 – als ontwerpvoorwaarde voor de applicatielogging.
- DPIA GGD Contact

Deze normen zijn door VWS omgezet in concrete maatregelen die zijn genomen bij de ontwikkeling en het beheer van GGD Contact. In het document Beveiliging GGD Contact is de toelichting en concrete invulling van bovenstaande normen opgenomen. Dit document wordt elke release van GGD Contact geüpdatet en beschikbaar gesteld aan de CISO van de GGD en de kwaliteitsmanager GGD GHOR.

3.2 Logging en monitoring

Applicatielogging is ingericht conform NEN7513. RDO geeft inzicht in een selectie van de logging ten behoeve van het herkennen van afwijkende handelingen in de applicatie om misbruik op te sporen. Dit deelt RDO met een partij die door de GGD is aangewezen om de monitoring uit te voeren. Daarnaast is (infrastructuur) logging - en monitoring onderdeel van de dienstverlening van RDO – dit wordt onder eigen beheer uitgevoerd. Afwijkingen worden gemeld aan GGD-GHOR SOC. Waar nodig deelt VWS logbestanden op verzoek van de GGD voor de uitvoering van verzoeken door toezichthouders of wettelijke verplichting in het kader van opsporing.

3.3 Beveiliging afnemer

Zowel dienstverlener als afnemer dienen invulling te geven aan de ministeriële regeling voor infectieziektebestrijding[5]. Met het tekenen van deze DVO bevestigen beide partijen hieraan te voldoen.

De wijze waarop de beveiliging van de informatie-uitwisseling met externe bronnen is ingericht moet worden vastgelegd conform de eisen uit de NEN 7512. De uitwisseling wordt pas gestart als deze maatregelen zijn vastgelegd.

[5] Regeling van de Minister van Volksgezondheid, Welzijn en Sport van 18 november 2008, nr. PG/ZP-2.892.655, houdende nieuwe eisen inzake de publieke gezondheid (Regeling publieke gezondheid)

4 Verantwoordelijkheden

Zowel de GGD als VWS zijn verantwoordelijk voor het niveau van dienstverlening, GGD in de rol van afnemer en VWS in de rol van leverancier. De verantwoordelijkheden zijn hieronder beschreven.

4.1 Verantwoordelijkheden VWS

- Het leveren van de diensten conform het dienstenniveau zoals in dit document beschreven.
- Het uitvoeren van de noodzakelijke patches en updates indien dit vanuit beheer en/of beveiliging noodzakelijk blijkt om de bestaande functionaliteit van de diensten in stand te houden.
- Het uitvoeren van applicatie-, en technisch beheer.
- Het contractueel vastleggen van afspraken met externe leveranciers.
- Signaleren en melden van risico's in de keten die invloed hebben op het functioneren van de applicatie, zoals beschreven in Bijlage 1 Procedurebeschrijving beheer GGD Contact.

4.2 Verantwoordelijkheden GGD

- Het melden van wijzigingen in de koppeling van eigen systemen, die op enige wijze relevant zijn voor de werking van de afgenomen diensten.
- Het melden van (beveiligings-)technische en functionele onvolkomenheden in de werking van de diensten en de gegevensuitwisseling.
- Het uitvoeren van functioneel beheer.
- Het bewaken van de kwaliteit van de (door de afnemer zelf) vast te leggen gegevens met betrekking tot tijdigheid, juistheid en volledigheid en het gebruik van deze gegevens.
- Het signaleren en melden van beveiligingsrisico's die effect hebben op de veiligheid/beveiliging van GGD Contact.
- Het gestructureerd en geprioriteerd melden van wensen voor doorontwikkeling, conform het wijzigingsproces als gespecificeerd in Bijlage 1 Procedurebeschrijving beheer GGD Contact.
- Afstemming over toevoeging van koppelingen (of wijzigingen hierop).

5 Communicatie

5.1 Rapporteren

Rapportage over de dienstverlening worden in afstemming met GGD GHOR vastgesteld en zijn onderdeel van het document Procedurebeschrijving beheer GGD Contact.

5.2 Overlegvormen

Overleggen ten behoeve van de te leveren dienstverlening zijn omschreven in de Bijlage 1 Procedurebeschrijving beheer GGD Contact.

6 Tekenblad

Door de ondertekening stemt ondergetekende in met de overeenkomst voor het gebruik van GGD Contact, als gevolg waarvan een overeenkomst ontstaat tussen VWS en de GGD.

Voor akkoord:

Partij:	Staat der Nederlanden (Ministerie VWS)
Datum:	…
Voor deze:	[redacted]

Tekenblad

Door de ondertekening stemt ondergetekende in met de overeenkomst voor het gebruik van GGD Contact, als gevolg waarvan een overeenkomst ontstaat tussen VWS en de GGD.

Voor akkoord:

Partij: Gemeentelijke Gezondheidsdienst GGD West-Brabant
Datum: …
Voor deze: [redacted]

Wob-verzoek SOLV/ICAM datalek 2021 coronasysteem

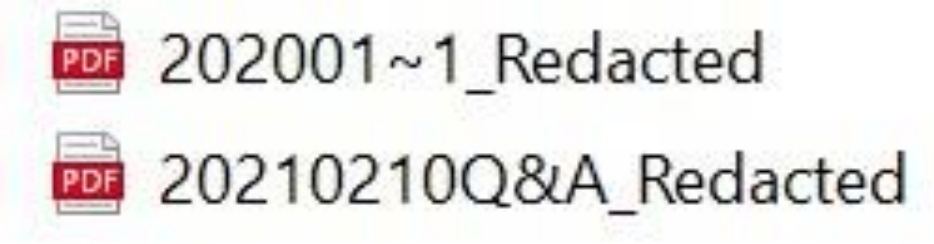
14.0 Tekst Wob-verzoek en register documenten

Tekst verzoek (xiv)

Informatie en documenten met betrekking tot de training van (externe) medewerkers ten aanzien van het gebruik van CoronIT en HPZone (Lite) en de omgang met persoonsgegevens, waaronder beleid, protocollen, instructies en presentaties

Register

Een screenshot van de verkennerpagina van map 14:



Gegevensbeschermingsbeleid GGD West-Brabant

Versie: 1.3
Classificatie: Intern
Datum: 2 januari 2020

Inhoud

2.1 Aard en positie van dit document 4
3.1 Aanleiding, ambitie en doelstellingen van het beleid 5
3.2 Begripsbepalingen 6
3.3 Juridisch kader 8
3.4 Doelgroep en toepassingsbereik 9
3.5 Inrichtingswijze gegevensverwerking 9
4.1 Rechten van betrokkenen 11
4.2 Recht op informatie en toegang tot gegevens 11
4.3 Recht op inzage en afschrift van gegevens 12
4.4 Recht op rectificatie (correctie, aanvulling) van gegevens 12
4.5 Recht op gegevenswissing 12
4.6 Recht op beperking van de verwerking 13
4.7 Recht op overdraagbaarheid van gegevens (dataportabiliteit) 13
4.8 Recht van bezwaar tegen verwerking 14
4.9 Recht niet te worden onderworpen aan geautomatiseerde individuele besluitvorming waaronder profilering 14
4.10 Klachten en vragen 14
4.11 Informeren van (keten)partners 14
4.12 Rechten en plichten aangaande het medisch dossier 15
5.1 Bewustwording 16
5.2 Verwerking van persoonsgegevens door derden 16
5.3 Documentatie over verwerking van persoonsgegevens 17
5.4 Informatiebeveiliging 18
5.5 Meldplicht voor inbreuken in verband met persoonsgegevens (datalekken) 19
5.6 DPIA’s (Data Protection Impact Assessments) 20
5.7 Beheer van persoonsgegevens 21
6.1 Functies en verantwoordelijkheden 24

1. Samenvatting

De GGD West-Brabant (hierna: “GGD”) verwerkt dagelijks veel gegevens over veel mensen. Bescherming van deze zogenaamde persoonsgegevens tegen oneigenlijk gebruik is noodzakelijk en evident maar tegelijkertijd niet altijd eenvoudig.

Met dit beleid vult de GGD nader in hoe zij uitvoering wenst te geven aan gegevensbescherming. Het document helpt om koers te bepalen, af te bakenen en te zien of er voldoende maatregelen zijn genomen om de persoonsgegevens te beschermen. Daarnaast wordt met naleving van dit beleid voldaan aan een wettelijke plicht en is het een manier waarmee de GGD aan zowel betrokkenen als de Autoriteit Persoonsgegevens toont dat de ze de Algemene verordening gegevensbescherming (“AVG”) naleeft.

Een beleid dat ziet op gegevensbescherming is niet nieuw, maar met de sinds de AVG een wettelijke verplichting voor organisaties die veel (bijzondere) persoonsgegevens verwerken, zoals de GGD.

Typisch vangt een gegevensbeschermingsbeleid aan met een antwoord op de vraag: ‘wat weet een organisatie allemaal over mensen en waarom?’. In dit geval is er voor gekozen om voor dit onderdeel te verwijzen naar het ‘register van verwerkingsactiviteiten’ van de GGD als losstaand document.
Dit document vangt aan met de wijze waarop mensen invloed kunnen uitoefenen of grip kunnen krijgen op (verwerking van) hun persoonsgegevens bij de GGD. Dit wordt ook wel ‘de rechten van betrokkenen’ genoemd.
Voorts worden de (verplichte) procedures en maatregelen beschreven die de GGD hanteert om invulling te geven aan de plichten uit de AVG. Hierbij wordt achtereenvolgens stilgestaan bij:

- bewustmaking van het personeel;
- (contractuele) afspraken bij (het inschakelen van) andere partijen;
- de (verplicht) aan te leggen documentatie;
- (technische én organisatorische) beveiliging van persoonsgegevens;
- (het melden van) datalekken;
- het uitvoeren van risicoanalyses bij verwerking van persoonsgegevens (DPIA’s) en
- het beheer van persoonsgegevens.

Er wordt afgesloten met het vastleggen van de ‘governancestructuur’ op het vlak van gegevensbescherming. Hierbij worden de rollen, taken en verantwoordelijkheden die betrekking hebben op de naleving van de bepalingen uit dit beleid nader uitgewerkt.

2. Inleiding

Op 25 mei 2018 trad de Algemene verordening gegevensbescherming (hierna: “AVG”) in werking. Dat betekent dat vanaf die datum dezelfde privacywetgeving geldt in de gehele Europese Unie. Lidstaten hebben slechts zeer beperkte vrijheid om aanvullende regelgeving vast te stellen. De Nederlandse wetgever bereidde daarvoor de Uitvoeringswet AVG (hierna: “UAVG”) voor. Feitelijk gaat het om modernisering van de wetgeving, die een kans biedt om maatschappelijk vertrouwen in technologie te versterken. Ook stelt het organisaties in de gelegenheid om de beveiliging van waardevolle gegevens te verbeteren en zo te komen tot een ‘AVG- proof’ werkomgeving.

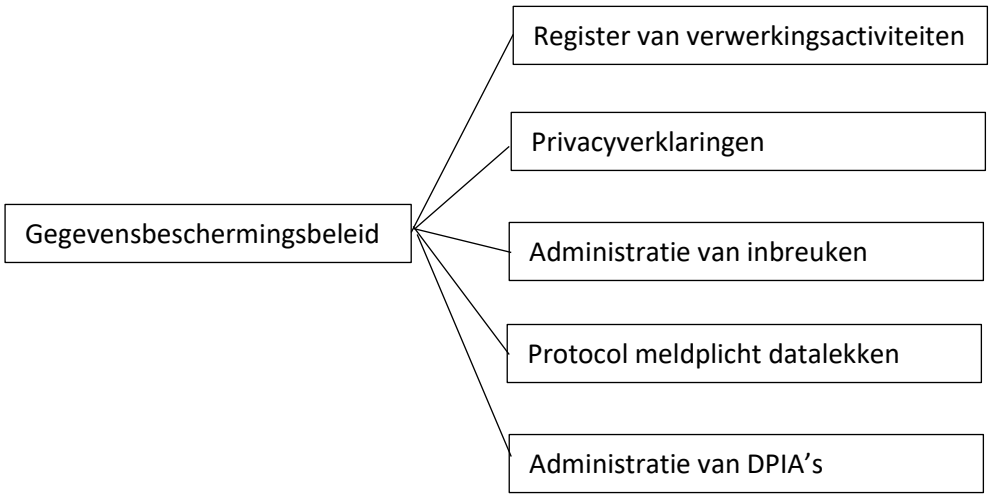
De AVG is dus een verplichting en wel één die ons in positieve zin uitdaagt om een stevige ambitie uit te spreken over het gegevensbeschermingsniveau van zowel cliënten, medewerkers als (keten)partners. Betrokkenen moeten er te allen tijde op kunnen vertrouwen dat hun gegevens bij ons in veilige handen zijn. Daarnaast is ook de samenleving kritischer en veeleisender geworden ten aanzien van de wijze waarop met gevoelige informatie wordt omgegaan.

Het beschermen van privacybelangen wordt vaak gezien als obstakel bij het uitvoeren van werkzaamheden, omdat moet worden getoetst of aan de privacywetgeving wordt voldaan. Maar privacy is een belangrijk grondrecht. In de Grondwet is verankerd dat de overheid niet zomaar persoonlijke gegevens mag gebruiken. Het is een wettelijke verplichting dat de GGD behoorlijk en zorgvuldig omgaat met persoonsgegevens in verband met de privacy van betrokkenen.

Deze ambitie heeft een vertaalslag gekregen in dit beleid en is nader uitgewerkt in onze strategische (beleids)uitgangspunten, een governancestructuur en onderliggende protocollen en werkafspraken.

2.1 Aard en positie van dit document

Dit beleid stelt de algemene kaders vast waarbinnen de GGD gegevensbescherming regelt. Het is een kapstokbeleid dat de basis is voor de uitwerking van alle aspecten van onze bedrijfsvoering, zowel binnen als buiten de organisatie, voor zover daarbij sprake is van de verwerking van persoonsgegevens.
Onderstaand schema toont de relatie van dit beleid met andere documenten.



Om het mogelijk te maken de hoofdstukken ook los van elkaar te lezen komt het incidenteel voor dat begrippen meer dan eens geduid worden.

3. Uitgangspunten

3.1 Aanleiding, ambitie en doelstellingen van het beleid

Binnen de GGD werken we veel met persoonsgegevens: van burgers, medewerkers en (keten)partners. Deze verzamelen we voornamelijk voor het goed uitvoeren van onze taak zoals op gesloten in de Wet publieke gezondheid (hierna: “Wpg”) of de Wet maatschappelijke ondersteuning 2015 (hierna: “Wmo”). Men moet er op kunnen vertrouwen dat wij zorgvuldig en veilig met persoonsgegevens omgaan.
Nieuwe technologische ontwikkelingen, innovatieve voorzieningen, globalisering en een steeds meer digitale overheid stellen andere eisen aan de bescherming van gegevens en privacy. De GGD is zich hier van bewust en zorgt dat de privacy gewaarborgd blijft, onder andere door maatregelen te treffen op het gebied van informatiebeveiliging, dataminimalisatie, transparantie en gebruikerscontrole.

Directe aanleiding voor dit beleid is de inwerkingtreding van de AVG. De AVG staat voor een versterking en uitbreiding van privacyrechten en meer verantwoordelijkheden voor organisaties. De bevoegdheden van de Europese toezichthouders, voor Nederland de Autoriteit Persoonsgegevens (hierna: “AP”), zijn uitgebreid. Een voorbeeld is de bevoegdheid om boetes tot €20 miljoen op te leggen.

De GGD heeft de ambitie, maar ook de wettelijke verplichting om zoveel mogelijk te voldoen aan de (kwaliteits)eisen voor gegevensbescherming uit de AVG. Wij stellen burgers, medewerkers en (keten)partners centraal en vinden dat ze moeten kunnen vertrouwen op een veilige verwerking van persoonsgegevens. Niet alleen vanwege de wettelijke verplichting en het risico op handhaving, maar juist omdat de GGD veel waarde hecht aan de bescherming van de persoonlijke levenssfeer van betrokkenen.
Daarnaast ambieert de GGD een actief gegevensbeschermingsbeleid, dat vooral gericht is op bewustwording, een transparante en kritische cultuur en kennisoverdracht. Bovendien willen wij medewerkers en klanten zoveel mogelijk betrekken bij het onderwerp gegevensbescherming en de bijbehorende dilemma’s. Goede, transparante communicatie met burgers is daarom van groot belang.
De GGD geeft met dit beleid duidelijk richting aan hoe er moet worden omgegaan met privacy en laat zien dat zij de bescherming van persoonsgegevens waarborgt en handhaaft. De GGD wil hiermee onder andere bereiken dat:

- de basis voor een goed geïmplementeerd beleid op het gebied van gegevensbescherming wordt gegarandeerd en dat alle medewerkers zich ten volle bewust zijn van de noodzakelijkheid van een zorgvuldige omgang met persoonsgegevens. Dit vormt de basis voor een toepassing van de wettelijke eisen en voor een respectvolle omgang met de persoonsgegevens van betrokkenen;
- de rechten van betrokkenen worden gerespecteerd en in procedures zijn verankerd;
- het vertrouwen van betrokkenen in de zorg en overheid niet wordt beschaamd;
- uitvoering van dit beleid binnen de GGD gericht wordt opgepakt, zodat de wettelijke eisen goed geïmplementeerd zijn;
- het onderwerp zowel op bestuurlijk- als medewerkersniveau breed wordt gedragen, als onderdeel van zowel uitvoering van de wettelijke opgave, goed werkgeverschap, opdrachtnemer- en opdrachtgeverschap;
- de kans op financiële schade door het oplopen van boetes en reputatieschade voor de GGD wordt geminimaliseerd en bijbehorende risico’s worden beheerst.

3.2 Begripsbepalingen

Accountability (verantwoordingsplicht)
Het kunnen aantonen op welke manier de persoonsgegevens worden verwerkt conform de AVG. Hiertoe dienen passende en effectieve maatregelen te worden genomen, zoals:

- documentatieplicht: het bijhouden van een register van verwerkingen;
- het beschermen van gegevens door ontwerp principes als Privacy by Design en Privacy by Default;
- indien voorkomende gevallen: het uitvoeren van een Data Protection Impact Assessment ("DPIA");
- het treffen van passende technische en organisatorische maatregelen, waaronder juridische en beveiligingsmaatregelen;
- het opstellen van een procedure om beveiligingsincidenten en datalekken te documenteren, alsmede een procedure voor het melden van een datalek aan AP;
- het aanstellen van een Functionaris Gegevensbescherming.

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

Autoriteit Persoonsgegevens
De Autoriteit Persoonsgegevens ("AP") staat voor het grondrecht op bescherming van persoonsgegevens. De AP is de toezichthoudende autoriteit verantwoordelijk voor het toezicht op de toepassing van de Verordening teneinde de grondrechten en fundamentele vrijheden van natuurlijke personen in verband met de verwerking van hun persoonsgegevens te beschermen en het vrije verkeer van persoonsgegevens binnen de Unie te vergemakkelijken.

Betrokkene
Degene op wie de persoonsgegevens betrekking hebben.

Big data
Een of meer datasets, zowel ongestructureerd als gestructureerd, die door middel van koppeling of hergebruik geschikt zijn voor analyse doeleinden, zoals bijvoorbeeld beleidsonderzoek, gedragsonderzoek, of (medisch) wetenschappelijk onderzoek.

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

DB
Het Dagelijks Bestuur van de GGD West-Brabant.

Derde
Een natuurlijke persoon of rechtspersoon, een overheidsinstantie, een dienst of een ander orgaan, niet zijnde de betrokkene, noch de verwerkingsverantwoordelijke, noch de verwerker, noch de personen die onder rechtstreeks gezag van de verwerkingsverantwoordelijke of de verwerker gemachtigd zijn om de persoonsgegevens te verwerken.

Functionaris voor gegevensbescherming

De functionaris voor gegevensbescherming (hierna: “FG”) is de interne toezichthouder op de verwerking van persoonsgegevens. De FG dient in alle onafhankelijkheid zijn werkzaamheden te kunnen uitvoeren en ontvangt daarbij geen instructies van opdrachtgevers of verwerkers. Hij is aangemeld bij de AP als contactpersoon en aanspreekpunt bij de meldingen van datalekken. Hij functioneert als tussenpersoon tussen verschillende belanghebbenden en is daarmee ook verlengstuk van de AP.

Geautomatiseerde (individuele) besluitvorming en profilering
Elke vorm van geautomatiseerde verwerking van persoonsgegevens waarbij aan de hand van persoonsgegevens bepaalde persoonlijke aspecten van een natuurlijke persoon worden geëvalueerd, met name met de bedoeling zijn beroepsprestaties, economische situatie, gezondheid, persoonlijke voorkeuren, interesses, betrouwbaarheid, gedrag, locatie of verplaatsingen te analyseren of te voorspellen.

Gegevensbescherming
Bescherming van persoonsgegevens tegen oneigenlijk gebruik.

Gegevensbeschermingseffectbeoordeling (Data protection impact assessment/DPIA)
Een instrument waarmee het effect van beoogde verwerkingsactiviteiten op de bescherming van persoonsgegevens op een gestructureerde en heldere manier in beeld in kaart wordt gebracht om vervolgens maatregelen te kunnen nemen om de risico’s te verkleinen.
Een analyse van de gevolgen voor gegevensbescherming als een project, beleid, dienst, product of ander initiatief wordt gestart of ingevoerd en het nemen van eventueel noodzakelijke mitigerende acties om een negatieve impact te voorkomen dan wel te verkleinen.

Governance
De wijze waarop de daadwerkelijke implementatie van richtlijnen en strategie is gegarandeerd, zodat vereiste processen op de juiste manier worden gevolgd om te kunnen voldoen aan weten regelgeving. Governance bevat het definiëren van rollen en verantwoordelijkheden, meten en rapporteren, nemen van acties om geïdentificeerde kwesties op te lossen.

Inbreuk in verband met persoonsgegevens (datalek)
Een inbreuk op de beveiliging die al dan niet per ongeluk op onrechtmatige wijze leidt tot de vernietiging, het verlies, de wijziging of de ongeoorloofde verstrekking van of de ongeoorloofde toegang tot doorgezonden, opgeslagen of anderszins verwerkte persoonsgegevens.

Informatiebeveiliging
Een verzameling van processen die zijn ingericht om de betrouwbaarheid van informatie te beschermen. Informatiebeveiliging heeft betrekking op:
- Beschikbaarheid: het zorg dragen voor het beschikbaar zijn van informatie en informatie verwerkende bedrijfsmiddelen op de juiste tijd en plaats voor de gebruikers;
- Integriteit: het waarborgen van de correctheid, volledigheid, tijdigheid en controleerbaarheid van informatie en informatieverwerking;
- Vertrouwelijkheid: het beschermen van informatie tegen kennisname en mutatie door onbevoegden. Informatie is alleen toegankelijk voor degenen die hiertoe geautoriseerd zijn.

Persoonsgegevens
Alle informatie over een geïdentificeerde of identificeerbare natuurlijke persoon.
Bij de GGD worden onder andere de volgende categorieën persoonsgegevens verwerkt:

- Personalia en identificatiegegevens

Persoonsgegevens, die betrekking hebben op persoonlijke bijzonderheden van betrokkene (naam, adres, woonplaats e.d.) om een persoon te kunnen identificeren.

- Medische gegevens

Persoonsgegevens, direct of indirect betrekking hebbend op de lichamelijke of geestelijke gesteldheid van betrokkene, verzameld door een beroepsbeoefenaar op het gebied van de (publieke) gezondheidszorg in het kader van zijn beroepsuitoefening.

- Financiële en administratieve gegevens

Gegevens die in de administratie van de GGD en de persoonsdossiers zijn opgenomen, niet zijnde personalia, identificatie-, medische of psychologische gegevens, die noodzakelijk zijn voor de financiering en/of administratieve afhandeling van de zorgverlening.

Toestemming van betrokkene
Elke vrije, specifieke en op informatie berustende ondubbelzinnige wilsuiting waarmee de betrokkene door middel van een verklaring of een ondubbelzinnige actieve handeling aanvaardt dat zijn persoonsgegevens worden verwerkt.

Tracking
Het volgen van mobiele datadragers zoals telefoons, bijvoorbeeld door Wifi- of bluetooth apparatuur waarbij (persoons)gegevens worden verzameld uit die datadragers.

Verwerker
Een verwerker is een persoons of organisatie die op basis van een opdracht van de verwerkingsverantwoordelijke en conform de aanwijzingen van deze verwerkingsverantwoordelijke persoonsgegevens verwerkt.

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

Verwerkingsverantwoordelijke
Een persoon of instantie die, alleen of samen met een ander, het doel en de middelen voor de verwerking van de persoonsgegevens vaststelt.
Binnen de GGD is het DB de verwerkingsverantwoordelijke. Het DB stelt het doel en de middelen vast voor de verwerking van persoonsgegevens. Het bestuur kan bepaalde taken overdragen aan de directeur publieke gezondheid (hierna: “DPG”) die hiermee de bevoegdheid krijgt om in naam van het bestuur besluiten te nemen.

3.3 Juridisch kader

3.3.1 Bij dit beleid wordt in aanmerking genomen:

- Burgerlijk Wetboek, Boek 7 (Wet op de geneeskundige behandelingsovereenkomst, ”WGBO”);
- Wet op de Beroepen in de individuele gezondheidszorg (Wet Big);
- Wet kwaliteit, klachten en geschillen zorg (“Wkkgz”);
- Algemene Verordening Gegevensbescherming (“AVG”);

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

3.4 Doelgroep en toepassingsbereik

3.4.1 Dit beleid is van toepassing op de gehele organisatie en op alle processen, onderdelen, objecten en gegevensverzamelingen van de GGD waarin persoonsgegevens worden verwerkt. Dit betreft zowel de taken die GGD op grond van de gemeenschappelijke regeling, al dan niet in mandaat, uitvoert voor de bestuursorganen van de gemeenten, alsmede de taken die de GGD uitvoert als openbaar lichaam in het kader van de Wet gemeenschappelijke regelingen (“Wgr”) en als werkgever. De GGD geldt hierbij als verwerkingsverantwoordelijke in de zin van de AVG.

3.4.2 Dit gegevensbeschermingsbeleid en een juiste uitvoering hiervan richt zich tot alle interne en externe medewerkers binnen de organisatie. Het is vooral gericht op diegenen die werken met persoonsgegevens, dan wel persoonsgegevens laten verwerken door externe partners.

3.4.3 Het beleid heeft betrekking op de hele “data levenscyclus”: van het genereren of verzamelen van persoonsgegevens, het dagelijkse gebruik ervan en de gegevensopslag tot en met de archivering en vernietiging ervan.

3.4.4 Het gegevensbeschermingsbeleid staat niet op zichzelf. Het heeft raakvlakken of vertoont overlap met andere beleidsthema’s als informatiebeveiliging, integriteit, kwaliteitszorg, personeel en organisatie en communicatie.

3.5 Inrichtingswijze gegevensverwerking

3.5.1 Door het cyclische karakter van de aangegeven maatregelen en door de bescherming van persoonsgegevens onderdeel te laten zijn van het managementsysteem van de GGD ontstaat een continu proces van veranderen en verbeteren. De kwaliteit van het omgaan met gegevensbeschermingsvraagstukken wordt immers verhoogd door op verschillende niveaus en vanuit verschillende rollen telkens weer de cyclus van plan-do-check-act (“PDCA”) te

doorlopen. Hierdoor ontstaat een evenwichtig beheersingssysteem. De GGD werkt zo actief aan bewustzijn, het opbouwen van kennis bij medewerkers en aan verantwoorde procesuitvoering op het gebied van gegevensbescherming.

3.5.2 Het borgen van de gegevensbescherming is onlosmakelijk verbonden met informatiebeveiliging. In dat kader werkt de GGD nauw samen met ‘Hét Service Centrum‘ (“HSC”).

4. Rechten van betrokkenen

4.1 Rechten van betrokkenen

4.1.1 De AVG brengt betrokkenen sterkere en nieuwe privacyrechten. Organisaties die persoonsgegevens verwerken krijgen meer verplichtingen. De nadruk ligt op de ‘accountability’, ofwel de verantwoordelijkheid van de GGD om te kunnen aantonen de organisatie zich aan de wet houdt.

4.1.2 De rechten van de betrokkene zijn binnen de GGD op transparante ingericht. Betrokkenen hebben recht op:

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

4.1.3 De GGD geeft hieraan onder andere uitvoering door betrokkenen op de website helder te informeren hoe van deze rechten kan worden gebruik gemaakt.

4.1.4 Om gebruik te maken van hun rechten kunnen de betrokkenen een verzoek indienen. Iemand kan een verzoek tot uitoefening van zijn of haar rechten via de website van de GGD of via andere gangbare publieksdienstverleningskanalen van de GGD doen. Dit verzoek is geldig ongeacht het middel waarmee het verzoek wordt gedaan onder voorwaarde van een deugdelijke identiteitsvaststelling.

4.1.5 Een beslissing op een verzoek wordt behandeld als een besluit in de zin van de Algemene wet bestuursrecht (“Awb”). Hiertegen kan bezwaar worden gemaakt.

4.2 Recht op informatie en toegang tot gegevens

4.2.1 Tijdens het eerste contact met een cliënt informeert de hulpverlener betrokkenen over de wijze waarop zijn persoonsgegevens worden verwerkt. Er wordt dan informatie verstrekt over het (a) doel van de gegevensverwerking, (b) de aard van de gegevens die worden verwerkt, (c) de grondslag van de verwerking, (d) de rechten die ten aanzien van de gegevensverwerking kunnen worden ingeroepen en (e) de identiteit van de verantwoordelijke.

4.2.2 Als het niet mogelijk is om de betrokkene tijdens het eerste contact te informeren, dan zorgt de hulpverlener dat de betrokkene zo spoedig als de situatie toe laat, alsnog over de gegevensverwerking wordt geïnformeerd.

4.2.3 Van het (uitstellen of niet) informeren van de betrokkene kan een aantekening worden gemaakt in het dossier.

4.2.4 De GGD verzamelt gegevens om haar taken te kunnen uitvoeren. Indien dit persoonsgegevens betreft en indien betrokkenen hiervan niet op de hoogte zijn informeert de GGD hen actief over de verwerking van hun persoonsgegevens zoals het doel daarvan, welke persoonsgegevens worden verwerkt, wie daarvoor verantwoordelijk is en of de gegevens aan anderen worden verstrekt.

4.2.5 De GGD informeert betrokkene, uiterlijk binnen vier weken na de verzameling van persoonsgegevens, indien de persoonsgegevens van derden afkomstig zijn.

4.3 Recht op inzage en afschrift van gegevens

4.3.1 Patiënten, medewerkers en andere betrokkenen kunnen altijd hun persoonsgegevens inzien wanneer zij hier om vragen en kunnen er op vertrouwen dat deze gegevens correct zijn dan wel worden aangepast wanneer noodzakelijk of door de betrokkene is aangegeven dat deze aangepast dienen te worden, voor zover een (wettelijke) verplichting dit niet onmogelijk maakt.

4.3.2 Betrokkenen hebben de mogelijkheid om te controleren of en op welke manier hun gegevens worden verzameld en verwerkt en het recht op inzage en afschrift van zijn dossier [1]. Uitzondering op deze regel is als de persoonlijke levenssfeer van een ander daardoor wordt geschaad. Bijvoorbeeld informatie die een partner aan een hulpverlener heeft verstrekt in het vertrouwen dat betrokkene deze informatie niet te zien krijgt.

4.3.3 De GGD verstrekt de betrokkene, binnen vier weken na ontvangst van het verzoek, kosteloos een kopie van de persoonsgegevens die worden verwerkt.

4.3.4 Indien de termijn van vier weken onhaalbaar blijkt, verlengt de GGD de termijn met twee maanden en brengt de betrokkene hier schriftelijk van op de hoogte.

4.3.5 Indien de betrokkene om bijkomende kopieën vraagt, kan de GGD een vergoeding rekenen niet hoger dan de kostprijs.

4.4 Recht op rectificatie (correctie, aanvulling) van gegevens

4.4.1 Als de GGD persoonsgegevens van betrokkenen verwerkt die naar hun oordeel onjuist zijn, kunnen zij een verzoek indienen bij de GGD om feitelijke onjuistheden in het dossier te corrigeren. Het gaat dan bijvoorbeeld om onjuiste adresgegevens. Niet wordt bedoeld dat de bijvoorbeeld de diagnose mag worden gewijzigd.

4.4.2 Er kan ook een verklaring aan het medisch dossier worden toegevoegd, bijvoorbeeld eigen visie van de betrokkene, ook als de hulpverlener het niet eens is met de verklaring moet deze worden opgenomen.

4.5 Recht op gegevenswissing

4.5.1 Betrokkenen hebben het recht persoonsgegevens te laten verwijderen indien de GGD niet langer een goede grond heeft voor het gebruik hiervan, bijvoorbeeld indien betrokkenen een

[1] Artikel 7:456 BW en artikel 15 van de AVG

gegeven toestemming intrekken, indien de gegevens onjuist zijn of de gegevens niet langer nodig zijn.

4.5.2 Het AVG recht op gegevenswissing geldt in principe niet voor medische dossiers. De betrokkene heeft het recht om op hem betrekking hebbende gegevens te laten verwijderen en op grond van de Wgbo heeft hij bovendien het recht dossiergegevens te laten vernietigen ongeacht of dit relevante gegevens zijn[2].

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

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

4.6 Recht op beperking van de verwerking

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

4.7 Recht op overdraagbaarheid van gegevens (dataportabiliteit)

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

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

4.7.3 De GGD treft voorzieningen in het kader van dataportabiliteit.

[2] Artikel 7: 455 BW

4.8 Recht van bezwaar tegen verwerking

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

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

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

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

4.10 Klachten en vragen

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

4.10.2 Binnen vier weken beoordeelt de GGD of het verzoek ontvankelijk is. De GGD laat binnen die termijn weten wat er met het verzoek gaat gebeuren, waaronder of de GGD de behandeling van het verzoek met twee maanden verlengt. De GGD behandelt het verzoek volgens de daarvoor door haar vastgestelde en bekendgemaakte procedure[3].

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

4.10.4 Indien naar de mening van de klant de beslissing op een klacht niet tot het gewenste resultaat heeft geleid, wordt gewezen op de mogelijkheid om diens klacht voor te leggen aan de Autoriteit Persoonsgegevens, Postbus 93374, 2509 AJ 's Gravenhage.

4.11 Informeren van (keten)partners

4.11.1 De GGD informeert relevante ketenpartners indien het verzoek wordt ingewilligd. Dit betreft o.a. organisaties met wie een verwerkersovereenkomst dan wel een gebruiksovereenkomst of een overeenkomst tot derde verstrekking is afgesloten. Indien relevant vraagt de GGD

[3] Klachtenregeling GGD West-Brabant 2017

actief om bevestiging van de betreffende ketenpartner(s) dat aan het betreffende verzoek is voldaan.

4.12 Rechten en plichten aangaande het medisch dossier

4.12.1 De Wet op de geneeskundige behandelingsovereenkomst (“WGBO”) verplicht de hulpverlener van de GGD om een medisch dossier in te richten. In het medisch dossier neemt de hulpverlener alle gegevens op over de gezondheid van de betrokkene en over de uitgevoerde verrichtingen, voor zover dit voor een goede hulpverlening noodzakelijk is.

4.12.2 De betrokkene kan de hulpverlener niet van deze verplichting ontheffen. De gegevens vallen onder het medisch beroepsgeheim: de hulpverlener heeft een geheimhoudingsplicht.

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

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

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

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

4.12.6 Een hulpverlener van de GGD mag uitsluitend een (medisch) dossier aanleggen in de hiervoor bestemde en door de GGD aangewezen (zorg)informatiesystemen.

5. Verplichte maatregelen en procedures

5.1 Bewustwording

5.1.1 De GGD zorgt voor bewustzijn op het gebied van gegevensbescherming voor al haar medewerkers. Hierbij dienen zij minimaal op de hoogte te zijn van de voor hun relevante wet- en regelgeving en bepalingen zodat zij deze in hun dagelijkse werk kunnen toepassen. Hierbij kan gedacht worden aan regels over toegang tot medische gegevens, maatregelen ter bescherming van bijzondere persoonsgegevens, datalekken en zwijgplicht.

5.1.2 Concreet kan de GGD bewustwording vormgeven door enerzijds te voorzien in algemene en op het thema afgestemde specifieke voorlichtingen op het gebied van gegevensbescherming. Anderzijds wil de GGD het bewustzijn op dit gebied door gegevensbescherming tot terugkerend agendapunt te maken van de verschillende overleggen. Daarmee worden dilemma's op het gebied van gegevensbescherming bespreekbaar en stimuleert de GGD medewerkers om beveiligingsincidenten en datalekken te melden. Tenslotte kan bewustwording bevorderd worden door bijvoorbeeld e-learning, nieuwsbrieven en informatie op het intranet.

5.2 Verwerking van persoonsgegevens door derden

Verwerkers en verwerkersovereenkomst(en)

5.2.1 Wanneer de GGD een externe partij of (keten)partner inschakelt om ten behoeve van de GGD persoonsgegevens te verwerken en het verwerken van de persoonsgegevens een hoofdzaak is van deze partij, kan deze partij worden beschouwd als verwerker.

5.2.2 De GGD schakelt enkel verwerkers in die afdoende garanties bieden met betrekking tot het toepassen van passende technische, procesmatige, communicatieve en organisatorische maatregelen[4].

5.2.3 De instructies omtrent verwerking(en) door een verwerker worden schriftelijk vastgelegd in een verwerkersovereenkomst[5] voordat de dienstverlening aanvangt.

5.2.4 De belangrijkste verwerkers zullen minstens eens per jaar door de GGD, middels de leveranciersbeoordeling, gecontroleerd worden op borging en naleving van de verplichtingen uit de verwerkersovereenkomst. Een dergelijke controle kan o.a. bestaan uit het opvragen van relevante certificeringen. Minder kritische verwerkers worden periodiek gecontroleerd.

5.2.5 De GGD hanteert als modelovereenkomst: (a) de gemeentelijke standaard verwerkersovereenkomst[6] of (b) de standaard model verwerkersovereenkomst voor de zorgsector[7].

[4] Artikel 28 lid 1 van de AVG
[5] Artikel 28 lid 3 van de AVG
[6] Zie: https://www.informatiebeveiligingsdienst.nl/product/handreiking-standaard-verwerkersovereenkomst-gemeenten/
[7] Zie: https://www.vgn.nl/nieuws/standaard-model-verwerkersovereenkomst-voor-de-zorgsector

5.2.6 Verwerkingen mogen niet plaatsvinden in landen die geen passend beveiligingsniveau kunnen bieden. Hiervan kan worden afgeweken met uitdrukkelijke toestemming van de betrokkenen of andere waarborgen die de autoriteiten hebben goedgekeurd. Een lijst met landen met een passend beveiligingsniveau is te vinden op: https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en

De GGD als verwerker

5.2.7 In voorkomende gevallen treedt de GGD op als verwerker voor derden. Hierbij zijn derden verwerkingsverantwoordelijk.

5.2.8 De GGD streeft na om voor deze verwerkingen heldere en eenduidige voorwaarden op te stellen die ook toepasbaar zijn voor gelijksoortige verwerkingen.

5.2.9 De GGD biedt daarbij aan de verwerkingsverantwoordelijke voldoende garanties voor het zorgvuldig verwerken van gegevens door het toepassen van passende technische en organisatorische maatregelen.

5.2.10 De afspraken omtrent de verwerking worden schriftelijk vastgelegd in een verwerkersovereenkomst, voordat de dienstverlening door de GGD aanvangt.

De GGD als gezamenlijke verwerkingsverantwoordelijke

5.2.11 Indien de GGD met een andere partij samenwerkt, die geen verwerker is, maar waarmee wel persoonsgegevens worden uitgewisseld waarbij een gezamenlijke verwerkingsverantwoordelijkheid bestaat maakt de GGD passende afspraken. In dat geval zal de GGD een regeling[8] sluiten omtrent de verwerking van persoonsgegevens, of samen met de andere partij een regeling vaststellen, waarin de respectievelijke verantwoordelijkheden worden vastgelegd.

5.2.12 De GGD plaatst genoemde regeling op haar website[9].

5.3 Documentatie over verwerking van persoonsgegevens

5.3.1 De FG schrijft namens de GGD de verwerkingen van persoonsgegevens waarvoor meld- of registratieplicht geldt bij in het daartoe bestemde register, daarin bijgestaan door de adviseur gegevensbescherming en de portefeuillehouder kwaliteit van het verantwoordelijke team.

5.3.2 Alle nieuwe of niet geregistreerde verwerkingen worden actief door de betreffende medewerker(s) (daar waar de verwerking plaatsvindt) aangemeld bij de FG.

Bij de inschrijving worden in ieder geval de volgende gegevens[10] vermeld:

a. de naam van de verwerking;
b. wie de verantwoordelijke is voor de verwerking;

[8] Artikel 26 lid 1 van de AVG
[9] Artikel 26 lid 2 van de AVG
[10] Artikel 30 lid 1 van de AVG

c. het doel van de verwerking;
d. de groep van personen van wie persoonsgegevens worden verwerkt (betrokkenen);
e. de categorie persoonsgegevens die bij de verwerking worden gebruikt;
f. de ontvangers van de gegevens;
g. de rechtmatige grondslag voor de verwerking van de persoonsgegevens;
h. eventuele verstrekkingen aan andere landen buiten de Europese Economische Ruimte;
i. de verwijderingstermijnen die in acht genomen worden;

5.3.3 De FG houdt toezicht op de volledigheid, juistheid en rechtmatigheid van de in het register ingeschreven verwerkingen van persoonsgegevens.

5.3.4 Bij wijzigingen van de bij de inschrijving opgenomen gegevens draagt de portefeuillehouder kwaliteit van het verantwoordelijke team. zorg voor wijziging hiervan in het register en informeert de FG hierover.

5.3.5 De GGD maakt het register van verwerkingsactiviteiten niet openbaar op de website.

5.4 Informatiebeveiliging

5.4.1 Het waarborgen van de beschikbaarheid, integriteit en vertrouwelijkheid van persoonsgegevens is een voorwaarde om te garanderen dat betrokkenen hun rechten op adequate wijze kunnen uitoefenen.

5.4.2 De GGD streeft de bepalingen uit de NEN 7510, NEN 7512, NEN 7513 en NTA 7516 normen na, ter bescherming van de verwerking van medische gegevens.

5.4.3 De GGD controleert steekproefsgewijs op toegang tot persoonsgegevens door onbevoegden.

Passende beschermende technische en organisatorische maatregelen

5.4.4 Wanneer de GGD persoonsgegevens verwerkt of laat verwerken door een derde, zorgt de GGD ervoor dat passende beveiligingsmaatregelen worden getroffen om de betreffende persoonsgegevens te beschermen tegen de verschillende risico's.

5.4.5 De GGD slaat gegevens zo op dat voldaan kan worden aan de wettelijke kaders van de AVG, dit betekent in verband met de doelbinding vaak gescheiden opslag. Concreet betekent dit bijvoorbeeld dat medische gegevens van klanten nooit worden opgeslagen in een boekhoudkundig systeem.

5.4.6 De GGD houdt actief, per informatiesysteem, een autorisatiemix bij en controleert steekproefsgewijze achteraf op (eventueel ongeautoriseerde) toegang.

5.4.7 De GGD beperkt de toegang tot inzage en wijzigen van gegevens tot degenen die dit vanuit hun functie nodig hebben; medewerkers worden actief aangesproken in geval van overschrijding van toegangsbevoegdheden.

5.4.8 De GGD beschermt persoonsgegevens onder andere door het aggregeren, versleutelen en anonimiseren van deze gegevens. Hierdoor wordt de mate waarin de verwerkte persoonsgegevens kunnen worden herleid tot een individu verminderd.

5.4.9 In beginsel, in het bijzonder bij gegevens aangaande de gezondheid, worden alle gegevensdragers en alle communicatie tussen de GGD en haar klanten en/of (keten)partners voorzien van encryptie (versleuteling).

5.4.10 Als uitgangspunt kiest de GGD voor technische maatregelen om 'gegevensbescherming door ontwerp' te waarborgen. Daar waar de technische mogelijkheden ontbreken of disproportioneel hoge kosten met zich meebrengen, zoekt de GGD naar organisatorische en of procesmatige maatregelen als alternatief voor of als aanvulling op de technische maatregelen. Dit wordt uiteraard samen en in overleg met informatiebeveiliging uitgewerkt.

5.4.11 Deze (technische, procesmatige, communicatie en organisatorische) maatregelen omvatten bij de verwerking van persoonsgegevens een op het risico afgestemd beveiligingsniveau. Hierbij wordt rekening gehouden met de stand van de techniek, de uitvoeringskosten, en ook met de aard, de omvang, de context en de verwerkingsdoeleinden etc. Tevens wordt rekening gehouden met de, qua waarschijnlijkheid en ernst, uiteenlopende risico's voor de rechten en vrijheden van personen.

Waar wenselijk omvatten de maatregelen onder meer het volgende:

- De pseudonimisering en versleuteling van persoonsgegevens;
- Het vermogen om op permanente basis de vertrouwelijkheid, integriteit, beschikbaarheid en veerkracht van de verwerkingssystemen en diensten te garanderen;
- Het vermogen om bij een fysiek of technisch incident de beschikbaarheid van en de toegang tot de persoonsgegevens tijdig te herstellen;
- Een procedure voor het op gezette tijdstippen testen, beoordelen en evalueren van de doeltreffendheid van de technische en organisatorische maatregelen ter beveiliging van de verwerking.

5.5 Meldplicht voor inbreuken in verband met persoonsgegevens (datalekken)

5.5.1 Indien zich een informatiebeveiligingsincident voordoet, waarbij bijvoorbeeld gegevens van personen in verkeerde handen kunnen komen of zijn gekomen, handelt de GGD in overeenstemming met de vastgestelde werkwijze in het Protocol Meldplicht en Afhandeling van (vermoedelijke) datalekken[11]. Dit protocol bevat een vastgesteld proces van te doorlopen stappen om de eventuele schade of de kans hierop, bij een 'datalek' te beperken en de getroffen perso(o)n(en) te beschermen.

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

5.5.3 De plicht tot het melden van een (vermoeden van een) 'datalek' geldt als er sprake is van een aanzienlijke kans op ernstige nadelige gevolgen voor betrokkene, dan wel ernstige nadelige gevolgen voor de bescherming van persoonsgegevens. Het betreft situaties van het

[11] Zie 'Protocol Meldplicht en Afhandeling van (vermoedelijke) datalekken'

(mogelijk) lekken van persoonsgegevens uit GGD bestanden en/of gegevens waarvoor de GGD verantwoordelijkheid draagt.

5.5.4 Wanneer er een dergelijk 'datalek' heeft plaatsgevonden, wordt dit zonder onredelijke vertraging, uiterlijk 72 uur nadat er kennis van de inbreuk is vernomen, gemeld aan de AP. Als dit later dan 72 uur is wordt er een motivering voor de vertraging bij de melding gevoegd.

5.5.5 Indien de inbreuk een hoog risico voor de rechten en vrijheden van de betrokkenen met zich meebrengt, word de inbreuk ook in eenvoudige en duidelijke taal aan de betrokkenen gemeld.

5.5.6 De GGD maakt de afweging of het informeren van de betrokkene in diens belang is of dat dit beter achterwege kan blijven om de betrokkene zelf of anderen te beschermen. Indien van informeren wordt afgezien zal de GGD dit besluit registreren en duidelijk motiveren.

5.5.7 De FG houdt namens de GGD een logboek bij waarin alle medeplichtige en niet-medeplichtige datalekken zijn opgenomen.

5.5.8 In het logboek worden in ieder geval de volgende gegevens vermeld:

a. Het onderwerp van het 'datalek'.
b. De datum van het 'datalek';
c. De duur van het 'datalek';
d. de aard van de inbreuk;
e. de instanties waar meer informatie over de inbreuk kan worden verkregen;
f. de aanbevolen maatregelen om de negatieve gevolgen van de inbreuk gevolgen te beperken.
g. een beschrijving van de gevolgen voor de verwerkte persoonsgegevens;
h. de maatregelen die de GGD heeft getroffen of voorstelt te treffen om deze gevolgen te verhelpen;
i. de kennisgeving aan betrokkenen.

5.5.9 De GGD maakt haar register van informatiebeveiligingsincidenten niet openbaar.

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

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

5.6 DPIA's (Data Protection Impact Assessments)

5.6.1 Voor de GGD is een DPIA een instrument waarmee het effect van beoogde verwerkingsactiviteiten op de bescherming van persoonsgegevens op een gestructureerde en heldere manier in beeld in kaart wordt gebracht om vervolgens maatregelen te kunnen nemen om de risico's te verkleinen.

5.6.2 De GGD voert DPIA's uit voor nieuwe maar ook bestaande verwerkingen van persoonsgegevens die een hoog privacyrisico opleveren voor de betrokkenen. De GGD volgt hierbij de lijst van de AP[12].

5.6.3 Indien naar oordeel van de FG sprake is van een verwerking, die gelet op de aard en de omvang, de context en de doeleinden een hoog risico inhoudt voor de rechten en vrijheden van natuurlijke personen dan wordt door middel van een DPIA aangetoond dat de privacy voldoende is gewaarborgd en worden de al dan niet te nemen maatregelen gemotiveerd.

5.6.4 De GGD neemt het initiatief tot het uitvoeren van een DPIA en betrekt relevante medewerkers bij het proces wat gecoördineerd wordt door de adviseur gegevensbescherming.

5.6.5 Voor nieuwe verwerkingen vindt een DPIA plaats voordat met de betreffende verwerking wordt gestart.

5.6.6 Ten aanzien van bestaande verwerkingen voert de GGD een DPIA uit indien de betreffende verwerkingen hier aan onderworpen dient te worden maar deze nog niet heeft plaatsgevonden.

5.6.7 Een DPIA wordt na maximaal 3 jaar herhaald ter evaluatie, alsmede bij wijzigingen waardoor de risico's van de verwerking toenemen.

5.6.8 Bij het uitvoeren van een DPIA wordt de FG altijd vooraf geïnformeerd.

5.6.9 De portefeuillehouder kwaliteit van een team ziet toe op het nemen van maatregelen die blijkens de DPIA nodig zijn om de risico's te verkleinen.

5.6.10 Het resultaat van de DPIA en de genomen maatregelen om het risico te beperken worden aan de FG voorgelegd ter toetsing en opneming in het register van verwerkingen.

5.6.11 Waar het nieuwe verwerkingen betreft wordt - voorafgaand aan de verwerking- de AP om advies gevraagd indien de GGD niet in staat is om voldoende maatregelen te treffen om de risico's te beperken en er een hoog restrisico bestaat.

5.6.12 DPIA's die binnen de GGD worden uitgevoerd vinden plaats volgens een door het MT bepaalde standaard.

5.6.13 De FG geeft over de uitgevoerde DPIA een advies aan het MT.

5.6.14 De GGD maakt de resultaten van uitgevoerde DPIA's niet openbaar. Deze dienen uitsluitend ter vaststelling van managementbeleid.

5.7 Beheer van persoonsgegevens

Big data en tracking

[12] https://autoriteitpersoonsgegevens.nl/nl/zelf-doen/data-protection-impact-assessment-dpia

5.7.1 Gegevens in big data en tracking mogen alleen worden verzameld, opgeslagen en gedeeld, als ze niet herleidbaar zijn tot een persoon en worden alleen verzameld voor onderzoek dat door of namens de GGD wordt uitgevoerd.

5.7.2 Voor big data en tracking wordt uitsluitend gebruik gemaakt van brongegevens die door daartoe geautoriseerde personen zijn verzameld.

5.7.3 Brongegevens die gebruikt worden voor big data toepassingen worden omgezet tot een dataset die geen persoonsgegevens bevat en dus geanonimiseerd is. Indien het noodzakelijk is om af te wijken wordt vooraf toestemming aangevraagd bij de FG die de aanvraag zal beoordelen in het kader van de rechtmatigheid en de doelmatigheid. Alleen bij een goedgekeurde aanvraag mogen de gegevens gepseudonimiseerd in plaats van geanonimiseerd worden.

Cameratoezicht, camerabewaking en overige inzet van camera's

5.7.4 De GGD past op verschillende plekken binnen haar organisatie registratie van bewegende beelden toe. Voorbeelden hiervan zijn beelden van bewakingscamera's in en rond de consultatiebureaus. Bij elke registratie van camerabeelden bepaalt en documenteert de GGD of en hoe lang deze worden bewaard.

5.7.5 De GGD plaatst de camera's niet zodanig dat deze uitsluitend of voornamelijk op de openbare ruimte zijn gericht.

5.7.6 Camerabewaking kan door particuliere bedrijven worden uitgeoefend onder voorwaarde dat indien er camera's in de openbare ruimte worden geplaatst dan wel delen van de openbare ruimte in beeld worden gebracht, er een daartoe strekkend besluit door of namens het MT is genomen en er een overeenkomst met de verantwoordelijke is gesloten voorafgaande aan de verwerking. Deze overeenkomst gaat in ieder geval in op:

- de grondslag voor de verwerking van persoonsgegevens;
- het verzamel- en verwerkingsdoel;
- de organisatorische en technische maatregelen die worden getroffen tegen verlies of onrechtmatige verwerking;
- de bewaartermijn;
- de wijze waarop voldaan wordt aan de meldplicht datalekken.

Bij inzet van camera's voor andere doeleinden dient voorafgaand aan deze inzet advies te worden gevraagd aan de FG.

Cookies en soortgelijke technieken

5.7.7 De GGD plaatst, indien noodzakelijk, alleen cookies die noodzakelijk zijn voor het correct functioneren van de website op de computers van betrokkenen en het analyseren hiervan, zgn. functionele en analytische cookies en maakt geen gebruik van tracking cookies.

Geheimhouding

5.7.8 Persoonsgegevens worden in beginsel niet verwerkt door medewerkers zonder (medisch) beroepsgeheim of zonder ondertekende geheimhoudingsverklaring.

Minimaal gebruik van persoonsgegevens (dataminimalisatie)

5.7.9 De GGD verzamelt (of vraagt om) niet meer gegevens dan strikt noodzakelijk.

5.7.10 De GGD verwerkt alleen gegevens voor het doel waarvoor zij zijn verzameld en verwerkt deze verder alleen op een manier die verenigbaar is met dit doel.

5.7.11 Bij configuratie van systemen kiest de GGD in voorkomende gevallen voor de privacy-vriendelijke variant (privacy by default).

5.7.12 De informatie die de GGD verwerkt is in beginsel correct en actueel.

5.7.13 De GGD maakt geen onnodige kopieën van verzamelingen van persoonsgegevens.

5.7.14 De GGD voert actief beleid om alle overbodige gegevensverzameling (bijvoorbeeld op – gestandaardiseerde- vragenlijsten en invulformulieren) te verwijderen.

5.7.15 Per team zijn de wettelijk verplichte bewaartermijnen per categorie van persoonsgegevens vastgesteld. De GGD bewaart persoonsgegevens niet langer dan strikt noodzakelijk (bijvoorbeeld op basis van de Belastingwet, de Archiefwet etc.) en verwijdert actief wat niet meer nodig is.

5.7.16 De GGD communiceert actief aan ketenpartners wanneer persoonsgegevens verwijderd dienen te worden waaronder begrepen het vragen van bevestiging dat betreffende persoonsgegevens door de ketenpartner zijn verwijderd.

Onderzoek

5.7.17 De GGD ontdoet bij onderzoek alle persoonsgegevens van direct identificerende kenmerken (anonimiseren).

Privacy by design (privacy door ontwerp)

5.7.18 De GGD hanteert achtereenvolgens de volgende acht data- en procesgeoriënteerde privacy strategieën om gegevensbescherming vanaf begin af aan mee te nemen bij het ontwerpen en bouwen van nieuwe systemen.

1. De verwerking van persoonsgegevens wordt zo veel mogelijk beperkt.
2. De verwerking van persoonsgegevens wordt zo veel mogelijk van elkaar gescheiden.
3. Het detail waarin persoonsgegevens worden verwerkt wordt zo veel mogelijk beperkt.
4. Persoonsgegevens worden afgeschermd of onherleidbaar. Er wordt voorkomen dat persoonsgegevens openbaar worden.
5. Klanten worden over de verwerking van hun persoonsgegevens geïnformeerd (voorafgaand aan de start van de nieuwe verwerking).
6. Klanten krijgen regie en invloed over de verwerking van hun persoonsgegevens.
7. Er wordt een privacy vriendelijke verwerking van persoonsgegevens afgedwongen.
8. Er wordt aangetoond dat persoonsgegevens op een privacy vriendelijke wijze zijn verwerkt

6. Governance

6.1 Functies en verantwoordelijkheden

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

1. Portefeuillehouder kwaliteit per team

- Verantwoordelijk voor de borging van de beschikbaarheid, integriteit en vertrouwelijkheid van de door het team verwerkte persoonsgegevens;
- Verantwoordelijk voor aanmelden van nieuwe (of veranderde) verwerkingen van persoonsgegevens bij de FG;
- In voorkomend geval verantwoordelijk voor de uitvoering van een (door de FG getriggerde) DPIA en borging van de hieruit voortvloeiende (verbeter)maatregelen;
- Het behandelen van verzoeken in het kader van de rechten van betrokkenen;
- Het afsluiten van verwerkersovereenkomsten en andere regelingen;
- Het onderzoeken en melden van informatieveiligheidsincidenten;
- Adviezen uit veiligheidsincidenten implementeren, onder supervisie van de adviseur gegevensbescherming

2. Functionaris voor gegevensbescherming (FG)

- Toezichthouder op de verwerking van persoonsgegevens (naleving van privacywetgeving)
- Informeren, adviseren, bewustmaking over AVG verplichtingen, verwerking, incidenten, klachten, DPIA, opstellen van beleid;
- Opzetten en beheer van register van de verwerkingsactiviteiten;
- Ziet, in overleg met de CISO, toe op de controle van de uitvoering van de maatregelen voor gegevensbescherming en informatiebeveiliging;
- Ziet toe op de ontwikkeling en uitvoering van een privacy-auditplan samen met de kwaliteitsfunctionaris en de portefeuillehouder kwaliteit van het betreffende team. Aan de hand hiervan kan de PDCA-cyclus worden doorlopen waarmee continu verbeteren wordt geborgd;
- Rapporteert tenminste jaarlijks aan het MT over de manier waarop de GGD de afgelopen periode met gegevensbescherming is omgegaan. Ook doet hij in zijn rapport aanbevelingen;
- Onderhoud contacten met de AP

3. CISO (Chief Information Security Officer)

- Actueel houden- en coördineren van de uitvoering van informatiebeveiligings- en gegevensbeschermingsbeleid, risicobeheersing en rapportage;
- Aanspreekpunt voor informatieveiligheid en privacy;
- Bevorderen van bewustzijn (veiligheid en privacy);
- Registratie van veiligheidsincidenten en verantwoordelijk voor afhandeling.

4. Privacybeheerder / adviseur gegevensbescherming

- Advisering, uitvoering en naleving van privacy wetgeving

- Beoordelen van- en adviseren over persoonsgegevensverwerking
- Coördineren van privacy werkzaamheden, inzage- en correctie verzoeken
- Afhandeling van veiligheidsincidenten
- Beheer van verwerkingsovereenkomsten, advisering en ondersteuning bij het afsluiten ervan

5. Directeur publieke gezondheid

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

6. Dagelijks- en Algemeen bestuur

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

7. Adviseur Informatiebeveiliging

- (Pro) actief adviseren over informatiebeveiliging en het informatiebeveiligingsbeleid
- Uitvoeren van gapanalyse (nulmeting) en advies over NEN7510/BIO (minimaal benodigde aanpassingen)
- Adviseren en ondersteunen van de GGD om het benodigde niveau van informatiebeveiliging te bereiken dat minimaal voldoet aan de wet- en regelgeving.
- Ervoor zorgdragen dat ondersteunde systemen en processen bij gegevensverwerker HSC voldoen aan wet- en regelgeving. (De behaalde NEN7510 certificering behouden).

8. Functioneel beheerders informatiesystemen

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

7. Slotbepalingen

De AVG is per 25 mei 2018 van toepassing. Dit beleid treedt in werking per 1 januari 2020, na vaststelling door de verantwoordelijke van de GGD. Het DB wordt hiervan in kennis gesteld.

Het beleid wordt elk jaar geëvalueerd en indien nodig herzien. Aanpassingen van dit beleid worden aangekondigd via het intranet. De meest actuele versie van het beleid is te vinden in het Document Management Systeem.

Aldus vastgesteld door het MT van de GGD West-Brabant op 24 december 2019 te Breda,

Q&A berichtgeving NOS over coronatest.nl

Datum: 10 februari 2021
Status: definitief

Deze Q&A is opgesteld naar aanleiding van een bericht van de NOS over de veiligheid van de website coronatest.nl. Dit bericht is in op 9 februari om 19;50 uur gepubliceerd. Deze Q&A is bedoeld voor medewerkers van de GGD om vragen van het publiek te beantwoorden. Krijgt u een vraag van een journalist over dit onderwerp, dan kunt u doorverwijzen naar het landelijke perspiketnummer: 06 – 83 77 59 07.

Q: Kan ik veilig gebruik maken van coronatest.nl?
A; Ja, de website is veilig. Dat is ook bevestigd door Logius. Dat is een organisatie van de overheid die DigID beheert en in de gaten houdt of organisaties die hier gebruik van maken hun website wel op orde hebben. Het klopt dat we op dit moment nog niet aan alle normeringseisen van Logius voldoen. Maar dat maakt de website niet onveilig. We verwachten begin maart aan alle eisen te voldoen.

Q: Blijft coronatest.nl bereikbaar?
A: Ja, de website blijft gewoon bereikbaar. Berichten in de media dat coronatest uit de lucht gehaald zou worden kloppen niet.

Q: Moet ik bang zijn dat mijn gegevens op straat liggen?
A: Nee, uw persoonsgegevens en testuitslag zijn gewoon veilig. Daar kunnen geen mensen bij die daar geen toestemming voor hebben.

Bericht en vragen
We hebben over dit onderwerp en bericht gebubliceerd op de website van GGD GHOR Nederland. Dat bericht vindt u hier.

Heeft u nog andere vragen, neem dan gerust contact op met het team datadiefstal, [redacted].

//////////////////

Wob-verzoek SOLV/ICAM datalek 2021 coronasysteem

15.0 Tekst Wob-verzoek en register documenten

Tekst verzoek (xv)

Informatie die in het kader van de melding van het datalek bij de Autoriteit Persoonsgegevens over en weer is gedeeld, alsmede informatie die over en weer is verstrekt ten behoeve van het onderzoek door de Autoriteit Persoonsgegevens
naar aanleiding van het datalek.

Register

Een screenshot van de verkennerpagina van map 15:

xxx

		Overleg crisisteam datadiefstal 4 februari 2021			
	Onderwerp	**Omschrijving actie/besluit**	**Wie**	**Afdoen voor**	**Status**
1,	[redacted]	• 25 formele verzoeken ontvangen m.b.t. verwijderen persoonsgegevens. De klachtenfunctionaris benaderen voor het bekijken/behandelen van de verzoeken • Ondersteuning AKD akkoord • Navraag of landelijke ondersteuning nodig is bij het verwijderen van gegevens? Indien nodig persoon inhuren c.q. hiervoor verantwoordelijk maken • Het kader (eventueel landelijk) voor verwijderen/vernietigen van gegevens. Bij vaccineren betreft het een medisch dossier, bij testen niet. Onderzoek behoud statistische gegevens versus persoonsgegevens	[redacted]	11 feb 11 feb	
2.	Communicatie	• [redacted] heeft 4 februari contact met de landelijke communicatieadviseur van GGD/GHOR NL. • Toegang tot systemen en veilig omgaan met data – [redacted] heeft een afspraak met [redacted] wat medewerkers minimaal nodig hebben om hun werk uit te voeren. Goed om afspraken te maken binnen de GGD hoe je software inzet • Er liggen vragen voor aanpassingen om op de website te plaatsen. [redacted] van HvB hiervoor benaderen voor de inhoudelijke check • Een voorstel maken hoe we voor de eigen website een digid inlog kunnen realiseren		11 feb 11 feb 11 feb 11 feb	
3	Personeel	• Raamovereenkomsten met uitzendbureaus – hier moet opgenomen worden dat de recente VOG (niet ouder dan 1 jaar) bij de GGD aanwezig moet zijn. Het proces wordt hierop aangepast. Inoverleg met TWB en JongJGZ dat zij deze ook aan moeten leveren. Dt geeft wel vertraging bij inzet van personeel. • Mensen zonder VOG hebben nu geen toegang tot te systemen totdat deze aanwezig is. Een check uitvoeren of dat dit ook het geval is. • Proces opleiden is opgestart, dient wel opvolging te krijgen • Whats app gebruik en mail gebruik– voor zover bekend wordt whats app niet gebruikt in de processen. Ook voor de is het van belang om persoonsgegevens te verwijderen. Actie ondernemen voor het opschonen van telefoons en bestanden waar mogelijk persoonsdata in zitten. Hier gaat het ook om gedragsregels. Hiervoor een plan maken.		4 feb 11 feb	gereed
4	ICT	• Aanscherpen proces Rollen en inhoud van medewerkers • Dashboards – navraag wanneer PC6 wordt opgenomen • Een update aanvragen voor Logging en controle. Hiervoor contact opnemen met [redacted].		11 feb	

5	Risicoanalyse	Uitvoeren risicoanalysen op datalekken in andere systemen	[redacted]		
6	Bestuurlijk	Er wordt een brief verzonden met de stand van zaken van dit moment en de genomen maatregelen naar bestuurders van WB en de VR.	[redacted]	4 feb	
7	Projectorganisatie	Landelijk wordt een projectorganisatie samengesteld. Besluit om deze ook voor GGD WB samen te stellen: • Projectleider – wellicht extern • ICT – [redacted] neemt dit op binnen zijn team • Kwaliteit – [redacted] • Communicatie - [redacted] • Ondersteuning – Nog te bepalen		11 feb	
	Volgend overleg 11 feb om 08.30u	• Actielijst • Projectgroep • Actualiteiten			

xxx

xxx

		Overleg crisisteam datadiefstal 11 februari 2021			
	Onderwerp	**Omschrijving actie/besluit**	**Wie**	**Afdoen voor**	**Status**
1,	[redacted]	• 36 formele verzoeken ontvangen m.b.t. verwijderen persoonsgegevens. • Het eerste verzoek dateert van 25 januari en dient binnen een maand afgehandeld te zijn. Er mag niet verdaagd worden zonder zwaarwegende redenen. • Voorbereiden ontvangstbevestigingen en versturen **Advies AKD** • **Stroomschema**, rechten-formulier, op de website plaatsen. Landelijke check dat wij voornemens zijn deze te publiceren via een link Bespreken tijdens de DPG-raad van 12 feb • Vragen van burgers komen nu in [redacted]-mailbox binnen. Aangezien alleen [redacted] toegang heeft ook [redacted] toegang geven. • **Verwijderverzoek**: 1. Werkinstructie verwijderen en anonimiseren uit verschillende systemen 2. Wie verwijdert welke gegevens? Opnemen met [redacted] 3. Persoonsgegevens verwijderen en record anonimiseren (landelijke richtlijn) Contact opnemen met NOG en landelijk toetsen. • **Inzage voor burgers** – uitdraai van de systemen waarin gegevens zijn vastgelegd. Check of DWH nieuwe updates geeft **Vaccinatiegegevens verwijderen**. • Wordt de lijn van WGBO gevolgd? Dit moet landelijk 1 lijn zijn. [redacted] checken dit via de landelijke kanalen. • We volgen de landelijke richtlijn indien er een verwijderingsverzoek binnenkomt na een eerste vaccinatie. • Bepalen wie het besluit neemt voor verwijderen van gegevens – [redacted] neemt met [redacted] op wie hiervoor het mandaat heeft. • Landelijke afstemming belangrijk voor de communicatie en hierna acties uitzetten.	[redacted]	12 feb	
2.	Communicatie	• **Stroomschema:** Rechtenformulier AKD op de website plaatsen en updaten		11 feb	Gereed

		• **Communicatie GGD NL** – Wachten op een reactie. • **Toegang systemen:** De toegang tot de systemen is inmiddels aangescherpt Systeem Trello (BCO) check op privacy, wellicht niet meer gebruiken. Toegang SharePoint – check dat niemand toegang heeft met een privé account • Er wordt een vereenvoudigd formulier gemaakt, speciaal voor meldingen inz. corona, en op de site geplaatst. HvB hanteert een andere procedure hierin. • Realiseren Digid inlog voor eigen website – deze zetten we on hold	[redacted]	19 feb 19 feb	
3	Personeel	• **VOG** is inmiddels opgenomen in de raamovereenkomst. Hier is ook een check op gedaan. Zonder VOG is er geen toegang tot de systemen. • **Opleiden** Dag coördinatoren - aandacht besteden aan het werken met privacy gevoelige data. **Testen/vaccineren** - check om dit mee te nemen in de briefing • Voor alle systemen/processen – opstellen van instructie m.b.t. gebruik van persoonsgegevens via diverse kanalen zoals whats app, mail in systemen.		11 feb 11 feb	Gereed
4	ICT	• Aanscherpen rollen: Extern zijn verwijderd, interne rollen nog aanscherpen • PC6 is weer opgenomen. •		19 feb	
5	Risicoanalyse	• Proces opstellen met betrekking tot gebruik van een systeem. • DPIA uitvoeren voordat met een systeem wordt getart – voor het onderdeel corona en daarnaast breder. Verzoek aan informatiemanager [redacted] of hij nu voor corona een risicoanalyse kan maken.		19 feb	
6	Bestuurlijk	• Brief is verstuurd		12 feb	gereed
7	Projectorganisatie	Formuleren van de opdracht voor de projectgroep specifiek gericht op dit onderwerp. • Projectleider – wellicht extern – contact [redacted] • ICT – [redacted] neemt dit op binnen zijn team • Kwaliteit – [redacted] • Communicatie - [redacted] • Ondersteuning – Nog te bepalen		19 feb	
	Volgend overleg	Donderdag 18 februari om 08.00u			

xxx

		Overleg crisisteam datadiefstal 25 februari 2021			
	Onderwerp		**Wie**	**Afdoen voor**	**Status**
1,	[redacted]	• Register aanwezig met alle formele verzoeken. De 1e verzoeken zijn van 26/1, Indiener uiterlijk antwoord op 26/2. De brieven zijn i.s.m. AKD opgesteld en gereed om verstuurd te worden. • Inzageverzoeken en doorsturen van informatie naar andere partijen/organisaties Besluit nemen en borgen wie en hoe onderstaande punten worden opgepakt, 1. Afhandelen testen/vaccineren via GGD/GHOR NL 2. HP-zone intern – volgen we hier de landelijke richtlijn? Navraag doen bij HvB en NOG, • Het DB is bevoegd om besluit te nemen. Organisatieverordening moet hiervoor aanwezig zijn. Besluiten nemen ovv van de burger, afwijzen, verdagen of toekennen. • Voor een eventueel bezwaar moet er een bezwarencommissie zijn. GGD WB heeft een onafhankelijke bezwarencommissie, HR is hiervan op de hoogte • WPO – verschillende zienswijze t.o.v. landelijk – er is discussie welke wettelijke basis van toepassing op de processen van vaccineren, testen en BCO. Vaccineren is een medische handeling, BCO niet. Bij testen is de discussie door wie dit verzoek moet worden afgehandeld. Bij testen wordt niet vastgesteld of iemand ziek is, geen medische handeling, Met betrekking tot verwijderingsverzoeken hierover een besluit nemen in het MT	[redacted]	26/2 3/3	gereed
2.	Communicatie	• Plaatsing informatie voor de burger op de website is gereed voor plaatsing– 26/2 live • Training voor medewerkers – we werken met ‘Good Habitz’, dit is een online platform. Onderdeel hiervan is de privacy training.. Informeren bij de GGD Academy of deze nog up to date is en weer onder de aandacht brengen bij medewerkers.		26/2	Gereed Mee bezig
3	Personeel	• Instructies in diverse briefing wordt inmiddels meegenomen. • Meer monitor houden op VOG			
4	ICT	• Rollen en verantwoordelijkheden, deze zijn intern en extern gereed. Er is een procedure voor validatie wie welke rechten heeft. Vraag aan [redacted] deze na te lopen. • [redacted] geeft aan dat er via het landelijk dashboard 2 pagina’s te benaderen zijn met persoonsgegevens met exportmogelijkheden –23/2 mail gestuurd om deze te		26/2	

		verwijderen. 8/12 is dit al kenbaar gemaakt aan GGD NL. [redacted] neemt dit mee in de DPG raad.			
5	Risicoanalyse	• Meenemen in de opdracht.. Ook organisatorische maatregelen meenemen in de opdracht. Als de Autoriteit Persoonsgegevens nu komt kunnen we aangeven hoe we zakengeregeld hebben en wat we nog moeten organiseren? [redacted] geeft de bevestiging dat we dit aan kunnen tonen.			
6	Bestuurlijk	• Het bestuur wordt regelmatig geïnformeerd. Op dit moment geen noodzaak richting bestuur te reageren.			
7	Projectorganisatie	• Voorstel: Externe projectleider met interne projectgroep. Opdracht: Handelingsperspectief en bewustzijn binnen de organisatie. Interne projectgroep: [redacted] 3 maart besluit door MT m.b.t. het verzoek voor het werven van een externe projectleider			
	Volgend overleg	Donderdag 4 maart 11.00u			

xxx

		Overleg crisisteam datadiefstal 4 maart 2021			
	Onderwerp		**Wie**	**Afdoen voor**	**Status**
1,	[redacted]	Verwijderings- en inzageverzoeken • 42 verzoeken binnen. Grootste gedeelte ontvangstbevestigingen verstuurd. Geen reactie op identificatie - Voorstel herinnering te sturen om binnen 2 weken te reageren. Blijft dit uit dan geen behandeling van het verzoek. Deze afspraak vastleggen en tekst laten controleren door AKD. • Verzoeken alle gegevens laten verwijderen van alle afdelingen- checkvraag of ze dit echt willen met alle gegevens. Verzoeken voor afdelingen moeten door de betreffende afdeling behandeld worden. - 1. Contact opnemen met de indiener door de klachtenfunctionaris en FG. Het betreft ca 10 personen - 2. Binnen de afdelingen checken wie deze verzoeken gaat uitvoeren. De instructie voor de afhandeling van verwijderverzoeken komt 5 maart beschikbaar vanuit GGD NL • Inzageverzoeken voor HP-zone en coronIT – uit laten voeren door in opdracht van het projectteam door IT. Het betreft ca 10 personen. • WGPO/WPG discussie – op MT 16 maart. Er komt ook een medisch advies. • Bezwarencommissie – Ingediende bezwaren komen binnen bij het directiesecretariaat en worden doorgeleid naar HR, [redacted]. Dit is bekend.	[redacted]	Eind mrt 16 maart	Doorlopend
2.	Communicatie	• Verkort formulier website is geplaatst en afgehandeld. • Good Habitz, en met name de training Privacy, wordt opgenomen in de projectgroep. Meenemen dat het geen vrijblijvendheid is om deze training te volgen. • GGD NI heeft partij ingehuurd die trainingen verzorg voor data en awareness			
3	Personeel	• VOG – bij inkoop de raamovereenkomst extra actualiseren voor mensen die inmiddels een jaar in dienst zijn waangezien de VOG een jaar geldig is. • Er zijn bij GGD NL 566 situaties bekend waarbij vraagtekens zijn over eventueel ongewenste downloads. Nog niet gehoord of dit bij GGD WB het geval is. Dit moeten wel onderzocht worden en in het project worden opgenomen.			
4	ICT	• Autorisaties, rollen en verantwoordelijkheden – Verzoek ligt bij de applicatiebeheerders om het autorisatieschema in kaart te brengen. Dit valt samen met de ongewenste downloads • Processen worden aangepast zoals uitgewerkt door GGD NL. [redacted] neemt dit op.			

		• Landelijke dashboard is inmiddels afgehandeld door GGD NL • Uitfaseren HP-zone is nu in volle gang – hier moet nog een DPIA voor komen		
5	Risicoanalyse	• Dit is het begin van de opdracht voor het projectteam Risicoanalyse in de breedte al gedaan binnen de GGD door [redacted] en gepresenteerd in het MT. Waak ervoor dat zaken niet dubbel worden uitgevoerd. Deze analyse richt zich voornamelijk op de privacy risico's.		
6	Bestuurlijk	Op dit moment geen noodzaak om te communiceren Actiepunten rondom digid zijn afgehandeld en gecommuniceerd	4/3	Gereed
7	Projectorganisatie	• [redacted] heeft 5 maart afspraak met de externe projectleider, [redacted] • De projectgroep gaat vanaf nu rapporteren aan het MT van [redacted] en [redacted] • De crisis overleggen die vanaf 2 februari tot nu toe gevoerd zijn komen nut te vervallen. • Er komt een aparte site op SharePoint.		
	AP	• De bevindingen van GGD [redacted] met betrekking tot het bezoek van de AP wordt gedeeld. Maandag 8 maart volgt het bezoek aan GGD [redacted] AP bezoekt steekproefsgewijs de GGD' en. Om ons zo goed mogelijk voor te bereiden het verzoek om contact op te nemen met AKD en wellicht Pels/Rijcken (zij adviseren bovenstaande GGD 'en) 1. Is AKD de juiste partij, hebben zij ervaring met AP? En is het mogelijk dat zij stand-by staan bij een mogelijk bezoek. 2. Wat zijn de bevoegdheden en verantwoordelijkheden van GGD NL en die van GGD WB en welke acties moeten wij hiervoor ondernemen.		

AUTORITEIT
PERSOONSGEGEVENS

Autoriteit Persoonsgegevens
Postbus 93374, 2509 AJ Den Haag
Bezuidenhoutseweg 30, 2594 AV Den Haag
T 070 8888 500 - F 070 8888 501
autoriteitpersoonsgegevens.nl

GGD GHOR Nederland
[redacted]
Zwarte Woud 2
3524 SJ Utrecht

Datum
8 november 2021

Ons kenmerk
z2021-02000

Contactpersoon
[redacted]

Onderwerp
Eindbrief onderzoek beveiliging persoonsgegevens GGD GHOR en GGD'en

Geachte [redacted],

Naar aanleiding van het op 22 januari 2021 door GGD GHOR Nederland (hierna: GGD GHOR), mede namens de regionale GGD'en aan de Autoriteit Persoonsgegevens (hierna: AP) gemelde datalek, de zorgwekkende berichtgeving in de media over de diefstal van en handel in persoonsgegevens afkomstig uit de systemen van GGD GHOR en de GGD'en alsmede de vele bezorgde signalen die de AP hierover vervolgens ontving, heeft de AP aangekondigd het toezicht op de GGD te intensiveren en in dat kader onderzoek te doen. De AP heeft onderzocht of door GGD GHOR en twee onderzochte GGD'en passende technische en organisatorische maatregelen zijn getroffen om de persoonsgegevens die worden verwerkt in het kader van het testen, vaccineren en bron- en contractonderzoek in verband met de coronapandemie passend te beveiligen. Met deze eindbrief informeert de AP u over de bevindingen van het onderzoek.

De AP is zich ervan bewust dat met het uitbreken van de pandemie de GGD'en en GGD GHOR voor een enorme opgave werden gesteld. Zij kregen de opdracht in zeer korte tijd zorg te dragen voor het op grote schaal testen van personen, het uitvoeren van bron- en contactonderzoek en het vaccineren van personen. De werkzaamheden om dit te realiseren werden onder grote tijdsdruk verricht.

Tegelijkertijd geldt dat van een uitzonderlijk grote groep burgers in dit verband bijzondere persoonsgegevens betreffende hun gezondheid werden en worden verwerkt en dat een grote groep, veelal speciaal voor dit doel aangetrokken, tijdelijke medewerkers hiertoe toegang hebben. Het treffen van technische en organisatorische maatregelen die zijn afgestemd op de hiermee gepaard gaande risico's voor de persoonsgegevens is dan ook van zeer groot belang. De bereidheid van burgers om zich te laten testen en vaccineren of medewerking te verlenen aan bron- en contactonderzoek hangt immers ook samen met

het vertrouwen in de wijze waarop in dat kader persoonsgegevens van burgers worden verwerkt en beveiligd. Mede hierom besloot de AP onderzoek te doen.

Conclusie

De AP constateert dat een aantal aangekondigde verbetermaatregelen zijn getroffen waardoor het risico op datalekken is verminderd. Wel ziet de AP nog wezenlijke risico's voor de beveiliging van persoonsgegevens die aanvullende verbetermaatregelen vereisen. Het gaat hier in het bijzonder om risico's die verband houden met het grote aantal partijen dat betrokken is bij de verwerkingen van persoonsgegevens in verband met het testen, vaccineren en bron- en contactonderzoek. In ieder geval zijn dit de 25 regionale GGD'en, de landelijke koepelorganisatie GGD GHOR, zes landelijke partnerorganisaties (callcenters en alarmcentrales)[1], diverse uitzendbureaus en IT-leveranciers. Duidelijke afspraken tussen de betrokken organisaties over bepaalde beveiligingsaspecten rondom de systemen die voor bron- en contactonderzoek worden gebruikt ontbreken. Dit geldt bijvoorbeeld ten aanzien van het autorisatiebeheer en de controle van logbestanden. Hierdoor is onvoldoende duidelijk wie waarvoor verantwoordelijk is en wie welke maatregelen in dit verband dient te treffen. Dat vergroot de kans op nieuwe tekortkomingen in de beveiliging van persoonsgegevens.

Verder werken het ministerie van Volksgezondheid, Welzijn en Sport, GGD GHOR en de GGD'en aan het vervangen van de systemen voor bron- en contactonderzoek (HPZone en HPZone Lite). In dit kader merkt de AP op dat vervanging van een systeem niet zonder meer leidt tot een betere beveiliging van de persoonsgegevens die daarin worden verwerkt. Hierbij wil de AP benadrukken dat bij de ontwikkeling en implementatie van een nieuw systeem nadrukkelijk rekening moet worden gehouden met de uit de Algemene verordening gegevensbescherming (hierna: AVG) voortvloeiende verplichtingen, zoals het vroegtijdig uitvoeren van een risicoanalyse in de vorm van een gegevensbeschermingseffectbeoordeling (artikel 35 AVG), de toepassing van gegevensbescherming door ontwerp en door standaardinstellingen (artikel 25 AVG) en het treffen van passende technische en organisatorische maatregelen ter beveiliging van persoonsgegevens (artikel 32 AVG), zoals bijvoorbeeld logging, controle op de logging en autorisatiebeheer.

Onderzoek

De AP heeft in het bijzonder onderzocht of voldoende verbetermaatregelen zijn getroffen met het oog op toegangsbeveiliging, verleende autorisaties en autorisatiebeheer, logging van de gebruikte systemen, controle op deze logging en om het ongeoorloofd exporteren/printen van persoonsgegevens uit de systemen te voorkomen. Ook heeft de AP gecontroleerd of de aangekondigde maatregelen met betrekking tot beperking van de zoekfuncties van gebruikers in de systemen ook daadwerkelijk zijn getroffen. Daarnaast is onderzocht of de betrokkenen die geraakt zijn door het datalek in overeenstemming met de

[1] Met de landelijke partners of partnerorganisaties worden bedoeld de callcenters en andere externe organisaties die worden ingezet om bron- en contactonderzoek uit te voeren en test- en vaccinatieafspraken te maken.

AVG zijn geïnformeerd over de inbreuk in verband met hun persoonsgegevens. Tenslotte heeft de AP – naar aanleiding van nieuwe zorgelijke berichtgeving in de media in februari 2021 – onderzocht of de website www.coronatest.nl aan de beveiligingseisen voldoet die gelden voor aansluiting op DigiD.

Het onderzoek was gericht op de systemen die worden gebruikt voor het verwerken van persoonsgegevens in het kader van de coronapandemie, namelijk voor het testen en vaccineren (CoronIT) en bron- en contractonderzoek (HPZone en HPZone Lite).

In het kader van het onderzoek heeft de AP controles uitgevoerd bij GGD GHOR en steekproefsgewijs bij twee regionale GGD'en en een van de landelijke partners die capaciteit leveren voor het uitvoeren van bron- en contactonderzoek. Onderstaande bevindingen zijn gebaseerd op de informatie die de AP tijdens het onderzoek heeft verzameld.

Bevindingen

1. Ter inleiding

Artikel 5, eerste lid, onderdeel f, AVG bevat het beginsel van vertrouwelijkheid en integriteit van persoonsgegevens. Door het nemen van passende technische en organisatorische maatregelen moeten persoonsgegevens op zodanige manier worden verwerkt dat een passende beveiliging ervan is gewaarborgd en dat zij onder meer zijn beschermd tegen ongeoorloofde of onrechtmatige verwerking. Artikel 32, eerste lid, AVG werkt dit beginsel uit en verplicht de verwerkingsverantwoordelijke passende technische en organisatorische maatregelen te treffen om een op het risico voor betrokkene afgestemd beveiligingsniveau te waarborgen. Hierbij houdt de verwerkingsverantwoordelijke rekening met de beschikbare technologie en de uitvoeringskosten en met de aard, omvang, context en doeleinden van de verwerking. Wanneer sprake is van verwerking van informatie in zorginformatiesystemen dient de verwerkingsverantwoordelijke bij de invulling van deze verplichting voorts rekening te houden met de Nederlandse normen voor informatiebeveiliging in de zorg (NEN7510, 7512 en 7513).[2]

2. Toegangsbeveiliging

Onderdeel van de beveiliging van persoonsgegevens en het waarborgen van een passend beschermingsniveau vormt het voorkomen van ongeoorloofde toegang en implementeren van een authenticatieproces. Dit laatste betreft het proces waarbij een gebruiker van een computer of applicatie de geclaimde identiteit moet bewijzen. Tweefactorauthenticatie is een beveiligingsmaatregel in het authenticatieproces waarbij de gebruiker zich met een combinatie van twee verschillende typen authenticatiefactoren moet authenticeren om toegang te krijgen tot bijvoorbeeld een systeem. Dit verhoogt de zekerheid dat de gebruiker is wie hij zegt dat hij is.

[2] Zie ook artikel 3 en 5 Besluit elektronische gegevensverwerking door zorgaanbieders.

De AP heeft geconstateerd dat de drie onderzochte systemen vanaf eigen apparatuur rechtstreeks kunnen worden benaderd via een URL en dus zonder dat vereist is om eerst te zijn ingelogd op een beveiligde werkomgeving. Bij het verkrijgen van toegang tot de drie onderzochte systemen wordt wel tweefactorauthenticatie toegepast.

Uit het onderzoek is voorts gebleken dat de twee onderzochte GGD'en laptops verstrekken aan een deel van hun medewerkers. Uit het onderzoek blijkt echter ook dat een grote groep medewerkers, waaronder medewerkers van de landelijke partners, op eigen apparatuur werkt. Hiervoor is geen eenduidig beleid aangetroffen. Daarnaast heeft de GGD GHOR aangegeven met de landelijke partners geen afspraken te hebben vastgelegd over het werken op eigen apparatuur.

De AP merkt op dat het gebruik van eigen apparatuur in combinatie met de mogelijkheid om op de onderzochte systemen in te loggen buiten een beveiligde werkomgeving, kan leiden tot beveiligingsrisico's. Dit houdt verband met het feit dat de eigen apparatuur niet in beheer is bij de werkgever. Hierdoor is niet bekend of de apparatuur aan bepaalde beveiligingseisen voldoet en is het niet mogelijk om bepaalde technische beveiligingsmaatregelen, zoals het uitvoeren van noodzakelijke beveiligingsupdates, op de apparatuur af te dwingen. Ook bestaat het risico dat software op de apparatuur wordt geïnstalleerd die risico's voor de bescherming van persoonsgegevens met zich meebrengt. Dit kan deze apparatuur bijvoorbeeld kwetsbaarder maken voor aanvallen van buitenaf. Een mitigerende maatregel voor de risico's van werken op eigen apparatuur kan zijn ervoor zorg te dragen dat uitsluitend toegang tot de systemen kan worden verkregen binnen een beveiligde werkomgeving. Het feit dat via een internetbrowser en dus ook buiten een beveiligde werkomgeving kan worden ingelogd op de onderzochte systemen, kan dan ook, zoals gezegd, tot beveiligingsrisico's leiden. Op deze wijze kunnen immers de in de beveiligde werkomgeving genomen beveiligingsmaatregelen worden omzeild.

Met inachtneming van deze risico's, dienen GGD GHOR en de GGD'en passende beveiligingsmaatregelen te nemen en beleid vast te stellen dat is afgestemd op de risico's voor betrokkenen. De AP draagt GGD GHOR en de GGD'en op per direct dergelijke maatregelen te onderzoeken en vervolgens te implementeren én beleid vast te stellen over het gebruik van eigen apparatuur. De AP verwacht in een voortgangsrapportage (zie onder paragraaf 9) een terugkoppeling van de verbetermaatregelen die in dit verband zijn of worden getroffen.

3. Autorisaties

Autorisatie is het proces waarin een persoon bepaalde aan hem of haar toegekende rechten krijgt binnen een systeem. Autorisaties en het juiste beheer daarvan, zoals het tijdige aanpassen of intrekken van een autorisatie, kunnen bijdragen aan een passend beveiligingsbeleid binnen een organisatie. Het doel hiervan is dat medewerkers enkel toegang hebben tot persoonsgegevens of functionaliteiten die noodzakelijk zijn voor de uitvoering van hun werk.

De AP concludeert dat het proces rond het tijdig aanpassen of intrekken van autorisaties nog niet altijd goed verloopt. Duidelijke afspraken tussen de betrokken partijen hierover zijn niet aangetroffen. Het

autorisatieproces tot HPZone en HPZone Lite is in principe decentraal bij de GGD'en belegd. Elke GGD verzorgt zelf de toegang tot deze systemen en kent rollen toe aan eigen en ingehuurde medewerkers. Voor de medewerkers die door landelijke partners (callcenters en alarmcentrales) worden ingezet ter ondersteuning van de GGD'en bij het bron- en contactonderzoek, verloopt het autorisatieproces iets anders. Zij krijgen eerst door de landelijke partner de rollen toegekend die nodig zijn voor hun werkzaamheden en krijgen daarmee toegang tot het systeem HPZone (Lite), maar nog niet tot de gegevens daarin. Vervolgens verleent de GGD waarvoor de desbetreffende medewerker gaat werken toegang tot de regionale gegevens van die GGD. Deze medewerker heeft daarna alleen toegang tot de gegevens in HPZone (Lite) van personen in de regio van de betreffende GGD. Wanneer de medewerker van de landelijke partner vervolgens bij een andere GGD wordt ingezet, dient de landelijke partner de desbetreffende GGD te verzoeken om de toegang tot de regionale gegevens weer in te trekken.

Uit controles die de twee onderzochte GGD'en hebben uitgevoerd na het datalek van januari 2021 bleek dat diverse medewerkers over autorisaties beschikten die zij voor hun werkzaamheden niet of niet langer nodig hadden. Naar aanleiding van deze controles hebben de twee onderzochte GGD'en de niet-noodzakelijke autorisaties ingetrokken. Door de onderzochte GGD'en is aangegeven dat zij niet altijd informatie van de landelijke partners ontvingen over gewijzigde werkzaamheden van medewerkers uit deze flexibele landelijke schil. De AP heeft tijdens het onderzoek geen duidelijke gedocumenteerde afspraken tussen de betrokken partijen aangetroffen, die zijn opgesteld naar aanleiding van het datalek in januari 2021, voor het toewijzen, wijzigen en intrekken van autorisaties.

Daarnaast heeft de AP geen toereikende documentatie aangetroffen die ten aanzien van HPZone en HPZone Lite inzichtelijk maakt welke specifieke rechten en functionaliteiten aan de verschillende rollen in de autorisatiematrix zijn gekoppeld.

Tegen deze achtergrond draagt de AP GGD GHOR en de GGD'en op om duidelijke afspraken te maken met de betrokken partijen met betrekking tot het autorisatieproces en de procedures eenduidig vast te leggen. Dit betreft zowel de huidige systemen zolang deze nog in gebruik zijn voor de bestrijding van de coronapandemie als de vervangende systemen wanneer deze in productie worden genomen. Voorts dienen GGD GHOR en de GGD'en de verleende autorisaties regelmatig te (blijven) beoordelen en ook hiervoor duidelijke afspraken te maken wie in dit verband welke acties dient te verrichten. De AP verwacht in een voortgangsrapportage een terugkoppeling van de verbetermaatregelen die in dit verband zijn of worden getroffen.

4. Logging en controle op de logging

Logging is het proces waarbij systeemactiviteiten, bijvoorbeeld bepaalde handelingen van een gebruiker in een systeem, worden vastgelegd in logbestanden. Het vastleggen van gebeurtenissen in logbestanden en regelmatige controle daarvan vormt een belangrijk onderdeel van informatiebeveiliging. Aan de hand van de logbestanden kan worden nagegaan wie bepaalde gegevens heeft bekeken of aangepast. Ook kunnen uit logbestanden pogingen om ongeautoriseerd toegang te krijgen worden geïdentificeerd. Op basis van de

verkregen loginformatie kan efficiënter in actie worden gekomen bij een datalek en/of worden bepaald of aanvullende technische en organisatorische maatregelen nodig zijn.

Uit het onderzoek van de AP is gebleken dat op alle drie de onderzochte systemen logbestanden werden en nog steeds worden gemaakt van gebeurtenissen die in die systemen plaatsvinden, maar dat de logbestanden voorafgaand aan het datalek van januari 2021 niet regelmatig werden gecontroleerd. De logbestanden van CoronIT werden enkel naar aanleiding van een incident of klacht gecontroleerd door de GGD GHOR. Of de logbestanden van HPZone en HPZone Lite werden gecontroleerd en zo ja, door wie, heeft de AP niet kunnen vaststellen.

In september 2020 heeft GGD GHOR, in antwoord op vragen van de AP naar aanleiding van een eerdere datalekmelding, aangegeven dat in het vierde kwartaal van 2020 geautomatiseerde controle van de logbestanden zou worden ingericht. Op basis van deze informatie besloot de AP destijds de datalekmelding af te sluiten. In januari 2021 bleek deze geautomatiseerde controle nog niet te zijn ingericht. Na het datalek van januari 2021 gaf GGD GHOR aan de geautomatiseerde controle in de vorm van SIEM-oplossing (*Security Information & Event Management*) versneld te zullen implementeren; deze zou eind maart 2021 gereed zijn. Ook deze planning is niet gehaald. De AP constateert dat de SIEM-oplossing in ieder geval ten tijde van het afronden van de onderzoeksfase in juni 2021 nog steeds niet was geïmplementeerd.

Als mitigerende en alternatieve maatregel heeft GGD GHOR, naar aanleiding van het datalek van januari 2021 en in afwachting van de SIEM-oplossing, dagelijkse handmatige controle van de logbestanden van alle drie de systemen ingericht. Deze controles worden met behulp van queries uitgevoerd door een team bij het Security Operations Center (SOC) van GGD GHOR. Dit gebeurt op basis van bepaalde criteria en procedures met het doel om afwijkende gebeurtenissen vast te stellen. In het kader van de SIEM-oplossing werkt het SOC in samenwerking met twee externe partijen aan relevante *use cases* en *business rules* op basis van de kennis opgedaan bij de handmatige controle van de logbestanden van CoronIT, HPZone en HPZone Lite, ten einde bepaalde onregelmatigheden vooraf te definiëren waarop automatisch kan worden gemonitord.

Met het oog op de aanstaande vervanging van de systemen HPZone en HPZone Lite, benadrukt de AP dat GGD GHOR en de GGD'en bij het in productie nemen van vervangende systemen van meet af aan de logging en de controle op de logging goed moeten inrichten zodat regelmatige controle van de logbestanden is verzekerd. De AP verwacht in een voortgangsrapportage een terugkoppeling van de maatregelen die in dit verband zijn of worden getroffen.

5. Export- en printfunctionaliteiten

Export- en printfunctionaliteiten maken het onder andere mogelijk om (lijsten met) persoonsgegevens gemakkelijk uit een systeem te halen. Door deze functionaliteiten alleen toe te kennen aan gebruikers die deze ook nodig hebben voor hun werkzaamheden, kan het risico op misbruik van persoonsgegevens worden verkleind.

De AP heeft vastgesteld dat naar aanleiding van het datalek van januari 2021 deze functionaliteiten in de drie onderzochte systemen zijn uitgeschakeld respectievelijk zijn teruggebracht tot een selecte groep gebruikers die deze nodig hebben voor hun werkzaamheden.

Voor CoronIT geldt dat de functionaliteit voor het uitprinten van afsprakenlijsten met persoonsgegevens kort na het datalek van januari 2021 is uitgeschakeld. Voor HPZone en HPZone Lite geldt dat de export- en printfunctie in HPZone is beperkt tot twee rollen en in HPZone Lite tot één rol. Deze rollen zijn aan een selecte groep van medewerkers toebedeeld die deze functionaliteit nodig hebben voor de uitvoering van hun werkzaamheden.

In het licht van de aanstaande vervanging van HPZone en HPZone Lite, benadrukt de AP dat reeds bij de ontwikkeling en implementatie van een nieuw systeem secuur moet worden gekeken naar welke gebruikers welke functionaliteiten nodig hebben en dat autorisaties daarmee in lijn moeten worden gebracht. De AP verwacht in een voortgangsrapportage een terugkoppeling van de verbetermaatregelen die in dit verband zijn of worden getroffen.

6. Zoekfunctionaliteiten

Door zoekfunctionaliteiten in een systeem te beperken, kan het risico dat onbevoegd persoonsgegevens van een specifieke persoon, bijvoorbeeld van een bekende Nederlander, worden opgezocht en ingezien, worden verminderd. Dit kan bijvoorbeeld door de zoekfunctionaliteit zodanig in te stellen dat het niet mogelijk is om de gegevens van een specifieke persoon op te zoeken aan de hand van algemeen bekende of gemakkelijk op te zoeken kenmerken.

De AP heeft geconstateerd dat naar aanleiding van het datalek in januari 2021 in CoronIT de zoekfunctionaliteit is aangepast. Hierdoor is het niet meer mogelijk om enkel op achternaam of een combinatie van achternaam en geslacht of achternaam en geboortedatum de gegevens van een specifieke persoon in dit systeem op te zoeken. Uit het onderzoek van de AP blijkt echter dat een vergelijkbare beperking van de zoekfunctionaliteit in HPZone en HPZone Lite niet is aangebracht, volgens GGD GHOR vanwege technische beperkingen bij de leveranciers. Wel zijn maatregelen getroffen om ervoor te zorgen dat in het resultaat van een zoekopdracht minder persoonsgegevens zichtbaar zijn.

In het kader van het besluit de systemen HPZone en HPZone Lite te vervangen, wijst de AP GGD GHOR en de GGD'en nadrukkelijk op het feit dat bij de ontwikkeling en implementatie van een of meer nieuwe systemen, ook aandacht moet worden besteed aan de risico's voor de bescherming van persoonsgegevens die gepaard kunnen gaan met een ruime zoekfunctionaliteit. De AP verwacht in een voortgangsrapportage een terugkoppeling van de maatregelen die in dit verband zijn of worden getroffen.

7. Beveiligingseisen voor aansluiting DigiD

De AP concludeert dat GGD GHOR ten aanzien van de website www.coronatest.nl op dit moment voldoet aan de normen die voortvloeien uit de "Norm ICT-beveiligingsassessments DigiD".

Ter toelichting geldt het volgende. Ten tijde van het lopende onderzoek verscheen in de media zorgelijke berichtgeving over de aansluiting van www.coronatest.nl op DigiD. Omdat niet aan alle beveiligingseisen zou zijn voldaan, bestond het risico dat www.coronatest.nl de aansluiting op DigiD zou verliezen. Gelet op het feit dat hierdoor mogelijk sprake was van een risico voor de bescherming van persoonsgegevens die via deze website werden verwerkt, besloot de AP de reikwijdte van het onderzoek uit te breiden en te monitoren of noodzakelijke verbetermaatregelen door GGD GHOR werden getroffen. Op basis van de beschikbare informatie heeft de AP kunnen concluderen dat GGD GHOR ten aanzien van www.coronatest.nl op dit moment voldoet aan de normen die voortvloeien uit de "Norm ICT-beveiligingsassessments DigiD".

8. Informeren van betrokkenen

Indien zich een datalek heeft voorgedaan dat waarschijnlijk een hoog risico voor de rechten en vrijheden van betrokkenen inhoudt, dient aan de betrokkenen hiervan onverwijld mededeling te worden gedaan, tenzij sprake is van een in artikel 34 AVG genoemde uitzondering. De mededeling moet in ieder geval de in artikel 34 AVG genoemde informatie te bevatten. Het belangrijkste doel daarvan is dat betrokkenen begrijpen wat er met hun persoonsgegevens is gebeurd en wat zij kunnen doen om zichzelf te beschermen.

Naar aanleiding van de datalekmelding bij de AP op 22 januari 2021, is er tussen 25 januari en 29 januari 2021 meermaals contact geweest tussen de AP en GGD GHOR over de kennisgeving richting betrokkenen op grond van artikel 34 AVG. De AP heeft geconstateerd dat GGD GHOR op 29 januari 2021 op haar website informatie aan betrokkenen heeft verstrekt over het datalek. Op 16 maart 2021 is voorts een aantal geïdentificeerde betrokkenen per brief geïnformeerd over het datalek. De informatie die aan betrokkenen is verstrekt omvatte de waarschijnlijke gevolgen van het datalek en maatregelen die zijn voorgesteld of genomen om het datalek aan te pakken en nadelige gevolgen te beperken. Betrokkenen zijn alert gemaakt op de mogelijke gevolgen van het datalek, waardoor zij zich hiertegen, voor zover dat mogelijk is, kunnen wapenen door bijvoorbeeld extra voorzorgsmaatregelen te treffen. Ook is informatie over een contactpunt verstrekt, waar betrokkenen meer informatie kunnen verkrijgen. De AP begrijpt dat het politieonderzoek dat naar aanleiding van het datalek is gestart nog loopt. Indien uit dit onderzoek nieuwe betrokkenen worden geïdentificeerd die geraakt zijn door het datalek, wijst de AP GGD GHOR en de GGD'en op de verplichting deze personen te informeren op vergelijkbare wijze waarop GGD GHOR, al dan niet in opdracht van de GGD'en, de eerder geïdentificeerde betrokkenen heeft geïnformeerd.

9. Ten slotte

Uit het onderzoek van de AP is gebleken dat een groot aantal partijen betrokken is bij de verwerking van persoonsgegevens in de drie onderzochte systemen. In de eerste plaats betreft dit de 25 regionale GGD'en.

Er bestaat in Nederland niet één GGD-organisatie. Er is een landelijk dekkend netwerk van 25 gemeentelijke gezondheidsdiensten (GGD'en). Dit zijn 25 afzonderlijke publiekrechtelijke rechtspersonen. Iedere GGD wordt aangestuurd door een eigen Directeur Publieke Gezondheid in de desbetreffende regio. Daarnaast bestaat GGD GHOR Nederland (GGD GHOR). GGD GHOR is de overkoepelende brancheorganisatie van de 25 regionale GGD'en en behartigt de belangen van de publieke gezondheid en veiligheid in Nederland. Ten behoeve van de werkzaamheden die de 25 GGD'en in het kader van de coronapandemie moesten verrichten (testen, vaccineren en bron- en contactonderzoek), heeft GGD GHOR een aantal zaken centraal op zich genomen. Dit betreft onder andere het laten ontwikkelen van applicaties die door alle 25 GGD'en worden gebruikt, zoals CoronIT en HP Zone Lite en het sluiten van overeenkomsten met landelijke partnerorganisaties die werkzaamheden voor de GGD'en verrichten zoals het maken van test- en vaccinatieafspraken en het uitvoeren van bron- en contactonderzoek.

Naast de 25 GGD'en en GGD GHOR zijn in ieder geval zes landelijke partnerorganisaties (callcenters en alarmcentrales) en de IT-leveranciers van de systemen betrokken bij de verwerking van persoonsgegevens in het kader van het testen, vaccineren en bron- en contactonderzoek. De landelijke partners en de GGD'en huren op hun beurt weer tijdelijk personeel in bij diverse uitzendbureaus.

De AP draagt GGD GHOR en de GGD'en op om onderling en met de overige betrokken partijen per direct duidelijke afspraken op het vlak van informatiebeveiliging te maken, vast te leggen en actueel te houden. Voor partijen dient duidelijk te zijn wie voor welke technische en/of organisatorische maatregelen verantwoordelijk is. Dat is nu onvoldoende geregeld. Uit de gesprekken is namelijk het beeld naar voren gekomen dat met name ten aanzien van HPZone Lite onduidelijkheid bestaat over de verantwoordelijkheidsverdeling. Voor zover sprake is van gezamenlijke verwerkingsverantwoordelijkheid, wijst de AP op artikel 26, eerste lid, AVG dat vereist dat partijen in een onderlinge regeling op transparante wijze hun respectievelijke verantwoordelijkheden voor naleving van de AVG vastleggen.

De AP verwacht in een voortgangsrapportage hierop een reactie en een overzicht van de verbetermaatregelen die in dit verband zijn of worden getroffen.

Ter afsluiting

De AP heeft onderzoek gedaan bij GGD GHOR en twee (regionale) GGD'en naar de beveiliging van persoonsgegevens die in het kader van de coronapandemie. worden verwerkt in CoronIT, HPZone en HPZone Lite. Deze systemen worden door alle 25 GGD'en gebruikt en de beveiliging van de daarin verwerkte persoonsgegevens is dus mede afhankelijk van maatregelen die alle 25 GGD'en afzonderlijk dan wel gezamenlijk treffen om de persoonsgegevens passend te beveiligen. De bevindingen van de AP zijn dan ook relevant voor alle 25 GGD'en. De AP verwacht daarom dat alle GGD'en de in deze brief genoemde noodzakelijke verbetermaatregelen - voor zover zij dat nog niet hebben gedaan - zullen treffen om een passend niveau van beveiliging van persoonsgegevens te waarborgen. Mede met het oog hierop zal deze brief ook aan de overige 23 GGD'en worden gezonden.

Datum
8 november 2021

Ons kenmerk
z2021-02000

Informatiebeveiliging is een continu proces waarin risico's en maatregelen periodiek moeten worden (her)beoordeeld zodat de technische en organisatorische beveiligingsmaatregelen steeds zijn afgestemd op de actuele risico's voor betrokkenen. Om deze reden benadrukt de AP met klem het belang om audits gericht op informatiebeveiliging te blijven uitvoeren en risico's en maatregelen periodiek te (her)beoordelen zodat, waar nodig, (aanvullende) technische en organisatorische maatregelen ter beveiliging van de (bijzondere) persoonsgegevens die worden verwerkt tijdig kunnen worden genomen.

De AP heeft inmiddels de bevindingen van het onderzoek in een gesprek aan GGD GHOR toegelicht en zal erop toezien dat noodzakelijke verbeteringen tijdig worden doorgevoerd. De AP verzoekt GGD GHOR dan ook om uiterlijk op 1 maart 2022 in een voortgangsrapportage op elk van de in deze brief aangegeven punten aan te geven welke verbetermaatregelen daadwerkelijk zijn of worden getroffen om de geïdentificeerde risico's ten aanzien van de beveiliging van persoonsgegevens die worden verwerkt in het kader van de coronapandemie te verminderen. Dit betreft zowel de huidige systemen zolang deze nog worden gebruikt voor de bestrijding van de coronapandemie als de vervangende systemen wanneer deze in productie worden genomen. Mocht de in de voortgangsrapportage genoemde implementatie van verbetermaatregelen onverhoopt vertraging oplopen, dan verwacht de AP daarover door GGD GHOR onverwijld te worden geïnformeerd.

Ik vertrouw erop u hiermee voldoende te hebben geïnformeerd. Voor eventuele vragen kunt u contact opnemen met bovengenoemd contactpersoon.

Een afschrift van deze brief zend ik aan de functionaris voor de gegevensbescherming van uw organisatie.

Hoogachtend,
Autoriteit Persoonsgegevens,

[redacted]

Ministerie van VWS
Directie Publieke Gezondheid
[redacted]
Postbus 20350
2500 EJ DEN HAAG

Datum: 4 november 2020
Kenmerk: 20-088.AR
Betreft: **Doorgeven gegevens meldingsplicht A-ziekte**

Geachte [redacted]

Via deze brief verzoek ik u om een aantal acties, teneinde per direct en in de toekomst de doorlooptijd tussen een positieve besmetting met een meldingsplichtige infectieziekte in de categorie A en het daaropvolgende bron- en contactonderzoek (hierna: BCO) te minimaliseren, de werkdruk voor betrokken GGD'en te verkleinen en hiermee de slagkracht in de strijd tegen pandemieën (zoals de huidige SARS-CoV-2-pandemie) in algemene zin te vergroten. In deze brief schets ik in het kort een beeld van de huidige praktijksituatie waarmee alle GGD'en worden geconfronteerd. Vervolgens ga ik in op de achtergrond van deze situatie, met in het bijzonder aandacht voor het juridische kader. Tenslotte vraag ik u om een drietal acties in te zetten.

Actualiteit t.a.v. meldingen van positieve casussen
Momenteel leveren de GGD'en een maximale krachtsinspanning om zicht en grip op het virus te houden, onze kwetsbaren te beschermen en de zorgcontinuïteit te garanderen. Doorlopend wordt de capaciteit van testafnames en BCO opgeschaald en doen collega's alles wat binnen hun mogelijkheden ligt om landelijk en regionaal het virus in te dammen. Hoewel het aantal besmettingen in Nederland lijkt te dalen, is het bij alle GGD'en nog steeds alle hens aan dek. Ook het BCO staat onder druk; door het hoge aantal besmettingen zijn GGD'en genoodzaakt om het BCO in afgeschaalde versie uit te voeren. Momenteel is dus alle beschikbare (landelijke én regionale) BCO-capaciteit nodig om de ontwikkeling van het virus zo goed mogelijk in beeld te houden. Een effectief BCO is gebaat bij een aantal zaken, waarbij een snelle start cruciaal is om effectief te zijn. Ik ontvang vanuit (vrijwel) alle GGD'en signalen dat zij hierbij sterk gehinderd worden door het feit dat zij niet altijd de beschikking hebben over de juiste gegevens om een BCO op te starten; in het bijzonder gaat het hierbij om het ontbreken van een telefoonnummer. Deze situatie doet zich steeds vaker voor, vooral in gevallen waarbij positieve testuitslagen door (ziekenhuis)labs gemeld worden via een (al dan niet beveiligde) email aan de GGD'en. Indien een afspraak is gemaakt via coronatest.nl of via het landelijke callcenter, beschikt de GGD automatisch over de juiste gegevens – deze zijn immers uitgevraagd via de website of door de callcentermedewerker. Echter, we vernemen dat in (sterk) toenemende mate GGD'en via mail

geconfronteerd worden met positieve testuitslagen, zonder dat deze vergezeld worden door de verplichte en benodigde (contact)gegevens om een BCO op te starten.[1]
Op verzoek van het ministerie hebben wij een aantal GGD'en verzocht om meer in detail de praktijk en gevolgen van bovenstaande te schetsen. Een uitvraag bij 5 GGD'en leert dat de situatie zich wijdverbreid voordoet. Al deze GGD'en geven aan deze problematiek te herkennen, dat hiermee (spaarzame) menskracht verloren gaat aan de uitvraag van corresponderende (contact)gegevens en dat de start van het BCO (en quarantaine van eventuele nauwe contacten) hiermee vertraging oploopt. GGD'en omschrijven het onderzoek naar (contact)gegevens als een speurtocht, waarbij zij van het kastje naar de muur worden gestuurd, omdat laboratoria deze gegevens ook niet van de aanvragend arts hebben ontvangen. Vanaf het moment dat GGD'en de positieven ontvangen moeten zij contactpersonen, labmedewerkers, ondersteunend personeel of soms zelfs aanvragend artsen – allemaal eveneens drukbezet met hun primair proces – benaderen om gegevens te achterhalen. Op de vraag welk percentage van het aantal positieven zonder voldoende gegevens wordt aangeleverd konden 2 GGD'en een inschatting maken. Zij gaven daarbij aan dat ze vermoeden dat het om 10-20% (!) van de ontvangen positieve casuïstiek gaat.
De vertraging die door ontbrekende gegevens ontstaat loopt per regio en casus sterk uiteen. Een aantal GGD'en geeft aan dat het enkele dagen kost om deze gegevens te achterhalen. Soms kost het achterhalen van een enkel telefoonnummer een BCO-medewerker wel 3 uur. Eén grotere GGD geeft aan dat zij momenteel een lijst heeft van 600 indexen waarbij het BCO (nog) niet is opgestart. De gemiddelde tijd tussen ontvangst van positieve uitslagen en de start van het BCO is voor die groep mensen door het ontbreken van gegevens en de hierboven beschreven benodigde actie zelfs meer dan een week (met uitschieters daarboven).
GGD'en proberen op verschillende wijze deze vertraging het hoofd te bieden. Eén GGD heeft een senior medewerker opdracht gegeven doorlopend contact met laboratoria en ketenpartners te onderhouden, teneinde de samenwerking en doorgifte van gegevens te verbeteren. Alle GGD'en zijn (broodnodige) menskracht kwijt om deze gegevens te achterhalen – in de grotere regio's wordt zelfs gesproken over meerdere FTE's. Er zijn bij elke bevraagde GGD meerdere laboratoria die onvolledig zijn in de verstrekking van gegevens. In deze eerste uitvraag geven deze 5 GGD'en aan dat problemen spelen voor 1 tot 9 laboratoria per GGD, in totaal tenminste. Het gaat hierbij onder andere om ziekenhuislaboratoria, maar ook om medisch-microbiologische laboratoria waarbij de testaanvraag niet via CoronIT is gedaan.

Als tussenconclusie lijkt het mij veilig om te stellen dat deze situatie zeer onwenselijk is en contrair aan datgene wij gezamenlijk trachten te bereiken. Hieronder ga ik in op de bredere achtergrond van de discussie over de meldingsplicht, die uiteraard niet alleen voor de huidige pandemie geldt en al langer speelt.

Achtergrond

[1] Ter illustratie: 2 maanden geleden ontving GGD Rotterdam circa 10% van de positieve uitslagen via ZorgMail. Inmiddels is dit opgelopen tot circa 35%. Deze mails vragen handmatige verwerking, deze verwerking is dus foutgevoeliger én de mails zijn (veel) vaker onvolledig qua (contact)gegevens.

Er is al enige tijd een discussie over de gegevens die artsen-microbioloog en behandelaren moeten doorgeven aan de GGD in het kader van de meldingsplicht bij vaststelling (of vermoeden) van een meldingsplichtige infectieziekte in de categorie A, zoals het nieuwe coronavirus. Er worden op dit moment door het laboratorium alleen de persoonsgegevens zoals expliciet genoemd in de Wet publieke gezondheid (Wpg) gemeld, maar geen contactgegevens of diagnostische uitslag. Na melding moet vanuit de GGD ondanks de meldplicht voor hoofden van laboratoria en behandelend artsen nu eerst contact opgenomen worden met de behandelaar voor het verkrijgen van contactgegevens van de patiënt. Bij het bron- en contactonderzoek in het kader van een coronabesmetting levert dit in sommige gevallen een week vertraging op, hetgeen zeer onwenselijk is. Daarnaast worden op dit moment ook de specifieke meetresultaten niet gedeeld. Deze gegevens heeft de GGD nodig om een risico-inschatting te kunnen maken of en hoe besmettelijk een persoon is. Zeker als de GGD geen gegevens krijgt van een behandelend arts – die niet is aangesloten op CoronIT – is het van belang dat de GGD gegevens van het laboratorium krijgt.
Het gaat hierbij om meldingen die plaatsvinden binnen zorginstellingen, bij cliënten/patiënten en/of medewerkers of bezoekers. Dit betreft dus met name positieve uitslagen die gemeld worden buiten CoronIT om. In het geval een ziekenhuis zelf aangeeft contactonderzoek te doen en te testen, dan dient dit ook gemeld te worden bij de GGD. Bij het beschikbaar komen van sneltesten die weer andere diagnostische procedures kennen, wordt dit probleem nog pregnanter.
Deze discussie liep reeds vóór de coronacrisis in het kader van alle meldingsplichtige infectieziekten, maar is nu bijzonder urgent in het kader van het tijdig en effectief kunnen uitvoeren van bron- en contactonderzoek (BCO) en het snel indammen van het virus. Op dit moment worden bij meldingen door laboratoria geen contactgegevens aangeleverd, met als argument dat hier vanuit de Algemene Verordening Gegevensbescherming (AVG) geen juridische basis voor zou bestaan. Verschillende juristen hebben in verband met deze kwestie gekeken naar de Wpg en de AVG. De juridische teksten en aangeleverde argumenten zijn op dit punt echter multi-interpretabel.

Juridisch kader

De GGD heeft op grond van de Wpg de wettelijke taak om bron- en contactopsporing uit te voeren bij een aantal specifieke in de wet genoemde meldingen (artikel 6 lid 1 sub c Wpg).
In de huidige praktijk blijkt zoals gezegd dat bij een groot aantal (mogelijke) besmettingen in een grootschalige epidemie het tijdig en effectief uitvoeren van BCO zeer moeilijk is. Hiervoor is op zijn minst noodzakelijk dat de GGD over de relevante en noodzakelijke gegevens beschikt.

Volgens de wet moet een arts die bij een door hem onderzocht persoon *een A-infectieziekte* vermoedt of vaststelt (artikel 22 lid 1 Wpg) dit onverwijld melden aan de GGD, en bij die melding de volgende gegevens (artikel 24 lid 1 Wpg) doorgeven:

- de naam, het adres, het geslacht, de geboortedatum, het burgerservicenummer en de verblijfplaats van de betrokken persoon,

- de infectieziekte dan wel een beschrijving van het ziektebeeld, de eerste ziektedag, de vaccinatietoestand, het gebruik van chemoprofylaxe, de vermoedelijke infectiebron, de datum van vermoeden of vaststelling van infectie, de wijze van vaststelling van die infectieziekte, en
- indien nodig, of de betrokken persoon dan wel een persoon in zijn directe omgeving beroeps- of bedrijfsmatig betrokken is bij de behandeling van eet- of drinkwaren of bij de behandeling, verpleging of verzorging van andere personen.

Voor het doorgeven van 'andere medische gegevens' is in beginsel toestemming nodig van de betrokken persoon, ofwel een daartoe strekkend verzoek van de burgemeester of voorzitter van de veiligheidsregio (artikel 24 lid 4 Wpg).

Daarnaast moet volgens de wet (artikel 25 lid 2 Wpg jo. artikel 3 lid 1 sub a Regeling publieke gezondheid) het hoofd van een laboratorium – waar de arts een onderzoek heeft aangevraagd – de vaststelling van een *verwekker* van een A-infectieziekte onverwijld melden bij de GGD, en daarbij de volgende gegevens doorgeven:

- de naam van de arts, de naam, de geboortedatum en het burgerservicenummer van de betrokken persoon.

Contactgegevens

Bij BCO is van het grootste belang dat de GGD zo snel mogelijk contact kan opnemen met betrokkene(n). Dat vereist de directe contactgegevens van betrokkene(n), namelijk e-mailadres en telefoonnummer. Volgens de limitatieve opsomming in artikel 24, eerste lid, aanhef en onder a, van de Wpg bevat een melding geen directe contactgegevens, maar enkel het adres en het burgerservicenummer. Dat geldt evenzeer voor de melding van artikel 25, eerste lid, van de Wpg, al ontbreekt in die melding ook het adres. Dat maakt het in de praktijk, in het bijzonder vanwege het grote aantal (mogelijke) besmettingen, onmogelijk om direct en op korte termijn contact te zoeken.

Dit lijkt een lacune in de wetgeving. Bij de overgang van de oude Infectieziektenwet naar de huidige Wpg is aan de opsomming van de bij een melding te verstrekken gegevens het burgerservicenummer toegevoegd. Redenen daarvoor zijn bron- en contactonderzoek mogelijk maken en het bieden van een extra waarborg om de identiteit van betrokkene(n) te verifiëren. In de toelichting bij artikel 24 van de Wpg wordt verder genoemd dat, indien bepaalde gegevens niet bekend zijn bij de arts (bijvoorbeeld woon- of verblijfplaats, of burgerservicenummer), dit de melding niet hoeft te vertragen en de arts de gegevens dient te verschaffen die deze redelijkerwijs heeft kunnen achterhalen. Voorts wordt in de toelichting bij artikel 25 van de Wpg in dat verband gewezen op de centrale rol die het laboratorium (meer nog dan voorheen) speelt in de infectieziektebestrijding.

Gelet op het bovenstaande lijkt het in lijn met de bedoeling van de wetgever dat ook contactgegevens van betrokkene(n) mogen worden verstrekt aan de GGD en dat dit niet alleen beperkt hoeft te blijven tot het verstrekken van het burgerservicenummer maar dat ook telefoonnummer en e-mailadres kunnen

worden doorgegeven. Het vereiste toestemming vragen aan de patiënt (artikel 24 lid 4 Wpg) betreft dan enkel ‘andere medische gegevens’.

Diagnostische uitslag

In het kader van BCO is, naast de melding van de (vermoedelijke) vaststelling van (de verwekker van) de infectieziekte, ook van groot belang om de uitslag van het meetresultaat te kennen. Op basis hiervan is namelijk in te schatten in hoeverre een persoon besmettelijk is.

Op grond van artikel 24, eerste lid, aanhef en onder b, van de Wpg moet een melding – onder meer – bevatten ‘de wijze van vaststelling van de infectieziekte’. Daaronder moet in ieder geval worden verstaan de gebruikte testmethode. Of daaronder ook kan worden verstaan het concrete meetresultaat is minder evident, maar ligt wel in de rede. Het antwoord op de vraag of iemand (vermoedelijk) besmet is, is immers direct afhankelijk van het meetresultaat als uitkomst van het uitgevoerde onderzoek. Dit geldt evenzeer voor de melding ingevolge artikel 25, tweede lid, van de Wpg, die gaat over de vaststelling van de verwekker van de infectieziekte. Temeer omdat het hoofd van het laboratorium op grond van het vijfde lid van voornoemd artikel op verzoek van de GGD nader onderzoek moet verrichten naar de ziekteverwekker en de GGD van het resultaat op de hoogte moet stellen.

Wie heeft meldingsplicht?

Momenteel geldt de wettelijke meldingsplicht voor artsen, hoofden van laboratoria en hoofden van instellingen. Ook als het laboratorium heeft gemeld, heeft de aanvragend/ontvangend arts meldingsplicht en vice versa. De ‘dubbele’ melding van zowel behandelaar als laboratorium voorkomt dat belangrijke signalen te laat worden opgemerkt. Dit impliceert dat iedereen die geen arts, hoofd van een laboratorium of hoofd van een instelling géén wettelijke meldingsplicht aan de GGD heeft. Met het oog op de snelle ontwikkeling van nieuwe vormen van testen (waarbij geen laboratorium nodig is) en ook het commercieel beschikbaar zijn van diagnostische testen voor niet-artsen, kunnen hierdoor meldingen van positieve testen gemist worden. Iedereen kan testen immers aanbieden zonder tussenkomst van een arts of laboratorium en hoeft een positieve uitslag niet te melden. Hierdoor bestaat het risico dat besmettingen gemist worden en we zicht op het virus verliezen.

Via deze brief wil ik u vragen om op korte termijn de volgende onderstaande acties op te pakken:

1. Uitsluitsel en uitleg geven over de toepassing van wet- en regelgeving in het kader van het delen van gegevens

Er is behoefte aan uitsluitsel van het ministerie van VWS over de uitleg van de toepasselijke wet- en regelgeving. Concreet wie meldingplicht heeft en vervolgens welke gegevens aangeleverd moeten worden bij vaststelling of vermoeden van een SARS-CoV-2 infectie (of een andere meldingsplichtige infectieziekte), zonder dat daarbij vooraf toestemming is gevraagd aan de betrokkene(n).
Gelet op het tijdig en effectief kunnen uitvoeren van BCO, is voor de GGD noodzakelijk dat de volgende gegevens worden aangeleverd:

- Naam arts/naam behandelaar;
- De naam, het adres, het geslacht, de geboortedatum, het burgerservicenummer en de verblijfplaats van de betrokken persoon;
- (Indien bekend): functie van betrokkene: patiënt/bewoner/bezoeker/werknemer van afdeling;
- Contactgegevens: e-mailadres en telefoonnummer;
- Methode van vaststelling.

De wettelijke bepaling over de meldingsplicht van het laboratorium biedt de mogelijkheid aan de minister van VWS om nadere regels te stellen omtrent de wijze waarop de melding plaatsvindt (artikel 25 lid 6 Wpg). De minister zou in een algemene maatregel van bestuur kunnen bepalen welke aanvullende gegevens door het laboratorium moeten worden verstrekt. Een vergelijkbare vraag betreft de gegevens die een arts-behandelaar dient aan te leveren. De opsomming in artikel 24 lid 1 dient uitgebreid te worden met e-mailadres en telefoonnummer.

Doel van bovenstaand verzoek is om uitvoerende (lab)professionals in de keten gerust te stellen dat het delen van contactgegevens in lijn is met gewenste handelingsperspectief vanuit het ministerie, afgeleid vanuit de huidige beleidsdoelstellingen.

2. Betrokken medisch (lab)personeel en zorginstellingen attenderen op het verzoek (van GGD'en/VWS) om mee te werken aan het delen van contactgegevens te delen ten behoeve van een spoedige uitvoer van bron- en contactopsporing.

Contactonderzoeken van positieve patiënten en medewerkers en bezoekers verlopen vaak via de afdelingen infectiepreventie, die onder supervisie staan van de arts-microbiologen in het ziekenhuis. De GGD ontvangt idealiter via een beveiligde mail per index (bewezen positieve) de contactlijsten van de indexen. De GGD-adviezen richten zich met name op de thuissituatie van deze contacten. Op deze contactlijsten staan:

- Naam;
- Geboortedatum;
- Opnamestatus contact of functie;
- Contactgegevens: Telefoonnummer (indien mogelijk e-mailadres);
- Datum eerste/ laatste contact van "nauwe" contacten en "overige" contacten conform de LCI-richtlijn;
- Gegevens index.

Contactgegevens zijn voor het zo snel mogelijk opstarten van BCO het meest essentieel. Op dit moment vertraagt het niet aanleveren van contactgegevens door de ziekenhuizen en andere zorginstellingen onnodig het BCO. Vanwege de grote hoeveelheid meldingen is de urgentie van het snel aanleveren van bovengenoemde gegevens zeer hoog, om het contactonderzoek zinvol te kunnen uitvoeren binnen de daarvoor vastgestelde termijnen. Deze gegevens kunnen beveiligd gedeeld worden via ZorgMail.
Doel van dit verzoek is om uitvoerend medisch (lab)personeel in de keten daadwerkelijk te laten handelen in lijn met de gewenste doelen vanuit het testbeleid (zo snel mogelijk BCO opstarten).

3. Bovengenoemde uitwisseling van persoonsgegevens in kader van bron- en contactopsporing faciliteren door deze vast te leggen in wet- en regelgeving

Voor de infectieziektebestrijding in Nederland is het van groot belang dat ook voor andere infectieziekten in de WPG het delen van een bredere set (persoons)gegevens tussen laboratorium en GGD wettelijk wordt gefaciliteerd.

Doel van deze wetswijziging is om huidige en toekomstige bestrijding van infectieziekten te versoepelen.

Ten slotte

We zouden het zeer waarderen als het ministerie van VWS op zeer korte termijn aan ons verzoek tegemoet kan komen.

Mocht deze brief nog vragen oproepen, dan beantwoorden wij die uiteraard graag.

Met vriendelijke groet,

Archived: woensdag 1 juni 2022 15:13:52
From: [redacted]
Sent: Thu, 18 Mar 2021 16:43:39 +0000Authentication
To [redacted]
Subject: FW: Gegevens datalek GGD West-Brabant
Sensitivity: Normal

Ha Bianca,

Zie hier; morgen even over hebben hoe we dit bestuurlijk delen zowel GGD als VR.

Groet, [redacted]

Van: Directiesecretariaat GGD GHOR Nederland <Directiesecretariaat@ggdghor.nl>
Verzonden: donderdag 18 maart 2021 17:04
Aan: [redacted]
CC: [redacted]
Onderwerp: Gegevens datalek GGD West-Brabant

Beste DPG,

\f0Bij deze geef ik graag een update over het informeren van de gedupeerden van de datadiefstal.

\f0Gistermiddag hebben wij het bestand ontvangen van de politie met daarin gegevens van de circa 1.000 gedupeerden. In jouw GGD-regio zelf gaat het om 30 gedupeerden.

\f0Wij zullen het aantal gedupeerden in de eigen regio vandaag ook delen met de communicatieadviseurs van de regio's, zoals gisteren in een overleg met alle communicatieadviseurs van de GGD'en met hen besproken is.

\f0De brieven worden vanmiddag gepost en zullen morgen (vrijdag) bij de gedupeerden worden bezorgd.

\f0Uiterlijk maandag ontvang je afschriften van de brieven die aan de gedupeerden in jouw regio zijn verstuurd. Over hoe dat precies gaat gebeuren volgt nadere informatie.

\f0Mocht je nog vragen hebben, dan kun je contact zoeken met [redacted] of met ondergetekende.

Met vriendelijke groet,

[redacted]

[redacted]
Verenigingssecretaris

GGD GHOR Nederland
Zwarte Woud 2
3524 SJ\u8239? Utrecht

E-mai[redacted]
Telefoo[redacted]
[redacted]nl
Twitter@GGDGHORNL

\f0

From:
To:
Subject: FW: mail aan AB mbt gedupeerden datadiefstal WB en vaccineren met Astra Zenica
Sensitivity: Normal
Archived: woensdag 1 juni 2022 15:20:12

Graag je aanvullingen.

Gr[redacted]

Van: [redacted]
Verzonden: maandag 22 maart 2021 12:57
Aan: [redacted]
Onderwerp: RE: mail aan AB mbt gedupeerden datadiefstal WB en vaccineren met Astra Zenica

Aangevuld 😊

Van: [redacted]
Verzonden: maandag 22 maart 2021 12:13
Aan: [redacted]
Onderwerp: mail aan AB mbt gedupeerden datadiefstal WB en vaccineren met Astra Zenica

Ha [redacted]

Wil jij onderstaande mail aanvullen? Dank!

Geachte leden van ons algemeen bestuur,

Bij deze wil ik u informeren over de laatste ontwikkelingen na de datadiefstal uit ICT systemen die de GGD'en en GGD GHOR Nederland gebruiken voor de Coronabestrijding, CoronIT en HPZone Lite, in het bijzonder over het informeren van de gedupeerden van deze datadiefstal.

Zoals ik u eerder meldde blijkt tot nu toe dat van ongeveer 1000 Nederlanders data gestolen zijn.
Momenteel is slechts in één geval aangetoond dat de datadiefstal daadwerkelijk tot identiteitsfraude heeft geleid.
Het onderzoek loopt nog, waardoor mogelijk meer gedupeerden in beeld kunnen komen of handel in data wordt gesignaleerd.

In onze regio West-Brabant betreft het 30 gedupeerden. Zij hebben op vrijdag 19 maart een brief ontvangen vanuit GGD GHOR NL, waarin zij op de hoogte worden gesteld van het feit dat hun gegevens zijn gestolen.
De brief bevat, naast excuses, informatie, een verwijzing naar de website van GGD GHOR Nederland waar vragen en antwoorden te vinden zijn en een telefoonnummer waar mensen naar toe kunnen bellen met vragen of zorgen.

Het is mogelijk dat gedupeerden naar aanleiding van de brief de GGD aansprakelijk stellen voor (potentieel) geleden schade. Op dit moment wordt er gewerkt aan een richtlijn voor een handelwijze in deze waarbij gestreefd wordt naar een zoveel als mogelijk landelijk uniforme aanpak.

Daarnaast wil ik u graag informeren over het feit dat we per 24 maart in onze regio weer gaan vaccineren met AstraZeneca. Het Europees Medicijnagentschap (EMA) heeft afgelopen donderdag bevestigd dat het vaccin van AstraZeneca veilig en effectief is, en dat de voordelen in de vorm van bescherming tegen het coronavirus vele malen groter zijn dan de risico's. De zorgmedewerkers waarvan de afspraak is afgezegd ontvangen een SMS waarin ze worden uitgenodigd voor het maken van een nieuwe afspraak.

Met vriendelijke groet,

[redacted]
Directeur Publieke Gezondheid

AUTORITEIT
PERSOONSGEGEVENS

Autoriteit Persoonsgegevens
Postbus 93374, 2509 AJ Den Haag
Bezuidenhoutseweg 30, 2594 AV Den Haag
T 070 8888 500 - F 070 8888 501
autoriteitpersoonsgegevens.nl

GGD West-Brabant
[redacted]
Postbus 3024
5003 DA Tilburg

Datum
8 november 2021

Ons kenmerk
z2021-16812

Contactpersoon
[redacted]
070 8888 500

Onderwerp
Eindbrief AP inzake onderzoek beveiliging persoonsgegevens GGD GHOR en GGD'en

Geachte [redacted],

Zoals u vermoedelijk weet heeft de Autoriteit Persoonsgegevens (hierna: AP) onderzoek gedaan naar de beveiliging van persoonsgegevens die worden verwerkt in het kader van de bestrijding van de coronapandemie in de systemen CoronIT, HPZone en HPZone Lite. Aanleiding voor het onderzoek was de datalekmelding van januari 2021 en berichtgeving over de diefstal van en handel in persoonsgegeven afkomstig uit de systemen van GGD GHOR Nederland en de GGD'en. In het kader van dat onderzoek heeft de AP onderzoek verricht bij GGD GHOR Nederland en twee regionale GGD'en.

De bevindingen van de AP die uit dit onderzoek voortvloeien zijn in een eindbrief beschreven die aan de drie onderzochte organisaties is toegezonden. Deze brief wordt op 9 november 2021 met een nieuwsbericht op de website van de AP gepubliceerd.

Aangezien de bevindingen van de AP relevant zijn voor alle 25 GGD'en stuur ik u hierbij een afschrift van de eindbrief. Zoals ook in de eindbrief is gesteld, worden de drie systemen waarop het onderzoek van de AP zich richtte door alle 25 GGD'en gebruikt. Dit betekent dat de beveiliging van de daarin verwerkte persoonsgegevens dus mede afhankelijk is van maatregelen die alle 25 GGD'en afzonderlijk dan wel gezamenlijk treffen om de persoonsgegevens passend te beveiligen. De AP verwacht dan ook dat alle GGD'en de in de eindbrief genoemde noodzakelijke verbetermaatregelen - voor zover zij dat nog niet hebben gedaan - zullen treffen om een passend niveau van beveiliging van persoonsgegevens te waarborgen. Aan GGD GHOR Nederland is verzocht de AP uiterlijk op 1 maart 2022 hierover in een voortgangsrapportage te informeren.

Bijlage(n)

Datum
3 november 2021

Ons kenmerk
z2021-16812

Ik vertrouw erop u hiermee voldoende te hebben geïnformeerd. Voor eventuele vragen kunt u contact opnemen met bovengenoemd contactpersoon.

Een afschrift van deze brief zend ik aan de functionaris voor de gegevensbescherming van uw organisatie.

Hoogachtend,
Autoriteit Persoonsgegevens,

[redacted]

Bijlage – Eindbrief onderzoek beveiliging persoonsgegevens GGD GHOR en GGD'en

Archived: donderdag 12 mei 2022 11:52:10
From: [redacted]
Sent: zondag 16 mei 2021 20:35:27
To: [redacted]
Subject: RE: Aanleveren documenten
Importance: Normal
Sensitivity: None

Dank je [redacted] ik hoor het wel.

groeten
[redacted]

Van: [redacted]
Verzonden: vrijdag 14 mei 2021 07:15
Aan: [redacted]
Onderwerp: Re: Aanleveren documenten

Hoi [redacted],

Ik heb een poging gedaan om bij de documenten te komen maar ben, logisch als externe, niet gerechtigd. Ik zal de vraag intern in de projectgroep beleggen. Alvast bedankt en als ik er niet uitkom, dan klop ik nog even bij je aan.

Met vriendelijke groet,

[redacted]

[redacted]

GGD West-Brabant

Doornboslaan 225-227, Breda
Postbus 3024, 5003 DA Tilburg
www.ggdwestbrabant.nl

[redacted]

Aanwezig: donderdag

Van: [redacted]
Verzonden: maandag 10 mei 2021 09:55
Aan: [redacted]
CC: [redacted]
Onderwerp: FW: Aanleveren documenten

Beste [redacted]

Zie hieronder de mailwisseling nav jouw vraag.

Alle documenten die wij kennen staan in het landelijke systeem van GGD GHOR. En vanuit daar worden ze ook geraadpleegd.

Ik vraag af wat je daar mee wilt want het lijkt me niet dat je deze allemaal wil downloaden !!

Ik hoor het graag.

groeten
[redacted]

[redacted]

Van: [redacted]
Verzonden: vrijdag 7 mei 2021 10:09
Aan: [redacted]
CC: [redacted]
Onderwerp: RE: Aanleveren documenten
Urgentie: Hoog

Hoi [redacted]

Alle documenten staan op de GGD GHOR Academy:

https://academy.ggdghor.nl/course/view.php?id=25

Ik neem aan dat jij voor jezelf wel toegang hebt of je kan dat regelen. Moet met authenticator app. Het is te veel om het allemaal te downloaden…

Nr 50: weet ik niets over te zeggen, dat hoort meer bij jou en [redacted] denk ik.

Nr 98: misschien weet [redacted] dit wel. [redacted] zei het niets…

Groetjes, [redacted]

Van: [redacted]
Verzonden: donderdag 6 mei 2021 17:43
Aan: [redacted]
CC: [redacted]
Onderwerp: RE: Aanleveren documenten

Haai [redacted]

Yes, kunnen we morgen aanleveren.

Ik zal aan [redacted] vragen of zij ook iemand van extern hierbij kunnen vragen.
Mogelijk zit er nog een document tussen wat niet bij ons bekend is, maar dan kunnen we dat per nummertje aangeven!

Gr [redacted]

Met vriendelijke groet,

[redacted]

[redacted]

[redacted]

[redacted]

GGD West-Brabant
Doornboslaan 225-227
4816 CZ Breda
www.ggdwestbrabant.nl
[redacted]

Van: [redacted]
Verzonden: donderdag 6 mei 2021 16:46
Aan: [redacted]>
Onderwerp: FW: Aanleveren documenten

Dames

Helpppppppppp wie kan mij helpen ????

Zie hieronder. Allemaal BCO documenten die jullie hopelijk kunnen aanleveren of waarvan jullie kunnen zeggen waar ze staan op SharePoint

Groetjes

[redacted]

Van: [redacted]
Verzonden: donderdag 6 mei 2021 14:56
Aan: [redacted]
Onderwerp: Aanleveren documenten

Beste [redacted],

Mijn naam is [redacted] en ben [redacted]. Het project is opgestart om zowel informatiebeveiliging als ook privacy naar een hoger niveau te tillen. Een van de onderwerpen heeft te maken met het landelijk datalek welke in het begin van dit jaar heeft plaatsgevonden. De kans bestaat namelijk dat wij, door het ontstaan van het genoemde datalek, bezoek zullen krijgen van de Autoriteit Persoonsgegevens (AP). Deze organisatie bewaakt de AVG (nieuwe privacywet welke sinds 2018 actief is) en kijkt of de AVG voldoende nageleefd wordt. Het niet voldoende naleven van de AVG kan tot hoge boetes leiden.

Deze mail gaat dus over het voorbereiden van een mogelijk bezoek van de AP aan onze organisatie. Tijdens zo'n bezoek zullen wij, onder andere, een aantal beleidsdocumenten, overeenkomsten en wat al niet meer moeten kunnen overleggen. Wij zijn nu op zoek naar deze documenten.

Vorige week hebben we in onze projectgroep de lijst met documenten besproken en hebben namen gekoppeld aan deze documenten. Namen van mensen die, volgens ons, deze documenten zouden kunnen opleveren. Mijn verzoek is om de genoemde documenten, veilig, naar mij te mailen. Als jij de documenten niet kunt aanleveren, dan verzoek ik je aan te geven bij wie ik dan moet zijn om de documenten op te kunnen halen.

Kijk hier om te kijken hoe je veilig kunt mailen.

Hieronder de lijst met documenten die specifiek voor jou zijn. Alvast bedankt.

	Overzicht verstrekte stukken aan AP	Wie
14	Werkinstructie BCO Fase 5 uitslagen doorbellen en voorlichting	[redacted]
18	Stroomschema BCO bij COVID-19	
19	Werkinstructie BCO Fase 1 volledig	
20	Werkinstructie BCO Fase 1B Volledig zonder monitoring	
21	Werkinstructie BCO Fase 2 risicogestuurd	
22	Werkinstructie BCO Fase 3 alleen index	
23	Werkinstructie BCO Fase 4 Lean	
35	Tabeloverzicht fases BCO onderzoek GGD GHOR 2.0	
36	Brieven en bijlagen BCO fase 5	
37	Tabellen BCO fase 5 uitslagen doorbellen	
38	Brieven en bijlagen BCO fase 3 risicogestuurd alleen index	
39	Brieven en bijlagen BCO fase 4 lean	
40	Tabellen BCO fase 3 risicogestuurd alleen index	
41	Tabellen BCO fase 4 risicogestuurd lean	
42	Brieven en bijlagen BCO fase 1	
43	Brieven en bijlagen BCO fase 1b zonder monitoring	
44	Brieven en bijlagen BCO fase 2 risicogestuurd	
45	Tabellen BCO fase 1 volledig	
46	Tabellen BCO fase 1b volledig zonder monitoring	
47	Tabellen BCO fase 2 risicogestuurd	
50	Taakverdeling hoofdproces bemensing 18-08-2020	
98	Werkinstructie SOS - 3. Werkinstructie IT v3.1	

Met vriendelijke groet,

[redacted]

[redacted]

GGD West-Brabant

Doornboslaan 225-227, Breda

Postbus 3024, 5003 DA Tilburg

www.ggdwestbrabant.nl

[redacted]

Aanwezig: donderdag

Wob-verzoek SOLV/ICAM datalek 2021 coronasysteem

16.0 Tekst Wob-verzoek en register documenten

Tekst verzoek (xvi)

Informatie en documenten over het onderzoek dat heeft plaatsgevonden naar de omvang van de groep gedupeerden en de potentiële schadelijke gevolgen van het datalek.

Register

Geen documenten aanwezig.