Hart voor Brabant

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

Kenmerk:	DSGGDHvB/uit229	Datum:	31 mei 2022
Behandeld door:	[redacted]	E-mail:	[redacted]
Onderwerp:	besluit Wob-verzoek ICAM 15-02-2022		

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 bij dit besluit. Wij begrijpen dat de Stichting ICAM deze informatie opvraagt vanwege haar aansprakelijkheidsstelling richting onder andere de GGD Hart voor Brabant.
De Veiligheidsregio Midden- en West-Brabant stuurde uw (soortgelijk) verzoek aan ons door en liet daarbij weten dat er geen documenten bij haar berusten. De Veiligheidsregio Brabant-Noord had ook geen documenten en stuurde u een brief daarover.
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 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

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

Documenten

Van de documenten waarom u verzocht en die wij hierbij openbaar maken, vindt u een overzicht aan het begin van de bijlage: dat is één bestand met alle documenten. We ordenden de documenten volgens uw eigen indeling (16 categorieën en een categorie 'overig'), met Romeinse cijfers; elke categorie begint met een overzicht met de bestandsnamen van de documenten.
Bij de documenten zitten ook e-mails (+ de daarbij horende (relevante) bijlagen) die vallen onder de reikwijdte van uw verzoek. 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, te herkennen door de aanhef 'Archived', gevolgd door de datum waarop we ze toevoegden.

In de documenten maakten wij, met een beroep op de Woo, enkele passages onleesbaar:

- 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.

Bij drie documenten vinden wij het belang van het goed functioneren van de GGD zwaarder wegen: openbaarheid van die documenten zou kunnen leiden tot misbruik van die informatie door derden. Die drie documenten maken wij daarom niet openbaar.

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 Hart voor Brabant,
namens deze,

[redacted]

[redacted]
directeur publieke gezondheid

bijlage: Wob-verzoek ICAM - datalek corona 2021
per mail verzonden aan: [redacted] en [redacted]
per brief verzonden aan SOLV B.V.

Hart voor Brabant

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

Kenmerk:		Datum:	18 juli 2022
Behandeld door:	[redacted]	E-mail:	[redacted]
Onderwerp:	tweede besluit Wob-verzoek ICAM 15-02-2022		

Geachte heer [redacted],
Geachte mevrouw [redacted],

In onze brief van 31 mei 2022 deelden wij u ons besluit mee over uw verzoek van 15 februari 2022, waarin u met een beroep op de Wet openbaarheid van bestuur verzocht om informatie. Wij stuurden u de openbaar gemaakte documenten tegelijk met dat besluit.
We verdaagden ons besluit waar het ging over tien documenten waarover wij aan derden een zienswijze wilden vragen. Dat duurde langer dan vier weken, waarvoor onze excuses.

Hierbij delen wij u ons (tweede) besluit mee over deze 10 documenten: wij maken ook deze tien openbaar. We namen ze op in de nieuwe set die wij u digitaal toesturen; het zijn de documenten met de nummers 1.12, 3.2, 3.4, 3.7, 3.8, 3.9, 3.10, 3.14, 3.15 en 13.1. Bij het weglakken van gegevens gebruikten we hetzelfde systeem als in de vorige set, zie onze brief van 31 mei 2022.
Wij verzoeken u om bij verdere acties uit te gaan van deze nieuwe versie.

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 Hart voor Brabant,
namens deze,

GGD Hart voor Brabant
Postbus 3024
5003 DA Tilburg
088 368 7000

www.ggdhvb.nl
info@ggdhvb.nl

[redacted]

[redacted]
directeur publieke gezondheid

bijlage: Wob-verzoek ICAM - datalek corona 2021
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 Hart voor Brabant
Postbus 3024
5003 DA Tilburg

Alsmede per e-mail: contact@ggdhvb.nl

Datum 15 februari 2022
Onze ref. Wob-verzoek GGD-datalek
Uw ref. -

Van [redacted]

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.

SOLV B.V. is gevestigd te Amsterdam (Handelsregister nr. 18060314). Op alle diensten en (overige) werkzaamheden van SOLV B.V. zijn haar Algemene Voorwaarden van toepassing, waarin onder meer een beperking van de aansprakelijkheid is opgenomen. SOLV B.V. is a private limited liability company with its seat in Amsterdam (Trade Register no. 18060314). The General Conditions of SOLV B.V., which include a limitation of liability, apply to all its services and (other) activities.

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] en [redacted].

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

[redacted]

SOLV Advocaten

[redacted]

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;

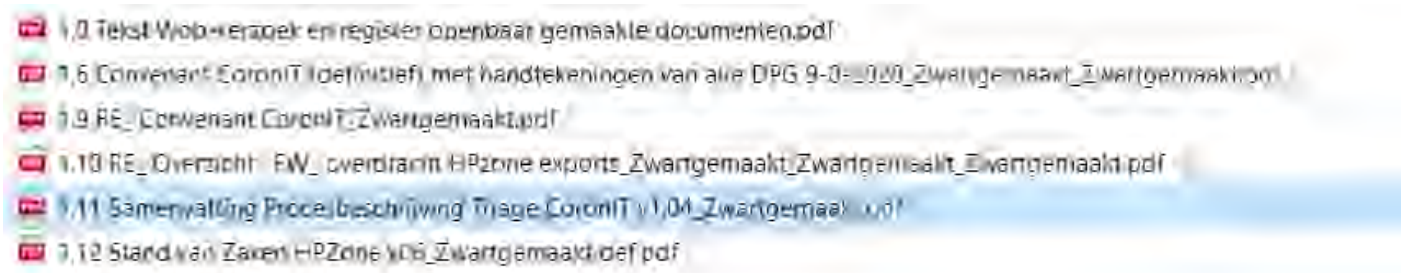
c) Plan van aanpak GGD GHOR Fase 2 incl. begroting d.d. 2 juni 2020;

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:



1.6
Gearchiveerd: dinsdag 3 mei 2022 08:49:45
Van: [redacted]
Verzonden: zondag 9 augustus 2020 22:17:33
Aan: [redacted]
Onderwerp: FW: Convenant CoronIT met handtekeningen van alle DPG en
Urgentie: Normal
Precisie: None
Bijlagen:
Convenant gegevensuitwisseling gezamenlijk verantwoordelijken.pdf;

Hai [redacted], ik stuur hem sowieso even door naar [redacted] maar verder weet ik het eerlijk gezegd niet,

Met vriendelijke groet,

P[redacted]

GGD Hart voor Brabant
Gezond doet leven!

Pettelaarpark 10, 5216 PD
's-Hertogenbosch
Postbus 3024, 5003 DA Tilburg
www.ggdhvb.nl

[redacted]

Van: Directiesecretariaat GGD Hart voor Brabant <directiesecretariaat@ggdhvb.nl>
Verzonden: vrijdag 24 juli 2020 10:58
Aan: [redacted]
Onderwerp: Convenant CoronIT met handtekeningen van alle DPG en

Dag [redacted],
Wie moet van dit convenant een exemplaar ontvangen? Ik zal zorgen voor archivering.
Groeten,
[redacted]

Van: [redacted]@ggdghor.nl>
Verzonden: maandag 20 juli 2020 15:53
Onderwerp: FW: Convenant CoronIT

Beste directiesecretaresses,

Het heeft even geduurd, maar hierbij in bijlage, voor jullie archief, het convenant gegevensuitwisseling gezamenlijk verantwoordelijken, met de handtekeningen van alle DPG'en.

Met vriendelijke groet,
[redacted]

Zwarte Woud 2
3524 SJ Utrecht
Telefoon: 030-2525050

E-mail: [redacted]
Website: www.ggdghor.nl
Twitter: @GGDGHORNL
Werkdagen: ma-vrij

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.

Van: [redacted]
Verzonden: woensdag 29 april 2020 16:21
Onderwerp: Convenant CoronIT

Beste directiesecretaresse,

In verband met 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'), moeten afspraken worden vastgelegd in het kader van de verwerking van persoonsgegevens. Om die afspraken tussen de GGD'en en GGD GHOR Nederland te borgen is gekozen voor het construct van een convenant. In de bijlage tref je dat convenant.

Ik wil je vriendelijk verzoeken om aan je DPG te vragen de voor jullie bestemde pagina (tussen pagina 9 en 35) in te vullen en te ondertekenen, en deze vervolgens aan mij terug te sturen. Ik hoop dat je het me z.s.m. kan sturen, ik kan er nl. pas een volledig document van maken als ik van iedereen reactie heb. Vervolgens zal ik je er eentje bezorgen met alle handtekeningen voor jullie archief.

Als ik mag kiezen ontvang ik de getekende overeenkomst het liefst in word, maar als het in pdf is, is het ook geen ramp. Graag geen andere bestandstypes.
Per post mag ook, naar onderstaand adres.

Alvast hartelijk dank (als er iets niet duidelijk is, laat het me weten).

Met vriendelijke groet,
[redacted]

Zwarte Woud 2
3524 SJ Utrecht
Telefoon: 030-2525050

E-mail: [redacted]
Website: www.ggdghor.nl
Twitter: @GGDGHORNL
Werkdagen: ma-vrij

De uitbraak van het nieuwe Coronavirus vraagt dat ook wij t/m 20 mei, in lijn met de maatregelen van de Rijksoverheid, zoveel mogelijk thuiswerken. U kunt mij goed bereiken via e-mail of via mijn mobiele telefoon.

1.6

1.9
Gearchiveerd: dinsdag 3 mei 2022 08:49:40
Van: [redacted]
Verzonden: donderdag 7 mei 2020 14:01:29
Aan: [redacted]
Onderwerp: RE: Convenant CoronIT
Urgentie: Normal
Precisie: None

Hoi [redacted]

Ja, inderdaad Ik ben ook nog steeds werkzaam bij de GGD regio Utrecht, maar ook hier bij geschakeld.

Het is inderdaad heel knullig (ik heb de fout pas gezien toen iemand mij dit vertelde, 30x overheen gelezen door 3 personen). Ik kan het convenant alleen niet meer laten wijzigen, omdat het al door veel GGD'en is getekend. Ik heb het wel aangegeven en aangeraden, maar het enige wat ik erdoor kon krijgen was het addendum, waar dit soort zaken in kunnen worden aangepast. Dit addendum wil ik uiterlijk begin volgende week af hebben.

Met vriendelijke groet,

[redacted]

cuccibu
Reduce Risk, Create Value

[redacted]

Cuccibu B.V.
+31 (0) 85 303 29 84
Boutenslaan 195-C, 5654 AN, Eindhoven
www.cuccibu.nl

Van: [redacted]ggdhvb.nl>
Verzonden: donderdag 7 mei 2020 13:58
Aan: [redacted]@cuccibu.nl>
Onderwerp: RE: Convenant CoronIT

Hoi [redacted]

Leuke opdracht! Ben je niet meer werkzaam voor GGD Utrecht?

De tekstuele verwijzing naar bijlage 2 die onjuist is in het convenant, zal er toch wel uit moeten. Dit kan je de DPG toch niet laten ondertekenen?

Met vriendelijke groeten,

[redacted]

[redacted] 1.9

[redacted]

Hart voor Brabant

Pettelaarpark 10 Den Bosch

Postbus 3024, 5003 DA Tilburg

www.ggdhvb.nl

[redacted]

Aanwezig op: ma-di-wo-do

Gezond doet leven!

Van: [redacted]@cuccibu.nl>
Verzonden: donderdag 7 mei 2020 13:36
Aan: [redacted]@ggdhvb.nl>
CC: [redacted]
Onderwerp: RE: Convenant CoronIT

Beste [redacted],

Het klopt inderdaad dat er in het convenant een aantal zaken staan die aangevuld dienen te worden of waarvan de situatie inmiddels is gewijzigd. Hiervoor wordt een addendum opgesteld om deze zaken tijdelijk op te lossen. Over 2 maanden, als helemaal vastligt hoe het proces exact loopt, zal een nieuw convenant worden voorgelegd, zodat alle opmerkingen die op het huidige convenant zijn gemaakt kunnen worden opgepakt en het convenant de complete situatie beschrijft.

De reden waarom andere partijen niet zijn meegenomen, is omdat zij het convenant niet hebben ondertekend. Met hen worden andere afspraken gemaakt.

Ten slotte wordt er inderdaad een DPIA uitgevoerd, die met alle GGD'en wordt gedeeld. Hiervoor is een teams-omgeving opgezet, waar de documenten kunnen worden bekeken. Dit voorkomt dat nieuwe versies telkens per mail moeten worden gestuurd. Als het goed is, zouden jullie ook een uitnodiging moeten hebben ontvangen voor de teams omgeving. Indien dat niet zo is, hoor ik het graag, dan gaan we zorgen dat jullie toegang krijgen. Daarbij moet worden opgemerkt dat de DPIA in concept is en blijft tot helder is hoe het proces uiteindelijk zal verlopen. Tot die tijd zal de DPIA telkens aan de dan geldende situatie worden aangepast.

Met vriendelijke groet,

[redacted]

cuccibu

[redacted]

Cuccibu B.V.
[redacted]
Boutenslaan 195-C, 5654 AN, Eindhoven
www.cuccibu.nl

1.9

Van: [redacted]@ggdghor.nl>
Verzonden: donderdag 7 mei 2020 10:32
Aan: [redacted]@ggdhvb.nl>
CC: [redacted]
Onderwerp: RE: Convenant CoronIT

Beste [redacted]

Via de CC haak ik [redacted] aan, onze project-FG. Die weet de antwoorden op je vragen veel beter dan ik

Met vriendelijke groet,
[redacted]

Informatiemanager

GGD GHOR NEDERLAND

Zwarte Woud 2
3524 SJ Utrecht
[redacted]

E-mail : [redacted]
Website : www.ggdghor.nl
[redacted]
Werkdagen : ma – vr

De uitbraak van het nieuwe Coronavirus vraagt dat ook wij tot 20 mei, 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]@ggdhvb.nl>
Verzonden: donderdag 7 mei 2020 10:31
Aan: [redacted]@ggdghor.nl>
CC: [redacted]@ggdhvb.nl>
Onderwerp: Convenant CoronIT

Hallo [redacted]

Ik weet niet of ik bij jou moet zijn, maar ik heb deze week het convenant CoronIT gelezen en heb daar een paar vragen over.

- Wat mij opvalt is dat de partijen zoals het laboratorium en de bedrijfsartsen/artsen etc. die ook toegang hebben tot het systeem niet worden genoemd. Mijn inziens zijn zij ook verwerkingsverantwoordelijk, in ieder geval voor de gegevens die zij zelf in het systeem invoeren.
- Rollen en verhoudingen (art. 4) is tekstueel onjuist: er wordt vermeld dat in bijlage 2 de geselecteerde partners zijn weergegeven, maar in bijlage 2 wordt gesproken over beveiligingsmaatregelen.
- Beveiligingseisen zijn ook overgenomen, waarbij ik vorig keer al de opmerking heb gemaakt dat wij als GGD Hvb niet aan de NEN voldoen. Of gaat het hier sec om het feit dat het systeem/software aan de NEN voldoet en niet de organisatie zelf?

- Moet er niet een DPIA uitgevoerd worden? Gaat iedere GGD dit zelfstandig doen?

Ik hoor het graag,

Met vriendelijke groeten,

[redacted]

Hart voor Brabant

Pettelaarpark 10 Den Bosch

Postbus 3024, 5003 DA Tilburg

www.ggdhvb.nl

[redacted]

Aanwezig op: ma-di-wo-do

Gezond doet leven!

Hallo,

- Ik ben het eens met de opmerkingen van [redacted] Ik zie dat de doelstelling eigenlijk één op één is overgenomen uit het convenant van iTBC. In de bijlage 1 wordt onder doel verwerking vermeld: bestrijding van COVID-19 kan zo landelijk worden gecoördineerd op basis van de Wet publieke gezondheid. Hier wordt geen toevoeging gedaan mbt regionale bestrijding. Vreemd.
- Beveiligingseisen zijn ook overgenomen, waarbij ik vorig keer al de opmerking heb gemaakt dat wij als GGD Hvb niet aan de NEN voldoen
- Rollen en verhoudingen (art. 4) is tekstueel onjuist: er wordt vermeld dat in bijlage 2 de geselecteerde partners zijn weergegeven, maar in bijlage 2 wordt gesproken over beveiligingsmaatregelen.
- Moet er niet een DPIA uitgevoerd worden? Gaat iedere GGD dit zelfstandig doen?

Wat ik mij afvraag is waarom de overig partijen niet worden genoemd als gezamenlijk verantwoordelijken. Ik kan mij voorstellen dat een laboratorium zelf verantwoordelijk is voor de invoer van het testresultaat en de bedrijfsarts voor de invoer van de persoonsgegevens van de nog te testen persoon. Of gaat dit te ver?

Gaat ieder voor zich de punten terugkoppelen aan GGD GHOR?

Met vriendelijke groeten,

[redacted]

Hart voor Brabant

Pettelaarpark 10 Den Bosch

Postbus 3024, 5003 DA Tilburg

www.ggdhvb.nl

[redacted]

Aanwezig op: ma-di-wo-do

Gezond doet leven!

Van: [redacted]1.9[redacted]@privacyforce.nl>
Verzonden: dinsdag 5 mei 2020 14:23
Aan: [redacted]
Onderwerp: Re: CoronIT

Goedemiddag,

[redacted], dank voor je opmerkingen. Wat je stelt m.b.t. art. 5 lid 4 zie ik in lijn met mijn opmerking bij art. 4 lid 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.

Mijn opmerking:
Deze bepaling snap ik niet. Is het niet in tegenspraak met de bepaling *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*? Zie hierboven.

Dit komt op mij over als dat GGD GHOR NL het systeem beheert maar dat de GGD'en verantwoordelijk zijn voor de door hen ingevoerde persoonsgegevens.

Het is ook in tegenspraak met de voorgaande volzin:
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.

Ik heb het samenwerkingsconvenant nog maar eens een keer doorgenomen. Extra opmerking:

Bijlage 3 Verwerkers (Topicus)
Als er een verwerker is moet er ook een onderliggende overeenkomst zijn. Gezien de structuur van de informatie-uitwisseling zou ik om een kopie van deze onderliggende overeenkomst en de verwerkersovereenkomst vragen.

GGD GHOR NL is een vereniging van de 25 GGD'en en de GHOR afdelingen. Puur in het kader van de AVG, zou ik o.b.v. dit document de GGD'en beoordelen als gezamenlijk verwerkingsverantwoordelijken, GGD GHOR NL als verwerker en Topicus als subverwerker. Ik realiseer me daarbij dat de zuiver juridische constructie geen recht hoeft te doen aan praktijk.

Bijgevoegd nogmaals het betreffende convenant met mijn opmerkingen. Ik ben heel benieuwd naar jullie mening.

Met vriendelijke groet,

[redacted]

[redacted]

1.9

Van: "[redacted]@drechtsteden.nl▷
Datum: dinsdag 5 mei 2020 om 10:28
Aan: [redacted]
Onderwerp: CoronIT

Hele goedemorgen,

Ik heb gisteren nog even de MS Teams meegedraaid met de FG's van andere GGD'en. En ik heb even gekeken naar het convenant met de opmerkingen van Arthur.

Gelet op de rolverdeling vind ik artikel 5 lid 4 wel apart.

Ik heb een puntsgewijs verslagje bijgevoegd van de meet via MS Teams gisteren.

Ik ben zelf o.a. nog wel benieuwd naar de selectiecriteria voor de aanbesteding, de praktische werking van de applicatie en de mogelijkheid tot onttrekken van data eruit.

Hebben jullie deze week nog tijd om te kijken?

met vriendelijke groet,

[redacted]

[redacted]

Werkdagen: maandag, dinsdag, woensdag, donderdag en vrijdagmorgen

Dienst Gezondheid & Jeugd ZHZ

Karel Lotsyweg 40 | 3318 AL Dordrecht

Postbus 166 | 3300 AD Dordrecht

[redacted]

w www.dienstgezondheidjeugd.nl

1.10
Archived: donderdag 12 mei 2022 09:29:00
From: [redacted]
Sent: maandag 25 januari 2021 13:32:55
To: [redacted]
Subject: RE: Overzicht FW: overdracht HPzone exports
Importance: Normal
Sensitivity: None

Hoi [redacted]

Vanuit de rapportageserver van CoronIT kunnen datadumps opgehaald worden door medewerkers met de autorisatierol "Onderzoeker (IZB/team onderzoek)". De volgende mensen hebben deze rol:

datum in behandeling	Achternaam	Tussen-voegsel	Voornaam	Pers.nr.	Inlognaam CoronIT
01-01-2020	[redacted]				[redacted]
01-01-2020					
01-01-2020					
14-10-2020					
06-10-2020					
25-01-2021					

Dezelfde onderzoekers hebben ook toegang tot HPZone om daar rapportages te maken. Daarnaast hebben onderstaande medewerkers dezelfde mogelijkheid:

Medewerkers met de rol "BCO Hoofdcoordinator"

datum in behandeling	Achternaam	Tussen-voegsel	Voornaam	Pers.nr.	Inlognaam CoronIT
18-09-2020	[redacted]				[redacted]
25-06-2020					
21-08-2020					
01-09-2020					
05-10-2020					
1-1-2020/25-09-2020					
10-8-2020/17-8-2020					
25-06-2020					
1-1-2020/23-07-2020					

En alle reguliere medewerkers van Team IZB plus de DIP'ers

Groeten,

[redacted]

Adviseur Informatievoorziening

Hart voor Brabant

Ringbaan West 227 Tilburg

Postbus 3024, 5003 DA Tilburg

www.ggdhvb.nl

[redacted]

Aanwezig op: di-wo-do-vr

Gezond doet leven!

Van: [redacted] <e.[redacted]ggdhvb.nl>
Verzonden: maandag 25 januari 2021 12:49
Aan: [redacted]
Onderwerp: Overzicht FW: overdracht HPzone exports

Hoi [redacted],

Heb jij een overzicht van medewerkers die een datadump kunnen maken voor beide systemen?

Met vriendelijke groeten,

[redacted]

[redacted]

[redacted]

Hart voor Brabant

Pettelaarpark 10 Den Bosch

Postbus 3024, 5003 DA Tilburg

www.ggdhvb.nl

[redacted]

Aanwezig op: ma-di-wo-do

Gezond doet leven!

Van: [redacted]>
Verzonden: vrijdag 22 januari 2021 14:37
Aan: [redacted]
CC: [redacted]
Onderwerp: RE: overdracht HPzone exports

Hoi [redacted]

Kunnen jullie [redacted] (functionaris gegevensbescherming) meenemen in deze communicatie. Zij is op zoek naar inzicht omtrent de handelingen die voor dit proces moeten worden uitgevoerd en wil graag weten welke personen deze taak op gaan pakken. Ik heb haar in de cc gezet.

Dank je.

Groet,

Daan 1.10

Met vriendelijke groet,

[redacted]

Business Analist

Hart voor Brabant

Pettelaarpark 10,

5216 PD 's Hertogenbosch

www.ggdhvb.nl

d.van.[redacted]ggdhvb.nl

Aanwezig op: ma-di-wo-do

[redacted]

Van: [redacted]
Verzonden: vrijdag 22 januari 2021 11:42
Aan: [redacted]
Onderwerp: RE: overdracht HPzone exports

Voor zover ik weet hebben HP invoer medewerkers toegang tot N schijf, maar G schijf weet ik niet. Ik ben nog aan het overleggen bij wie we dit het beste kunnen leggen. Zit zelf ook te denken aan onze procescoordinatoren. Werk vandaag niet dus zal maandag nogmaals kijken en wanneer we weten wie het gaat doen meteen authorisatie aanvragen.

Van: [redacted]
Verzonden: vrijdag 22 januari 2021 08:27
Aan: [redacted]
Onderwerp: RE: overdracht HPzone exports

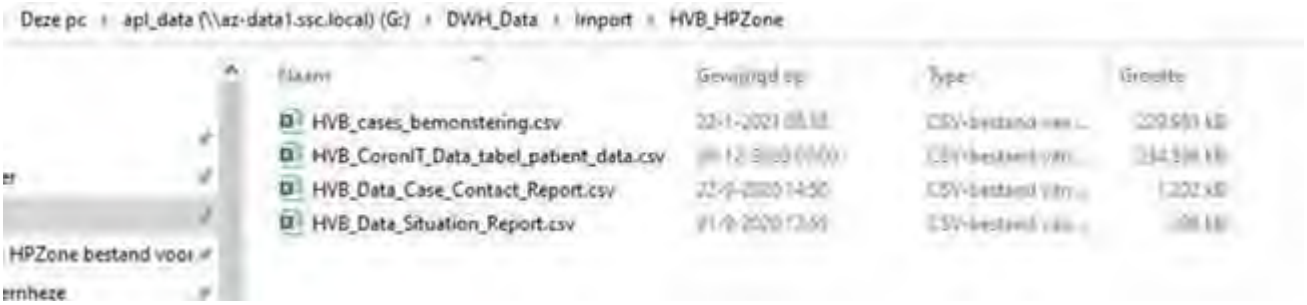
Beste [redacted]

Heel fijn!

He is wel belangrijk dat de personen die dit gaan doen toegang hebben tot HPzone en tot

onderstaande map waar zij het bestand in moeten wegschrijven.

Alvast dank!



Met vriendelijke groet,

[redacted]

onderzoeker 1.10

Vogelstraat 2 's-Hertogenbosch

Postbus 3024, 5003 DA Tilburg

www.ggdhvb.nl/onderzoek

mo.[redacted]ggdhvb.nl

Aanwezig op: ma-di-do-vr

9:30-14:30

[redacted]

Gezond doet leven!

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

Van: [redacted]
Verzonden: donderdag 21 januari 2021 12:18
Aan: [redacted]
Onderwerp: RE: overdracht HPzone exports

Hoi [redacted]

ik heb inderdaad begrepen dat jullie dit al geruime tijd doen, maar dat het een handeling is die ook elders belegd kan worden, dus fijn als we jullie daarmee kunnen ontlasten.

Ik zal het hier bespreken en dan stuur ik de uitnodiging door naar degene die dit op zich zal nemen.

Met vriendelijke groet,

[redacted]

Arts, Coordinator Bron en Contactonderzoek

Team Infectieziekten

Pettelaarpark 10, 5216 PD 's-Hertogenbosch

Postbus 3024, 5003 DA Tilburg

www.ggdhvb.nl

[redacted]ggdhvb.nl

Ma,di,wo,do

Gezond doet leven!

Van: [redacted]
Verzonden: donderdag 21 januari 2021 12:15
Aan: [redacted]
Onderwerp: overdracht HPzone exports

Beste [redacted]

Wij hebben van [redacted] begrepen dat we met jou de overdracht van de HPzone exports t.b.v corona dashboard kunnen regelen.

Wij doen dit nu al ruim 9 maanden en dragen het graag over.

Ik heb een meeting in teams ingepland.

Als jij al weet wie de exports (iedere ochtend voor 8:45) gaan uitvoeren kunnen we die personen misschien ook al uitnodigen.

Dan kunnen we zo snel mogelijk overdragen.

Alvast dank!

Met vriendelijke groet,

[redacted]

onderzoeker

GGD Hart voor Brabant

Vogelstraat 2 's-Hertogenbosch

Postbus 3024, 5003 DA Tilburg

www.ggdhvb.nl/onderzoek

mo.[redacted]ggdhvb.nl

Aanwezig op: ma-di-do-vr

9:30-14:30

[redacted]

Gezond doet leven!

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

1. Inleiding

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

1.1. Scope

Deze procesbeschrijving is van toepassing op de door het SOC uit te voeren onderzoeken naar afwijkend gedrag van medewerkers, die werken met privacygevoelige informatie. Het doel is te voorkomen dat privacygevoelige informatie door individuele medewerkers voor andere doeleinden wordt gebruikt dan waarvoor deze informatie door de GGD’en is verzameld.

1.2. *Rollen en verantwoordelijkheden*

De Manager SOC is verantwoordelijk voor de inhoud van het proces Triage en het SOC voert de onderzoeken uit, onderhoudt de procesbeschrijving en communiceert deze naar de betrokken partners.

2. Proces voor Triage

2.1. Het hoofdproces + 2.3 Subproces: Besluiten wat te doen en het starten van acties

Bij het proces Triage CoronIT worden de volgende stappen doorlopen:

1. De SOC-analist ziet mogelijk afwijkend gedrag
2. De SOC-analist doet een quick scan en eventueel een check bij een collega
3. De SOC-analist besluit of een onderzoek nodig is
4. Start van een onderzoek
5. Afronding van een onderzoek
6. Review van een onderzoek
7. Wekelijkse dossier review
8. Besluit wat te doen met het dossier en het starten van acties:
   - Niets doen
   - Verrijken van het dossier
   - Opsturen naar ketenpartner
   - Een laatste check bij de Informatiemanager GGD GHOR NL
   - Indien dossier overdragen aan de Politie: Manager SOC bij de Politie verifiëren of account van een nog actieve medewerker wel of niet moet worden dichtgezet.
   - Het dossier aanmelden bij de Politie
   - Het dossier sluiten
9. Check follow up status
10. Informeren van de CISO en CIO

Bij iedere stap geldt: de SOC-analist meldt urgente issues zo spoedig mogelijk aan de Manager SOC.

2.2. Subproces: Triageonderzoek

De te analyseren gegevens worden via verschillende kanalen zoals Topicus, FoxIT en Teleperformance aan het SOC Team verstrekt. Zodra de gegevensexports door het SOC Team zijn ontvangen, voeren de SOC-analisten verschillende screening- en controlesessies uit.

De processtappen voor het tirageonderzoek zijn:

1. Opvragen data export, oftewel de logs van Topicus met alle handelingen van de medewerkers en beheerders die toegang hebben tot CoronIT.
2. Data plaatsen in logbestanden Topicus map
3. Aanmaken onderzoeksmap (specifieke medewerker > In progress)
4. Ruwe data verwerken in Template aanleveren bewijslast
5. Opvragen call logs indien nodig
6. Data toevoegen aan template en uitvoeren van het triageonderzoek
7. Onderzoeksmap verplaatsen naar (Specifieke medewerker > Done > To do)
8. Na wekelijkse meeting besluiten om dossier over te dragen aan de Politie of niet
9. Onderzoeksmap verplaatsen naar (Specifieke medewerker > Done > Verder)
10. Onderzoeksmap verplaatsen naar (Specifieke medewerker > Done > Archive)

2.4. Door Teleperformance te leveren informatie en doelbinding

Op basis van de AVG geldt dat persoonsgegevens alleen mogen worden verwerkt om een bepaald doel te bereiken. Het doel is in dit geval om vast te stellen of een medewerker zich wel of niet aan de

gedragsregels heeft gehouden. Hiertoe mogen identificerende gegevens van medewerkers en identificerende gegevens van door hen gemuteerde of geraadpleegde patiëntdossiers worden overgedragen aan het SOC. Deze informatie is voor het SOC noodzakelijk om de analyses uit te kunnen voeren.

Logs worden bij Teleperformance opgevraagd door de informatiemanager GGD GHOR NL. In de geleverde logs staan onder andere de volgende gegevens:

-
- Dit wordt door het SOC gebruikt om te controleren welke medewerker het dossier van een specifieke patiënt heeft gemuteerd of geraadpleegd.
- Medewerkernummer: Aan de hand van dit nummer kan het gedrag van een specifieke medewerker worden geanalyseerd door het SOC.
- E-mail werk medewerker

2.5. Informatie verstrekken aan Teleperformance en doelbinding

Teleperformance levert medewerkers die calls afhandelen en testen en vaccinaties inplannen. Een onderzoeksdossier van de SOC-analist bevat persoonsgegevens van een specifiek onderzochte medewerker van Teleperformance, maar ook van andere medewerkers en van patiënten. Op basis van de AVG geldt dat persoonsgegevens alleen mogen worden verwerkt om een bepaald doel te bereiken. Het doel is in dit geval om vast te stellen of een medewerker zich wel of niet aan de gedragsregels heeft gehouden. Hiertoe mag informatie over de medewerker in kwestie worden uitgewisseld met Teleperformance, maar niet over derden zoals andere medewerkers of patiënten. Teleperformance gebruikt de verstrekte gegevens vervolgens om met de betreffende medewerker te overleggen en, indien noodzakelijk, disciplinaire maatregelen te treffen.

2.6. Informatie delen met de politie

Op het moment dat een casus of een specifieke medewerker als verdacht wordt aangemerkt, bespreekt de SOC-analist dit met een tweede SOC-analist als een dubbelcheck. Als de tweede SOC-analist het eens is met de eerste SOC-analist, meldt de eerste SOC-analist dit aan de Manager SOC.

- Indien het een GGD-medewerker betreft: De Manager SOC zal contact opnemen met de verantwoordelijke GGD, overleggen of aangifte gepast is en afstemmen wie welke vervolgstappen zal nemen. De GGD is hierin de eindverantwoordelijke, SOC kan in dit proces faciliteren en contact met de Politie verzorgen.
- Indien het een medewerker van een verwerker betreft: Manager SOC is eindverantwoordelijk voor de aangiftebeslissing en opvolging daarvan als gemandateerde van GGD GHOR NL.

2.7. Informatie delen met een GGD

Een triage-onderzoek naar een medewerker van een GGD kan worden gestart op expliciet verzoek van een geautoriseerde functionaris bij een GGD of door een SOC-analist die mogelijk afwijkend gedrag signaleert. Het SOC zal bij een vermoeden van afwijkend gedrag door een medewerker van een GGD altijd eerst contact opnemen met de betreffende GGD. Daarnaast zal het SOC alleen met expliciete en vastgelegde toestemming van de aangewezen HRM-contactpersoon of de DPG van de betreffende GGD contact opnemen met de Politie of een onderzoeksbureau.

Onderzoek naar software en het ontwikkelproces

- Uitgevoerd door *Utilus* in de periode 29 januari – 5 februari 2021
- “Ondanks enkele stappen die de leverancier heeft genomen in de richting van modernisering is het systeem niet geschikt om ingezet te worden voor het ondersteunen van de duizenden gebruiken waarvan nu sprake is.”
- “Technisch gezien zijn HPZone Lite en HPZone één systeem, ze hebben dezelfde techniek, database en *broncode*.”
- “Door de jaren heen is er functionaliteit aan toegevoegd, maar er is geen structurele verbetering doorgevoerd.”
- “De structuur van het systeem is niet geschikt voor grootschalig gebruik. Er zijn geen voorzieningen getroffen om de performance of de beschikbaarheid te garanderen.
- “De software wordt overwegend handmatig getest. Handmatige tests zijn tijdrovend en kostbaar, en daardoor per definitie van beperkte omvang.”
-

Analyse van de database HPZone

- Uitgevoerd door *Axis into ICT* in de periode 13 januari – 4 februari 2021
- “Er zijn elementaire fouten gemaakt in het datamodel met grote gevolgen voor de performance.”
- [redacted]
- “Omdat controle door de database, vanwege het datamodel, ontbreekt kunnen er fouten [in de gegevens] ontstaan.”
- “Een substantieel deel van de load [belasting] is het gevolg van het niet onderhouden van de database.”
- “De pre-processing van de data voor het RIVM is nu dus een verantwoordelijkheid van de GGD geworden. Wanneer het RIVM iets wil aanpassen aan bijvoorbeeld codes etc. dan moet er ook binnen HPZone development plaatsvinden om aan de informatie/eisen van het RIVM te voldoen.”
- “Verder gaan op de huidige weg is ABSOLUUT af te raden.”

Overzicht van verbeterpunten / bevindingen:

HPZone gebruikersinterface

- Complex in gebruik, foutgevoelig
- Voldoet niet aan wettelijke vereisten van toegankelijkheid

HPZone programmatuur

- Niet opgezet volgens principes software engineering
- Technische documentatie ontbreekt;
- Kan inconsistentie (invaliditeit) data veroorzaken
- Grotendeels handmatig getest
- geen structurele verbetering in de loop van de jaren
- Ca 10% van de HPZone-specifieke broncode wordt in opdracht van RIVM t.b.v. Osiris onderhouden, zonder juridische basis

HPZone database

- **Inefficiënt / slechte performance (o.a. door ontwerp en zoekvragen)**
- **Geen onderhoud op gegevens, database stroomt vol tot fysieke grens**
- Bevat scripts die periodiek fouten door software corrigeren

inFact (leverancier HPZone)

- Erkent belang van specifieke IT-expertise (architectuur, user experience,…) niet
- Er is geen plan om het systeem te moderniseren
- Eigenaar / productmanager inFact heeft tevens fulltime aanstelling bij
- Onduidelijk wie verantwoordelijk is voor kwaliteitsaspecten, zoals performance, beschikbaarheid en beveiliging

Risico voor continuïteit

Risico voor opschaling

Risico voor onderhoud

Overige risico’s (governance, conformiteit, contract, imago)

1.12

HPZone en normen/standaarden in de sector*:

- inFact en HPZone voldoen niet aan NEN7510/NEN7512/ISO27001/AVG
- [redacted]
- HPZone ondersteunt geen gangbare uitwisselingsstandaarden (zoals HL7 of EDIFACT)
- [redacted]
- HPZone voldoet niet aan de Web Content Accessibility Guidelines (WCAG 2.1, wettelijke verplichting)

* In verband met de korte doorlooptijd zijn de constateringen opgebouwd uit zowel direct als indirect bewijs.

Consequenties/risico’s

- [redacted]
- [redacted]
- Gebruik van HPZone is moeilijk om te leren; voor het oplossen van daaruit ontstane fouten is capaciteit van GGD nodig.
- Aanpassing en onderhoud van HPZone door inFact is langzaam en onvoorspelbaar.
- [redacted]
- De grote afhankelijkheid van inFact staat niet in verhouding tot de continuïteit en professionaliteit die deze kleine organisatie kan bieden.
- Ontbrekende eisen en afspraken leiden tot juridische en contractuele complicaties.
- De knelpunten stralen negatief af op het imago van de GGD’en, GGD GHOR NL en de publieke gezondheidszorg.

Conclusies

- HPzone /HPZone Lite stelt de GGD’en niet in staat te voldoen aan in zorgsector gangbare wetten en normeringen. Continuering van het gebruik is mogelijk ongeoorloofd.
- Er bestaat een reëel continuïteitsrisico t.a.v. de schaalbaarheid van HPZone(Lite) gedurende een 3e (of navolgende) golf ten gevolge van zowel toenemend gebruik, als de hoeveelheid data.
- Het doorontwikkelen van de huidige software wordt zeer sterk afgeraden op grond van beide, externe analyses.
- Een alternatief dient aangeschaft te worden o.b.v. een standaard product of te worden gerealiseerd door een nieuw team.

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:

1.6
Gearchiveerd: dinsdag 3 mei 2022 08:49:45
Van: [redacted]
Verzonden: zondag 9 augustus 2020 22:17:33
Aan: [redacted]
Onderwerp: FW: Convenant CoronIT met handtekeningen van alle DPG en
Urgentie: Normal
Precisie: None
Bijlagen:
Convenant gegevensuitwisseling gezamenlijk verantwoordelijken.pdf;

Hai [redacted], ik stuur hem sowieso even door naar [redacted] maar verder weet ik het eerlijk gezegd niet,

Met vriendelijke groet,

P[redacted]

GGD Hart voor Brabant
Gezond doet leven!

Pettelaarpark 10, 5216 PD
's-Hertogenbosch
Postbus 3024, 5003 DA Tilburg
www.ggdhvb.nl

[redacted]

Van: Directiesecretariaat GGD Hart voor Brabant <directiesecretariaat@ggdhvb.nl>
Verzonden: vrijdag 24 juli 2020 10:58
Aan: [redacted]
Onderwerp: Convenant CoronIT met handtekeningen van alle DPG en

Dag [redacted],
Wie moet van dit convenant een exemplaar ontvangen? Ik zal zorgen voor archivering.
Groeten,
[redacted]

Van: [redacted]@ggdghor.nl>
Verzonden: maandag 20 juli 2020 15:53
Onderwerp: FW: Convenant CoronIT

Beste directiesecretaresses,

Het heeft even geduurd, maar hierbij in bijlage, voor jullie archief, het convenant gegevensuitwisseling gezamenlijk verantwoordelijken, met de handtekeningen van alle DPG'en.

Met vriendelijke groet,
[redacted]

Zwarte Woud 2
3524 SJ Utrecht
Telefoon: 030-2525050

E-mail: [redacted]
Website: www.ggdghor.nl
Twitter: @GGDGHORNL
Werkdagen: ma-vrij

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.

Van: [redacted]
Verzonden: woensdag 29 april 2020 16:21
Onderwerp: Convenant CoronIT

Beste directiesecretaresse,

In verband met 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'), moeten afspraken worden vastgelegd in het kader van de verwerking van persoonsgegevens. Om die afspraken tussen de GGD'en en GGD GHOR Nederland te borgen is gekozen voor het construct van een convenant. In de bijlage tref je dat convenant.

Ik wil je vriendelijk verzoeken om aan je DPG te vragen de voor jullie bestemde pagina (tussen pagina 9 en 35) in te vullen en te ondertekenen, en deze vervolgens aan mij terug te sturen. Ik hoop dat je het me z.s.m. kan sturen, ik kan er nl. pas een volledig document van maken als ik van iedereen reactie heb. Vervolgens zal ik je er eentje bezorgen met alle handtekeningen voor jullie archief.

Als ik mag kiezen ontvang ik de getekende overeenkomst het liefst in word, maar als het in pdf is, is het ook geen ramp. Graag geen andere bestandstypes.
Per post mag ook, naar onderstaand adres.

Alvast hartelijk dank (als er iets niet duidelijk is, laat het me weten).

Met vriendelijke groet,
[redacted]

Zwarte Woud 2
3524 SJ Utrecht
Telefoon: 030-2525050

E-mail: [redacted]
Website: www.ggdghor.nl
Twitter: @GGDGHORNL
Werkdagen: ma-vrij

De uitbraak van het nieuwe Coronavirus vraagt dat ook wij t/m 20 mei, in lijn met de maatregelen van de Rijksoverheid, zoveel mogelijk thuiswerken. U kunt mij goed bereiken via e-mail of via mijn mobiele telefoon.

1.6

1.9
Gearchiveerd: dinsdag 3 mei 2022 08:49:40
Van: [redacted]
Verzonden: donderdag 7 mei 2020 14:01:29
Aan: [redacted]
Onderwerp: RE: Convenant CoronIT
Urgentie: Normal
Precisie: None

Hoi [redacted]

Ja, inderdaad Ik ben ook nog steeds werkzaam bij de GGD regio Utrecht, maar ook hier bij geschakeld.

Het is inderdaad heel knullig (ik heb de fout pas gezien toen iemand mij dit vertelde, 30x overheen gelezen door 3 personen). Ik kan het convenant alleen niet meer laten wijzigen, omdat het al door veel GGD'en is getekend. Ik heb het wel aangegeven en aangeraden, maar het enige wat ik erdoor kon krijgen was het addendum, waar dit soort zaken in kunnen worden aangepast. Dit addendum wil ik uiterlijk begin volgende week af hebben.

Met vriendelijke groet,

[redacted]

cuccibu
Reduce Risk, Create Value

[redacted]

Cuccibu B.V.
+31 (0) 85 303 29 84
Boutenslaan 195-C, 5654 AN, Eindhoven
www.cuccibu.nl

Van: [redacted]ggdhvb.nl>
Verzonden: donderdag 7 mei 2020 13:58
Aan: [redacted]@cuccibu.nl>
Onderwerp: RE: Convenant CoronIT

Hoi [redacted]

Leuke opdracht! Ben je niet meer werkzaam voor GGD Utrecht?

De tekstuele verwijzing naar bijlage 2 die onjuist is in het convenant, zal er toch wel uit moeten. Dit kan je de DPG toch niet laten ondertekenen?

Met vriendelijke groeten,

[redacted]

[redacted] 1.9

[redacted]

Hart voor Brabant

Pettelaarpark 10 Den Bosch

Postbus 3024, 5003 DA Tilburg

www.ggdhvb.nl

[redacted]

Aanwezig op: ma-di-wo-do

Gezond doet leven!

Van: [redacted]@cuccibu.nl>
Verzonden: donderdag 7 mei 2020 13:36
Aan: [redacted]@ggdhvb.nl>
CC: [redacted]
Onderwerp: RE: Convenant CoronIT

Beste [redacted],

Het klopt inderdaad dat er in het convenant een aantal zaken staan die aangevuld dienen te worden of waarvan de situatie inmiddels is gewijzigd. Hiervoor wordt een addendum opgesteld om deze zaken tijdelijk op te lossen. Over 2 maanden, als helemaal vastligt hoe het proces exact loopt, zal een nieuw convenant worden voorgelegd, zodat alle opmerkingen die op het huidige convenant zijn gemaakt kunnen worden opgepakt en het convenant de complete situatie beschrijft.

De reden waarom andere partijen niet zijn meegenomen, is omdat zij het convenant niet hebben ondertekend. Met hen worden andere afspraken gemaakt.

Ten slotte wordt er inderdaad een DPIA uitgevoerd, die met alle GGD'en wordt gedeeld. Hiervoor is een teams-omgeving opgezet, waar de documenten kunnen worden bekeken. Dit voorkomt dat nieuwe versies telkens per mail moeten worden gestuurd. Als het goed is, zouden jullie ook een uitnodiging moeten hebben ontvangen voor de teams omgeving. Indien dat niet zo is, hoor ik het graag, dan gaan we zorgen dat jullie toegang krijgen. Daarbij moet worden opgemerkt dat de DPIA in concept is en blijft tot helder is hoe het proces uiteindelijk zal verlopen. Tot die tijd zal de DPIA telkens aan de dan geldende situatie worden aangepast.

Met vriendelijke groet,

[redacted]

cuccibu

[redacted]

Cuccibu B.V.
[redacted]
Boutenslaan 195-C, 5654 AN, Eindhoven
www.cuccibu.nl

1.9

Van: [redacted]@ggdghor.nl>
Verzonden: donderdag 7 mei 2020 10:32
Aan: [redacted]@ggdhvb.nl>
CC: [redacted]
Onderwerp: RE: Convenant CoronIT

Beste [redacted]

Via de CC haak ik [redacted] aan, onze project-FG. Die weet de antwoorden op je vragen veel beter dan ik

Met vriendelijke groet,
[redacted]

Informatiemanager

GGD GHOR NEDERLAND

Zwarte Woud 2
3524 SJ Utrecht
[redacted]

E-mail : [redacted]
Website : www.ggdghor.nl
[redacted]
Werkdagen : ma – vr

De uitbraak van het nieuwe Coronavirus vraagt dat ook wij tot 20 mei, 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]@ggdhvb.nl>
Verzonden: donderdag 7 mei 2020 10:31
Aan: [redacted]@ggdghor.nl>
CC: [redacted]@ggdhvb.nl>
Onderwerp: Convenant CoronIT

Hallo [redacted]

Ik weet niet of ik bij jou moet zijn, maar ik heb deze week het convenant CoronIT gelezen en heb daar een paar vragen over.

- Wat mij opvalt is dat de partijen zoals het laboratorium en de bedrijfsartsen/artsen etc. die ook toegang hebben tot het systeem niet worden genoemd. Mijn inziens zijn zij ook verwerkingsverantwoordelijk, in ieder geval voor de gegevens die zij zelf in het systeem invoeren.
- Rollen en verhoudingen (art. 4) is tekstueel onjuist: er wordt vermeld dat in bijlage 2 de geselecteerde partners zijn weergegeven, maar in bijlage 2 wordt gesproken over beveiligingsmaatregelen.
- Beveiligingseisen zijn ook overgenomen, waarbij ik vorig keer al de opmerking heb gemaakt dat wij als GGD Hvb niet aan de NEN voldoen. Of gaat het hier sec om het feit dat het systeem/software aan de NEN voldoet en niet de organisatie zelf?

- Moet er niet een DPIA uitgevoerd worden? Gaat iedere GGD dit zelfstandig doen?

Ik hoor het graag,

Met vriendelijke groeten,

[redacted]

Hart voor Brabant

Pettelaarpark 10 Den Bosch

Postbus 3024, 5003 DA Tilburg

www.ggdhvb.nl

[redacted]

Aanwezig op: ma-di-wo-do

Gezond doet leven!

Hallo,

- Ik ben het eens met de opmerkingen van [redacted] Ik zie dat de doelstelling eigenlijk één op één is overgenomen uit het convenant van iTBC. In de bijlage 1 wordt onder doel verwerking vermeld: bestrijding van COVID-19 kan zo landelijk worden gecoördineerd op basis van de Wet publieke gezondheid. Hier wordt geen toevoeging gedaan mbt regionale bestrijding. Vreemd.
- Beveiligingseisen zijn ook overgenomen, waarbij ik vorig keer al de opmerking heb gemaakt dat wij als GGD Hvb niet aan de NEN voldoen
- Rollen en verhoudingen (art. 4) is tekstueel onjuist: er wordt vermeld dat in bijlage 2 de geselecteerde partners zijn weergegeven, maar in bijlage 2 wordt gesproken over beveiligingsmaatregelen.
- Moet er niet een DPIA uitgevoerd worden? Gaat iedere GGD dit zelfstandig doen?

Wat ik mij afvraag is waarom de overig partijen niet worden genoemd als gezamenlijk verantwoordelijken. Ik kan mij voorstellen dat een laboratorium zelf verantwoordelijk is voor de invoer van het testresultaat en de bedrijfsarts voor de invoer van de persoonsgegevens van de nog te testen persoon. Of gaat dit te ver?

Gaat ieder voor zich de punten terugkoppelen aan GGD GHOR?

Met vriendelijke groeten,

[redacted]

Hart voor Brabant

Pettelaarpark 10 Den Bosch

Postbus 3024, 5003 DA Tilburg

www.ggdhvb.nl

[redacted]

Aanwezig op: ma-di-wo-do

Gezond doet leven!

Van: [redacted]1.9[redacted]@privacyforce.nl>
Verzonden: dinsdag 5 mei 2020 14:23
Aan: [redacted]
Onderwerp: Re: CoronIT

Goedemiddag,

[redacted], dank voor je opmerkingen. Wat je stelt m.b.t. art. 5 lid 4 zie ik in lijn met mijn opmerking bij art. 4 lid 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.

Mijn opmerking:
Deze bepaling snap ik niet. Is het niet in tegenspraak met de bepaling *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*? Zie hierboven.

Dit komt op mij over als dat GGD GHOR NL het systeem beheert maar dat de GGD'en verantwoordelijk zijn voor de door hen ingevoerde persoonsgegevens.

Het is ook in tegenspraak met de voorgaande volzin:
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.

Ik heb het samenwerkingsconvenant nog maar eens een keer doorgenomen. Extra opmerking:

Bijlage 3 Verwerkers (Topicus)
Als er een verwerker is moet er ook een onderliggende overeenkomst zijn. Gezien de structuur van de informatie-uitwisseling zou ik om een kopie van deze onderliggende overeenkomst en de verwerkersovereenkomst vragen.

GGD GHOR NL is een vereniging van de 25 GGD'en en de GHOR afdelingen. Puur in het kader van de AVG, zou ik o.b.v. dit document de GGD'en beoordelen als gezamenlijk verwerkingsverantwoordelijken, GGD GHOR NL als verwerker en Topicus als subverwerker. Ik realiseer me daarbij dat de zuiver juridische constructie geen recht hoeft te doen aan praktijk.

Bijgevoegd nogmaals het betreffende convenant met mijn opmerkingen. Ik ben heel benieuwd naar jullie mening.

Met vriendelijke groet,

[redacted]

[redacted]

1.9

Van: "[redacted]@drechtsteden.nl▷
Datum: dinsdag 5 mei 2020 om 10:28
Aan: [redacted]
Onderwerp: CoronIT

Hele goedemorgen,

Ik heb gisteren nog even de MS Teams meegedraaid met de FG's van andere GGD'en. En ik heb even gekeken naar het convenant met de opmerkingen van Arthur.

Gelet op de rolverdeling vind ik artikel 5 lid 4 wel apart.

Ik heb een puntsgewijs verslagje bijgevoegd van de meet via MS Teams gisteren.

Ik ben zelf o.a. nog wel benieuwd naar de selectiecriteria voor de aanbesteding, de praktische werking van de applicatie en de mogelijkheid tot onttrekken van data eruit.

Hebben jullie deze week nog tijd om te kijken?

met vriendelijke groet,

[redacted]

[redacted]

Werkdagen: maandag, dinsdag, woensdag, donderdag en vrijdagmorgen

Dienst Gezondheid & Jeugd ZHZ

Karel Lotsyweg 40 | 3318 AL Dordrecht

Postbus 166 | 3300 AD Dordrecht

[redacted]

w www.dienstgezondheidjeugd.nl

1.10
Archived: donderdag 12 mei 2022 09:29:00
From: [redacted]
Sent: maandag 25 januari 2021 13:32:55
To: [redacted]
Subject: RE: Overzicht FW: overdracht HPzone exports
Importance: Normal
Sensitivity: None

Hoi [redacted]

Vanuit de rapportageserver van CoronIT kunnen datadumps opgehaald worden door medewerkers met de autorisatierol "Onderzoeker (IZB/team onderzoek)". De volgende mensen hebben deze rol:

datum in behandeling	Achternaam	Tussen-voegsel	Voornaam	Pers.nr.	Inlognaam CoronIT
01-01-2020	[redacted]				[redacted]
01-01-2020					
01-01-2020					
14-10-2020					
06-10-2020					
25-01-2021					

Dezelfde onderzoekers hebben ook toegang tot HPZone om daar rapportages te maken. Daarnaast hebben onderstaande medewerkers dezelfde mogelijkheid:

Medewerkers met de rol "BCO Hoofdcoordinator"

datum in behandeling	Achternaam	Tussen-voegsel	Voornaam	Pers.nr.	Inlognaam CoronIT
18-09-2020	[redacted]				[redacted]
25-06-2020					
21-08-2020					
01-09-2020					
05-10-2020					
1-1-2020/25-09-2020					
10-8-2020/17-8-2020					
25-06-2020					
1-1-2020/23-07-2020					

En alle reguliere medewerkers van Team IZB plus de DIP'ers

Groeten,

[redacted]

Adviseur Informatievoorziening

Hart voor Brabant

Ringbaan West 227 Tilburg

Postbus 3024, 5003 DA Tilburg

www.ggdhvb.nl

[redacted]

Aanwezig op: di-wo-do-vr

Gezond doet leven!

Van: [redacted] <e.[redacted]ggdhvb.nl>
Verzonden: maandag 25 januari 2021 12:49
Aan: [redacted]
Onderwerp: Overzicht FW: overdracht HPzone exports

Hoi [redacted],

Heb jij een overzicht van medewerkers die een datadump kunnen maken voor beide systemen?

Met vriendelijke groeten,

[redacted]

[redacted]

[redacted]

Hart voor Brabant

Pettelaarpark 10 Den Bosch

Postbus 3024, 5003 DA Tilburg

www.ggdhvb.nl

[redacted]

Aanwezig op: ma-di-wo-do

Gezond doet leven!

Van: [redacted]>
Verzonden: vrijdag 22 januari 2021 14:37
Aan: [redacted]
CC: [redacted]
Onderwerp: RE: overdracht HPzone exports

Hoi [redacted]

Kunnen jullie [redacted] (functionaris gegevensbescherming) meenemen in deze communicatie. Zij is op zoek naar inzicht omtrent de handelingen die voor dit proces moeten worden uitgevoerd en wil graag weten welke personen deze taak op gaan pakken. Ik heb haar in de cc gezet.

Dank je.

Groet,

Daan 1.10

Met vriendelijke groet,

[redacted]

Business Analist

Hart voor Brabant

Pettelaarpark 10,

5216 PD 's Hertogenbosch

www.ggdhvb.nl

d.van.[redacted]ggdhvb.nl

Aanwezig op: ma-di-wo-do

[redacted]

Van: [redacted]
Verzonden: vrijdag 22 januari 2021 11:42
Aan: [redacted]
Onderwerp: RE: overdracht HPzone exports

Voor zover ik weet hebben HP invoer medewerkers toegang tot N schijf, maar G schijf weet ik niet. Ik ben nog aan het overleggen bij wie we dit het beste kunnen leggen. Zit zelf ook te denken aan onze procescoordinatoren. Werk vandaag niet dus zal maandag nogmaals kijken en wanneer we weten wie het gaat doen meteen authorisatie aanvragen.

Van: [redacted]
Verzonden: vrijdag 22 januari 2021 08:27
Aan: [redacted]
Onderwerp: RE: overdracht HPzone exports

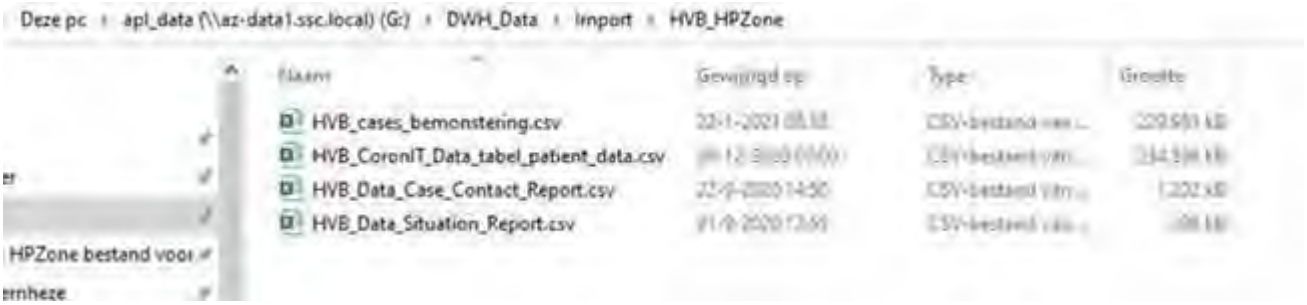
Beste [redacted]

Heel fijn!

He is wel belangrijk dat de personen die dit gaan doen toegang hebben tot HPzone en tot

onderstaande map waar zij het bestand in moeten wegschrijven.

Alvast dank!



Met vriendelijke groet,

[redacted]

onderzoeker 1.10

Vogelstraat 2 's-Hertogenbosch

Postbus 3024, 5003 DA Tilburg

www.ggdhvb.nl/onderzoek

mo.[redacted]ggdhvb.nl

Aanwezig op: ma-di-do-vr

9:30-14:30

[redacted]

Gezond doet leven!

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

Van: [redacted]
Verzonden: donderdag 21 januari 2021 12:18
Aan: [redacted]
Onderwerp: RE: overdracht HPzone exports

Hoi [redacted]

ik heb inderdaad begrepen dat jullie dit al geruime tijd doen, maar dat het een handeling is die ook elders belegd kan worden, dus fijn als we jullie daarmee kunnen ontlasten.

Ik zal het hier bespreken en dan stuur ik de uitnodiging door naar degene die dit op zich zal nemen.

Met vriendelijke groet,

[redacted]

Arts, Coordinator Bron en Contactonderzoek

Team Infectieziekten

Pettelaarpark 10, 5216 PD 's-Hertogenbosch

Postbus 3024, 5003 DA Tilburg

www.ggdhvb.nl

[redacted]ggdhvb.nl

Ma,di,wo,do

Gezond doet leven!

Van: [redacted]
Verzonden: donderdag 21 januari 2021 12:15
Aan: [redacted]
Onderwerp: overdracht HPzone exports

Beste [redacted]

Wij hebben van [redacted] begrepen dat we met jou de overdracht van de HPzone exports t.b.v corona dashboard kunnen regelen.

Wij doen dit nu al ruim 9 maanden en dragen het graag over.

Ik heb een meeting in teams ingepland.

Als jij al weet wie de exports (iedere ochtend voor 8:45) gaan uitvoeren kunnen we die personen misschien ook al uitnodigen.

Dan kunnen we zo snel mogelijk overdragen.

Alvast dank!

Met vriendelijke groet,

[redacted]

onderzoeker

GGD Hart voor Brabant

Vogelstraat 2 's-Hertogenbosch

Postbus 3024, 5003 DA Tilburg

www.ggdhvb.nl/onderzoek

mo.[redacted]ggdhvb.nl

Aanwezig op: ma-di-do-vr

9:30-14:30

[redacted]

Gezond doet leven!

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

1. Inleiding

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

1.1. Scope

Deze procesbeschrijving is van toepassing op de door het SOC uit te voeren onderzoeken naar afwijkend gedrag van medewerkers, die werken met privacygevoelige informatie. Het doel is te voorkomen dat privacygevoelige informatie door individuele medewerkers voor andere doeleinden wordt gebruikt dan waarvoor deze informatie door de GGD’en is verzameld.

1.2. *Rollen en verantwoordelijkheden*

De Manager SOC is verantwoordelijk voor de inhoud van het proces Triage en het SOC voert de onderzoeken uit, onderhoudt de procesbeschrijving en communiceert deze naar de betrokken partners.

2. Proces voor Triage

2.1. Het hoofdproces + 2.3 Subproces: Besluiten wat te doen en het starten van acties

Bij het proces Triage CoronIT worden de volgende stappen doorlopen:

1. De SOC-analist ziet mogelijk afwijkend gedrag
2. De SOC-analist doet een quick scan en eventueel een check bij een collega
3. De SOC-analist besluit of een onderzoek nodig is
4. Start van een onderzoek
5. Afronding van een onderzoek
6. Review van een onderzoek
7. Wekelijkse dossier review
8. Besluit wat te doen met het dossier en het starten van acties:
   - Niets doen
   - Verrijken van het dossier
   - Opsturen naar ketenpartner
   - Een laatste check bij de Informatiemanager GGD GHOR NL
   - Indien dossier overdragen aan de Politie: Manager SOC bij de Politie verifiëren of account van een nog actieve medewerker wel of niet moet worden dichtgezet.
   - Het dossier aanmelden bij de Politie
   - Het dossier sluiten
9. Check follow up status
10. Informeren van de CISO en CIO

Bij iedere stap geldt: de SOC-analist meldt urgente issues zo spoedig mogelijk aan de Manager SOC.

2.2. Subproces: Triageonderzoek

De te analyseren gegevens worden via verschillende kanalen zoals Topicus, FoxIT en Teleperformance aan het SOC Team verstrekt. Zodra de gegevensexports door het SOC Team zijn ontvangen, voeren de SOC-analisten verschillende screening- en controlesessies uit.

De processtappen voor het tirageonderzoek zijn:

1. Opvragen data export, oftewel de logs van Topicus met alle handelingen van de medewerkers en beheerders die toegang hebben tot CoronIT.
2. Data plaatsen in logbestanden Topicus map
3. Aanmaken onderzoeksmap (specifieke medewerker > In progress)
4. Ruwe data verwerken in Template aanleveren bewijslast
5. Opvragen call logs indien nodig
6. Data toevoegen aan template en uitvoeren van het triageonderzoek
7. Onderzoeksmap verplaatsen naar (Specifieke medewerker > Done > To do)
8. Na wekelijkse meeting besluiten om dossier over te dragen aan de Politie of niet
9. Onderzoeksmap verplaatsen naar (Specifieke medewerker > Done > Verder)
10. Onderzoeksmap verplaatsen naar (Specifieke medewerker > Done > Archive)

2.4. Door Teleperformance te leveren informatie en doelbinding

Op basis van de AVG geldt dat persoonsgegevens alleen mogen worden verwerkt om een bepaald doel te bereiken. Het doel is in dit geval om vast te stellen of een medewerker zich wel of niet aan de

gedragsregels heeft gehouden. Hiertoe mogen identificerende gegevens van medewerkers en identificerende gegevens van door hen gemuteerde of geraadpleegde patiëntdossiers worden overgedragen aan het SOC. Deze informatie is voor het SOC noodzakelijk om de analyses uit te kunnen voeren.

Logs worden bij Teleperformance opgevraagd door de informatiemanager GGD GHOR NL. In de geleverde logs staan onder andere de volgende gegevens:

-
- Dit wordt door het SOC gebruikt om te controleren welke medewerker het dossier van een specifieke patiënt heeft gemuteerd of geraadpleegd.
- Medewerkernummer: Aan de hand van dit nummer kan het gedrag van een specifieke medewerker worden geanalyseerd door het SOC.
- E-mail werk medewerker

2.5. Informatie verstrekken aan Teleperformance en doelbinding

Teleperformance levert medewerkers die calls afhandelen en testen en vaccinaties inplannen. Een onderzoeksdossier van de SOC-analist bevat persoonsgegevens van een specifiek onderzochte medewerker van Teleperformance, maar ook van andere medewerkers en van patiënten. Op basis van de AVG geldt dat persoonsgegevens alleen mogen worden verwerkt om een bepaald doel te bereiken. Het doel is in dit geval om vast te stellen of een medewerker zich wel of niet aan de gedragsregels heeft gehouden. Hiertoe mag informatie over de medewerker in kwestie worden uitgewisseld met Teleperformance, maar niet over derden zoals andere medewerkers of patiënten. Teleperformance gebruikt de verstrekte gegevens vervolgens om met de betreffende medewerker te overleggen en, indien noodzakelijk, disciplinaire maatregelen te treffen.

2.6. Informatie delen met de politie

Op het moment dat een casus of een specifieke medewerker als verdacht wordt aangemerkt, bespreekt de SOC-analist dit met een tweede SOC-analist als een dubbelcheck. Als de tweede SOC-analist het eens is met de eerste SOC-analist, meldt de eerste SOC-analist dit aan de Manager SOC.

- Indien het een GGD-medewerker betreft: De Manager SOC zal contact opnemen met de verantwoordelijke GGD, overleggen of aangifte gepast is en afstemmen wie welke vervolgstappen zal nemen. De GGD is hierin de eindverantwoordelijke, SOC kan in dit proces faciliteren en contact met de Politie verzorgen.
- Indien het een medewerker van een verwerker betreft: Manager SOC is eindverantwoordelijk voor de aangiftebeslissing en opvolging daarvan als gemandateerde van GGD GHOR NL.

2.7. Informatie delen met een GGD

Een triage-onderzoek naar een medewerker van een GGD kan worden gestart op expliciet verzoek van een geautoriseerde functionaris bij een GGD of door een SOC-analist die mogelijk afwijkend gedrag signaleert. Het SOC zal bij een vermoeden van afwijkend gedrag door een medewerker van een GGD altijd eerst contact opnemen met de betreffende GGD. Daarnaast zal het SOC alleen met expliciete en vastgelegde toestemming van de aangewezen HRM-contactpersoon of de DPG van de betreffende GGD contact opnemen met de Politie of een onderzoeksbureau.

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:

3.1

R 1115162

Dienst Justis
Ministerie van Justitie en Veiligheid

Gedragsverklaring Aanbesteden

> Retouradres Postbus 16115 2500 BC Den Haag

Timing Uitzendteam B.V.
T.a.v. [redacted]
Deventerstraat 15 2
7311 BH APELDOORN

Datum 21 februari 2019
Ons kenmerk 20190205003795
Naam rechtspersoon Timing Uitzendteam B.V.

hierna te noemen: betrokken rechtspersoon

heeft een Gedragsverklaring Aanbesteden aangevraagd.

Ik heb een onderzoek naar het gedrag van betrokken rechtspersoon en bij de rechtspersoon betrokken natuurlijke personen ingesteld. Uit het onderzoek zijn geen bezwaren gebleken tegen betrokkenen in verband met inschrijving op overheidsopdrachten, speciale-sectoropdrachten, concessieovereenkomsten voor openbare werken of prijsvragen.

Op grond van artikel 4.1 van de Aanbestedingswet geef ik de Gedragsverklaring Aanbesteden af.

De Minister voor Rechtsbescherming,
namens deze,

[redacted]

Justis, de screeningsautoriteit

Certificate of Conduct for Procurement

The Dutch State Secretary of Security and Justice has conducted an investigation into the behaviour of the person mentioned in this certificate and declares that no objections against this person have resulted from this investigation. The State Secretary hereby issues the Certificate of Conduct for Procurement, pursuant to article 4.1 of the Dutch Procurement Act.

3.1

R1115161

Dienst Justis
Ministerie van Justitie en Veiligheid

Gedragsverklaring Aanbesteden

In het kader van de Gedragsverklaring Aanbesteden met aanvraagnummer 20190205003795 zijn de volgende rechtspersonen onderzocht:

Naam rechtspersoon Timing Uitzendteam B.V.
KvK- Inschrijvingsnr 38019621
Vestigingsadres Deventerstraat 15 2
Vestigingsplaats 7311BH Apeldoorn
Land Nederland

Naam rechtspersoon ADG Beheer B.V.
KvK- Inschrijvingsnr 64166627
Vestigingsadres Plesmanweg 24
Vestigingsplaats 7602PE Almelo
Land Nederland

Justis, de screeningsautoriteit
Ministerie van Justitie en Veiligheid
Ministry of Justice and Security
Rijksoverheid
Government of the Netherlands

3.1

R 1115160

Dienst Justis
Ministerie van Justitie en Veiligheid

Gedragsverklaring Aanbesteden

In het kader van de Gedragsverklaring Aanbesteden met aanvraagnummer 20190205003795 zijn de volgende natuurlijke personen onderzocht:

Geslachtsnaam [redacted]
Tussenvoegsels
Voorna(a)m(en)
Geboortedatum
Geboorteplaats 's-Gravenhage
Geboorteland Nederland

Geslachtsnaam [redacted]
Tussenvoegsels
Voorna(a)m(en)
Geboortedatum
Geboorteplaats Heerde
Geboorteland Nederland

Justis, de screeningsautoriteit
Ministerie van Justitie en Veiligheid
Ministry of Justice and Security
Rijksoverheid
Government of the Netherlands

14-juni-2020

RAAMOVEREENKOMST

GGD HART VOOR BRABANT

YOURCE

Regionaal contact- en brononderzoek

Inhoud

Artikel 1. Onderwerp van deze Overeenkomst 3
Artikel 2. Duur van de Raamovereenkomst 4
Artikel 3. Gegevens en bestanden 4
Artikel 4. Bijzondere wet of regelgeving 5
Artikel 5. Prijzen, facturen en betalingsvoorwaarden 6
Artikel 6. Inspectie 6
Artikel 7. Intellectuele eigendomsrechten 6
Artikel 8. Geheimhouding 7
Artikel 9. Subcontractors 7
Artikel 10. Aansprakelijkheid en Verzuim 7
Artikel 11. Tussentijdse beëindiging 8
Artikel 12. Geschillen 8
Artikel 13. Toepasselijk recht 8
Artikel 14. Bijlagen, voorgaande overeenkomsten, wijzigingen en nietigheid 8

DE ONDERGETEKENDEN:

1) Gemeentelijke of Gemeenschappelijke Gezondheidsdienst, Hart voor Brabant (GGD), statutair gevestigd en kantoorhoudende te <<In te vullen door GGD>>, ingeschreven in het handelsregister van de Kamer van Koophandel onder nummer <<In te vullen door GGD>>, hierna ook te noemen: "Verantwoordelijke", hierbij vertegenwoordigd door <<In te vullen door GGD>>; hierna te noemen “GGD”;

en

2) De besloten vennootschap met beperkte aansprakelijkheid Yource Outsourcing b.v. (en alle aan haar gelieerde partijen binnen de Yource Group), statutair gevestigd en kantoorhoudende te (1311 RK) Almere aan de Louis Armstrong 26, ingeschreven in het handelsregister van de Kamer van Koophandel onder nummer 52217051, hierna ook te noemen "Verwerker", hierbij vertegenwoordigd door de heer [redacted], hierna te noemen “Yource”;

GGD en Yource worden hierna gezamenlijk aangeduid als “Partijen” en afzonderlijk als een “Partij”;

OVERWEGENDE DAT:

1) Yource houdt zich bezig met het verrichten van diensten op het gebied van contact center activiteiten ten behoeve van derden;
2) GGD aan Yource opdracht heeft gegeven tot het leveren van dergelijke dienstverlening vanuit de kantoren van Yource bestaande uit klantcontact activiteiten ter ondersteuning;
3) Partijen door middel van deze Raamovereenkomst (verder te noemen: Overeenkomst) de afspraken met betrekking tot de uitvoering van de dienstverlening wensen vast te leggen.
4) Inkoopvoorwaarden van VNG van toepassing zijn met uitzondering dat Yource positiewisselingen van onderzoekers niet hoeft te melden noch toestemming te vragen.

VERKLAREN HET VOLGENDE TE ZIJN OVEREENGEKOMEN:

Artikel 1. Onderwerp van deze Overeenkomst

1.1 Deze Overeenkomst heeft betrekking op de diensten “Inkomend- en uitgaand telefoonverkeer ter ondersteuning van bron- en contactonderzoek” dat GGD aan Yource wenst uit te besteden. De specifieke rechten en verplichtingen ter uitvoering van deze Diensten worden nader gespecificeerd in de bijlagen van deze Overeenkomst. De bijlagen maken een integraal onderdeel uit van deze Overeenkomst.

1.2 Yource zal de Diensten verlenen in overeenstemming met de doelstellingen en resultaten zoals met GGD overeengekomen en neergelegd in **Bijlage 1 Dienstenovereenkomst.**

1.3 GGD is niet verplicht om gedurende de looptijd van deze Overeenkomst opdrachten tot het verrichten van diensten te verstrekken, maar is daartoe gerechtigd. Yource kan daarom geen

aanspraak maken op exclusiviteit en het verkrijgen van opdrachten tot het verrichten van diensten gedurende de looptijd van deze Overeenkomst.

1.4 De voorwaarden van deze Overeenkomst zijn integraal van toepassing op alle nadere overeenkomsten die gedurende de looptijd van deze Overeenkomst worden afgesloten, tenzij in een nadere overeenkomst uitdrukkelijk hiervan wordt afgeweken. In een nadere overeenkomst wordt vastgelegd met betrekking tot welke specifieke diensten en gedurende welke periode de desbetreffende nadere overeenkomst wordt aangegaan. De nadere overeenkomst komt tot stand doordat Yource een contractvoorstel doet voor een nadere overeenkomst en GGD deze schriftelijk aanvaard.

Artikel 2. Duur van de Raamovereenkomst

2.1 De Raamovereenkomst wordt aangegaan voor de duur van 7maanden, ingaande 31 mei 2020 en - behoudens indien verlenging wordt overeengekomen conform lid 2 van dit artikel - van rechtswege eindigende op 31 december 2020.

2.2 Een maand voor het verstrijken van de in lid 1 van dit artikel genoemde expiratiedatum zal tussen Partijen overleg plaatsvinden over een eventuele verlenging van deze Raamovereenkomst met drie maanden. Stilzwijgende verlenging is mogelijk met een maximum van 48 maanden.

2.3 Partijen zijn gerechtigd de Raamovereenkomst tussentijds op te zeggen met in acht name van een opzegtermijn van drie (3) maanden. Ná stilzwijgende verlenging is de raamovereenkomst maandelijks opzegbaar: opzegging geldt alleen als deze schriftelijk wordt gedaan en kan alleen per kalendermaand.

2.4 Ingeval van beëindiging van deze Raamovereenkomst en/of een Opdracht zal Opdrachtnemer - voor zover redelijkerwijs verlangd kan worden - alle benodigde medewerking verlenen teneinde te bewerkstelligen dat de uitvoering door een derde dan wel GGD zelf naar behoren kan worden verricht.

Artikel 3. Gegevens en bestanden

3.1 Indien de Werkzaamheden meebrengen dat GGD gegevens, waaronder ook begrepen bestanden en applicaties (“Gegevens”) heeft aan te reiken aan Yource, dan wel dat Yource toegang dient te hebben tot zich onder GGD bevindende Gegevens (waaronder begrepen gegevens in de eigen (klant)systemen van GGD, zal GGD deze Gegevens steeds volledig, tijdig en op juiste wijze aanreiken, dan wel daartoe toegang bieden.

3.2 GGD is verantwoordelijk voor de goede werking en inrichting van haar eigen (klant)systemen alsmede voor het treffen van afdoende beveiligingsmaatregelen ten aanzien van de zich onder GGD bevindende Gegevens. GGD draagt er zorg voor via autorisatie of andere adequate beveiligingsmaatregelen dat Yource slechts toegang krijgt tot dat gedeelte van de eigen (klant)systemen van GGD en de zich onder GGD bevindende gegevens, dat nodig is voor het verrichten van de Werkzaamheden. Yource is niet aansprakelijk voor enige schade voortvloeiend uit het niet-nakomen van deze verplichting door GGD.

3.3 GGD staat in voor de juistheid en toepasbaarheid van de Gegevens. GGD staat er voorts voor in dat Yource gerechtigd is met betrekking tot de Gegevens die handelingen uit te voeren, die nodig zijn voor het verrichten van de Werkzaamheden.

3.4 Yource ontvangt dossiernummers welke tot de juiste contactinformatie leidt om de gevraagde werkzaamheden uit te voeren na inloggen in HP-zone. Het versturen van persoonsgegevens buiten de HP-zone vindt niet plaats.

3.5 Voor zover de Gegevens ook persoonsgegevens betreffen, is GGD de verantwoordelijke en Yource de bewerker in de zin van de Algemene Verordening Gegevensbescherming.

3.6 Indien deze Gegevens persoonsgegevens betreffen, is Yource niet gerechtigd andere werkzaamheden of handelingen met betrekking tot de Gegevens te verrichten dan die in het Project Plan omschreven. Yource zal, onverminderd het bepaalde in Artikel 3.2, afdoende technische en organisatorische maatregelen treffen om de persoonsgegevens te beveiligen tegen verlies of tegen enige vorm van onrechtmatige verwerking. Deze maatregelen zullen, rekening houdend met de stand van de techniek en de kosten van de tenuitvoerlegging, een passend beveiligingsniveau garanderen, gelet op de risico's die de verwerking en de aard van de te beschermen persoonsgegevens met zich brengen.

3.7 In het geval van een vermoedelijk(e) of daadwerkelijk(e) (i) data lek (inbreuk op de beveiliging die leidt tot de vernietiging, het verlies, de wijziging of de ongeoorloofde verstrekking van of de ongeoorloofde toegang tot doorgezonden, opgeslagen of anderszins verwerkte gegevens); (ii) schending van beveiligingsmaatregelen; (iii) schending van de geheimhoudingsplicht of (iv) verlies van persoonsgegevens zal Yource direct doch uiterlijk binnen 24 uur na de eerste ontdekking van het incident hierover, informeren. Yource zal alle rederlijkwijs benodigde maatregelen treffen om (verdere) onbevoegde kennisneming, wijziging, en verstrekking dan wel anderszins onrechtmatige verwerking te voorkomen of te beperken en een schending van beveiligingsmaatregelen, schending van de geheimhoudingsplicht of verder verlies van persoonsgegevens te beëindigen en in de toekomst te voorkomen, onverminderd enig recht van GGD en/of Verwerkingsverantwoordelijke op schadevergoeding of andere maatregelen.

3.8 Partijen zullen elkaar over en weer vrijwaren voor aanspraken van derden die jegens de gevrijwaarde partij mochten worden ingesteld wegen een aan de vrijwarende partij toe te rekenen schending van de AVG, tenzij de vrijwarende partij aantoont dat de betreffende schending (mede) aan de andere partij is toe te rekenen.

3.9 GGD is te allen tijde gerechtigd op eigen kosten door een register auditor te laten controleren of Yource het bepaalde in dit artikel naleeft. Yource is gerechtigd te verlangen dat de register auditor een geheimhoudingsverklaring ondertekent ten gunste van Yource. De geheimhoudingsverklaring zal die voorwaarden bevatten die gebruikelijk zijn voor dit soort verklaringen. Dergelijke controles zullen worden afgestemd met Yource, opdat de bedrijfsvoering van Yource zo min mogelijk wordt verstoord.

Artikel 4. Bijzondere wet of regelgeving

4.1 Yource verplicht zich dat alle diensten worden uitgevoerd conform, en dat alle resultaten van alle diensten voldoen aan, alle ter zake geldende wet- en regelgeving, waaronder maar niet beperkt tot regelgeving op het gebied van intellectuele eigendom en marketingcommunicatie. In Nederland vallen hieronder, doch niet uitsluitend: de Auteurswet, het Benelux-Verdrag inzake de intellectuele eigendom, het Burgerlijk Wetboek, de Telecommunicatiewet, de Algemene Verordening Gegevensbescherming, de Nederlandse Reclame Code, Wet op Oneerlijke Handelspraktijken en de Wet Koop op Afstand.

4.2 Yource is in deze als Verwerker gemachtigd om de Bijzondere Persoonsgegevens van de patiënten van de GGD conform AVG Artikel 9 lid 3 te mogen verwerken. De grondslagen voor deze Verwerking zijn vastgelegd in de Verwerkersovereenkomsten.

Artikel 5. Prijzen, facturen en betalingsvoorwaarden

5.1 De door GGD aan Yource te betalen vergoedingen voor de Werkzaamheden en overige financiële overeenkomsten zijn vermeld in **Bijlage 1, Dienstenovereenkomst.**

5.2 De administratieve gegevens van Yource zullen bepalend zijn voor de vaststelling van de verschuldigde bedragen, tenzij door GGD schriftelijk tegenbewijs wordt verschaft. Op verzoek van GGD zal Yource inzage geven in de onderliggende administratieve gegevens, zodat deze eventueel nader onderzocht kunnen worden.

5.3 Facturen zullen op wekelijkse basis door Yource worden verzonden aan GGD conform de methodiek zoals beschreven in **Bijlage 1, Dienstenovereenkomst.** Uitgangspunt is dat de uren [redacted] en GGD [redacted], zodat Yource de factuur met PO nummer [redacted] versturen. GGD stuurt de PO nummers naar het volgende emailadres: [redacted]

5.4 Facturen zullen, zonder enige vorm van verrekening, binnen 30 dagen door GGD zijn voldaan.

5.5 Indien een factuur niet binnen de genoemde termijn van 30 dagen is voldaan, heeft Yource recht, [redacted]

5.6 Alle prijzen zijn in euro's (EUR). Alle prijzen zullen worden vermeerderd met 21% BTW.

5.7 Alle prijzen zullen ieder jaar [redacted] worden aangepast overeenkomstig indexcijfer [redacted] van het Centraal Bureau voor de Statistiek, dan wel (mocht het CBS dit indexcijfer niet langer hanteren) het indexcijfer dat hiermee het meest overeenstemt. [redacted]
De formule voor het jaarlijks indexeren van de prijzen staat vermeld in **Bijlage 1 Dienstenovereenkomst**.

Artikel 6. Inspectie

6.1 Indien de Werkzaamheden worden verricht vanuit een door Yource beheerd contact center, heeft GGD het recht om te allen tijde dit contact center te inspecteren, mede in het kader van het toezicht op de naleving van het bepaalde in Artikel 3.5, op voorwaarde dat GGD Yource daarvan tijdig schriftelijk op de hoogte heeft gesteld en op voorwaarde dat GGD bij de inspectie de redelijke aanwijzingen van Yource opvolgt.

Artikel 7. Intellectuele eigendomsrechten

7.1 Niets in deze Overeenkomst kan worden opgevat als de toestemming aan een Partij voor het eigen gebruik van enig intellectueel eigendomsrecht van de andere Partij.

7.2 Niets in deze Overeenkomst kan worden opgevat als de overdracht van enig intellectueel eigendomsrecht van de ene Partij aan de andere Partij.

7.3 Alle ontwikkelingen die Yource in opdracht van de GGD heeft uitgevoerd en door de GGD is betaald, inzake scripting en content, zal na afloop van de opdracht door Yource om niet worden overgedragen. Alle ondersteunende systemen zelf blijven in bezit van Yource.

Artikel 8. Geheimhouding

8.1 Partijen zullen geen mededelingen doen aan enige derde met betrekking tot deze Overeenkomst of enige derde toestemming geven deze Overeenkomst in te zien, tenzij Partijen hierover van tevoren schriftelijk overeenstemming hebben bereikt.

8.2 Indien een Partij echter een wettelijke verplichting heeft enige mededeling te doen met betrekking tot deze Overeenkomst of een wettelijke verplichting heeft enige derde toestemming te geven deze Overeenkomst in te zien, zal deze Partij de andere Partij daarvan zo spoedig mogelijk op de hoogte stellen.

8.3 Iedere Partij zal geheimhouding betrachten ten aanzien van alle vertrouwelijke informatie met betrekking tot de andere Partij, die bij de uitvoering van deze Overeenkomst in haar bezit komt en zal deze vertrouwelijke informatie niet gebruiken voor andere doeleinden dan de uitvoering van deze Overeenkomst.

8.4 De in Artikellid 9.3 bedoelde vertrouwelijke informatie omvat de door GGD aan Yource te verschaffen Gegevens. Deze Gegevens zullen door Yource in overeenstemming met de geldende wettelijke regelgeving worden behandeld.

8.5 Yource draagt er zorg voor dat haar werknemers en de derden die betrokken zijn bij de uitvoering van deze Overeenkomst zich zullen houden aan het bepaalde in dit Artikel 9.

8.6 De werknemers die Yource inzet voor de GGD moeten een door de GGD aangeleverde geheimhoudingsverklaring ondertekenen en over een VOG beschikken. Zonder correct ondertekende geheimhoudingsverklaring en een VOG mogen de medewerkers van Yource niet werkzaam zijn voor de GGD.

Artikel 9. Subcontractors

9.1 Yource heeft het recht om, na voorafgaande afstemming van GGD, voor het verrichten van de Werkzaamheden subcontractors in te schakelen. Voor de inzet van staffunctionarissen is voorafgaande goedkeuring van de GGD benodigd.

Artikel 10. Aansprakelijkheid en Verzuim

10.1 Indien een Partij van oordeel is dat de andere Partij deze Overeenkomst niet naar behoren is nagekomen, dient zij de tekortkomende Partij daarvan, onder opgave van de tekortkoming, schriftelijk in kennis te stellen met vermelding van een redelijke termijn waarbinnen de tekortkoming dient te zijn verholpen.

10.2 Partijen zijn gehouden om de tekortkomende Partij alle medewerking te verlenen teneinde de tekortkomende Partij in staat te stellen een vermeende tekortkoming te onderzoeken en desgewenst binnen de in Artikellid 11.1 gestelde termijn te herstellen.

10.3 Indien Partijen overeenkomstig de Artikelleden 11.1 en 11.2 hebben gehandeld en de tekortkoming

niet binnen de in Artikellid 11.1 gestelde termijn is hersteld, is de tekortkomende Partij ten aanzien van haar tekortkoming aansprakelijk, mits deze aan haar dient te worden toegerekend. Iedere aansprakelijkheid voor indirecte en/of gevolgschade, waaronder geleden verlies en gederfde winst, is uitdrukkelijk uitgesloten.

10.4 De omvang van iedere aansprakelijkheid van de tekortkomende Partij is steeds beperkt tot een maximum van [redacted]

10.5 De beperking van aansprakelijkheid als bedoeld in Artikellid 11.4 is niet van toepassing in geval van opzet of bewuste roekeloosheid van leidinggevende ondergeschikten van Partijen

Artikel 11. Tussentijdse beëindiging

11.1 Indien de tekortkomende Partij de in Artikellid 11.1 bedoelde tekortkoming niet binnen de aldaar genoemde termijn heeft verholpen, heeft de andere Partij het recht de tekortkomende Partij bij aangetekend schrijven met bericht van ontvangst te berichten deze Overeenkomst tegen een datum van haar keuze te beëindigen.

11.2 Iedere Partij heeft het recht deze Overeenkomst met onmiddellijke ingang te beëindigen, indien aan de andere Partij (voorlopige) surseance van betaling is verleend of de andere Partij in staat van faillissement is verklaard dan wel haar eigen faillissement heeft aangevraagd.

Artikel 12. Geschillen

12.1 Alle geschillen die mochten ontstaan naar aanleiding van deze Overeenkomst, dan wel nadere overeenkomsten die daarvan het gevolg mochten zijn, zullen worden beslecht door de rechtbank te Den Bosch.

Artikel 13. Toepasselijk recht

13.1 Op deze Overeenkomst en alle nadere overeenkomsten die daarvan het gevolg mochten zijn, is Nederlands recht van toepassing.

Artikel 14. Bijlagen, voorgaande overeenkomsten, wijzigingen en nietigheid

14.1 De overwegingen en de aan deze Overeenkomst gehechte Bijlagen (waaronder het Project Plan) vormen een integraal onderdeel van deze Overeenkomst. Voor zover een bepaling uit de Overeenkomst strijdig is met een bepaling in een Bijlage, prevaleert het gestelde in de Overeenkomst.

14.2 Deze Overeenkomst treedt in de plaats van alle eerdere afspraken die Partijen ter zake van de Werkzaamheden voor GGD hebben gemaakt.

14.3 Deze Overeenkomst kan slechts worden gewijzigd of aangevuld door middel van door beide Partijen ondertekende stukken.

14.4 Indien enige bepaling uit deze Overeenkomst (inclusief de Bijlagen) nietig of onafdwingbaar blijkt te zijn, zal dit geen gevolgen hebben voor de geldigheid van de overige bepalingen van deze Overeenkomst.

14.5 Indien enige bepaling uit deze Overeenkomst (inclusief de Bijlagen) nietig of onafdwingbaar blijkt te zijn, zullen Partijen een vervangende bepaling vaststellen die zoveel mogelijk beantwoordt aan het doel en de strekking van de nietige of onafdwingbare bepaling.

14.6 Bij deze Raamovereenkomst horen 2 bijlagen: 1. De dienstenovereenkomst en 2. De verwerkersovereenkomst.

Getekend in tweevoud te [*vermeld plaats*] op [*vermeld datum*]

_____

[vermeld volledige statutaire naam] B.V. ***of*** N.V.

door: [vermeld naam en functie]

_____

Yource Outsourcing b.v.

door: [redacted]

11-augustus-2020

ADDENDUM

GGD HART VOOR BRABANT

YOURCE

Regionaal contact- en brononderzoek

ADDENDUM:

Behorend bij de Raamovereenkomst contact center activiteiten d.d. 24 juni 2020 tussen Gemeentelijke of Gemeenschappelijke Gezondheidsdienst, Hart voor Brabant en Yource Outsoucing b.v.

DE ONDERGETEKENDEN:

1) Gemeentelijke publiekrechtelijke rechtspersoon Gemeentelijke of Gemeenschappelijke Gezondheidsdienst, Hart voor Brabant (GGD), statutair gevestigd en kantoorhoudende te 5216PD te 's-Hertogenbosch aan de Pettelaarpark 10 ingeschreven in het handelsregister van de Kamer van Koophandel onder nummer 17247544 hierna ook te noemen: "Verantwoordelijke", hierbij vertegenwoordigd door [redacted]; hierna te noemen "GGD";

en

2) De besloten vennootschap met beperkte aansprakelijkheid Yource Outsourcing b.v. (en alle aan haar gelieerde partijen binnen de Yource Group), statutair gevestigd en kantoorhoudende te (1311 RK) Almere aan de Louis Armstrong 26, ingeschreven in het handelsregister van de Kamer van Koophandel onder nummer 52217051, hierna ook te noemen "Verwerker", hierbij vertegenwoordigd door de [redacted], hierna te noemen "Yource";

GGD en Yource worden hierna gezamenlijk aangeduid als "Partijen" en afzonderlijk als een "Partij";

OVERWEGENDE DAT:

1) Dit addendum behoort bij de door de Gemeentelijke of Gemeenschappelijke Gezondheidsdienst, Hart voor Brabant en Yource Outsoucing b.v. aangegane raamovereenkomst contact center d.d. 24 juni 2020 inzake diensten op het gebied van contact centeractiviteiten;
2) Partijen aanvullende afspraken hebben gemaakt ten aanzien van artikel 7.1 uit de Dienstenovereenkomst;
3) Partijen het vorenstaande in dit addendum op de Hoofdovereenkomst wensen vast te leggen;
4) De in de Hoofdovereenkomst geldende definities hebben dezelfde betekenis in dit addendum.

VERKLAREN HET NAVOLGENDE EN KOMEN OVEREEN ALS VOLGT:

Aanvullende afspraken

Artikel 7.2 uit de Dienstenovereenkomst wordt aangevuld als volgt:

- De Yource BCO onderzoekers ontvangen [redacted] per uur [redacted]
- Het uurtarief per onderzoeker [redacted]
- Ingangsdatum: 31 augustus 2020

De Hoofdovereenkomst, inclusief de hiermee gemaakte wijziging(en), blijft onverkort tussen Partijen van kracht.

Getekend in tweevoud te [*vermeld plaats*] op [*vermeld datum*]

_____

GGD Hart voor Brabant

door: [redacted]

_____

Yource Outsourcing b.v.

door: [redacted]

Aanbiedingsbrief

Apeldoorn, 25 januari 2021

Geachte leden van het beoordelingsteam,

Met veel zin en overtuiging biedt Timing Uitzendteam B.V. (hierna: Timing) u hierbij haar voorstel aan voor de inhuur van administratieve uitzendkrachten ten behoeve van perceel 6. Met onze aanbieding willen wij ons graag voorstellen om vervolgens een succesvolle samenwerking aan te gaan.

Voor u is Timing geen onbekende, want in de periode 2010-2014 hadden wij ook een overeenkomst voor het perceel administratie. Toch willen wij ons nog even kort voorstellen. Timing is onderdeel van de ADG dienstengroep. ADG dienstengroep heeft haar oorsprong in het door [redacted] in 1952 opgerichte schoonmaakbedrijf Asito. Alle Stof In Twente Opruimen, zo begon het 65 jaar geleden. Inmiddels bestaat ADG uit elf groepsmaatschappijen met in totaal 50.000 medewerkers, waar Timing ook toe behoort. ADG een 100% familiebedrijf.

Sinds 1994 zijn wij, Timing, actief als uitzendorganisatie, met onze eerste vestiging in Coevorden. Met een landelijke dekking en een hoofdkantoor in Apeldoorn en ruim 950 medewerkers zijn er dagelijks ongeveer 15.000 uitzendkrachten werkzaam bij uiteenlopende opdrachtgevers van logistiek tot overheid, van ziekenhuizen tot callcenters en van schoonmaak tot productie. Hiermee behoren wij tot de top drie van grootste uitzenders in Nederland. Met meerdere vestigingen in Brabant, waaronder Tilburg zijn wij goed vertegenwoordigd in uw verzorgingsgebied. Mede door de overname van In Person in 2019 is ons vestigingennetwerk en aantal ingeschreven kandidaten nog verder toegenomen.

Als flexpartner zien wij het als onze taak om u volledig te ontzorgen in het gehele flexproces, levering te garanderen en u van actuele strategische informatie te voorzien. Dit doen wij door werk en alles daaromheen makkelijker, sneller en slimmer in te richten, vanzelfsprekend binnen de kaders en doelen die we hiervoor zijn bepaald. Om een succesvolle samenwerking aan te gaan, doen wij een realistisch voorstel waarbij niet alleen kwantiteit belangrijk is, maar ook kritisch gekeken wordt naar de kwaliteit van de dienstverlening om levering te allen tijde te blijven realiseren.

Timing, als uitzendspecialist, heeft ruime ervaring met de door de u omschreven taakgebieden zoals:

- Leveren van Uitzendkrachten binnen meerdere GGD’s;
- Korte- en directe communicatielijnen met vaste aanspreekpunten;
- Leveren op een basis (adhoc) aanvragen met uiteenlopende wensen en een grote diversiteit aan functies;
- Adhoc voorzien in uw flexbehoefte;
- Organiseren van adequate (digitale) managementinformatie en documentatie;

Voorstel

In onderliggend voorstel nemen wij u mee in de dienstverlening die wij u gaan bieden. Ons voorstel is toekomstgericht en gebaseerd op behaalde resultaten bij soortgelijke inleners en aandachtspunten uit uw bestek en nota van inlichtingen. Belangrijke uitgangspunten in ons voorstel zijn:

- De communicatie met aangesloten opdrachtgevers als uitzendkrachten is proactief;
- U heeft een single point of contact voor al uw (aan)vragen;
- Levering op alle functies binnen gestelde termijn volgens gestelde leveringspercentages;
- Meedenken in procesoptimalisatie door inzet van innovatieve instrumenten;
- Kwaliteit en kwantiteit van levering door goede samenwerking met uw andere contractpartner;
- Een zeer goede kwaliteit van onze totale dienstverlening, die jaarlijks beoordeeld moet worden met een cijfer > 8.

Ons personeel is uw visitekaartje

Uitgaande van de visie van Timing om praktische en resultaatgerichte oplossingen te bieden aan uw organisatie, betekent ook dat zij hoge eisen stelt aan haar interne HRM-beleid in het algemeen en haar personeel in het bijzonder. Medewerkers op onze vestiging moeten immers optreden als visitekaartje voor opdrachtgever. Timing investeert dan ook in haar medewerkers en voert een actief opleidings-, trainings- en certificeringsbeleid vanuit haar eigen talentacademie, om de professionaliteit en deskundigheid op hoog niveau te houden. Naast uw vaste contactpersoon en diens back-up stelt Timing na gunning een groter team samen, dat primair verantwoordelijk is voor uw totale flexbehoefte.

Mocht u naar aanleiding van deze inschrijving nog vragen of opmerkingen hebben, dan kunt u te allen tijde contact opnemen met [redacted], telefoonnummer [redacted].

Timing vertrouwt er op dat zij u een passend voorstel heeft gedaan en kijkt uit naar een prettige samenwerking.

Met vriendelijke groet,
Timing Uitzendteam B.V.

[redacted]
[redacted]

[redacted]
[redacted]

26 juni 2020

Addendum - Dienstenovereenkomst

GGD Hart voor Brabant

YOURCE

Inhoud

BEPALINGEN ADDENDUM 4
KOSTENOVERZICHT 5
ONDERTEKENING 5

DE ONDERGETEKENDEN:

1) De publiekrechtelijke rechtspersoon Gemeentelijke of Gemeenschappelijke Gezondheidsdienst, Hart voor Brabant (GGD), statutair gevestigd en kantoorhoudende te 's-Hertogenbosch aan het Pettelaarpark 10, ingeschreven in het handelsregister van de Kamer van Koophandel onder nummer 17.24.75.44 hierna ook te noemen: "Verantwoordelijke", hierbij vertegenwoordigd door mevr. [redacted], hierna te noemen "GGD";

en

2) De besloten vennootschap met beperkte aansprakelijkheid Yource Outsourcing b.v. (en alle aan haar gelieerde partijen binnen de Yource Group), statutair gevestigd en kantoorhoudende te (1311 RK) Almere aan de Louis Armstrong 26, ingeschreven in het handelsregister van de Kamer van Koophandel onder nummer 52217051, hierna ook te noemen "Verwerker", hierbij vertegenwoordigd door de heer [redacted], hierna te noemen "Yource";

GGD en Yource worden hierna gezamenlijk aangeduid als "Partijen" en afzonderlijk als een "Partij";

IN AANMERKING NEMENDE DAT:

1) Partijen een Raamovereenkomst met daaraan een Dienstenovereenkomst, Verwerkersovereenkomst en een Geheimhoudingsverklaring hebben gesloten m.b.t. tot het uit voeren van telefonische werkzaamheden in het kader van Bron- en Contactonderzoek.
2) Partijen in aanvulling op de Dienstenovereenkomst de volgende afspraken wensen vast te leggen in onderhevig addendum (hierna te noemen: het "Addendum")

OVERWEGENDE DAT:

1) De initieel overeengekomen afname, zoals beschreven in de Dienstenovereenkomst, wordt aangepast naar de in dit Addendum opgenomen afname volumes.
2) Vernietiging of nietigheid van één der bepalingen van dit Addendum tast de rechtsgeldigheid van de overige bepalingen niet aan. Wijzigingen van de voorwaarden en condities van dit Addendum dienen schriftelijk tussen Partijen te worden overeengekomen.
3) De overige bepalingen van de Dienstenovereenkomst blijven onverkort van kracht. In geval van strijdigheid tussen dit Addendum en de Dienstenovereenkomst, prevaleert dit Addendum.

BEPALINGEN ADDENDUM

1.1. In tegenstelling tot hetgeen opgenomen in artikel 8.2 van de Dienstenovereenkomst zal Yource in de implementatiefase een groep van [redacted] medewerkers opleiden tot de functie “Bron- en contactonderzoeker”.

1.2. In tegenstelling tot hetgeen opgenomen in artikel 8.3 van de Dienstenovereenkomst gaat Yource een standaard weekbezetting verzorgen waarin een basisgroep BCO-onderzoekers vanuit Yource minimaal [redacted] Bron – en Contactonderzoeken per dag zal verwerken.

1.3. Aanvullende aan de basisgroep ingepalnde BCO-onderzoekers, welke minimaal [redacted] Bron- en Contactonderzoeken kunnen afhandelen, plant Yource standaard een standby-groep BCO-onderzoekers in, welke minimaal [redacted] Bron- en Contactonderzoeken per dag aanvullend kunnen verwerken.

1.4. De vergoeding voor de ingeplande uren van de standby-groep BCO-onderzoekers [redacted] Yource brengt [redacted] van de ingeplande uren per week van de stand-by groep BCO-onderzoekers in rekening bij GGD Hart voor Brabant, conform de in artikel 9 van de Dienstenovereenkomst opgenomen facturatieprocedure.

1.5. Op basis van de in 1.2. genoemde basisgroep BCO-onderzoekers kan Yource het aantal Bron- en Contactonderzoeken per dag opschalen naar [redacted] stuks.

1.6. Indien het dag aanbod Bron – en Contactonderzoeken boven het in 1.3 vastgestelde maximum komt te liggen, waardoor Yource structureel de basisgroep BCO-onderzoekers zal moeten vergroten, wordt in onderling overleg vastgesteld in welke mate, tegen welke vergoeding en binnen welke termijn Yource de basisgroep BCO-onderzoekers kan vergroten.

1.7. Naast de basisgroep BCO-onderzoekers en de standby-groep BCO-onderzoekers blijven de in de Dienstenovereenkomst geformuleerde functies in het besturingsapparaat, zoals omschreven in artikel 8.3, gelijk. Dit betreffen de functies, [redacted]

KOSTENOVERZICHT

BASELINE - GGD Hart voor Brabant							
Functies - Besturingsapparaat		**Minimaal aantal BCO**	**uur per BCO**	**min uren per dag**	**min uren per week**	**uurtarief excl. 21%**	**Kosten per week**
Basisgroep BCO-onderzoekers	(individuele medewerkers)						
Standbygroep BCO-onderzoekers							
BCO-onderzoeker - MV (senior onderzoeker)							
Teamleiders (teamleider)							
Trainer							
Project Manager							
	Totale kosten per week						

MAXIMAALE OPSCHALING - GGD Hart voor Brabant							
Functies - Besturingsapparaat		**Maximaal aantal BCO**	**uur per BCO**	**min uren per dag**	**min uren per week**	**uurtarief excl. 21% Btw**	**Kosten per week incl. Btw**
Basisgroep BCO-onderzoekers	(individuele medewerkers)						
Standbygroep BCO-onderzoekers							
BCO-onderzoeker - MV (senior onderzoeker)							
Teamleiders (teamleider)							
Trainer							
Project Manager							
	Totale kosten per week						

ONDERTEKENING

Aldus in tweevoud opgemaakt en ondertekend, op 26 juni 2020

Namens GGD Hart voor Brabant,

Namens Yource Outsourcing B.V.

3.8

Supervisieplan uitvoering BCO's GGD HvB door Yource.

Inleiding
GGD Hart voor Brabant heeft als opdracht gekregen vanuit GGD GHOR om voldoende capaciteit te organiseren om tot 37 BCO's Corona uit te kunnen voeren. GGD Hart voor Brabant kiest er hierbij voor om een groot deel van deze capaciteit uit te laten voeren door regionale samenwerkingspartner Yource. Desondanks dat het geen voorbehouden handeling betreft, ligt de formele regie en verantwoordelijkheid bij de arts M&G infectieziekten. In dit document is uitgewerkt hoe GGD HvB concreet invulling geeft aan de supervisierol op het werk dat Yource namens GGD Hart voor Brabant uitvoert.

Vereisten medewerkers Yource
Alle medewerkers van Yource tekenen voor zij starten met het uitvoeren van BCO-werkzaamheden een geheimhoudingsverklaring. Ook dienen zij een Verklaring Omtrent Gedrag te kunnen overleggen. GGD voert hier steekproefsgewijs controle op uit. BCO-medewerkers van Yource zijn niet perse medisch onderlegd, met uitzondering van de meewerkend voormannen/-vrouwen.

Geprotocolleerd werken
Yource voert haar werk uit vanuit de naam van GGD Hart voor Brabant. Zij werkt daarbij als een verlengde arm van de GGD. Yource maakt voor haar werk gebruik van de werkwijze de GGD heeft ontwikkeld. Op een sharepointsite die voor alle medewerkers BCO van GGD en Yource en toegankelijk is (https://hetservicecentrum.sharepoint.com/sites/HvBPBCO) staan ten alle tijden de meest actuele versies van procesbeschrijvingen, werkinstructies en informatiebrieven. De regie voor de juistheid van deze procesbeschrijvingen is belegd bij de verpleegkundigen IZB van de GGD. BCO-medewerkers kunnen geen wijzigingen aanbrengen in deze documenten. Het is voor medewerkers van Yource niet toegestaan om afdrukken te maken van werkinstructies, omdat we hen vragen altijd volgens de meest actuele instructie te werken. Eens per week informeert de GGD alle gebruikers over wijzigingen in instructies.

Kwaliteitsvereisten en kwaliteitsbeoordeling
De kwaliteitseisen ten aanzien van registratie zijn vastgelegd in invulformats. Deze formats zijn onderdeel van de werkinstructies op Sharepoint. In de invulformats kan de medewerker van Yource precies zien welke velden gevuld moeten worden en op welke manier. Vanuit GGD HvB is een toezichthouder HP aangewezen die op alle werkdagen controleert of registratie op correcte wijze wordt uitgevoerd (zowel qua proces als qua inhoud registratie). Als er problemen worden gesignaleerd worden deze direct teruggekoppeld aan Yource en de verpleegkundigen IZB, zodat noodzakelijke acties ingezet kunnen worden (zoals aanspreken medewerkers / aanpassen werkinstructies).

Om te toetsen of BCO inhoudelijk juist is uitgevoerd zet GGD Hart voor Brabant BIG-geregistreerde artsen in om de BCO's te beoordelen voordat deze afgesloten worden. Yource sluit nooit zelfstandig een BCO af, maar legt deze altijd ter controle voor aan de dienstdoende arts*. Mocht deze twijfelen over de correcte afhandeling, dan stemt hij/zij hierover af met de dienstdoende arts M&G infectieziekten. Bij het constateren van onvolledigheden door de arts wordt dit aangegeven bij de BCO-medewerker met daarin de aanvullende acties die nog benodigd zijn.

Complexe vragen tijdens kantooruren (8.30 uur tot 16.30 uur)
Bij beantwoording van vragen gebruikt Yource altijd de richtlijnen van het LCI en het RIVM. Als de richtlijnen onverhoopt geen antwoord geven stemt de BCO-medewerker af met de meewerkend voormannen/-vrouwen. Als zij geen antwoord kunnen geven of hierover twijfelen stemmen zij dit af met de BCO coördinator van de GGD. Deze coördinator stemt waar nodig weer af met verpleegkundige/arts IZB.

Complexe vragen buiten kantooruren (16.30 uur tot 08.30 uur)
Yource belt mensen tussen acht uur in de ochtend en acht uur in de avond. Buiten onze kantoortijden kan in uitzonderlijke situaties, waarbij twijfel is of een complexe BCO tot de volgende dag kan wachten, de manager van Yource bellen met de provinciale achterwacht arts zodat de GGD intern kan opschalen. Denk aan situaties waarbij mogelijk media aandacht te verwachten is. Vragen die kunnen wachten worden de volgende ochtend volgens het proces "complexe vragen tijdens kantooruren" opgepakt.

Complexe casuïstiek
De coördinator BCO van de GGD voert op basis van het triagemodel complexe casuïstiek (zie bijlage) triage uit op alle benodigde BCO's. De meest complexe casuïstiek voert de GGD zelf uit. De overige casussen worden aan een situation Yource gehangen, waarna Yource deze oppakt. Als Yource gedurende het uitvoeren van een BCO tegen complexe problematiek aanloopt of als er signalen zijn dat er mogelijk sprake is van clustervorming en/of betrokkenheid (zorg)instellingen dan stemmen zij via de voorman van Yource en de coördinator BCO af of Yource deze BCO kan afmaken of dat deze wordt overgedragen aan de GGD. Met het geven van een overdracht wordt niet gewacht tot einde van de werkdag. De GGD BCO coördinator werkt dagelijks relevante signalen voor Yource bij in de situation "Signalen van Yource en GGD" zo dat zij op de hoogte zijn van belangrijke signalen bij de GGD. Yource plaatst bijzonderheden in events per casus in deze situation welke dagelijks beoordeelt worden door de arts die BCO's van Yource checkt.
Uitgangspunt is dat Yource alleen contact heeft met individuele patiënten en contacten. Contact met instellingen, organisaties of bedrijven doet de GGD zelf. Complexe casussen zijn bijvoorbeeld clusters van kwetsbare mensen (zorg setting, school, opvang etc.) of kans op overdracht via personeel. Individueel kunnen casussen complex zijn als er bijvoorbeeld een taalbarrière is, een verstandelijke beperking of iemand is arbeidsmigrant.

Kwaliteitsoverleg
Yource gaat vanaf 15 juni steeds meer BCO's uitvoerend namens GGD Hart voor Brabant. Tijdens de eerste twee weken wordt iedere dag om 4 uur (als ook de caseload voor de volgende dag wordt besproken) besproken in hoeverre er kwaliteitsissues zijn ontstaan. Bij dit overleg is een verpleegkundige IZB aanwezig die waar nodig de Arts M&G IZB informeert / aansluit. Na twee weken samenwerking vind een groot kwaliteitsoverleg uitvoering BCO plaats waarbij ook de arts M&G IZB aansluit. Dan wordt bepaalt met welke frequentie het kwaliteitsoverleg verder opgepakt moet worden.

Dataveiligheid en privacy
Yource maakt gebruik van HP Zone voor de registratie. Als HP Zone Light volledig operationeel is stapt Yource over op het gebruik van HP Zone Light. Groot voordeel hierbij is dat de medewerkers van Yource vanaf dat ogenblik niet langer bij niet Corona gerelateerde casussen kunnen. Tot de tijd dat dit georganiseerd is voert de GGD controles uit (in de persoon van de HP Toezichthouder) om te kijken of geen dossiers worden geraadpleegd die niet tot het taakpakket van Yource horen.
In email en Whatsapp contact tussen GGD en Yource wordt gecommuniceerd over HP-nummers, namen worden niet genoemd. In de rapportage in HP zone worden in een case géén namen genoteerd van andere mensen. Contacten, andere cases of situations kunnen aan een case of gehangen worden om informatie te bundelen.

* Mocht na een maand blijken dat het werken goed functioneert kan de taak wellicht worden gedelegeerd naar een hiervoor opgeleide (IZB)verpleegkundige.

3.9

Werkafspraken Yource – GGD HvB

BCO Corona

Processtappen	Basis activiteit	Notitie
A. HP Zone & privacy	Als HP Zone light beschikbaar komt stapt Yource hier zo snel als mogelijk op over. Voor medewerkers die in HP Zone (regulier) werken geldt dat zij tekenen voor geheimhoudingsverklaring (als onderdeel van personeelsregistratieformulier GGD) en dat zij beschikken over een verklaring omtrent gedrag. Casuïstiek op te pakken door Yource wordt door coördinator BCO op de GGD in HP zone onder “situation Yource” gehangen. Overige casuïstiek wordt door Yource niet opgepakt. In mails en Whatsapp contact tussen GGD en Yource wordt gecommuniceerd over HP-nummers, namen worden niet genoemd. In de rapportage in HP zone worden in een case géén namen genoteerd van andere mensen. Contacten, andere cases of situations kunnen aan een case of gehangen worden om informatie te bundelen.	GGD voert controles uit of geen dossiers worden geopend waar toegang niet noodzakelijk is. GGD vraagt middels steekproeven VOG op.
B. Achterwacht	Yource werkt met BCO medewerkers 10-15 per team met 1 medisch onderlegde voorman. Deze medisch voorman is coördinator BCO van dit team en schakelt met de BCO coördinator van de GGD bij vragen op inhoud. BCO coördinator van Yource/GGD schakelt zo nodig met de IZB vpk/arts op de werkvloer BCO.	
C. Kwaliteit en supervisie	Kwaliteitstoetsing op inhoud van BCO’s door Yource vindt in de eerste 2 weken dagelijks plaats door een arts van de GGD onder supervisie van de arts M&G Infectieziekten. Yource maakt na afronding van het BCO een actie aan voor de GGD arts “[redacted]” genaamd “Yource BCO nakijken & sluiten” voor de volgende dag. Hiernaast wordt de BCO casus aan de situation “5. BCO Klaar nakijken”.	GGD actie: Eventueel ondersteuning 2e arts, 37 BCO’s per dag checken = te veel
D. Bereikbaarheid	De GGD is iedere dag bereikbaar voor Yource, ook in het weekend, 08.30-17.00 uur. Buiten deze tijden kan in uitzonderlijke situaties, waarbij twijfel is of een complexe BCO tot de volgende dag kan wachten contact opgenomen worden met de provinciale achterwacht arts. Denk aan situaties waarbij mogelijke media aandacht wordt verwacht. Alléén de manager van Yource mag in geval van nood contact opnemen met de provinciale achterwacht.	Telefoonnummer [redacted] in te loggen door BCO coördinator op GGD als Yource coördinator niet meer dagelijks op GGD is.
E. Overdracht	Yource doet ook complexe BCO’s. De Voorman BCO schakelt bij vragen direct met de BCO coördinator op de GGD. Met het geven van een overdracht wordt niet gewacht tot einde van de werkdag. De GGD BCO coördinator werkt dagelijks relevante signalen voor Yource bij in de situation Signalen van Yource en GGD zo dat zij op de hoogte zijn van belangrijke signalen bij de GGD. Yource plaatst bijzonderheden in events per casus in deze situation welke dagelijks beoordeelt worden door de arts die BCO’s van Yource checkt.	

BCO Corona

F.	Omgang complexe casuïstiek	Uitgangspunt is dat Yource alleen contact heeft met individuele patiënten en contacten. Contact met instellingen, organisaties of bedrijven doet de GGD zelf. Complexe casussen zijn bijvoorbeeld clusters van kwetsbare mensen (zorg setting, school, opvang etc.) of kans op overdracht via personeel. Individueel kunnen casussen complex zijn als er bijvoorbeeld een taalbarrière is, een verstandelijke beperking of iemand is arbeidsmigrant	Triagemodel complexe casuïstiek

24-juni-2020

DIENSTOVEREENKOMST

GGD HART VOOR BRABANT

YOURCE

Regionaal contact- en brononderzoek

Inleiding 3
Beschrijving Dienstverlening 4
Service Level afspraken 6
Forecasting 8
Training 10
Quality Monitoring (QM) 13
Rapportage 14
Tarieven 15
Implementatie; kosten en doorlooptijd 17
Facturatieproces 20
Calamiteiten 22
Change management procedure 23
Communicatie & betrokkenheid 26
ICT 29

Inleiding

Dit betreft de Dienstenovereenkomst tussen GGD Hart voor Brabant (hierna te noemen Opdrachtgever) en Yource Outsourcing b.v. (hierna te noemen Opdrachtnemer) die een bijlage vormt bij de Raamovereenkomst 2020. (Hierna te noemen Hoofdovereenkomst).

In deze Dienstenovereenkomst wordt het stelsel van afspraken met betrekking tot samenwerking, sturing, doelstellingen en operationele uitvoering in detail beschreven. Deze Dienstenovereenkomst heeft dezelfde looptijd als de Hoofdovereenkomst. Bij het aflopen van de Hoofdovereenkomst, handelt Opdrachtnemer de reeds in behandeling genomen Bron-en Contactonderzoeken (BCO's) af. Ook indien deze afhandeling na de afloopdatum van deze Hoofdovereenkomst en Dienstovereenkomst plaatsvindt. Opdrachtgever en Opdrachtnemer bespreken het afschaalscenario, mocht deze situatie zich voordoen.

De Dienstenovereenkomst zal minimaal 1 maal per half jaar worden geëvalueerd. In overleg tussen de partijen kunnen ook tussentijds bijstellingen plaats vinden van de Dienstenovereenkomst. Deze bijstellingen kunnen alleen schriftelijk overeengekomen worden conform met de Hoofdovereenkomst.

In de kwartaal overleggen worden de wijzigingsformulieren (hierna RFC's) van het afgelopen kwartaal besproken en waar nodig vertaald naar een aanpassing van de Dienstenovereenkomst.

In de periodieke Review tussen Opdrachtgever en Opdrachtnemer zullen de wijzigingen en gewenste wijzigingen worden besproken, tevens zal de Dienstenovereenkomst worden geëvalueerd en zal deze met de doorgevoerde wijzigingen schriftelijk worden geformaliseerd conform de Hoofdovereenkomst.

Beschrijving Dienstverlening

1.1 Inleiding

Het hoofddoel bij de afhandeling van alle contact center activiteiten is het uitvoeren van het bron- en contact onderzoek (BCO) in het kader van de COVID-19 uitbraak conform het kernproces in bijlage 4 van de Dienstovereenkomst. Opdrachtnemer staat ervoor in dat hij de dienstverlening conform deze Dienstovereenkomst en meer in het bijzonder conform het kernproces in bijlage 4 en de offerte in bijlage 6 zal uitvoeren. Op dagelijkse basis worden er door de landelijke huisartsen, de GGD-en alsmede via diverse kanalen COVID-19 testen afgenomen. Vervolgens ontvangt de GGD de dossiers, van positieve uitslagen, digitaal en voert een eerste triage uit.

De index patiënten die positief op COVID-19 worden getest, worden gebeld door een telefonische onderzoeker. Vervolgens vindt er aan de hand van een vragenlijst een inventarisatie plaats van het risicoprofiel en de contacten die de patiënt in de afgelopen periode heeft gehad.

Die contacten worden ook weer telefonisch benaderd en gemotiveerd om thuis in quarantaine te gaan. Op die manier ontstaat inzicht in de omvang van de verspreiding van het virus en kan verdere uitbraak beperkt blijven.

Gezien de vertrouwelijkheid van de gesprekken is het van belang dat er gekwalificeerde onderzoekers worden ingezet en dat er wordt gestuurd op kwaliteit. Daarbij wordt gestuurd op de volgende parameters:

- Volledigheid van dossiervulling
- Juistheid van informatie

1.2 Contact kanalen

Dagelijks worden er in de middag dossiers met index patiënten op naam van Opdrachtnemer gezet in HP Zone. Deze patiënten moeten uiterlijk binnen 24 uur gebeld worden. Indien een patiënt niet kan worden bereikt, wordt er een nieuwe belpoging in een ander tijdsvenster ingepland. Tevens en indien mogelijk laat Opdrachtnemer een voicemail bericht achter bij indexpatiënten waarin hen wordt verzocht telefonisch contact op te nemen met Opdrachtnemer.

Support matrix

1.2.1 Index patiënten

In bijlage 1 is een samenvatting van de logging tabel opgenomen welke voorziet in de supportmatrix van de contacten. Dit overzicht geeft een overzichtelijk beeld van alle activiteiten die Opdrachtnemer op verzoek van Opdrachtgever verricht.

De samenvatting van deze logging tabel beperkt zich in de bijlage tot:

- Onderwerp

- Reden

1.2.2 Locatie contact center

Opdrachtnemer zal haar diensten vanuit de [redacted] te Nijmegen uitvoeren en deels vanuit huis waarbij Yource gedurende de startfase (train-de-trainer) ook vanaf het kantoor van de GGD Breda werkt. Op de locatie Breda zal dagelijks een medewerker van Yource werkzaam zijn. Indien Opdrachtnemer haar diensten vanuit een andere site wil uitvoeren, zal zij hiervoor in overleg treden met Opdrachtgever. Bij een eventuele verhuizing van de diensten naar een andere site garandeert de Opdrachtnemer de kwaliteit van de diensten en blijft Opdrachtnemer voldoen aan de overeengekomen KPI's.

1.2.3 Openingstijden contactcenter

Bij aanvang van de overeenkomst zijn de openingstijden als volgt:

	Ma t/m vr	Zat/zon
Openingstijden	08:00 – 20:00 uur	08:00 – 20:00 uur

Op onderstaande feestdagen is het Contact Center gesloten:

- 1e en 2e kerstdag; Oud- en Nieuwjaar
- 1e en 2e paasdag
- Koningsdag
- Hemelvaartsdag
- 1e en 2e Pinksterdag

In overleg en vastgelegd via RFC kan hiervan worden afgeweken en dit wordt in de Forecast opgenomen.

Service Level afspraken

2.1 Inleiding
Bij de beschrijving van de Service Level afspraken wordt onderscheid gemaakt tussen Key Performance Indicators (KPI) en Performance Indicators (PI). De KPI's vormen de basis van de servicelevel afspraken waarbij de PI's fungeren als indicator van achterliggende processen. De indicatie kan helpen bij het verhogen van het inzicht in de performance voor zowel Opdrachtgever als Opdrachtnemer.

De normen zoals opgenomen bij de KPI's gelden als bindend (resultaatsverbintenissen) terwijl de normen behorende bij de PI's inspanningsverbintenissen vormen. Significante afwijkingen in de PI's worden besproken tussen Opdrachtgever en Opdrachtnemer in relatie tot mogelijk impact op de KPI-performance.

De overeengekomen doelstellingen van de Service Level afspraken gelden voor de openingstijden zoals beschreven in hoofdstuk 2.

2.2 Evaluatie en vaststelling Service Level Afspraken
In de review zullen de Servicelevel afspraken, zoals opgenomen in hoofdstukken 3.3. en 3.4 worden geëvalueerd, vastgesteld en geformaliseerd. Onder servicelevel afspraken wordt verstaan [redacted]

2.3 Key Performance Indicators

- In [redacted]% van de dossiers per week vindt de 1ste belpoging binnen [redacted] uur, na overdracht van het dossier door de GGD aan Yource, plaats.

- Opdrachtgever draagt ervoor zorgt dat hij gedurende de looptijd van de Overeenkomst ten minste voldoende gekwalificeerd personeel beschikbaar is voor de GGD om [redacted]% van het maximaal af te nemen werkaanbod uit te voeren;

- Van alle afgehandelde BCO's per week is [redacted]% volledig ingevuld, conform instructies van de GGD,

- Van alle afgehandelde BCO's per week is [redacted]% correct ingevuld, o.b.v. de door patiënt verschafte gegevens,

- Opdrachtnemer doet binnen [redacted] dagen na overdracht van het dossier door de GGD aan Yource [redacted] belpogingen per BCO alvorens we deze als "niet bereikbaar" beschouwen.

- [redacted]% van de dossiers wordt afgehandeld in de cyclus van [redacted] en [redacted] dagen "follow-up"

2.4 Performance Indicators

- Onderzoekers voldoen aan de beoogde gesprekstechnieken (format op te leveren door GGD).

- Opdrachtnemer heeft altijd beschikking over door GGD beschikbaar gesteld medisch geschoold personeel t.b.v. het BCO-onderzoeksteam

2.5 Niet Meetbare dagen

Bij Niet Meetbare dagen is sprake van bijzondere omstandigheden die buiten de invloedssfeer van de Opdrachtnemer liggen waardoor niet meer redelijkerwijs van de Opdrachtnemer kan worden verlangd dat de service level doestellingen op die dag worden behaald.

Van een Niet Meetbare dag is onder meer sprake:

- Bij een telefonisch verkeersaanbod dat [redacted]% of meer boven het geprognosticeerde volume ligt
- Bij systeemstoringen aan de systemen van GGD.
- Bij overmacht en calamiteiten.

Indien een van de hiervoor opgesomde oorzaken zich voordoet dan meldt Opdrachtnemer dat onverwijld aan Opdrachtgever. Een tekort aan personeel wordt in ieder geval niet tot overmacht of calamiteit gerekend. Opdrachtnemer zal niet later dan [redacted] GGD informeren over de invloed van een voorval dat leidt tot een Niet Meetbare dag gedurende deze week.

In elk [redacted] worden de Niet Meetbare dagen besproken en onderbouwd toegelicht door Opdrachtnemer in overleg met Opdrachtgever.

Forecasting

3.1 Inleiding

Opdrachtnemer ontvangt iedere week (indien gewijzigd) van Opdrachtgever een Forecast. Deze Forecast wordt door Opdrachtgever besproken met Opdrachtnemer en daarna door beide partijen geaccordeerd. Een Forecast wil zeggen dat de voorspelling van klantcontacten iedere week door Opdrachtgever aangepast kan worden aan eventueel nieuw verkregen inzichten over de ontwikkeling van klantcontact volumes. Op deze wijze heeft Opdrachtnemer de mogelijkheid om op weekbasis haar geplande personele bezetting op de Forecast af te stemmen.

3.2 Frequentie methodiek

Na aanlevering en goedkeuring van de Intraweek Forecast, zal Opdrachtnemer de Forecast uitsplitsen. Vervolgens plant de Opdrachtnemer op weekbasis de personeelspool in en kan er op dag basis worden geschoven. Hierbij wordt gewerkt met een planning: ; op dat moment is de Opdrachtnemer in het kader van de Wet Arbeidsmarkt in Balans verplicht om de onderzoekers een vaste minimale urengarantie geven.

Doordat er gebruik wordt gemaakt van getrainde parttimers is de Opdrachtnemer in staat om af te schalen tot % van de bezetting. Indien gedurende het project blijkt, dat het werk aanzienlijk afneemt, kan de pool in onderling overleg tussen partijen tussentijds worden verkleind. Op deze wijze kan de flexibiliteit blijven bestaan en op periodieke basis optimaal gepland worden.

3.3 Planning

Opdrachtnemer doet de aanname, dat circa % van de gebudgetteerde uur per BCO wordt besteed in fase A (start dag BCO) en dat % na dagen en % na dagen wordt besteed. Zodoende wordt er gestart in week met uur per dag en in week met per dag (zie de tabel op deze pagina)

Dagen	ma	di	wo	do	vr	za	zo
BCO's							
Fase A Start							
Fase B dagen							
Fase C dagen							
WEEK 01							
Fase B dagen							
WEEK 02							
Fase C dagen							
WEEK 03							

3.10

Tijdens [redacted] wordt de GGD Pool in Nederland (in [redacted] en [redacted]) getraind en kan gebruik worden gemaakt van de [redacted] pool met ervaring om operationeel alvast te starten. In [redacted] is een getrainde pool opgebouwd die [redacted] uur per dag kan invullen.

Training

4.1 Inleiding

[redacted] worden in rekening gebracht. Dit geldt bij [redacted], [redacted], [redacted] van de dienstverlening die Opdrachtnemer voor Opdrachtgever uitvoert na voorafgaande toestemming van Opdrachtgever via een RFC.

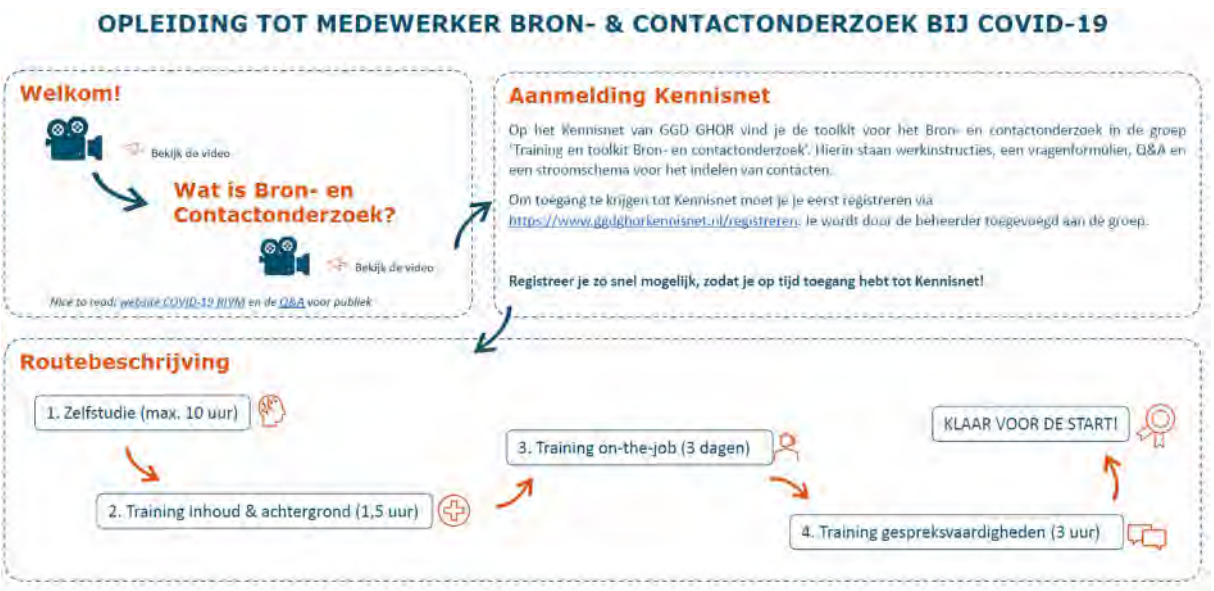
4.2 Tarieven en mate van doorbelasting training

De duur van de instroomtraining is ingeschat op [redacted] uur. De inhoud van de training wordt vooraf in overleg vastgesteld met de verantwoordelijke persoon van Opdrachtgever. Voor de doorbelasting van de verschillende trainingskosten geldt als uitgangspunt het onderstaand schema:

Soort training	Trainingskosten doorbelast aan Opdrachtgever	
	A	B
	Medewerkers Opdrachtnemer bij toename van geprognosticeerde volumes	Aanvullen pool van onderzoekers
Agent Uurtarief	[redacted]	
E-learning	[redacted]	[redacted]
Introductie Opdrachtnemer	[redacted]	[redacted]
Communicatietraining:	[redacted]	[redacted]
Introductie Opdrachtgever diensten	[redacted]	[redacted]
Vaardigheidstraining applicaties GGD	[redacted]	[redacted]
Toets (max. [redacted] minuten)	[redacted]	[redacted]
Specifieke training Opdrachtgever van nieuwe diensten	[redacted]	[redacted]
Refreshment toets (max. [redacted] minuten)	[redacted]	[redacted]

4.3 Inhoud training

Opdrachtgever is verantwoordelijk voor het aanleveren van de inhoud en vorm van de training voor wat betreft producten, diensten en applicaties van Opdrachtgever. Opdrachtnemer is verantwoordelijk voor de overige noodzakelijke trainingsmodules [redacted] en (afgenomen) applicaties van Opdrachtnemer. De trainingsopzet ziet er uit conform onderstaand model:



Indien Opdrachtgever tijdens de uitvoering van de dienstverlening bemerkt dat een bepaalde situatie zich voordoet waarin de training niet voorziet, meldt hij dit onverwijld aan Opdrachtnemer.

4.4 Training vereisten & Kosten

Van alle medewerkers van Opdrachtnemer wordt verwacht dat ze bij aanvang van de werkzaamheden met succes de kennistoets (e-learning) van Opdrachtgever hebben afgelegd. Voorwaarde hierin is dat de medewerker de toets heeft gehaald. Indien een onderzoeker stopt binnen [redacted] en vervangen moet worden om de poolcapaciteit op orde te houden, dan zullen die betreffende trainingskosten voor rekening van Opdrachtnemer komen.

In bijlage 2 van de Dienstovereenkomst zijn de `verwachtingsprofielen gedefinieerd waaraan de Opdrachtgever agent en Teamleider moet voldoen. Opdrachtgever staat ervoor in dat het door hem ingezette personeel aan dit verwachtingsprofiel voldoet en neemt alle mogelijke maatregelen om daaraan te voldoen.

Verantwoordelijke persoon van Opdrachtgever verneemt uiterlijk [redacted] voor aanvang van de training de trainingsdata.

Opdrachtgever en Opdrachtnemer volgen samen het kennis- en vaardigheidsniveau van de medewerkers aan de hand van uitkomsten kennis toetsen, medewerkers tevredenheidsonderzoeken en Quality Monitoring uitkomsten. Refreshment trainingen

vinden periodiek plaats en hebben als doel kennis en vaardigheden van de medewerkers op peil te brengen c.q. te houden. Inrichting, uitvoering en verrekening van deze trainingen worden vastgelegd en bijgehouden in een RFC.

Quality Monitoring (QM)

5.1 Inleiding

Opdrachtnemer dient iedere medewerker op het project van Opdrachtgever minimaal [redacted] keer per [redacted] te monitoren met als doel de continue kwaliteit van de medewerker te borgen en als onafhankelijke toets van de gesprekskwaliteit. Qua meet systematiek wordt het principe van [redacted] gehanteerd. De kosten van de Quality Monitoring zijn voor rekening van de Opdrachtnemer. Indien GGD aanvullende Quality Monitoring wenst geldt een aparte regeling, waarbij de Quality Monitoring kosten als additioneel component zijn opgenomen in het agent uurtarief.

5.2 Proces Quality monitoring

In bijlage 3 van de Dienstenovereenkomst staan de scoringsheets behorende bij het Quality Monitor proces. Het Quality Monitoring proces bestaat samengevat tenminste uit [redacted] sessie bestaande uit [redacted]. Een transactie is een uniek contact via call. Iedere sessie wordt gemonitord met het daarvoor met Opdrachtgever afgestemde scoringsheets. Alle gemonitorde sessies worden geregistreerd en verwerkt tot (K)PI rapportages, detail uitkomsten kunnen desgewenst door Opdrachtgever worden ingezien.

Indien een medewerker niet slaagt voor een monitor sessie (bestaande uit [redacted]) zal door Yource (en voor rekening van Yource) een verbetertraject als beschreven in het detail procesbeschrijving worden opgestart. Een Teamleider zal [redacted] side-by-side meeluisteren met zijn agents en daarbij coachen op basis van de monitoringsheet. Wanneer een agent niet slaagt voor een officiële monitoring sessie zal de Teamleider in samenwerking met de Auditor een actieve rol gaan spel in het verbeterplan volgens detail procesbeschrijving.

5.3 Steekproefgrootte

Opdrachtnemer zal Quality Monitoring uitvoeren ten aanzien van een representatieve steekproefgrootte over alle activiteiten uitgevoerd zoals beschreven in deze Dienstovereenkomst.

5.4 Kalibratie

Indien gewenst kan er [redacted] een zogenaamde Kalibratie sessie met Opdrachtgever worden georganiseerd. Tijdens de Kalibratie sessie zullen minimaal [redacted] transacties beoordeeld worden door zowel Opdrachtgever als Auditoren van Opdrachtnemer met als doel een eenduidige beoordeling van de transacties te bereiken. Auditoren mogen maximaal [redacted]% op [redacted] en [redacted]% op [redacted] onderdelen afwijken van Opdrachtgever om te slagen voor de Kalibratie waarbij de score van Opdrachtgever leidend is volgens beschreven procedures. Een Auditor die niet slaagt voor de Kalibratie zal van Opdrachtnemer training ontvangen

Rapportage

6.1 Inleiding
In dit onderdeel wordt inzicht gegeven in de rapportagemogelijkheden met betrekking tot de dienstverlening.

6.2 Standaardrapportages
Voor wat betreft standaardrapportages wordt onderscheid gemaakt tussen kernrapportages en detailrapportages.

De kernrapportages voorzien in de volgende informatiebehoefte:
- Inzicht ontwikkeling van de KPI's en PI's
- Basis voor facturatieproces
- Basis voor Forecasting
- Algemene management informatievoorzieningen

De detailrapportages geven de door Opdrachtgever gewenste aanvullende inzichten. Naast de gedefinieerde standaard rapportages die voortvloeien uit de dienstverlening zoals die is uitbesteed, zijn er zogenaamde aanvullende klantrapportages. Deze categorie rapportages worden op verzoek van Opdrachtgever vervaardigd door opdrachtnemer.

Opdrachtgever is voor de rapportages geen aanvullende vergoeding verschuldigd.

6.3 Beschikbaarheid Rapportages
De vastgestelde rapportages zullen op vastgestelde tijdstippen beschikbaar gesteld worden en in geval van afwijking zullen de partijen elkaar informeren over oorzaak vertraging en verwacht herstel. De mate waarbij de gedefinieerde rapportages tijdig beschikbaar gesteld worden wordt in een performance indicator inzichtelijk gemaakt.

Beschikbaarheid van de rapportage is mogelijk afhankelijk van de input vanuit Opdrachtgever. Opdrachtgever is verantwoordelijk voor het tijdig aanleveren van de onderliggende rapportages zoals bepaald in overleg met Opdrachtnemer. Indien meer of andere input nodig is voor het opmaken van rapportages zal Opdrachtnemer dat onverwijld aan Opdrachtgever melden en vragen om specifieke aanvullende informatie.

Opdrachtnemer zal op verzoek van Opdrachtgever werken vanuit HP Zone. Als gevolg hiervan zal Opdrachtnemer geen automatische dailer inrichten om tot de gesprekken te komen. Door deze keuze is de gedetailleerdheid van de rapportages beperkt tot:
- Aantal gesprekken
- Gespreksduur per gebeld nummer (niet gekoppeld aan dossier)
- Gespreksduur gemiddeld (niet gekoppeld aan dossiers)
- Afboekcode per uitgaand gesprek
- Afboekcodes totaal
- Afboekcodes in relatie tot duur van het gesprek

Tarieven

7.1 Inleiding

In dit onderdeel worden de tarieven voor de standaard dienstverlening weergegeven. Er wordt gefactureerd op basis van een tarief per ingezet uur: het aantal te bestede uren van [redacted] per dossier is een gemiddelde inschatting. Deze inschatting is afhankelijk van de complexiteit van een dossier en van de mogelijke ontwikkeling van technologische communicatiemethodieken, zoals de app.

7.2 Standaardtarieven

GGD-tarieven	Tarief
Client Manager	[redacted]
Teamleider	
Trainer	
Projectmanager	
Projectcoördinator	
Specials	
Onderzoekers	

De uurtarieven zijn inclusief de volgende prijselementen:

- Loonkosten en werkgeverslasten van de onderzoekers, teamleaders, trainer, projectcoördinator en projectmanager.
- Aansturing van Client Manager.
- Weekendtoeslagen, onkosten en reiskosten.
- Hardware, software, IT support, werkplekken, quality monitoring, trafficking en workforce management (planning).
- De kosten voor de belminuten.
- De mogelijkheid om met [redacted]% af te schalen naar [redacted] uur per dag (de baseline), op weekbasis wordt er gepland ([redacted]).
- Inzetbaarheid van de flexibele schil vanuit [redacted] in het geval van “specials”.

De uurtarieven zijn exclusief:

- 21% BTW
- Kosten Tolken Telefoon

** Als Projectmanager gaan we [redacted] inhuren: hij heeft jarenlange ervaring binnen het klantcontact als projectmanager.*

7.3 Dienstreizen

De medewerkers vanuit Opdrachtnemer die, op verzoek van de GGD-en, werkzaam zijn op de hoofdlocaties van de GGD-en krijgen de reisafstand tussen het Opdrachtnemer kantoor in [redacted] en het GGD-kantoor in [redacted] vergoed tegen [redacted] excl. Btw per kilometer onder de vermelding “dienstreis”. De regeling, zoals hierboven beschreven is alleen van toepassing op de periode van week [redacted]: [redacted] 2020 t/m [redacted] 2020. Ter volledigheid, wij zullen de reiskosten die het betreft onder vermelding van “dienstreis” weergeven op de factuur.

Implementatie; kosten en doorlooptijd

8.1 Inleiding

In het volgende onderdeel wordt een uiteenzetting gegeven van de planning rondom de implementatie en de kosten.

8.2 Implementatiekosten

- Uitgaande van de startdatum per maandag [redacted] 2020 (week [redacted]) wordt de implementatie per maandag [redacted] 2020 (week [redacted]) opgestart.
- Voor de implementatiefase wordt een Trainer fulltime ingezet gedurende [redacted] weken (week [redacted]).
- De Projectmanager start fulltime in week [redacted] en zal zich per week [redacted] bezighouden met de verdere implementatie ([redacted]%) en de operationele projectcoördinatie.
- Uitgaande van de ervaringen in [redacted] zullen de onderzoekers circa [redacted] uur training per persoon krijgen; in dit model wordt uitgegaan uit van [redacted] uur instroomtraining.
- De totale implementatiekosten komen zodoende uit op [redacted]

Implementatie	Tarief	Totaal uren	Kosten
Onderzoekers (training [redacted] x)	[redacted]		
Teamleaders (training [redacted] x)			
Trainer			
Projectmanager			
Projectcoördinator			
Client Manager			
Specials			
Sommatie			[redacted]

8.3 Besturingsapparaat

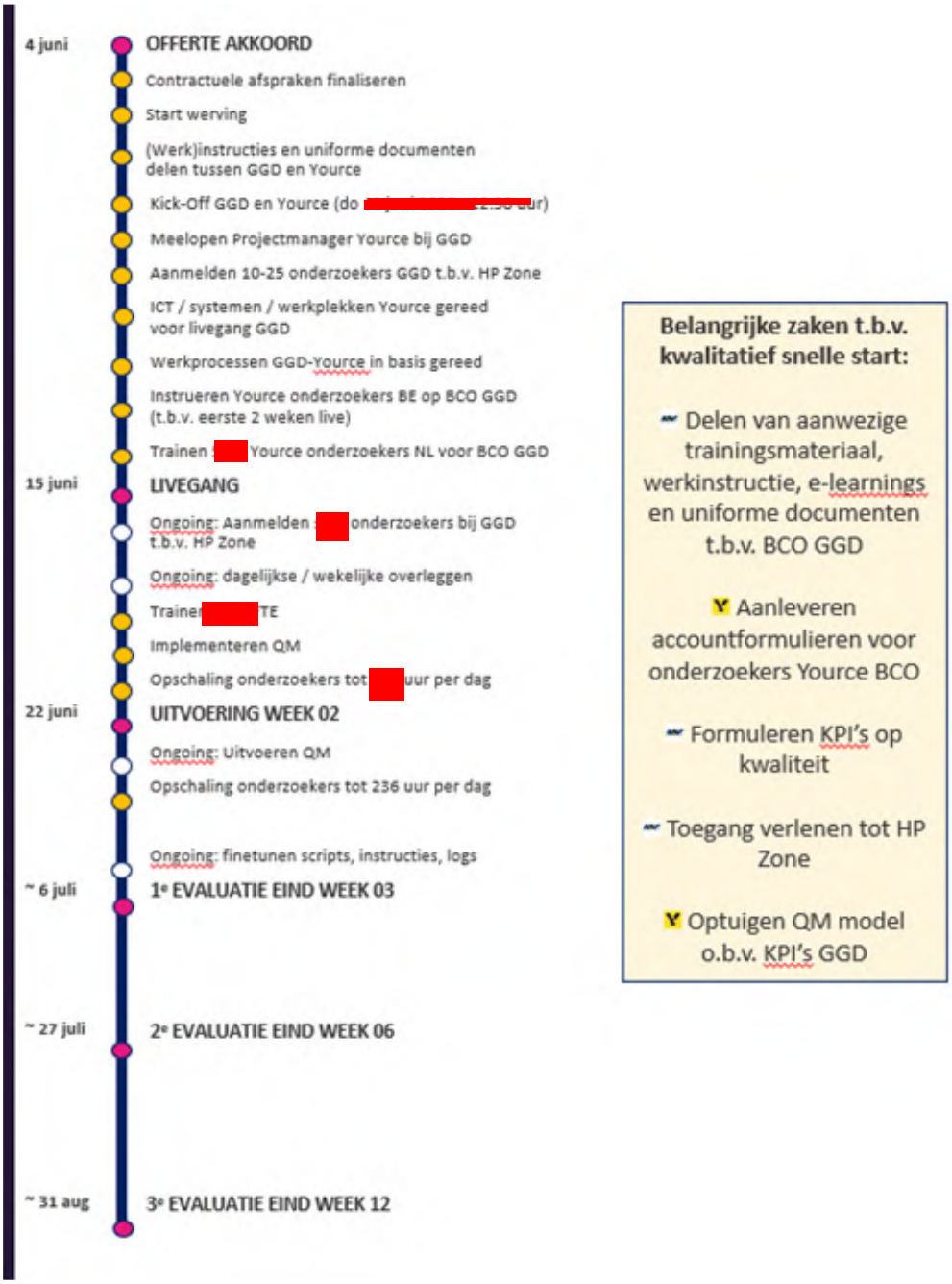
Na implementatie zullen de ingezette uren van de onderzoekers afhangen van het aantal BCO's. Kijkend naar de vaste bezetting, is het voorstel om de trainer voor minder uur wél blijven inzetten om continu in te spelen op de dynamiek in benodigde kennis.

De Projectenmanager wordt naar verwachting voor [redacted] uur in de week, tot eind [redacted] 2020 ingezet. Zodra alle processen staan en geborgd zijn kunnen de uren van de Projectmanager worden afgebouwd.

Hieronder in een tabel de weergave van de “vaste” operationele kosten op weekbasis t/m september 2020 en ná 01 oktober 2020.

		Operatie tot 01 okt 2020		Operatie ná 01 okt 2020	
	Tarief	Uren week xx	Kosten	Uren week xx	Kosten
Onderzoekers	[redacted]				
Team leaders					
Trainer					
Project manager					
Projectcoördinator					
Client Manager					
Specials					
Sommatie			[redacted]		

8.4 Planning



Belangrijke zaken t.b.v. kwalitatief snelle start:

- Delen van aanwezige trainingsmateriaal, werkinstructie, e-learnings en uniforme documenten t.b.v. BCO GGD
- Aanleveren accountformulieren voor onderzoekers Yource BCO
- Formuleren KPI's op kwaliteit
- Toegang verlenen tot HP Zone
- Optuigen QM model o.b.v. KPI's GGD

Facturatieproces

9.1 Inleiding
In het volgende onderdeel wordt een uiteenzetting gegeven van het facturatieproces.

9.2 Procedure
[redacted] dagen na afloop van de betreffende maand waarin de factuur is ontvangen ingediend te zijn.

De facturen dienen digitaal in PDF-format aangeleverd te worden via crediteuren@hetservicecentrum.nl, t.a.v. crediteurenadministratie en onder vermelding van de betreffende opdrachtgever.
Factuuradres:

GGD Hart voor Brabant
Pettelaarpark 10
5216PD te 's-Hertogenbosch

Een factuur dient te voldoen aan alle gestelde wettelijke eisen en dient minimaal onderstaande gegevens te bevatten:

- NAW-gegevens Opdrachtnemer;
- Factuurnummer van Opdrachtnemer;
- Het verplichtingennummer/ Ordernummer als verstrekt door Opdrachtgever;
- Het Kamer van Koophandel nummer van Opdrachtnemer;
- IBAN-nummer van Opdrachtnemer;
- Het btw-nummer van Opdrachtnemer;
- Indien van toepassing SWIFT/BIC van Opdrachtnemer;
- Factuurdatum;
- Factuurperiode;
- Factuurbedrag exclusief BTW, BTW en factuurbedrag inclusief BTW;
- Eenduidige omschrijving van de geleverde diensten;
- Naam en gegevens van de ingezette arbeidskrachten;
- Locaties van inzet;
- Gewerkte uren en tarief per uur (weekendtoeslag specificatie);

Eventuele creditnota's dienen apart te worden verstuurd. In het geval van een creditfactuur, vermeldt de Opdrachtnemer het factuurnummer en het verplichtingennummer van de corresponderende debet factuur.

Bij correcte facturering geschiedt betaling zo spoedig mogelijk binnen de in de Raamovereenkomst genoemde termijn. Goedkeuring van de factuur geschiedt op basis van de in de Raamovereenkomst overeengekomen tarieven en voorwaarden.

Overschrijding van (een) betalingstermijn(en) door Opdrachtgever of niet-betaling door Opdrachtgever van (een) fact(u)ur(en) op grond van vermoede inhoudelijke onjuistheid van die fact(u)ur(en) of van ondeugdelijkheid van de gefactureerde prestaties, geeft Opdrachtnemer niet het recht zijn prestaties op te schorten c.q. te beëindigen.

Calamiteiten

10.1 Inleiding
In dit onderdeel wordt inzichtelijk gemaakt wat de procedure is in geval van een calamiteit.

10.2 Niet beschikbaar zijn van Opdrachtgever applicaties
De Opdrachtnemer verplicht zich ertoe dat zij storingen aan Opdrachtgever applicaties direct meldt via de Contract Manager van de betreffende serviceafdeling. Opdrachtnemer verplicht zich tevens tot assistentie binnen en buiten kantooruren teneinde Opdrachtgever de mogelijkheid te geven om de storing op te lossen.

Indien Opdrachtnemer als gevolg van een storing in cruciale systemen van Opdrachtgever geen calls kan ontvangen, geldt de Change managementprocedure zoals beschreven in hoofdstuk 11 van de Dienstovereenkomst met als uitgangspunt de Forecast garantieregeling van deze Dienstenovereenkomst (op dag basis).

10.3 Niet beschikbaar zijn van Opdrachtnemer applicaties
Indien de Opdrachtnemer in een Calamiteit verkeert, zal Opdrachtnemer Opdrachtgever hierover uiterlijk binnen [redacted] na ontstaan van de Calamiteit zo volledig mogelijk informeren over de omvang van de Calamiteit en ondernomen acties ter beperking van de impact op de uitvoering van de Diensten. Opdrachtnemer dient eerst zelf proberen tot een oplossing te komen door:

- Verplaatsing activiteiten/ personeel naar een andere locatie of zelfs naar een locatie van Opdrachtgever;
- inzet van extra gekwalificeerd personeel.

Opdrachtnemer verplicht zich te allen tijde een actueel calamiteitenplan beschikbaar te hebben. Opdrachtgever heeft het recht dit plan steeds op locatie in te kunnen zien mits op redelijke termijn vooraf aangekondigd en onder de voorwaarde dat dit de normale bedrijfsvoering van Opdrachtnemer niet in de weg staat.

Change management procedure

11.1 Inleiding

Dit hoofdstuk beschrijft de procedure welke doorlopen moet worden om bedoelde wijzigingen en/of uitbreidingen van de dienstverlening van Opdrachtnemer aan Opdrachtgever door te kunnen voeren en heeft als bijlage een formulier wat daartoe gebruikt dient te worden. Deze procedure is zowel geldig voor RFC's van Opdrachtgever naar Opdrachtnemer als omgekeerd.

Het Change Management omvat de volgende onderdelen:

- Telefonie
- Infrastructuur
- Applicaties
- Processen en procedures
- Trainingen en opleidingen

11.2 Procesbeschrijving

Het doorvoeren van een verzoek tot wijziging (hierna te noemen Request For Change, afgekort tot RFC) zal volgens het hieronder vastgestelde proces verlopen. Hierin zijn een aantal processtappen te onderscheiden welke verder worden toegelicht.

11.3 Indienen RFC

Iedere RFC kan alleen schriftelijk worden ingediend. Hierbij worden toegestaan de verzoeken zoals ingediend middels postbestelling, fax of e-mail. Voor het indienen van een verzoek wordt gebruik gemaakt van een standaardformulier zoals beschreven in - bijlage 5. De RFC wordt ingediend bij de verantwoordelijke persoon van de GGD.

Het formulier dient volledig te zijn ingevuld en ondertekend door een daartoe bevoegd, conform Overeenkomst, persoon. Iedere RFC wordt uniek gekenmerkt door een RFC-nummer, waarvan de opbouw verderop wordt beschreven. Nadat een RFC is ontvangen zal de ontvanger binnen een vastgestelde termijn van [redacted] dagen een ontvangstbevestiging sturen met vermelding van het RFC-nummer aan de operationeel manager van Opdrachtnemer.

11.3.1 Urgentie

Nadat een RFC is geaccepteerd zal als eerste de urgentie worden vastgesteld. Hierbij zijn drie niveaus van urgentie te onderscheiden:

1. Urgent: een RFC heeft de status "urgent" als het doorvoeren van een RFC noodzakelijk is om de contractueel vastgestelde service Levels op zeer korte termijn te kunnen handhaven. Dit kan bijvoorbeeld het geval zijn indien het verwachte call volume groter dreigt te worden dan voorzien, dus fundamenteel afwijkend van de hoeveelheden welke middels de normale Forecast procedures zijn gepland. De doorlooptijd voor het afhandelen van een urgente RFC bedraagt maximaal [redacted] kalenderdagen. In overleg is een eventuele workaround, welke hetzelfde effect beoogt als de RFC, bespreekbaar.

2. Standaard: een RFC heeft de status "standaard" als het doorvoeren van een RFC een maximale doorlooptijd van [redacted] kalenderdagen mag bedragen. Indien deze RFC niet doorgevoerd wordt binnen [redacted] dagen mag verwacht worden dat dit leidt dit tot degradatie in de dienstverlening. De projectleider geeft op het formulier de grove planning aan.
3. Geen urgentie: een RFC heeft de status "niet urgent" als het doorvoeren van een RFC een maximale doorlooptijd van [redacted] maanden mag bedragen. De projectleider levert een gedetailleerde planning aan.

11.3.2 Soort RFC

Op het RFC-formulier wordt aangegeven welk soort RFC het betreft. Er zijn 2 soorten te onderscheiden:

- RFC valt binnen de kaders van de contractafspraken en heeft derhalve geen invloed op overeengekomen prijsstelling en/of tarieven.
- RFC valt buiten de kaders van de contractafspraken. Opdrachtnemer zal daartoe de implementatie van de RFC vooraf doen gaan aan een kostenopgave en zal Opdrachtgever hiertoe om accordering vragen.

In beide gevallen geeft Opdrachtnemer aan welke financiële consequenties zijn verbonden aan de RFC en op welke grondslag uren worden gefactureerd ([redacted]).

11.3.3 Implementatie

Afhankelijk van urgentie en impact kan al dan niet direct begonnen worden met implementatie, zoals eerder vermeld alleen na een akkoord door Opdrachtgever en Opdrachtnemer. Bij RFC's met "standaard urgentie" of "geen urgentie" stelt de projectleider een planning op en communiceert deze met Opdrachtgever/ Opdrachtnemer. De planning is gericht op het gereed melden van de RFC op de door Opdrachtgever/ Opdrachtnemer aangegeven einddatum. Indien Opdrachtgever of Opdrachtnemer constateert dat genoemde einddatum niet kan worden gehaald, zal hij terstond contact opnemen met de andere partij om de consequenties en vervolgacties te bespreken. Dit laat onverlet dat de partijen al het mogelijke zullen doen om alsnog de gewenste opleverdatum te kunnen realiseren. Indien Opdrachtnemer bepaalde input of medewerking van Opdrachtgever daarvoor nodig heeft, zal hij dat onverwijld aan Opdrachtgever melden en de specifieke input of medewerking vragen.

11.3.4 Testen

De projectleider bepaalt welke test of testprocedure moet worden doorlopen en stelt afhankelijk van impact en urgentie een meer of minder uitgebreid testplan op. Deze testprocedures worden besproken met Opdrachtgever/ Opdrachtnemer en de projectleider zal daarbij aangeven welke inspanning van Opdrachtgever/ Opdrachtnemer verwacht wordt om de testen goed te kunnen afronden. Opdrachtgever/ Opdrachtnemer dient een akkoord te geven voor het testplan en dient in de regel kennis te nemen van de testresultaten.

11.3.5 Gereed melding

Aan het einde van de testfase zal de projectleider, bij goed gevolg hiervan, een gereed melding doen bij Opdrachtgever/ Opdrachtnemer.

Gereed melding geschiedt schriftelijk bij de aanvrager en is daarmee de formele oplevering. Opdrachtgever/ Opdrachtnemer dient formeel te accepteren, bij voorkeur aan de hand van vooraf gestelde criteria.

11.3.6 Besturing

In het operationeel overleg wordt de voortgang van RFC's besproken. Opdrachtnemer/ Opdrachtgever houdt hiertoe een overzicht actueel van openstaande en afgewikkelde RFC's.

11.3.7 Facturering

Daar waar een RFC leidt tot financiële verplichtingen van Opdrachtgever, geldt dat facturen eerst dan betaalbaar worden gesteld als bij de factuur [redacted]

11.3.8 Formulier

Voor het doorvoeren van een RFC wordt gebruik gemaakt van een standaardformulier (zie bijlage 5). Hieronder volgt een korte toelichting op het gebruik van het formulier.

- RFC-nummer: het RFC nummer wordt als volgt opgebouwd: jaartal + 3 - cijferig volgnummer bijv. 2007001
- Referentie: hier kan een nummer of tekst worden gegeven voor eigen gebruik
- Urgentie: aan te geven door aanvrager
- Impact: aan te geven door projectleider Opdrachtnemer/ Opdrachtgever
- Soort RFC: aan te geven door aanvrager
- Omschrijving: korte omschrijving van de gewenste wijziging
- Implementatie voorstel: korte toelichting op de voorgestelde implementatie. Bij grote impact wordt hier verwezen naar een implementatieplan
- Impact op business: korte toelichting op het effect bij NIET doorvoeren
- Impact op KPI's
- Impact op processen en werkinstructies
- Workaround voorstel: hier kan de aanvrager of projectleider aangeven of bij een urgente RFC een workaround mogelijk is
- Planning: alle relevante data in te vullen door de projectleider
- Akkoord: zowel een vertegenwoordiger van Opdrachtgever als Opdrachtnemer tekenen voor akkoord. Zonder ondertekening van beiden kan NIET met implementatie worden begonnen
- Contactpersoon: voor beide bedrijven een contactpersoon opgeven
- Risico: korte toelichting indien er risico's verbonden zijn aan de implementatie
- Kosten/ tarief: indien er prijstechnische consequenties verbonden zijn aan het implementeren van de RFC dient dit door de projectleider duidelijk te worden aangegeven

Communicatie & betrokkenheid

12.1 Inleiding

In de zogenaamde Involvement Matrix wordt inzichtelijk welke collega's van Opdrachtnemer betrokken zijn bij het GGD-project en bij welke onderdelen zij betrokken zijn.

Bij de communicatiestructuur tussen Opdrachtgever en Opdrachtnemer wordt gebruik gemaakt van de PDCA-methode. De PDCA-cyclus bestaat uit vier stappen: **Plan, Do, Check en Act.** Deze cyclus geeft veel mogelijkheden om het kwaliteitsmanagement verder te professionaliseren. Maar de cyclus kan ook helpen om de strategie aan te scherpen en biedt goede handvatten om deze verder te verfijnen en ontwikkelen, terwijl tegelijkertijd de bedrijfsprocessen geoptimaliseerd kunnen worden.

12.2 Involvement Matrix

Involvement Matrix	Client Team	Manager	Project	People	IT	Recruitment	Director Belgium	CEO
Contracting	Y							Y
Profiling	Y	Y	Y			Y		
Implementation OpdrachtnemerJourney	Y			Y				
Implementation Operations	Y	Y	Y		Y			
Daily Project Meeting (DPM)		Y	Y					
Weekly Project Meeting (WPM)	Y	Y	Y					
Milestone after 06 weeks	Y	Y	Y			Y	Y	Y
Milestone after 12 weeks	Y	Y	Y			Y	Y	Y
Monthly Business Review (MBR)	Y	Y	Y			Y		Y

"Tech Sessions" (periodically)	Y	Y			Y			Y
Piketservice 24/7	2		1					3
Specials	Y	Y	Y				Y	Y

12.3 Toelichting involvement matrix

Opdrachtnemer staat ervoor in dat het ingezette personeel telkens gekwalificeerd is voor de dienstverlening en diens desbetreffende functie en taken.

12.4 Communicatiematrix

Naam	Bedrijf	Functie	Telefoonnummer	E-mailadres
Algemeen HR	GGD West-Brabant	HR Algemeen		HR@ggdwestbrabant.nl
Algemeen HR	GGD HvB	HR Algemeen		HR@ggdhvb.nl
[redacted]	GGD HvB	[redacted]	[redacted]	[redacted]@ggdhvb.nl
[redacted]	GGD West-Brabant	[redacted]	[redacted]	[redacted]@ggdwestbrabant.nl
[redacted]	Yource	[redacted]	[redacted]	[redacted]@yource-group.com
[redacted]	Yource	[redacted]	[redacted]	[redacted]@yource-group.com
[redacted]	GGD West-Brabant	Verpleegkundige	[redacted]	[redacted]@ggdwestbrabant.nl
[redacted]	GGD Het Servicecentrum	[redacted]		[redacted]@hetservicecentrum.nl
[redacted]	GGD HvB	[redacted]	[redacted]	[redacted]@ggdhvb.nl
[redacted]	Yource	[redacted]	[redacted]	[redacted]@yource.work
[redacted]	GGD HvB	[redacted]	[redacted]	[redacted]@ggdhvb.nl
[redacted]	GGD HvB	[redacted]	0031-	[redacted]@ggdhvb.nl
[redacted]	GGD HvB	[redacted]	[redacted]	[redacted]@ggdhvb.nl
[redacted]	GGD West-Brabant	[redacted]	[redacted]	[redacted]@ggdwestbrabant.nl
[redacted]	GGD West-Brabant	[redacted]	[redacted]	[redacted]@ggdwestbrabant.nl
[redacted]	GGD Het Servicecentrum	[redacted]	[redacted]	[redacted]@hetservicecentrum.nl
[redacted]	GGD HvB	[redacted]	[redacted]	[redacted]@ggdhvb.nl
[redacted]	GGD HvB	[redacted]	[redacted]	[redacted]@ggdhvb.nl
[redacted]	Yource	[redacted]	[redacted]	[redacted]@yource-group.com
[redacted]	GGD HvB	[redacted]	[redacted]	[redacted]@ggdhvb.nl
[redacted]	Yource	[redacted]	[redacted]	[redacted]@yource-group.com
[redacted]	GGD HvB	[redacted]	[redacted]	[redacted]@ggdhvb.nl
[redacted]	Yource	[redacted]	[redacted]	[redacted]@yource-group.com
[redacted]	GGD HvB	[redacted]	[redacted]	[redacted]@ggdhvb.nl
[redacted]	Yource	[redacted]	[redacted]	[redacted]@yource.work
[redacted]	GGD HvB	[redacted]	[redacted]	[redacted]@ggdhvb.nl
[redacted]	GGD West-Brabant	[redacted]	[redacted]	[redacted]@ggdwestbrabant.nl
[redacted]	GGD HvB	[redacted]	[redacted]	[redacted]@ggdhvb.nl
[redacted]	Yource	[redacted]	[redacted]	[redacted]@yource-group.com
[redacted]	Yource	[redacted]	[redacted]	[redacted]@yource-group.com
[redacted]	GGD West-Brabant	[redacted]	[redacted]	[redacted]@ggdwestbrabant.nl
[redacted]	Yource	[redacted]	[redacted]	[redacted]@yource-group.com
[redacted]	GGD West-Brabant	[redacted]	[redacted]	[redacted]@ggdwestbrabant.nl
[redacted]	GGD HvB	[redacted]	[redacted]	[redacted]@ggdhvb.nl
[redacted]	GGD Het Servicecentrum	[redacted]	[redacted]	[redacted]@hetservicecentrum.nl
[redacted]	Yource	[redacted]	[redacted]	[redacted]@yource-group.nl
[redacted]	Yource	[redacted]	[redacted]	[redacted]@yource-group.nl
[redacted]	GGD HvB	[redacted]	[redacted]	[redacted]
[redacted]	GGD West-Brabant	[redacted]	[redacted]	[redacted]

12.5 Review Set

Ná 3, 6 en ná 12 weken vanaf de start wordt een evaluatiemoment ingelast, om zowel de kwaliteit als de planning te bespreken. Hieronder een specifieke weergave van de te bespreken elementen tijdens deze 3 evaluatie momenten:

Evaluatie 03 weken na start

- Eerste indruk samenwerking.
- Evaluatie implementatieproces
- Opdrachtnemer is operationeel op baseline niveau.
- Trainers en Teamleads van Opdrachtnemer zijn getraind door GGD-IZB trainer

Evaluatie 06 weken na start

- Kwaliteitssysteem evalueren

Evaluatie 12 weken na start

- Capaciteit bespreken.
- [redacted] BCO afwikkeling door Opdrachtnemer per [redacted] 2020 bepalen.

ICT

13.1 Inleiding

In dit onderdeel wordt het ICT-landschap voor de dienstverlening beschreven.

13.2 IT Werkplekken en beheer

GGD werkt met een webbased applicatie HP Zone, welke via een werkplek met internetverbindingen te benaderen is. Daarbij is het wenselijk dat Opdrachtnemer e-mails kan versturen uit naam van corona.contactonderzoek@ggdwestbrabant.nl.

Opdrachtnemer werk verder op eigen server, op eigen devices, gebruikt eigen telefoniesysteem met accessoires.

GGD maakt geen gebruik van de telefonie mogelijkheden van Opdrachtnemer in de zin van dailers en registratiemodules e.d.

Aldus overeengekomen, vastgelegd op 29 pagina's tekst en 6 Bijlagen.

Ondertekening,

GGD Hart voor Brabant:

Naam: [redacted]

Functie: [redacted]

Datum:

Yource Outsourcing b.v.:

Naam: [redacted]

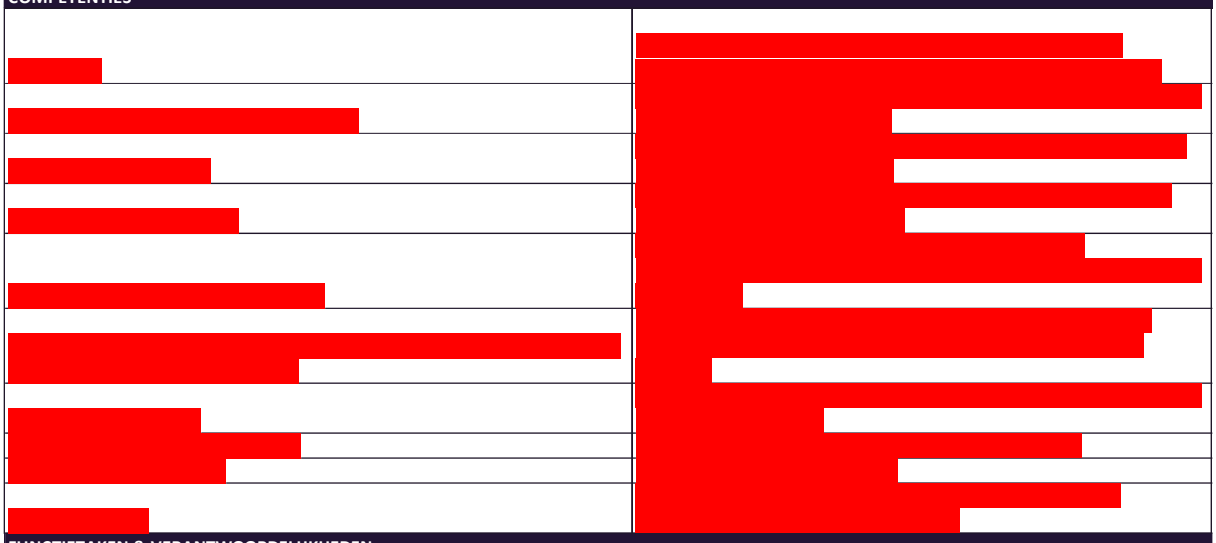
Functie: [redacted]

Datum:

Bijlage 1 Loggingtabel

Bijlage 2 Verwachtingsprofielen

VERWACHTINGSPROFIEL - BCO Onderzoeker	YOURCE
VERWACHTINGSPROFIEL	
Functietitel	BCO Onderzoeker
Divisie	Outsourcing
Subdivisie	Operations
Functie- & Salarisschaal	Project GGD
VERWACHTING	
De verwachting is dat jij als medewerker van Yource vol energie de doelstellingen probeert te halen binnen jouw campagne. Veel belangrijker nog is de samenwerking met jouw collega's om het optimale resultaat te behalen. Je bent een voorbeeld voor collega's en je bent een ambassadeur voor de klant welke je bedient binnen jouw campagne. Als BCO Onderzoeker weet je als geen ander dat het geruststellen en adviseren van de patiënt het primaire doel is van alle type klantcontacten. Hierin weet jij dan ook perfect de juiste normen en waarden in toe te passen. Daarnaast zorg je er voor dat je over voldoende kennis beschikt om alle klanten op jouw campagne optimaal te kunnen bedienen. Als je deze kennis niet hebt of bepaalde vaardigheden onvoldoende beheerst vraag je pro-actief aan jouw Teamleider en Seniors om support. Je bent volledig op de hoogte van de richtlijnen op jouw campagne en denkt actief mee in eventuele verbetermogelijkheden.	
FUNCTIE-EISEN	
Jij hebt:	
HBO Werk- en denkniveau	
Een service gedreven instelling met daarbij commerciele vaardigheden	
Uitstekende mondelinge en schriftelijke communicatieve vaardigheden	
Bij voorkeur ervaring binnen de zorg dan wel medische achtergrond	
Ervaring met het doorvragen en voeren van uitstekende gesprekken	
Jij bent:	
Een teamspeler en werkt graag aan gezamenlijke doelstellingen	
Energiek, positief en enthousiast. Denkt in oplossingen, niet in problemen	
Een persoon die streeft naar continue verbetering	
Minimaal 16 tot 32 of 20 tot 40 uur per week beschikbaar en daarin flexibel	
Empatisch en adviserend richting de patiënt	
In staat om vanuit processen en protcollen te werken in de systemen van de GGD	
COMPETENTIES	
[redacted]	
FUNCTIETAKEN & VERANTWOORDELIJKHEDEN	
Het verwerken van dossiers van patiënten die besmet zijn met het COVID-19 virus	
Je kunt doormiddel van jouw empatisch vermogen de patiënt adviseren en geruststellen	
Je kunt doormiddel van jouw sterke gesprekstechnieken alle contacten van de patiënt in kaart brengen en deze ook benaderen om hen te adviseren	
Het nauwlettend volgen van de juiste procedures en richtlijnen	
Volledige naleving van de planning	
Nauwkeurigheid in de werkzaamheden	
Het correct afhandelen van administratie in diverse systemen.	
RESULTAATGEBIEDEN	
Naleving huisregels op de campagne inclusief houding en gedrag	
KPI's op norm v.w.b. eigen performance tijdens BCO onderzoeker gerelateerde werkzaamheden	

VERWACHTINGSPROFIEL - TEAMLEADER	YOURCE
VERWACHTINGSPROFIEL	
Functietitel	BCO Teamleader
Divisie	Outsourcing
Subdivisie	Operations
Functie- & Salarisschaal	GGD Project
VERWACHTING	
De teamleader verantwoordelijk voor de operationele aansturing van zijn/haar team. Hij/zij bezit de competenties die nodig zijn om de werkzaamheden van contactcenter agents aan te sturen, te begeleiden, te beoordelen, te coördineren, te organiseren en te bewaken op een wijze die elke agent in staat stelt om de gewenste klantcontacten binnen de gegeven kwalitatieve en kwantitatieve richtlijnen af te handelen. Doelstelling hierbij is om de dienstverlening aan de klanten te optimaliseren binnen de gestelde tijdsplanning en kwaliteitseisen, op efficiënte wijze. De focus van de teamleader ligt naast de inhoudelijke kennis voornamelijk op de medewerker, waarbij een optimale medewerktevredenheid het doel is. (Yource cultuur). Een teamleider rapporteert rechtstreeks aan de Projectmanager en Senior Client Manager voor het project GGD Yource is een dynamische organisatie. Jouw werkzaamheden zullen dan ook niet altijd gelimiteerd zijn tot hetgeen in dit verwachtingsprofiel staat beschreven. Deze dient echter wel als basis en uitgangspunt. Aanvullend maak jij met je leidinggevende continu afspraken die in meer detail jouw doelstellingen beschrijven op basis van de klanten en projecten waarvoor jij werkzaam bent.	
FUNCTIE-EISEN	
Jij hebt:	
HBO werk- en denkniveau met relevante leidinggevende werkervaring	
Goed ontwikkelde people management skills. Weet medewerkers te stimuleren en enthousiasmeren met behoud van doelstellingen	
Een grote mate van zelfstandigheid en verantwoordelijkheid	
Sterk ontwikkelde coachingsvaardigheden en beheerst alle coachingstechnieken optimaal. Uitgebreide kennis op het gebied van Contact Center KPI	
Een sterke mate van kritische zelfreflectie en zoekt binnen de eigen kaders naar mogelijkheden om de gestelde doelen te behalen	
Jij bent:	
Flexibel. Bereid om in de avonden en weekenden te werken. Bereid om op verschillende vestigingen te werken	
Een positief persoon die denkt in kansen i.p.v. beperkingen/problemen. De mens (medewerker) staat bovenaan en jij bent bereid tot het uiterste te gaan om	
Communicatief vaardig, zowel schriftelijk als mondeling.	
Een persoon die vragen stelt aan zijn/haar omgeving om een idee, wat is geannalyseerd, meetbaar te maken en te implementeren	
Proactief en weet het algemeen belang en de individuele belangen te harmoniseren	
Iemand die vanuit een organisatieboodschap een communicate kan uitrollen binnen zijn eigen team van operational members om draagvlak te creeren	
Een persoon die vanuit de beoordelingsmethodiek en oprechte interesse in de mens, de operational members te binden, te ontwikkelen en te betrekken met	
Een teamspeler, integer en professioneel	
COMPETENTIES	
	
FUNCTIETAKEN & VERANTWOORDELIJKHEDEN	
Coachen en aansturen. Het aansturen en coachen van agents op productiviteit, efficiency en kwaliteit in de processen en protocollen van de GGD, om	
HR gerelateerde werkzaamheden zoals het voeren van beoordeling- en functioneringsgesprekken, selectiegesprekken, exitgesprekken en verzuimgesprekken	
Interne (collega's en leidinggevenden) en externe (klanten en contactpersonen) contacten onderhouden	
Het uitvoeren van quality monitorings volgens de kwantitatieve en kwalitatieve richtlijnen vanuit de GGD e Yource.	
Het voeren van coachingsgesprekken met de medewerkers mede n.a.v. de input vanuit de QM, waarbij de coach d.m.v. diverse coachingstechnieken (bijv. de 5	
Actieve en/of leidende rol binnen de job die we uitvoeren voor de GGD.	
RESULTAATGEBIEDEN	
Uitdrager en exponent van de gewenste Yource cultuur en gedrag.	
Coachen, begeleiden, motiveren van de teamleden	
Zorgen voor juiste kwantitatieve en kwalitatieve bezetting.	
Is verantwoordelijk voor de algehele performance van het project inclusief alle geldende KPI's	
Uitvoeren van HR gerelateerde onderwerpen	
Interne en externe contacten onderhouden	

Bijlage 3 Scoring sheets Quality Monitoring

In onderstaande tabel wordt een voorbeeld gegeven van het scoringssheet zoals dat bij het BCO in België wordt toegepast. In overleg met GGD kan het scoringssheet worden aangepast.

Criteria	Weging	Score 0/1
AANVANG		
Begroeting/intro		
Identificatie van de contactpersoon		
Reden van de oproep		
ANALYSE		
Vragen en doorvragen		
Herformuleren		
Interactie/Dialoog		
Leiding nemen in het gesprek		
ANTWOORD		
Correcte en volledige informatie		
Correct gebruik van het systeem/de scripting		
Accuratie en details in genoteerde info		
Omgaan met bezwaren/gebrek aan medewerking		
ATTITUDE		
Actief luisteren		
Stemgebruik		
Respectvol/professioneel taalgebruik/authentiek		
Betrokkenheid/empathie/gevoel contactpersoon		
Integriteit		
AFRONDING		
Correcte afsluiting		
Correct gebruik wrap up codes		
TOTAAL		
OPMERKING:		

Bijlage 4 Kernproces GGD

2 Landelijke beldienst[1] kan in overleg complexe BCO'en weer terugverwijzen naar regionale GGD (1/2)

TER AFSTEMMING

Criteria	Omschrijving
Originele triagecriteria	Indien index patiënt op basis van nieuwe informatie toch blijkt te voldoen aan de triagecriteria, kan de casus in overleg terugverwezen worden naar de regio
Risico naar kwetsbare groepen	• Kwetsbare contacten (70+ en/of onderliggend lijden) • Personen die thuiszorg ontvangen
Risico met beheersing verspreiding	• Aard en hoeveelheid van contacten[2] • Meerdere zieke collega's • Complexiteit met isoleren index patiënt in woning • Specifieke doelgroep (dak/thuis/status-lozen of studenten) • Aanwijzingen van weigerende houding index patiënt of contact t.o.v. quarantaine maatregelen
Overige overwegingen	• Taalbarrière: Op basis van de specifieke taal moet er gekeken worden of regio of landelijk de beste capaciteiten heeft[3] • A-typisch beloop of beeld: Indien arts van de landelijke beldienst een a-typisch beloop of beeld vaststelt, dient er gebeld te worden met de regio voor nadere afstemming

- Tijdens **elke stap** van het BCO-proces kan de landelijke beldienst[1] vaststellen dat het de voorkeur heeft om de **casus terug te verwijzen**
- De beldienst overlegt met de regionale GGD of **alle of een deel van de contacten overdragen worden**
- Dit kan er ook toe leiden dat de landelijke beldienst het BCO afrondt, maar met **aanvullende vragen/opdracht** om e.e.a. uit te vragen

Disclaimer: De set criteria kan door regio's gebruikt worden als uitgangspunt voor terugverwijzing. Er is gekozen voor relatief zachte terugverwijscriteria waarbij het uitgangspunt is dat het een lerend proces gaat zijn en de criteria daartoe kunnen worden aangepast. Bij twijfel moet er te allen tijde overleg tussen de landelijke beldienst en de GGD regio plaatsvinden. Het overleg is leidend in de beslissing om een casus al dan niet terug te verwijzen, niet de criteria.

1. Er wordt nog gekeken naar de formulering van 'landelijke beldienst' (i.v.m. detacheringsconstructie)
2. Het aantal contacten is niet gekwantificeerd daar de interpretatie van dit criterium maatwerk vereist
3. Bij voorkeur wordt er bij de landelijke werving gelet op diversiteit aan talen

3

Bijlage 5 RFC formulier

Basisgegevens Request for Change					
RFC - nummer		Datum			
Order-nummer	.....	RFC-naam			
Invuller formulier (aanvrager)	Naam: Tel nr.:		Verzendlijst RFC	Aan: CC:	
Projectleider aanvrager (indien van toepassing)	Naam: Functie:			Tel.nr.: E-mail:	
Projectleider ontvanger (indien van toepassing)	Naam: Functie:			Tel.nr.: E-mail:	

Omschrijving change		**Akkoord ontvanger**
1. Omschrijving change		
2. Resultaat van de change (vanuit perceptie Opdrachtgever)		
3. Contractuele consequenties		☐ Binnen contract ☐ Buiten contract, zie opm.
4. Implementatie: A. Kosten (andere kosten dan training) B. Datum	..... ☐ in overleg ☐ anders : ☐ z.s.m. :	☐ Geen implementatiekosten ☐ Wel implementatiekosten, zie opm. ☐ Ja ☐ Nee, zie opm.

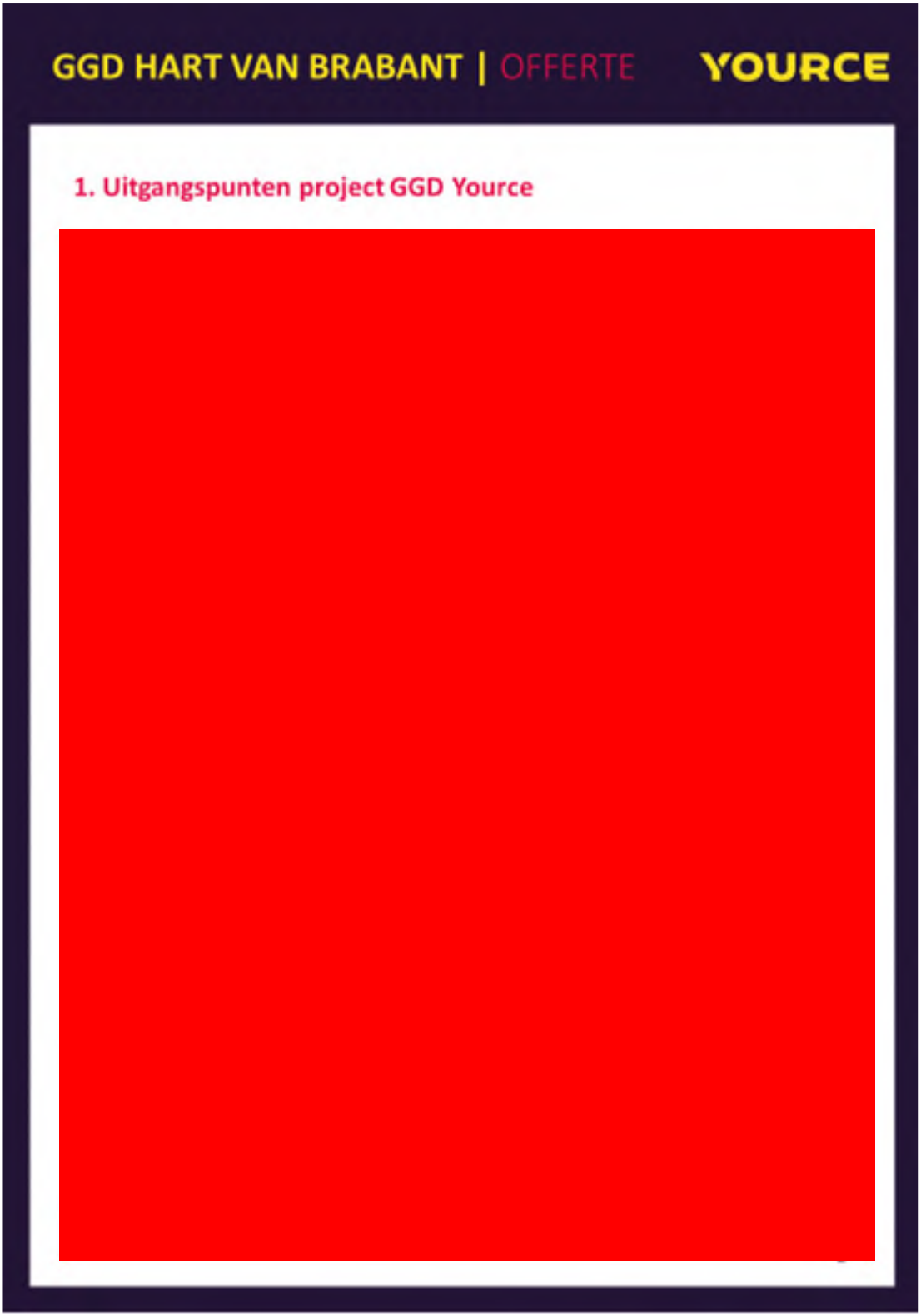
5. Doorlooptijd change	☐ Small Change (implementatie < 2 weken) ☐ Medium Change(implementatie< 6 weken) ☐ Large Change (implementatie > 6 weken)	☐ Ja ☐ Nee, zie opm. ☐ Ja ☐ Nee, zie opm. ☐ Ja ☐ Nee, zie opm.
6. Volume inschatting	FTE's: …… Volume: ……minuten Norm: …… (t.a.v. AHT)	☐ Ja ☐ Nee, zie opm.
7. Invloed op contactkanaal	☐ Schriftelijk/postbus, toelichting zie bijlage ☐ Telefonie, toelichting zie bijlage ☐ E-mail, toelichting zie bijlage ☐ Internet, toelichting zie bijlage ☐ IVR, toelichting zie bijlage	☐ Ja ☐ Nee, zie opm.
8. Invloed op andere processen (intern/extern Opdrachtnemer)	☐ Frontline: …… ☐ Back Office onderdeel: …….. ☐ Overig: ……	☐ Ja ☐ Nee, zie opm. ☐ Ja ☐ Nee, zie opm. ☐ Ja ☐ Nee, zie opm.
9. Wijze van factureren	☐ Opnemen in bestaande facturatie ☐ Aparte factuur (opvragen PO nr. GGD)	☐ Ja ☐ Nee, zie opm. ☐ Ja ☐ Nee, zie opm.

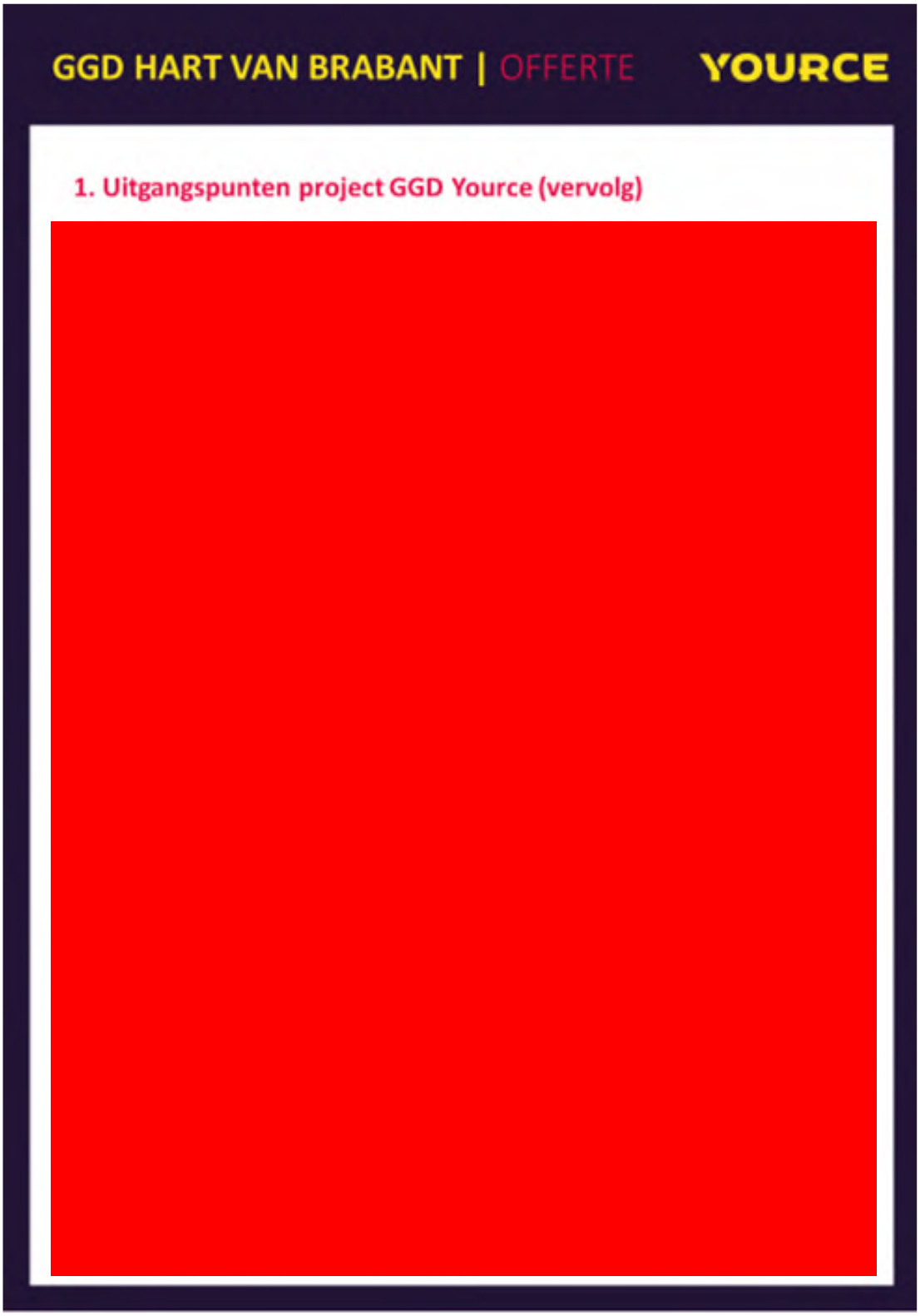
Opmerking 1	…….
Opmerking 2	…….
Opmerking 3	…….
Opmerking 4	…….

Accordering change			
Akkoord	Namens GGD	Naam: Functie:	Datum:
	Handtekening	……	

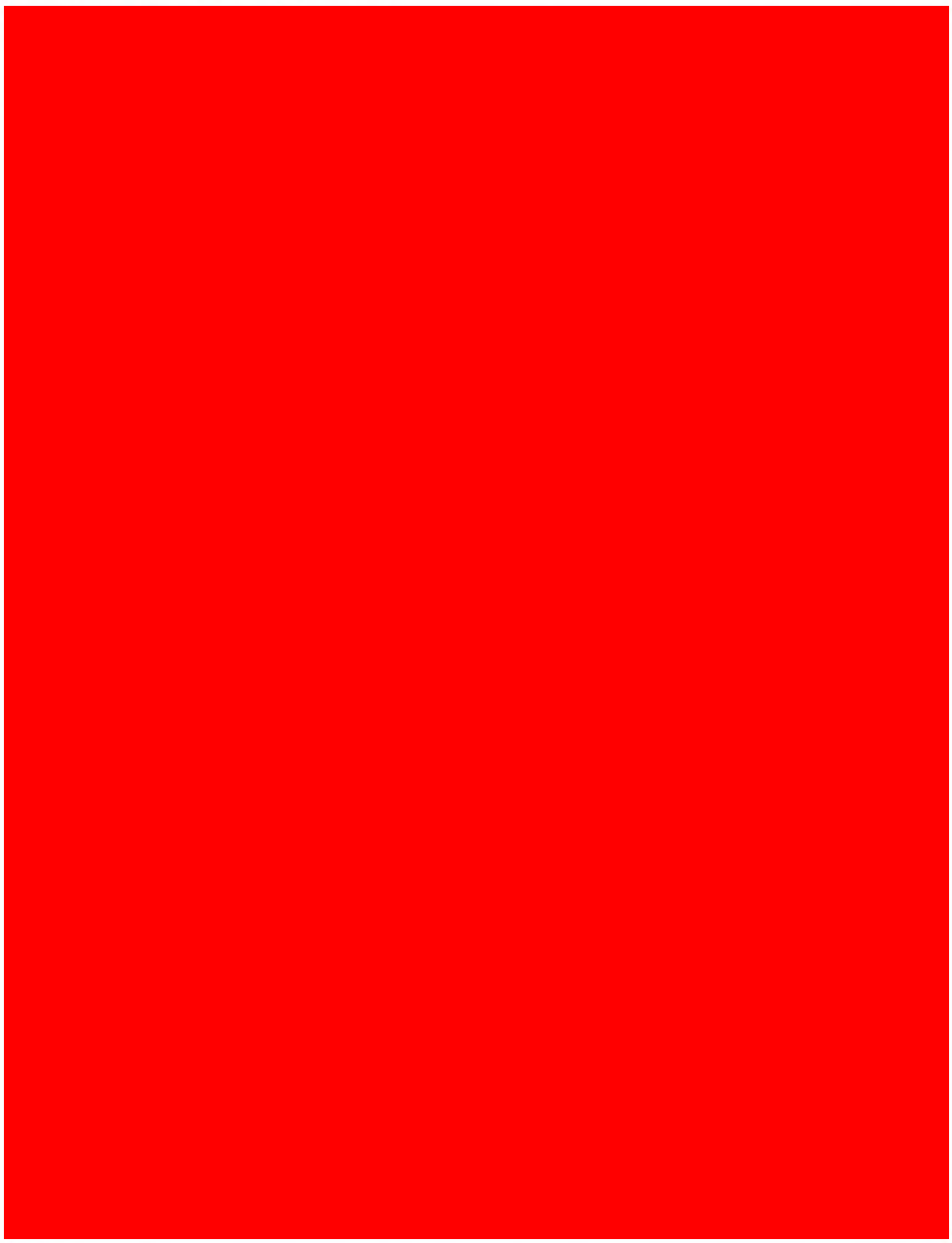
	Namens Yource	Naam: Functie:	Datum:
	Handtekening	…….	

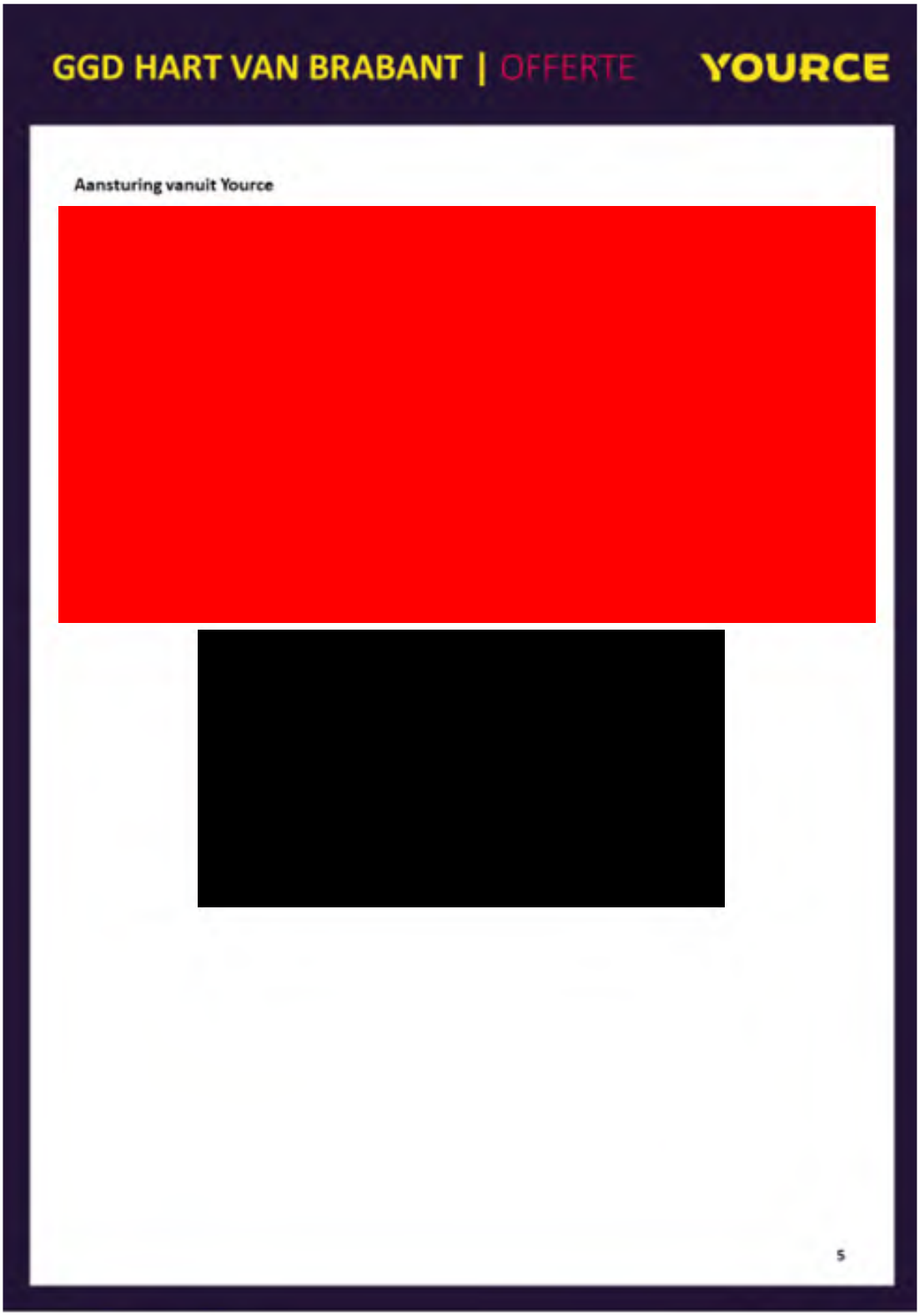
Bijlage 6 Offerte Hart voor Brabant: 07 juni 2020

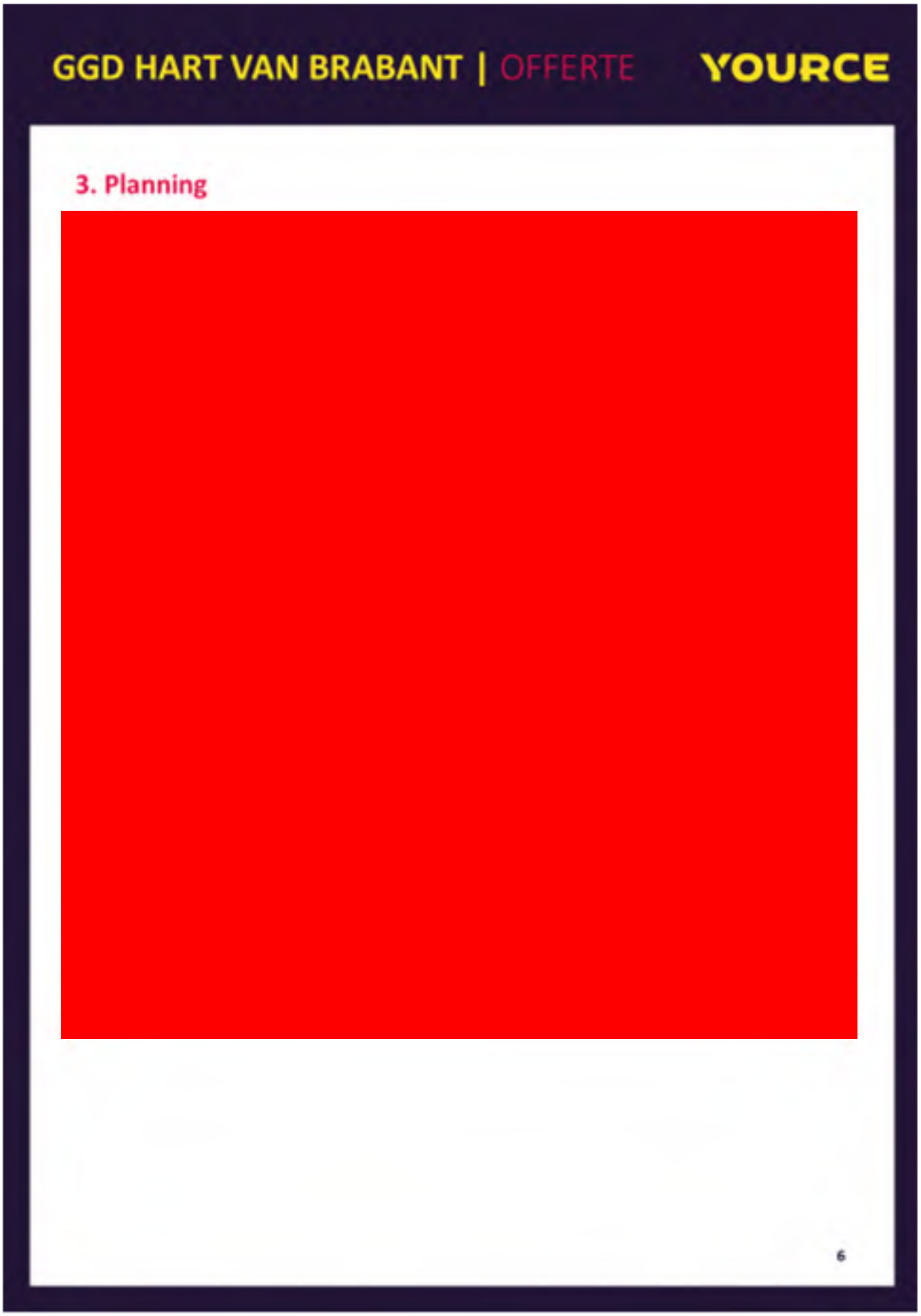

GGD HART VAN BRABANT | OFFERTE
YOURCE
1. Uitgangspunten project GGD Yource

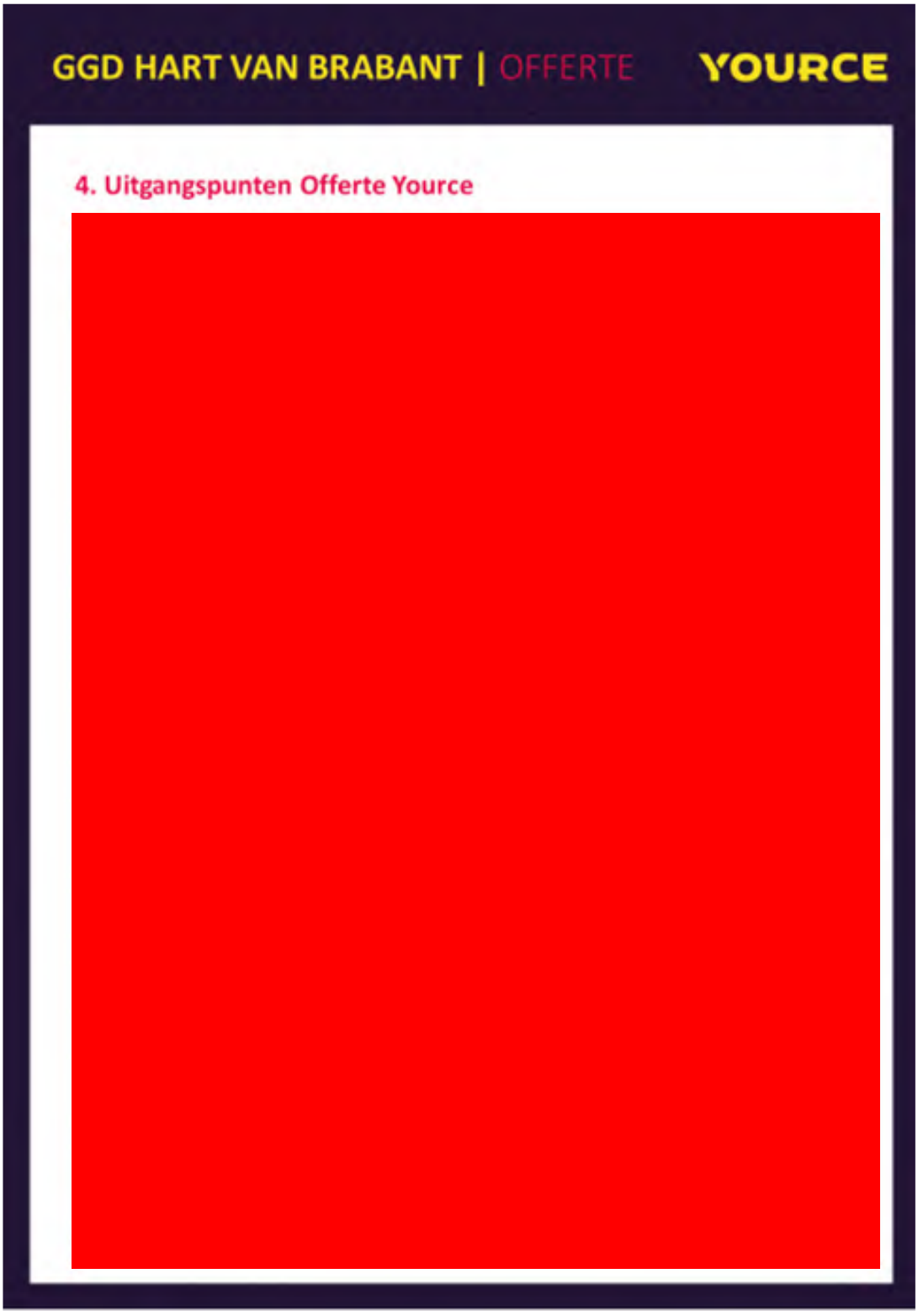

GGD HART VAN BRABANT | OFFERTE
YOURCE
1. Uitgangspunten project GGD Yource (vervolg)

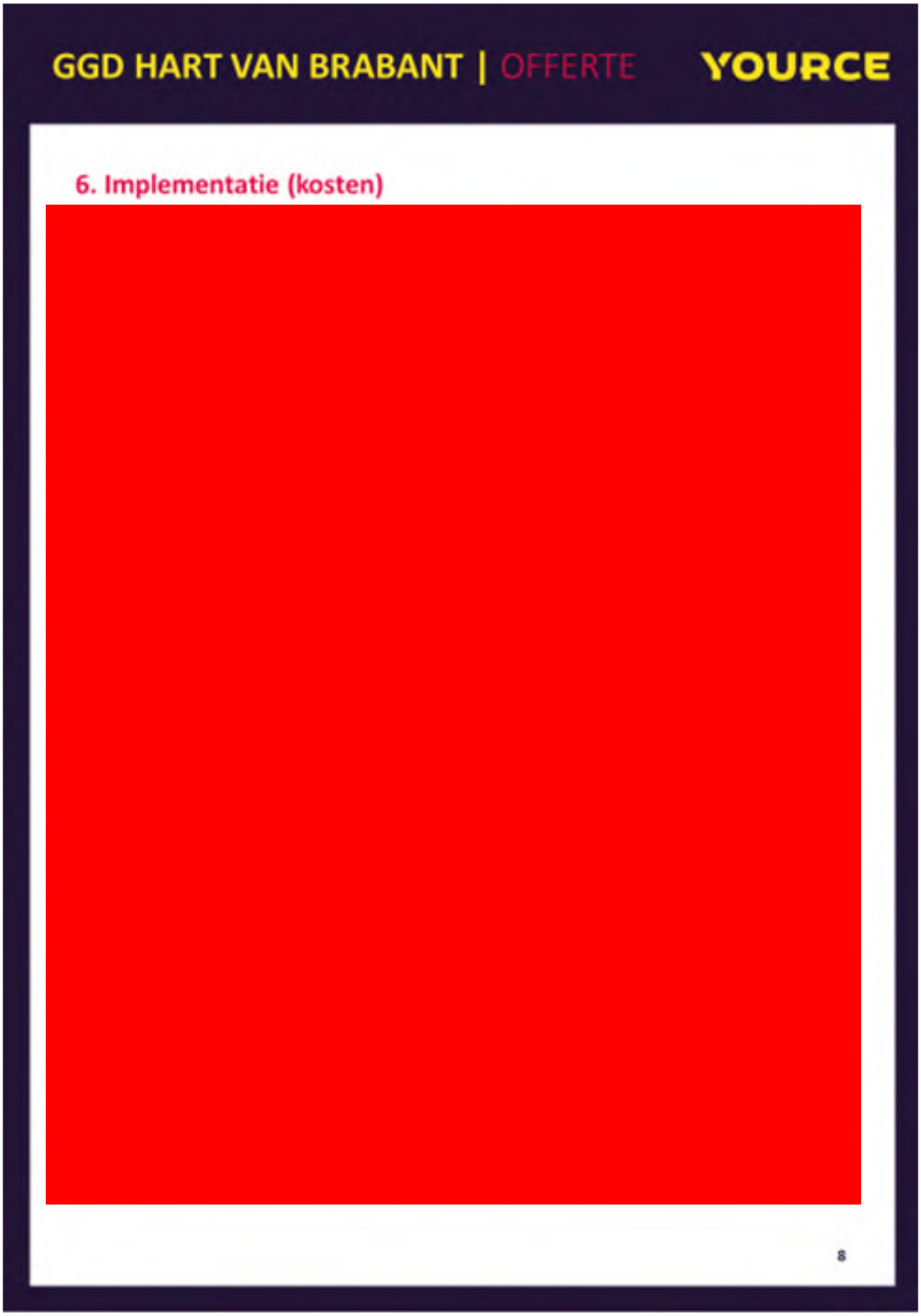
2. Inzet Yource & kwaliteit

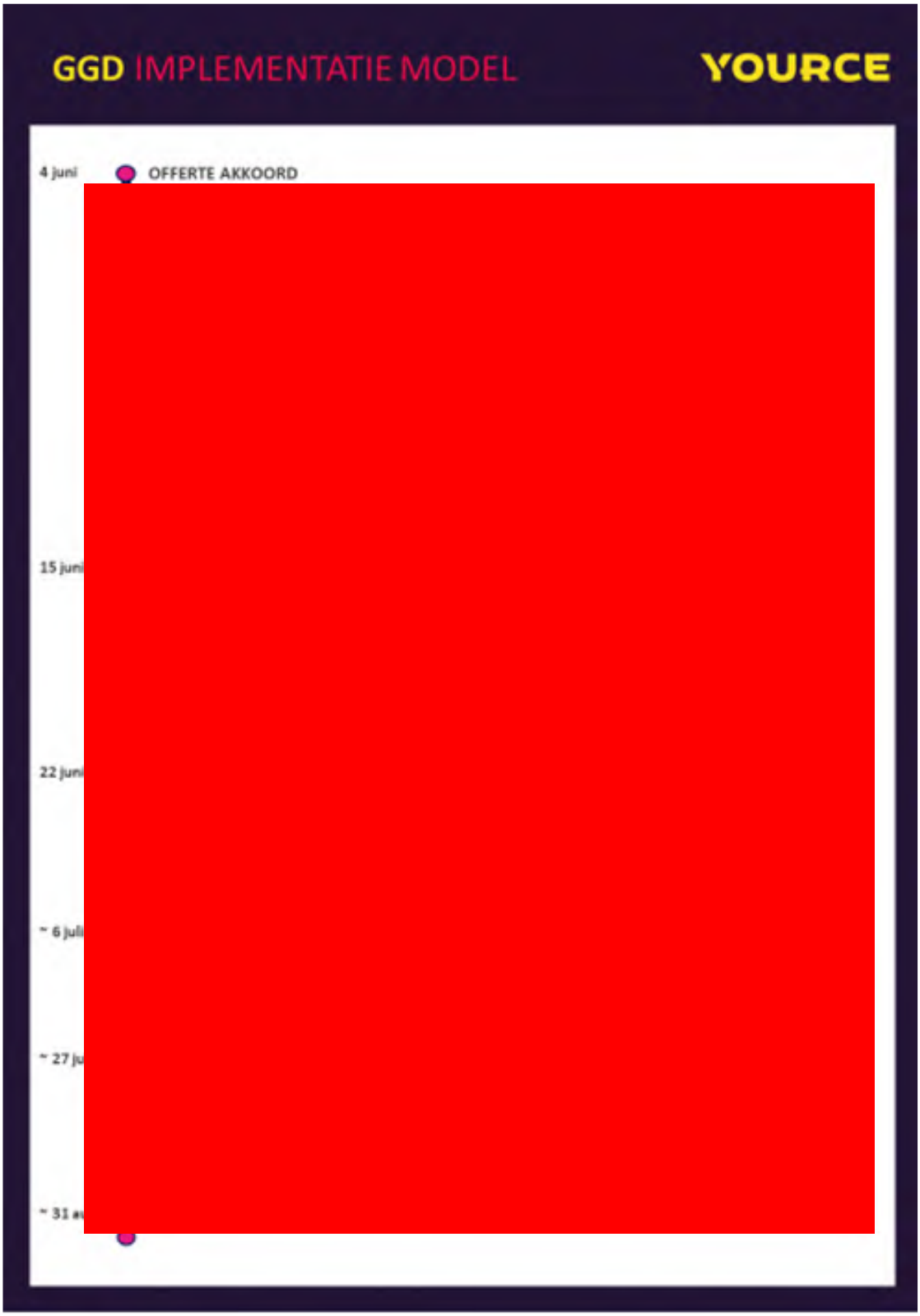


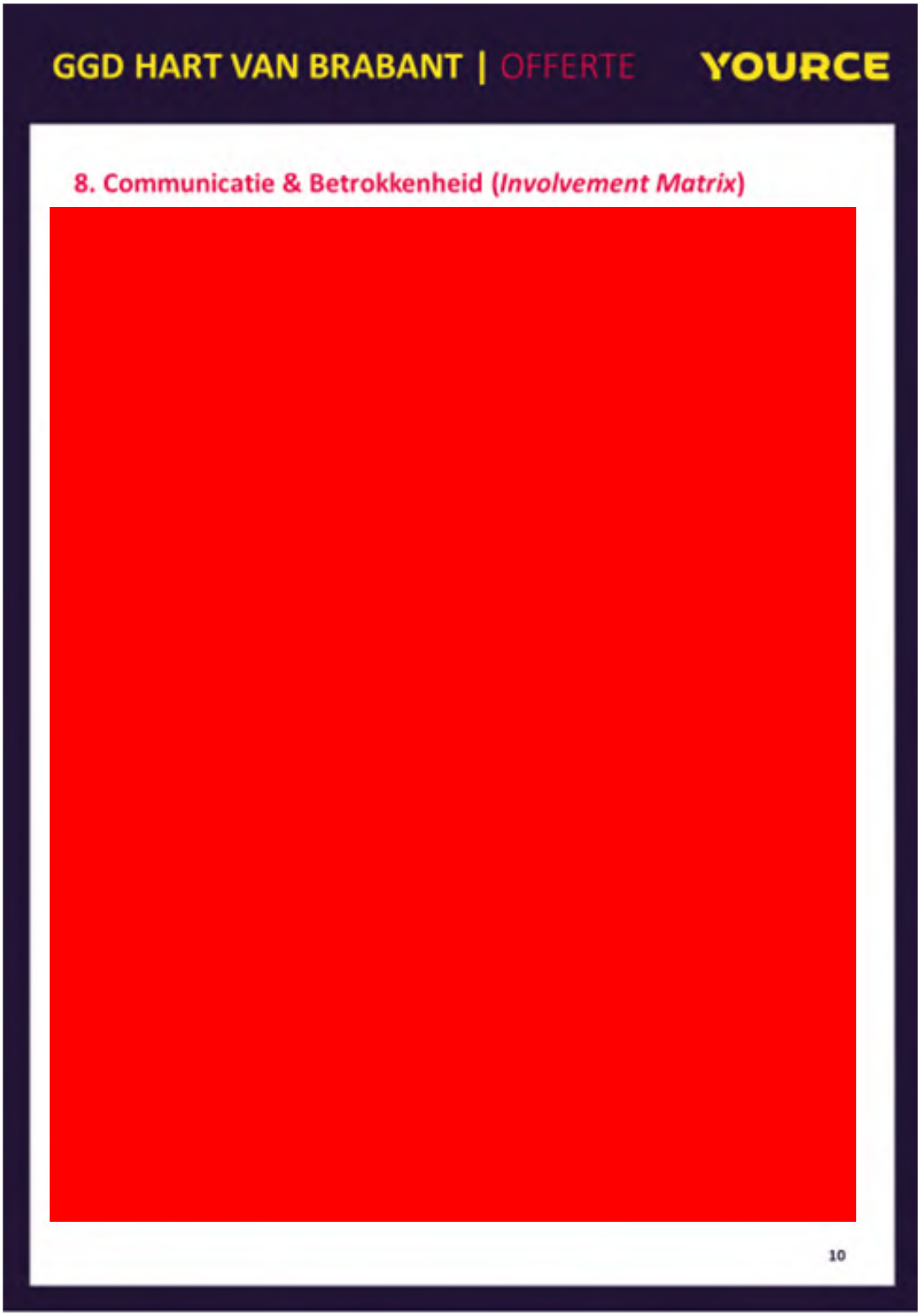

GGD HART VAN BRABANT | OFFERTE
YOURCE
Aansturing vanuit Yource
5

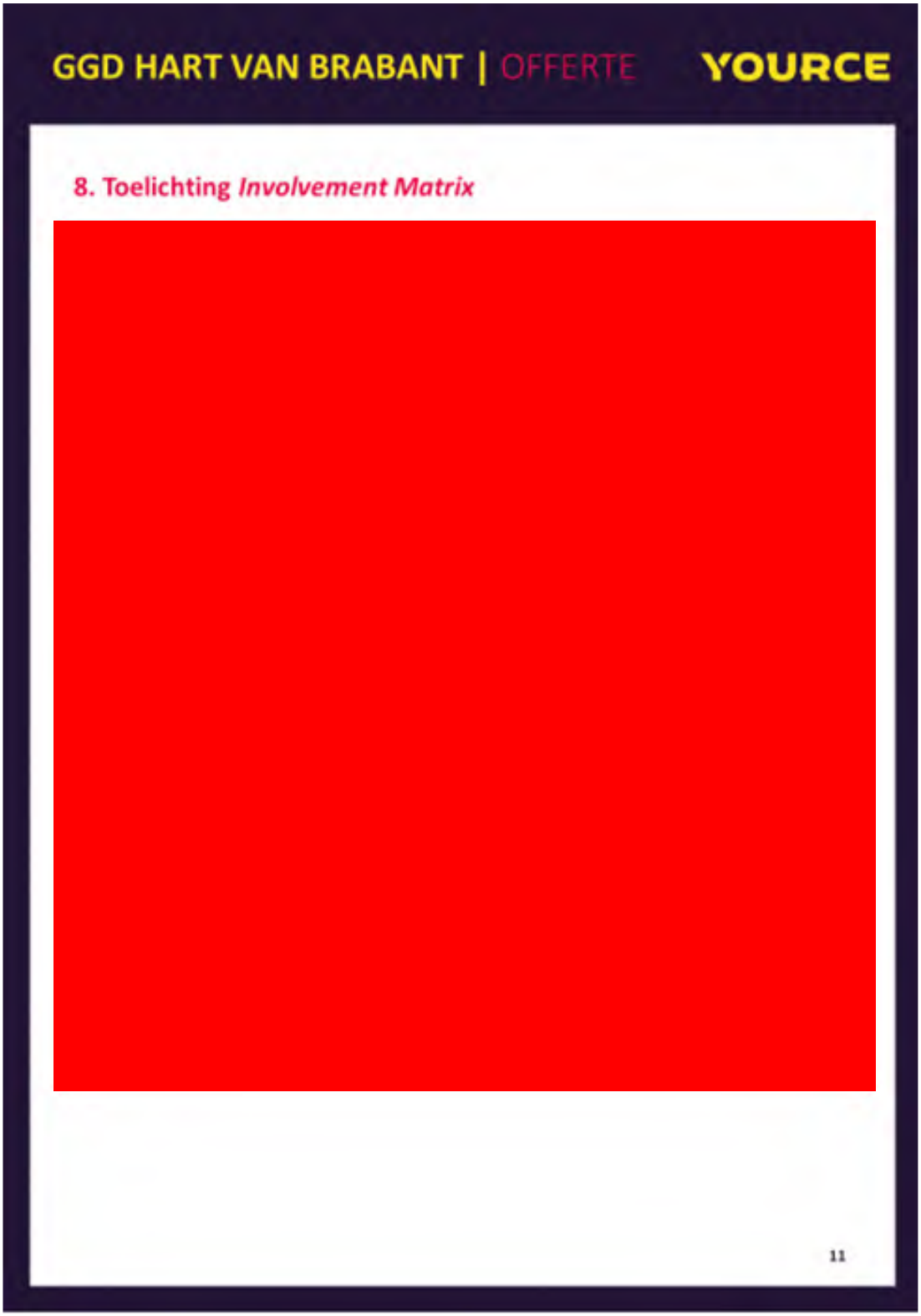

GGD HART VAN BRABANT | OFFERTE
YOURCE
3. Planning
6


GGD HART VAN BRABANT | OFFERTE
YOURCE
4. Uitgangspunten Offerte Yource


GGD HART VAN BRABANT | OFFERTE
YOURCE
6. Implementatie (kosten)
8


GGD IMPLEMENTATIE MODEL
YOURCE
4 juni
OFFERTE AKKOORD
15 juni
22 juni
~ 6 juli
~ 27 ju
~ 31 a


GGD HART VAN BRABANT | OFFERTE
YOURCE
8. Communicatie & Betrokkenheid (*Involvement Matrix*)
10


GGD HART VAN BRABANT | OFFERTE
YOURCE
8. Toelichting *Involvement Matrix*
11

Truly
YOURCE

Verklaring van registratie

Het bestuur van de Stichting Normering Arbeid verklaart dat door een geaccrediteerde inspectie-instelling is vastgesteld dat

Driessen B.V.

HELMOND

voldoet aan de normen zoals vastgelegd in het Handboek Normen SNA en is opgenomen in het Register Normering Arbeid.
Het register is te raadplegen op www.normeringarbeid.nl.

Datum: 06-01-2021

KvK nr.: 67396313

Deze verklaring is alleen geldig in combinatie met een actuele vermelding in het register. Het register is hierin te allen tijde leidend. Aanpassingen in het register vinden dagelijks plaats.

Postbus 4076, 5004 JB Tilburg
info@normeringarbeid.nl | www.normeringarbeid.nl

Voor het invullen dient het UEA te zijn geopend met Acrobat Reader.
Invullen van dit PDF formulier met gebruik van een ander programma dan Acrobat Reader kan leiden tot onjuiste weergave van de ingevulde gegevens na het digitaal versturen van het document, waardoor de inhoud van het UEA een andere kan worden dan bedoeld.

Ministerie van Economische Zaken en Klimaat

Uniform Europees Aanbestedingsdocument

Verwijzing naar de ***relevante aankondiging***[1] die bekend is gemaakt in het Publicatieblad van de Europese Unie:

Nummer aankondiging in PB EU S *(alleen indien u beschikt over dit nummer)*:

_____ /S _____ - _____

Vermeld, wanneer bekendmaking van een aankondiging in het Publicatieblad van de Europese Unie niet is vereist, andere gegevens op basis waarvan ondubbelzinnig kan worden vastgesteld om welke aanbestedingsprocedure het gaat (bijvoorbeeld verwijzing naar een bekendmaking op nationaal niveau):

_____

Deze aanbesteding betreft:

- (●) **Een procedure boven de van toepassing zijnde Europese aanbestedingsdrempel**
- ( ) **Een procedure onder de van toepassing zijnde Europese aanbestedingsdrempel**
- ( ) **Een procedure van een speciale-sectorbedrijf**

[1] Voor aanbestedende diensten: ofwel een vooraankondiging die als oproep tot mededinging wordt gebruikt of een aankondiging van een opdracht. Voor aanbestedende entiteiten: een periodieke indicatieve aankondiging die als oproep tot mededinging wordt gebruikt, een aankondiging van een opdracht of een aankondiging inzake het bestaan van een erkenningsregeling.

Gebruikersinstructie

Hoe vul ik de gegevensvelden in?
De tekstvelden van het UEA Model zijn zo ingericht dat ze meebewegen met de hoeveelheid in te vullen tekst. Let op: bij het typen zelf beweegt het typveld nog niet direct mee, pas wanneer je overschakelt naar het volgende tekstveld past het document zich aan op de hoeveelheid ingevulde tekst.

Deel I Gegevens over de aanbestedingsprocedure en de aanbestedende dienst of aanbestedende entiteit (inclusief speciale-sectorbedrijven)

*De **aanbestedende dienst of entiteit** kruist aan wat van toepassing is op deze pagina én in deel III.*
*Alle overige gegevens in alle delen van het UEA moeten door de **ondernemer** worden ingevuld.*

Identiteit van de aanbesteder[2]	Hét Service Centrum (HSC)
Om welke aanbesteding gaat het? *> Titel of beknopte beschrijving van de aanbesteding*[3]	Inhuur flexibele arbeidskrachten ten behoeve van de GGD Hart voor Brabant GGD West Brabant en de RAV Brabant Midden West Noord
Referentienummer van het dossier bij de aanbestedende dienst of aanbestedende entiteit (indien van toepassing)[4]	Z-20026859

[2] Uit deel I, punt I.1, van de betreffende aankondiging over te nemen gegevens. Vermeld in geval van gezamenlijke aanbesteding de namen van alle betrokken aanbesteders.

[3] Zie de punten II.1.1 en II.1.3 van de betreffende aankondiging.

[4] Zie punten II.1.1 van de betreffende aankondiging.

Deel II Gegevens met betrekking tot de ondernemer

Deel II A Gegevens over de ondernemer

Identificatie

Naam	Driessen Holding B.V.
BTW-nummer	NL8152.47.011.B01
KvK-nummer	17185869
Vermeld indien er geen BTW-nummer of KvK-nummer van toepassing is, een ander nationaal identificatienummer, indien vereist en toepasselijk.	n.v.t.
Postadres	Postbus 748, 5700 AS Helmond
Telefoonnummer	0492 - 50 66 66
E-mail adres	aanbestedingen@driessengroep.nl
Internet adres	www.driessengroep.nl
Contactpersoon of -personen	[redacted]

Algemene informatie

Is de ondernemer een micro-, kleine of middelgrote onderneming[5]

○ Ja ◉ Nee

[5] In de zin van de aanbeveling van de Commissie van 6 mei 2003 betreffende de definitie van micro-, kleine en middelgrote ondernemingen (PB L 124 van 20.5.2003, blz. 36). Deze informatie is uitsluitend vereist voor statistische doeleinden. Micro-ondernemingen: een onderneming met minder dan 10 werknemers en met een jaaromzet en/of jaarlijks balanstotaal van niet meer dan 2 miljoen euro. Kleine ondernemingen: een onderneming met minder dan 50 werknemers en met een jaaromzet en/of jaarlijks balanstotaal van niet meer dan 10 miljoen euro; middelgrote ondernemingen, ondernemingen die micro noch klein zijn en met minder dan 250 personen werknemers en een jaaromzet van niet meer dan 50 miljoen euro en/of een jaarlijks balanstotaal van niet meer dan 43 miljoen euro.

Alleen wanneer de aanbesteding voorbehouden is[6]

Is de ondernemer een sociale werkplaats of een "sociale onderneming"[7] of zorgt de onderneming voor de uitvoering van de overeenkomst in het kader van programma's voor beschermde arbeid?

○ Ja ◉ Nee

[6] Zie punt III.1.5 van de aankondiging van de opdracht.

[7] Zoals bedoeld in artikel 2.82 aanbestedingswet 2012

Wijze van deelneming

Neemt de ondernemer samen met anderen deel aan de aanbestedingsprocedure[9]?

○ Ja ◉ Nee

[9] Met name als deel van een combinatie, consortium, joint venture, enz.

Percelen

Vermeld, indien van toepassing, het perceel/de percelen waarop de ondernemer wil inschrijven

Perceel 6: Administratief en perceel 8: HR specialisten

Deel II B Informatie over de vertegenwoordigers van de ondernemer

Vermeld, indien van toepassing, naam/namen en adres/adressen van de persoon/personen die gemachtigd is/zijn om de ondernemer bij deze aanbestedingsprocedure te vertegenwoordigen.

Alleen nodig indien afgeweken wordt van de vertegenwoordigingsbevoegdheid zoals opgenomen in het KvK Handelsregister.

Vertegenwoordiger 1

Volledige naam

Geboortedatum

Functie/optredend als

Postadres

Telefoonnummer

E-mail adres

Vermeld zo nodig gedetailleerde informatie over de vertegenwoordiging > *(vorm, reikwijdte, doel, enz.)*

Deel II C Informatie over beroep op draagkracht van andere entiteiten

Draagkracht kan betrekking hebben op financiële en economische draagkracht, maar ook op bijvoorbeeld technische bekwaamheid, beroepsbevoegdheid of het bezit van certificaten.

Doet de ondernemer beroep op de draagkracht van andere entiteiten om te voldoen aan de selectiecriteria van deel IV en de (eventuele) criteria en regels van onderstaande deel V?

○ Ja ○ Nee

Deel II D Informatie betreffende onderaannemers op wier draagkracht de ondernemer geen beroep doet

*(Gedeelte dat alleen moet worden ingevuld wanneer de aanbestedende dienst of aanbestedende entiteit **expliciet** om deze gegevens vraagt.)*

Is de ondernemer van plan een gedeelte van de opdracht in onderaanneming aan derden te geven?	○ Ja ○ Nee

Deel III Uitsluitingsgronden

Deel III A Gronden die verband houden met strafrechtelijke veroordelingen

Gronden in verband met strafrechtelijke veroordelingen krachtens nationale bepalingen waarbij de in artikel 57, lid 1, van de richtlijn vermelde gronden worden omgezet.

Artikel 57, lid 1, van Richtlijn 2014/24/EU vermeldt de volgende uitsluitingsgronden:

1. *Deelneming aan een criminele organisatie*[10]
2. *Corruptie*[11]
3. *Fraude*[12]
4. *Terroristische misdrijven of strafbare feiten in verband met terroristische activiteiten*[13]
5. *Witwassen van geld of financiering van terrorisme*[14]
6. *Kinderarbeid en andere vormen van mensenhandel*[15]

Aan te kruisen door aanbestedende dienst, aanbestedende entiteit *indien het een procedure onder de Europese aanbestedingsdrempel of een procedure van een speciale-sectorbedrijf betreft.*

Bij deze aanbestedingsprocedure zijn de volgende uitsluitingsgronden van toepassing:

- ☐ Geen
- ☒ 1 Deelneming aan een criminele organisatie
- ☒ 2 Corruptie
- ☒ 3 Fraude
- ☒ 4 Terroristische misdrijven of strafbare feiten in verband met terroristische activiteiten
- ☒ 5 Witwassen van geld of financiering van terrorisme
- ☒ 6 Kinderarbeid en andere vormen van mensenhandel

Is de ondernemer zelf of iemand die lid is van het bestuurs-, leidinggevend of toezichthoudend orgaan van de ondernemer of daarin vertegenwoordigings-, beslissings- of controlebevoegdheid heeft, om een van de hiervoor genoemde redenen veroordeeld bij onherroepelijk vonnis, welk vonnis niet later dan vijf jaar geleden is gewezen of dat expliciet een uitsluitingsperiode bevat die nog steeds van toepassing is?

○ Ja ◉ Nee

Vermeld, indien de relevante stukken elektronisch beschikbaar zijn:

Internetadres

Afgevende entiteit

Precieze referentienummers van de stukken

Deel III B Gronden die verband houden met de betaling van belastingen of sociale premies

Aan te kruisen door aanbestedende dienst, aanbestedende entiteit *indien het een procedure onder de Europese aanbestedingsdrempel of een procedure van een speciale-sectorbedrijf betreft.*

Bij deze aanbestedingsprocedure zijn de volgende uitsluitingsgronden van toepassing:

- ☒ Betaling van belastingen of sociale premies

Heeft de ondernemer voldaan aan al zijn verplichtingen met betrekking tot de betaling van belastingen of sociale premies, zowel in het land waar hij is gevestigd als in de lidstaat van de aanbestedende dienst of aanbestedende entiteit indien dit een ander land is dan het land van vestiging?

Belastingen ◉ Ja ○ Nee

Sociale premies ◉ Ja ○ Nee

Deel III C Gronden met betrekking tot insolventie, belangenconflicten of beroepsfouten[18]

Aan te kruisen door aanbestedende dienst, aanbestedende entiteit

Deze gronden zijn facultatief zowel boven als onder de Europese aanbestedingsdrempel.

Bij deze aanbestedingsprocedure zijn de volgende uitsluitingsgronden van toepassing:

- ☐ Geen
- ☒ Schending verplichtingen o.b.v. milieu-, sociaal- of arbeidsrecht
- ☒ Faillissement, insolventie of gelijksoortig
- ☐ Ernstige beroepsfout
- ☒ Vervalsing van de mededinging
- ☐ Belangenconflict
- ☐ Betrokken bij de voorbereiding
- ☐ Prestaties uit het verleden
- ☒ Valse verklaring
- ☒ Onrechtmatige beïnvloeding

Er zij op gewezen dat in het kader van deze aanbesteding sommige van de volgende uitsluitingsgronden preciezer omschreven kunnen zijn in de nationale wetgeving, de betreffende aankondiging of de aanbestedingsstukken. De nationale wetgeving kan bijvoorbeeld bepalen dat het begrip "ernstige beroepsfout" verschillende gedragingen kan omvatten.

Schending verplichtingen o.b.v. milieu-, sociaal of arbeidsrecht

Heeft de ondernemer, voor zover hij weet, zijn verplichtingen op het gebied van het milieu-, sociaal of arbeidsrecht geschonden[18]?

○ Ja ◉ Nee

[18] Zie artikel 57, lid 4, van Richtlijn 2014/24/EU.

Faillissement, insolventie of gelijksoortig

Is op de ondernemer een van de volgende situaties van toepassing:
a) Hij is failliet, of
b) Hij verkeert in insolventie of liquidatie, of
c) Hij heeft een regeling met schuldeisers getroffen, of
d) Hij verkeert in een andere, vergelijkbare toestand ingevolge een soortgelijke procedure uit hoofde van nationale wet- of regelgeving[19], of
e) Zijn activa worden beheerd door een curator of door de rechtbank, of
f) Zijn bedrijfsactiviteiten zijn gestaakt?

○ Ja ◉ Nee

[19] Zie de nationale wetgeving, de betreffende aankondiging of de aanbestedingsstukken.

Vervalsing van de mededinging

Heeft de ondernemer met andere ondernemers overeenkomsten gesloten die gericht zijn op vervalsing van de mededinging?

○ Ja ◉ Nee

Valse verklaring

Kan de ondernemer bevestigen dat:
a) hij zich niet in ernstige mate schuldig heeft gemaakt aan valse verklaringen bij het verstrekken van de informatie die nodig is om te controleren of er geen gronden voor uitsluiting zijn dan wel of aan de selectiecriteria wordt voldaan,
b) hij dergelijke informatie niet heeft achtergehouden,
c) hij de door de aanbestedende dienst of aanbestedende entiteit gevraagde ondersteunende documenten onverwijld heeft kunnen overleggen

◉ Ja ○ Nee

Onrechtmatige beïnvloeding

Kan de ondernemer bevestigen dat: d) hij niet heeft getracht het besluitvormingsproces van de aanbestedende dienst of aanbestedende entiteit onrechtmatig te beïnvloeden, om vertrouwelijke informatie te verkrijgen die hem onrechtmatige voordelen in de aanbestedingsprocedure kan bezorgen, of om verwijtbaar misleidende informatie te verstrekken die een belangrijke invloed kan hebben op besluiten inzake uitsluiting, selectie of gunning?	◉ Ja ○ Nee

Deel IV Selectiecriteria

Bedoeld worden geschiktheidseisen zoals vermeld in de Aanbestedingswet 2012.

α: Algemene aanwijzing voor alle selectiecriteria

De ondernemer verklaart met betrekking tot de selectiecriteria dat, hij voldoet aan de voorgeschreven selectiecriteria

○ Ja ○ Nee

Deel V Beperking van het aantal gekwalificeerde gegadigden

Het navolgende geldt uitsluitend voor niet-openbare procedures, mededingingsprocedures met onderhandeling, concurrentiegerichte dialogen en innovatiepartnerschappen.
De ondernemer hoeft uitsluitend informatie te verstrekken wanneer de aanbestedende dienst of aanbestedende entiteit de objectieve en niet-discriminerende criteria of regels heeft vastgesteld die moeten worden toegepast om het aantal gegadigden dat tot indiening van een inschrijving of tot een dialoog zal worden uitgenodigd, te beperken. Deze informatie, die vergezeld kan gaan van vereisten met betrekking tot de eventueel te overleggen (soorten) certificaten of andere vormen van bewijsstukken, wordt vermeld in de betreffende aankondiging of in de in die aankondiging bedoelde aanbestedingsstukken.

Bedoeld worden selectiecriteria zoals vermeld in de Aanbestedingswet 2012.

De ondernemer verklaart dat:

Er wordt op de volgende wijze voldaan aan de objectieve en niet-discriminerende criteria en regels te beperking van het aantal gegadigden.

Geef, in geval bepaalde certificaten of andere vormen van bewijsstukken zijn vereist, aan of de ondernemer over de vereiste documenten beschikt:

○ Ja ○ Nee

Uniform Europees Aanbestedingsdocument

Ministerie van Economische Zaken en Klimaat

Deel VI Slotopmerkingen

Ondergetekende(n) verklaart/verklaren formeel dat de door hem/haar/hen hiervoor in de delen II–V verstrekte informatie accuraat en correct is en dat hij/zij zich volledig bewust is/zijn van de consequenties van het afleggen van een valse verklaring.

Ondergetekende(n) verklaart/verklaren formeel desgevraagd en onverwijld de hiervoor bedoelde certificaten en andere vormen van bewijsstukken te kunnen overleggen, tenzij:

a) de aanbestedende dienst of instantie de betrokken ondersteunende documenten rechtstreeks kan verkrijgen door raadpleging in een lidstaat van een gratis toegankelijke nationale databank[23] of

b) de aanbestedende dienst of instantie met ingang van uiterlijk 18 oktober 2018[24] reeds over de betrokken informatie beschikt.

Ondergetekende(n) stemt/stemmen er formeel mee in dat de aanbestedende dienst of aanbestedende entiteit bedoeld in deel I, afdeling A toegang krijgt tot stukken tot staving van de informatie die is verstrekt in dit Uniform Europees Aanbestedingsdocument met het oog op de onderhavige aanbestedingsprocedure.

[23] Op voorwaarde dat de ondernemer de noodzakelijke informatie heeft verstrekt (internetadres, afgevende entiteit, precieze referentienummers van de stukken) waardoor de aanbestedende dienst of aanbestedende instantie daartoe in staat wordt gesteld. Indien voorgeschreven, moet dit vergezeld gaan van de betreffende instemming met een dergelijke raadpleging.

[24] Afhankelijk van de nationale uitvoering van artikel 59, lid 5, tweede alinea van Richtlijn 2014/24/EU.

Datum, plaats en, indien vereist of noodzakelijk, handtekening(en):
(Ondertekenen kan alleen schriftelijk na printen.)

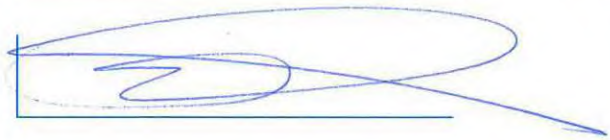
Naam 1 [redacted]

Functie [redacted]

Plaats Helmond

Datum maandag 18 januari 2021

Handtekening



24-juni-2020

VERWERKERSOVEREENKOMST

GGD HART VOOR BRABANT

YOURCE

De ondergetekenden:

1. De publiekrechtelijke rechtspersoon Gemeentelijke of Gemeenschappelijke Gezondheidsdienst Hart voor Brabant, statutair gevestigd en kantoorhoudende te 5216 PD, 's Hertogenbosch te Pettelaarpark 10, ingeschreven in het handelsregister van de Kamer van Koophandel onder nummer 17247544, hierna ook te noemen: "Verantwoordelijke", hierbij vertegenwoordigd door mevr. [redacted]; en

2. De besloten vennootschap met beperkte aansprakelijkheid Yource Outsouring b.v. (en alle aan haar gelieerde partijen binnen de Yource Group), statutair gevestigd en kantoorhoudende te (1311 RK) Almere aan de Louis Armstrong 26, ingeschreven in het handelsregister van de Kamer van Koophandel onder nummer 52217051, hierna ook te noemen "Verwerker", hierbij vertegenwoordigd door de heer [redacted].

Gezamenlijk hierna ook te noemen ***"Partijen",***

Overwegende dat:

I. Verantwoordelijke gebruik wil maken van de diensten van Verwerker;
II. Partijen hiertoe op 31 mei 2020 een overeenkomst zijn aangegaan ten aanzien van de door Verwerker te verrichten dienst (hierna: "Overeenkomst";
III. Verwerker in het kader van de Overeenkomst persoonsgegevens (hierna: "Persoonsgegevens") zal verwerken ten behoeve van Verantwoordelijke;
IV. Alle begrippen in deze Verwerkersovereenkomst de betekenis als bedoeld in de Algemene Verordening Gegevensbescherming (hierna: "AVG") hebben;
V. Partijen - mede ter uitvoering van het bepaalde in artikel 14 lid 2 AVG - in de onderhavige Verwerkersovereenkomst voorwaarden wensen vast te leggen die van toepassing zijn op hun relatie in verband met de uitvoering van de Overeenkomst.

Verklaren te zijn overeengekomen als volgt:

Artikel 1. Onderwerp van de Verwerkersovereenkomst

1. Verantwoordelijke is de verwerkingsverantwoordelijke voor de verwerking van de Persoonsgegevens in het kader van de Overeenkomst. Verwerker heeft geen zelfstandige zeggenschap over de Persoonsgegevens. Verwerker verwerkt Persoonsgegevens slechts in opdracht van Verantwoordelijke in het kader van de uitvoering van de Overeenkomst, in overeenstemming met de door Verantwoordelijke bepaalde doeleinden en middelen, met inachtneming van de wettelijke bewaartermijn, alsmede in overeenstemming met door de Verantwoordelijke verstrekte schriftelijke instructies.
2. De Persoonsgegevens worden door Verwerker verwerkt ter uitvoering van de Overeenkomst. Het doel van de verwerking en het soort persoonsgegevens en categorie van betrokkenen zijn beschreven in de bijlagen bij deze Verwerkersovereenkomst.
3. Verwerker onderkent dat hij bijzondere categorieën Persoonsgegevens verwerkt op de voet van artikel 9 lid 2 AVG zoals beschreven in Bijlage 2 bij deze Verwerkersovereenkomst en verbindt zich om deze Persoonsgegevens zeer zorgvuldig te verwerken, alsmede in overeenstemming met de toepasselijke wet- en regelgeving.
4. Verwerker verwerkt de Persoonsgegevens niet verder dan in dit artikel 1 is bepaald. In geen geval zal Verwerker de Persoonsgegevens aanwenden voor eigen doeleinden of deze (laten) exploiteren.
5. Verwerker verschaft enkel toegang tot Persoonsgegevens aan haar medewerkers voor zover dit nodig is voor de uitvoering van de Overeenkomst en de Verwerkersovereenkomst en met inachtneming van het bepaalde in artikel 6.

6. De zeggenschap over de Persoonsgegevens berust te allen tijde bij Verantwoordelijke. Dat betekent onder meer dat Verwerker geen zeggenschap heeft over het doel en de middelen voor de Verwerking van Persoonsgegevens en geen beslissingen neemt over de ontvangst en het gebruik van de Persoonsgegevens, de verstrekking aan derden en de duur van de opslag van Persoonsgegevens.

Artikel 2. Technische en organisatorische voorzieningen (beveiliging)

1. Verwerker alle zal passende technische en organisatorische maatregelen ten uitvoer leggen om de Persoonsgegevens te beveiligen tegen i) vernietiging, ii) verlies, iii) vervalsing, iv) niet toegelaten verspreiding en/of toegang tot, dan wel v) enige andere vorm van onrechtmatige verwerking ("Datalek").
2. Deze maatregelen zullen, rekening houdend met de stand der techniek en de aard, omvang van de persoonsgegevens en verwerkingsdoeleinden, een passend beveiligingsniveau garanderen, gelet op de risico's die de verwerking en de aard van de te beschermen gegevens met zich meebrengen. De maatregelen zijn er mede op gericht onnodige verzameling en verdere Verwerking van Persoonsgegevens te voorkomen. Onder de in dit artikel bedoelde beveiligingsmaatregelen worden in ieder geval begrepen de maatregelen als beschreven in bijlagen bij deze Verwerkersovereenkomst en de Dienstovereenkomst.
3. Verantwoordelijke kan aanpassing van de beveiligingsmaatregelen weigeren of voorwaarden aan een wijziging verbinden. Verantwoordelijke heeft de bevoegdheid om aanpassing van de beveiligingsmaatregelen te eisen, indien de beveiligingsmaatregelen aantoonbaar onbetrouwbaar zijn, bijvoorbeeld vanwege een wijziging van de stand van de techniek.
4. Verwerker zal ieder Datalek alsmede ieder redelijk vermoeden dat een Datalek plaatsvindt of heeft plaatsgevonden, onverwijld - maar uiterlijk binnen 24 uur- nadat het Datalek ter kennis van Verwerker is gekomen, meedelen aan Verantwoordelijke waarna Verwerker de instructies van Verantwoordelijke steeds strikt en onverwijld zal opvolgen.
5. In het geval van een Datalek treft Verwerker onverwijld herstelmaatregelen en verstrekt Verwerker Verantwoordelijke, op diens verzoek, onverwijld alle noodzakelijke informatie en medewerking om de Verantwoordelijke in staat te stellen zo spoedig mogelijk de oorzaak, omvang en de gevolgen van het Datalek vast te stellen.
6. Zolang het Datalek voortduurt, informeert Verwerker Verantwoordelijke iedere 24 uur in ieder geval over de status en de aard van het Datalek, de geconstateerde en de vermoedelijke gevolgen van het Datalek, de instanties waar meer informatie over het Datalek kan worden verkregen en de aanbevolen maatregelen om de negatieve gevolgen van het Datalek te beperken.
7. Uitsluitend voor zover dat noodzakelijk is voor de nakoming van de Overeenkomst door Verwerker, verschaft Verwerker haar werknemers toegang tot de Persoonsgegevens. De werknemers van Verwerker mogen slechts die handelingen met betrekking tot de Persoonsgegevens verrichten, die noodzakelijk zijn voor nakoming van de Onderliggende Overeenkomst door Verwerker.
8. Indien naar het oordeel van Verwerker een voorwaarde uit de Verwerkersovereenkomst of een schriftelijke instructie van Verantwoordelijke op grond van de Verwerkersovereenkomst, in strijd is met de AVG of enige andere regel die geldt voor de Verwerking van Persoonsgegevens, zal Verwerker Verantwoordelijke hierover onmiddellijk informeren

Artikel 3. Inschakeling derden

1. Verwerker is slechts gerechtigd de uitvoering van de werkzaamheden geheel of ten dele uit te besteden aan derden na voorafgaande schriftelijke toestemming van Verantwoordelijke. Verantwoordelijke kan aan de schriftelijke toestemming voorwaarden verbinden, onder meer op het gebied van geheimhouding, ter naleving respectievelijk controle van de verplichtingen uit de Verwerkersovereenkomst. Verwerker blijft bij de uitbesteding aan een of meer derden te allen

tijde aanspreekpunt en verantwoordelijk voor de naleving van de bepalingen uit de Verwerkersovereenkomst, de AVG. Niet naleving van enige bepaling uit de Verwerkersovereenkomst of uit het bij of krachtens de wet gestelde, door inschakeling van derden komt voor rekening en risico van Verwerker.

2. Verwerker zal met de ingeschakelde derden (subVerwerkers) een rechtsgeldige verwerkersovereenkomst sluiten die minimaal dezelfde voorwaarden bevatten als de voorwaarden in deze Verwerkersovereenkomst.
3. Op de voet van artikel 3 ingeschakelde derden (subVerwerkers) mogen op hun beurt zelf geen derden (subsubVerwerkers) inschakelen dan na voorafgaande schriftelijke toestemming van Verantwoordelijke.

Artikel 4. Grondgebied verwerking

Verwerker mag de Persoonsgegevens uitsluitend buiten het Europese deel van Nederland Verwerken, indien Verantwoordelijke daarvoor uitdrukkelijk en schriftelijk toestemming heeft gegeven.

Artikel 5. Verzoeken betrokkenen en naleven verplichtingen AVG

1. Verwerker zal Verantwoordelijke de volledige medewerking verlenen die noodzakelijk is voor Verantwoordelijke om te kunnen voldoen aan verzoeken van betrokkenen wiens Persoonsgegevens worden verwerkt als bedoeld in hoofdstuk III van de AVG.
2. Verwerker zal, rekening houdend met de aard van de verwerking en de hem ter beschikking staande informatie, Verantwoordelijke bijstand verlenen bij het doen nakomen van de verplichtingen uit hoofde van de artikelen 32 tot en met 36 van de AVG.

Artikel 6. Vertrouwelijkheid

3. Verwerker, alsmede alle medewerkers die handelen onder het gezag van Verwerker en op de voet van art. 3 ingeschakelde derden die toegang hebben tot de Persoonsgegevens, zullen de Persoonsgegevens waarvan zij kennisnemen geheimhouden, tenzij een wettelijk voorschrift hen tot mededeling verplicht, in welk geval Verwerker Verantwoordelijke voorafgaand aan de mededeling zal informeren.
4. Verwerker zal al haar medewerkers die betrokken zijn bij de uitvoering van de Overeenkomst terzake een geheimhoudingsverklaring laten tekenen.

Artikel 7. Verstrekking & vernietiging

1. Verwerker is ten alle tijde verplicht alle of een deel van de Persoonsgegevens op eerste verzoek van Verantwoordelijke en onder alle omstandigheden onverwijld, volledig en onherroepelijk aan Verantwoordelijke of op verzoek van Verantwoordelijke aan een derde ter beschikking te stellen en/of te verwijderen of vernietigen.
2. Na beëindiging van de Overeenkomst, op welke grond of wijze dan ook, stelt Verwerker op eigen kosten en uit eigen beweging, maar uiterlijk binnen vier (4) werkdagen na het einde van de Overeenkomst, alle Persoonsgegevens ter beschikking aan Verantwoordelijke op de wijze en in het technisch formaat dat Verantwoordelijke wenst.
3. Onverminderd andersluidende schriftelijke opdracht van Verantwoordelijke, zal Verwerker na teruglevering van de Persoonsgegevens of indien Verantwoordelijke daarom verzoekt:
    - alle aan haar ter beschikking gestelde Persoonsgegevens op een door Verantwoordelijke nader te bepalen wijze en binnen een door Verantwoordelijke nader te bepalen termijn vernietigen;
    - van de vernietiging een aan Verantwoordelijke te verstrekken verslag maken, en;
    - aan Verantwoordelijke bewijs van de vernietiging overleggen.
    - De kosten van deze werkzaamheden komen voor rekening van Verwerker.
4. Indien naar het redelijk oordeel van Verwerker een zelfstandige wettelijke verplichting van Verwerker het geheel of gedeeltelijk vernietigen door Verwerker verbiedt of beperkt zal zij Verantwoordelijke zo spoedig mogelijk schriftelijk in kennis stellen van de wettelijke verplichting en daarbij alle relevante informatie verstrekken die Verantwoordelijke redelijkerwijs nodig heeft om te bepalen of vernietiging kan plaatsvinden en, zo ja, onder welke voorwaarden. Indien naar het redelijk oordeel van Verantwoordelijke de wettelijke verplichting (gedeeltelijke) vernietiging van Persoonsgegevens door Verwerker toelaat zal Verwerker daartoe op verzoek van Verantwoordelijke onverwijld overgaan. Is Verantwoordelijke van oordeel dat vernietiging niet mag plaatsvinden, dan zal zij Verwerker daarvan schriftelijk op de hoogte stellen. Verwerker garandeert in dat geval de vertrouwelijkheid van Persoonsgegevens jegens Verantwoordelijke en zal Persoonsgegevens niet Verwerken behalve ter voldoening aan haar bovenbedoelde wettelijke verplichting of na schriftelijke opdracht van Verantwoordelijke.

Artikel 9. Verantwoording, controle & toezicht

1. Verwerker rapporteert op verzoek van Verantwoordelijke over de opzet en werking van het stelsel van maatregelen en procedures, gericht op de naleving van de Verwerkersovereenkomst.
2. Verwerker zal aan de verwerkingsverantwoordelijke alle informatie ter beschikking stellen die nodig is om de nakoming van de in deze Verwerkersovereenkomst aan te tonen.
3. Verwerker is gehouden op verzoek van Verantwoordelijke dan wel door Verantwoordelijke aan te wijzen (externe) deskundigen, conform de beveiligingsnormen, steeds onvoorwaardelijke en ongelimiteerde inzage- en controlerecht te (doen) verschaffen in haar automatiseringssystemen, verwerkingsorganisatie en alle verdere relevante bescheiden in het kader van de uitvoering van de Verwerkersovereenkomst en de Overeenkomst, zodat Verantwoordelijke in staat is om de naleving van hetgeen Partijen zijn overeengekomen adequaat te kunnen toetsen. Tevens zal toegang worden verschaft aan de toezichthouders van Verantwoordelijke in het kader van de uitoefening van hun wettelijke taken.
4. Verantwoordelijke draagt de kosten voor controle met uitzondering van de kosten van het personeel van Verwerker dat de controle begeleidt en tenzij uit de audit blijkt dat Verwerker in strijd handelt met de Verwerkersovereenkomst, de AVG of andere regelgeving waarin eisen worden gesteld aan het Verwerken van Persoonsgegevens. Deze laatste kosten komen voor rekening van Verwerker. Indien uit de controle blijkt dat Verwerker tekortgeschoten is in de nakoming van enige verplichting op grond van de Verwerkersovereenkomst, herstelt Verwerker de tekortkomingen onmiddellijk.

Artikel 10. Overige bepalingen

5. In geval van strijdigheid van (een of meer bepalingen uit) de Verwerkersovereenkomst met (een of meer bepalingen uit) andere overeenkomsten tussen Verantwoordelijke en Verwerker, prevaleert de Verwerkersovereenkomst.
6. Deze Verwerkersovereenkomst heeft een looptijd gelijk aan de Overeenkomst en eindigt op het tijdstip dat de Overeenkomst eindigt. Artikelen die gezien hun aard, onder meer in het kader van de afwikkeling van deze overeenkomst, bestemd zijn om na het einde van de Verwerkersovereenkomst van toepassing te blijven, waaronder - maar niet beperkt tot - artikel 1 lid 4, artikel 6 (Vertrouwelijkheid) en artikel 7 (Verstrekking & verwijdering) van kracht na beëindiging van de Verwerkersovereenkomst.
7. Wijziging van de Verwerkersovereenkomst is slechts mogelijk door schriftelijke overeenstemming door Partijen.
8. In het geval enige bepaling van de Verwerkersovereenkomst nietig wordt verklaard of vernietigd wordt, zullen de overige bepalingen onverminderd van kracht blijven. Partijen zullen dan een nieuwe bepaling vaststellen ter vervanging van de nietige/vernietigde bepaling, waarbij zoveel mogelijk de strekking van de nietige/vernietigde bepaling in acht zal worden genomen.

Ondertekening

Verantwoordelijke GGD Hart voor Brabant:

Naam: [redacted]
Datum:

Verwerker Yource Outsourcing b.v.:

Naam: [redacted]
Datum:

Bijlage 1 Omschrijving overeenkomst

Het hoofddoel bij de afhandeling van alle contact center activiteiten is het uitvoeren van het bron- en contact onderzoek (BCO) in het kader van de Corona uitbraak conform het kernproces in bijlage 4. Op dagelijkse basis worden er door de landelijke huisartsen via diverse kanalen testen afgenomen. Vervolgens ontvangt de GGD de dossiers digitaal en voert een eerste triage uit.

De index patiënten die positief op Corona worden getest, worden nagebeld door een telefonische onderzoeker. Vervolgens vindt er aan de hand van een vragenlijst een inventarisatie plaats van het risicoprofiel en de contacten die de patiënt in de afgelopen periode heeft gehad.

Die contacten worden ook weer telefonisch benaderd en gemotiveerd om thuis in quarantaine te gaan. Op die manier ontstaat inzicht in de omvang van de verspreiding van het virus en kan verdere uitbraak beperkt blijven.

Gezien de vertrouwelijkheid van de gesprekken is het van belang dat er gekwalificeerde onderzoekers worden ingezet en dat er wordt gestuurd op kwaliteit. Daarbij wordt gestuurd op de volgende parameters:

- Volledigheid van dossiervulling
- Juistheid van informatie
    - Hieronder valt ook de controle of daadwerkelijk met de juiste persoon wordt gesproken.

Bellen met Coronapatiënten gebeurt met de dialer van Yource. In de dialer worden alleen de Naam en Telefoongegevens (NT gegevens) opgenomen.
De aanlevering van de NT gegevens is beveiligd door gebruik van het S-FTP platform van Yource. Alleen geautoriseerd personeel van Yource heeft toegang tot deze bestanden om de contactgegevens in de Dialer te plaatsen.

Bijlage 2 Datatypes

Bij de uitvoering van de opdracht worden datatypes verwerkt. In Bijlage 2 wordt per type gesprek aangegeven welke datatypes worden gebruikt.

Positief Geteste Coronapatiënt (inventarisatie en samenstelling risicoprofiel)

- **Naam**
- Adres
- Woonplaats
- **Telefoon**
- E-mail
- GGD registratienummer
- BSN nummer
- Geboortedatum
- Corona status
- Contacten
- Datum laatste contact
- Locatie met laatste contact
- Contact NAWTE gegevens
- Ingangsdatum quarantaine
- Quarantaine status

Alleen de **Dik** gelijste datatypes worden opgeslagen in de omgeving van Yource om de patiënten te kunnen bellen. De overige informatie wordt opgeslagen op de GGD systemen

Contact van Positief geteste Coronapatiënt

- **Naam**
- Adres
- Woonplaats
- **Telefoon**
- E-mail
- GGD registratienummer
- BSN nummer
- Geboortedatum
- Corona status
- Contacten
- Naam van Positief Corona geteste contact
- Datum laatste contact
- Locatie met laatste contact
- Ingangsdatum quarantaine
- Quarantaine status

Alleen de **Dik** gelijste datatypes worden opgeslagen in de omgeving van Yource om de patiënten te kunnen bellen. De overige informatie wordt opgeslagen op de GGD systemen

Bijlage 3 Grondslagen

Voor de verwerking van Bijzondere Persoonsgegevens gelden specifieke voorwaarden waaronder de verwerking mag en dient plaats te vinden. De verwerking van Bijzondere Persoonsgegevens is slechts toegestaan voor zover daarvoor een wettelijke grondslag als bedoeld in artikel 6 lid 1 AVG bestaat en het verbod op de verwerking van bijzondere persoonsgegevens, waaronder gezondheidsgegevens, te verwerken (artikel 9 lid 1 AVG) niet van toepassing.

In onder meer artikel 9 lid 2 AVG en de artikelen 22 tot en met 30 Uitvoeringswet AVG wordt aangegeven onder welke voorwaarden de verwerking van die gegevens toch mogelijk is.

De wettelijke grondslagen voor de verwerking van (bijzondere) persoonsgegevens door de GGD betreffen artikel 9, tweede lid, aanhef en onder h en i, AVG jo. artikel 6, eerste lid, aanhef en onder e, AVG jo. artikel 6, eerste lid, aanhef en onder c, Wpg.

Doordat de GGD de feitelijke regie houdt over het uitvoeren van het bron- en contactonderzoek en in dat kader het doel en middelen bepaalt, treedt Yource op als Verwerker in de zin van artikel 4, aanhef en onder 8, AVG. Yource kan daardoor de bevoegdheid om Bijzondere Persoonsgegevens te verwerken, ontlenen aan de bevoegdheid van de GGD, mits Yource handelt overeenkomstig de instructies van de GGD. De verwerkingen door Yource vinden daarmee plaats ‘onder de verantwoordelijkheid van een beroepsbeoefenaar die krachtens door bevoegde instanties vastgestelde regels aan het beroepsgeheim is gebonden.’ (artikel 9, derde lid, AVG).

Yource is bevoegd om de Bijzondere Persoonsgegevens te verwerken.

Bijlage 4, Certificeringen en selectiepersoneel

Yource Nederland is bezig met de ISO27001 certificering voor alle locaties. Locaties Almere en Nijmegen zijn sinds 2016 ISO27001 en ISO9001 gecertificeerd. Met de ISO27001 certificering wordt voldaan aan de gestelde eisen t.a.v. techniek en organisatie.

Vestiging Zwolle is sinds 2018 gecertificeerd en Vestiging Amersfoort sinds 2019.

De overige vestigingen worden eind 2020 begin 2021 opgenomen in het certificeringsprogramma van Yource.

Werkinstructie Yource: afspraken m.b.t. registratie/proces in HPZone

Rollen	Basis activiteit	Notitie
Coördinator Yource	a) Uitlezen van de situation 9. BCO door Yource. Onderverdelen van de casussen onder de BCO'ers b) Wanneer er sprake is van onvolledigheid van gegevens wordt de eerste voorman van Yource op de GGD geraadpleegd. Mocht deze de informatie niet kunnen verkrijgen wordt de case terug overgedragen aan de GGD. c) De case wordt ontkoppeld van de situation 9. BCO door Yource en aan de situation 3. BCO regulier d) Wanneer er sprake is van een case die niet in onze GGD regio woont wordt de case terug overgedragen aan de GGD. De case wordt ontkoppeld van de situation 9. BCO door Yource en aan de situation 3. BCO regulier	**Handleiding HPZone en Osiris** **- H11: een situation koppelen / ontkoppelen** www.GGD.nl
BCO'er	e) Voert BCO uit volgens de vragenlijst BCO en werkinstructie registratie en proces BCO (gebruik recentste versie) f) Voert registratie van BCO uit in HPZone. Gebruik de handleiding van HPZone en Osiris voor de registratie. g) Een afgeronde BCO (contact index + monitoring contacten dag 1) wordt ontkoppeld van de situation 9. BCO door Yource en aan de situation 11. BCO's afgerond door Yource gehangen. h) Mocht bij uitvoeren BCO men erachter komen dat de case een PRIO case is (bv een (zorg)instelling is betrokken, index is een zorgmedewerker, index is een arbeidsmigrant, AZC is betrokken) doe dan het volgende: i) Vraag zoveel mogelijk uit a.d.h.v. de BCO vragenlijst. Geef geen beleidsmatige adviezen. j) Bespreek case met de coördinator van Yource. Wordt case terug overgedragen naar de GGD? k) Maak een event aan in de case waarom de case terug overgedragen moet worden, welke acties al afgerond zijn en welke nog verricht moeten worden. l) Hang de case aan de situation 12. Signalen van Yource. Deze situation wordt door de coördinator GGD 3x per dag uitgelezen. Acute zaken kunnen overgedragen worden per telefoon. m) Wanneer er enkel een signaal overgedragen moet worden en dus niet een volledige case wordt ook de situation 12. Signalen van Yource gebruikt. Maak een event aan in de situation met het 'signaal'. De coördinator BCO van de GGD pakt deze dan vervolgens op.	**Handleiding HPZone en Osiris** **- H11: een situation koppelen / ontkoppelen** **- H8: events aanmaken**

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:

4.1 2.5.1 Advies inr...Brabant_Redacted

4.10 RE_ hpzone_Redacted

4.11 RE_ Overzicht...ed_Zwartgemaakt

4.12 211007 Inste...lite)_Zwartgemaakt

4.13 FW_ Toegang...ms_Zwartgemaakt

4.14 Instemmingsv...te)_Zwartgemaakt

4.2 2.c. Informatie...210205_Redacted

4.3 4.5 Cultuuraudit_Redacted

4.4 FW_ gevolgen...ted_Zwartgemaakt

4.5 FW_ Update d...ted_Zwartgemaakt

4.6 Impact_overga...eem (1)_Redacted

4.7 nog een paar d...en_Zwartgemaakt

4.8 RE_ Persoons...akt_Zwartgemaakt

4.9 Update progra..._ 09_06_Redacted

4.1 2.5.1 Advies inrichting...art voor Brabant_Redacted

4.2 2.c. Informatiebrief aan...diefstal 210205_Redacted

4.3 4.5 Cultuuraudit_Redacted

4.4 FW_ gevolgen datalek...r_Redacted_Zwartgemaakt

4.5 FW_ Update datadiefst..._Redacted_Zwartgemaakt

4.6 Impact_overgang_nieu...ICT-systeem (1)_Redacted

4.7 nog een paar dingen e...er 3 weken_Zwartgemaakt

4.8 RE_ Persoonsgegeven...artgemaakt_Zwartgemaakt

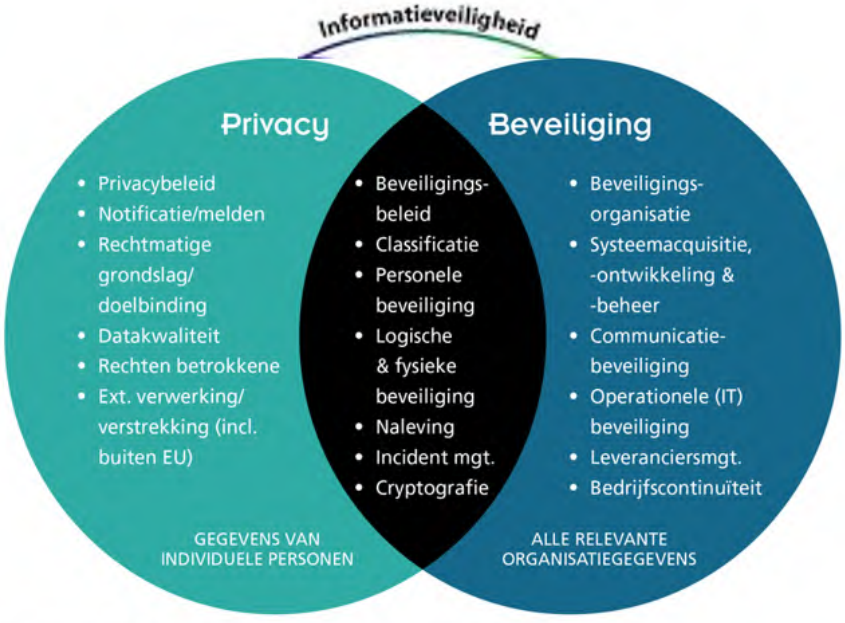
4.9 Update programma Corona _ 09_06_Redacted

Advies inrichting Privacy en Informatiebeveiliging

Aanleiding

Bij de GGD Hart voor Brabant is er momenteel een toenemende aandacht voor het onderwerp Privacy en Informatiebeveiliging. De recente datadiefstal bij de GGD GHOR en de reputatieschade als gevolg daarvan zorgen ervoor dat de GGD Hart voor Brabant Privacy & Informatiebeveiliging met grote urgentie opgepakt moet worden. De privacy-uitdagingen binnen de GGD Hart voor Brabant zijn nog legio, zoals het opstellen van een interen gegevensbeschermingsbeleid, het actualiseren en verbeteren van het privacy statement op de website, het uitvoeren van diverse DPIA's etc. (zie ook het [redacted] jaarverslag 2019). Het is zaak om orde te krijgen in de veelheid van vragen en de verschillende organisatorische verbeterpunten die er nog zijn, zodat wij als organisatie compliant zijn.

De onderwerpen Privacy en informatiebeveiliging kunnen niet los van elkaar gezien worden, zoals onderstaand afbeelding weergeeft.



FIGUUR 1: PRIVACYBESCHERMING EN INFORMATIEBEVEILIGING

Privacy en Informatieveiligheid dient verder ontwikkeld en geborgd te worden binnen de GGD Hart voor Brabant. Dit voorstel is een eerste aanzet tot een degelijke en structurele invulling van informatiebeveiliging en bescherming van persoonsgegevens in onze reguliere organisatie.

Grofweg zijn er 2 aandachtspunten voor de organisatie, gezien vanuit het perspectief van de [redacted]

I. Voldoen aan de wettelijke vereisten van de AVG (verantwoordingsplicht).

Specifiek gaat het om:

a. het opstellen en implementeren van een intern gegevensbeschermingsbeleid (privacy beleid) waarin taken, rollen en verantwoordelijkheden zijn vastgelegd. Dit beleid implementeert de uitgangspunten en is een verplichting uit de AVG. Een belangrijk onderdeel van een intern gegevensbeschermingsbeleid is tevens de inrichting van de organisatie van privacy binnen de GGD (Governance). Een gedegen en werkbaar intern privacy beleid staat of valt met de privacy beleving bij de medewerkers. Medewerkers dienen zich bewust te zijn van de gevoeligheid en hoeveelheid van persoonsgegevens die verwerkt worden. Uit gesprekken met medewerkers, de vragen die gesteld worden en de gemelde incidenten is gebleken dat medewerkers zich bewust zijn van privacy. Echter is de werkwijzen en de manier waarop wij met persoonsgegevens omgaan nog niet vertaald naar consistent vastgelegd beleid op het gebied van privacy. Medewerkers dienen handvatten en/of kaders geboden te worden die ze kunnen gebruiken bij het verwerken van persoonsgegevens. Het aanbieden van deze handvatten en kaders kan, en moet, plaatsvinden middels het op orde hebben van een intern beleid.

b. het actualiseren en verbeteren van het privacy statement op de website

Met de komst van de AVG komt er tevens strengere regelgeving op het gebied van de informatieplicht die een verwerkingsverantwoordelijke ten opzichte van de betrokkenen heeft. Ons huidige privacy statement is vergeleken met andere organisaties zeer summier opgesteld en voorziet de burger nauwelijks van informatie. Het opstellen van een volledig privacy statement vergelijkbaar met andere organisaties is noodzakelijk.

c. het opstellen en implementeren van een informatiebeveiligingsbeleid gericht op NEN 7510 norm

Het is van belang dat persoonsgegevens adequaat beveiligd worden. De AVG eist daarom dat er passende technische en organisatorische maatregelen genomen worden teneinde persoonsgegevens te beschermen tegen verlies of andere onrechtmatige verwerkingen. De maatregelen dienen een passend niveau van beveiliging te bieden waarbij rekening wordt gehouden met de stand van de techniek, de kosten van de uitvoering, de risico's van de gegevensverwerkingen en de aard van de persoonsgegevens. Het normenkader voor de GGD Hart voor Brabant is de NEN 7510 (zorgaanbieder).

II. Formatie

De uitvoering van de werkzaamheden van de [redacted] wordt bepaald door de hoeveelheid tijd die beschikbaar is. Op dit moment is dit 10 uur per week. Begin 2020 is in het jaarverslag 2019 van de [redacted] reeds aangegeven dat de beschikbare formatie niet toereikend is. Een organisatie met de omvang van de GGD Hart voor Brabant moet in staat geacht worden invulling te geven aan functiescheiding en dus in het invullen van de verschillende functies m.b.t. privacy- en informatiebeveiliging (zie voor verduidelijking bijlage 1). Omdat de [redacted] ook als contactpersoon fungeert tussen de organisatie en de AP is er duidelijk sprake van een ongewenste situatie. De AVG stelt in dit verband dat de verwerkingsverantwoordelijke middelen beschikbaar moet stellen voor het uitvoeren van de [redacted] taken (AVG, art 38 lid 2).

Voorstel

Gezien alle ontwikkelingen en de grote hoeveelheid vragen op dit moment is het advies van de [redacted] om op zeer korte termijn de verschillende functies voor het uitvoeren van privacy- en informatiebeveiligingstaken in te vullen, zodat de belangrijkste werkzaamheden opgepakt kunnen worden en de organisatie stappen kan maken compliant te worden, zodat de GGD Hart voor Brabant aan de verantwoordingsplicht richting de Autoriteit Persoonsgegevens kan voldoen.

Voorstel [redacted] is als volgt:

1. Aanstelling van een masterstudent (trainee) voor minimaal 3 maanden voor de volgende werkzaamheden:

a. Opstellen en implementeren intern gegevensbeschermingsbeleid

b. het actualiseren en verbeteren van het privacy statement op de website

Het advies is om met een masterstudent (trainee) aan de slag te gaan. GGD BZO en GGD NOG hebben reeds voor deze oplossing gekozen om privacy werkzaamheden uit te laten voeren. De trainee is per direct inzetbaar en kan in een korte tijd een belangrijke bijdrage leveren aan het compliant worden van de organisatie. Het gaat om hoog opgeleide Young Professionals die een tweejarige Post-master opleiding volgen aan de Antwerpen Management School en opgeleid worden tot een gecertificeerd Security- en privacy professional. Middels de inzet van een Young Professional kunnen wij als GGD Hart voor Brabant een bijdrage leveren aan de ontwikkeling van talent en hebben we mogelijk een topstudent in ‘the house’ voor toekomstige werkzaamheden.

Er is bewust gekozen voor de inzet van een trainee zodat we meters kunnen maken om een aantal wettelijke verplichte zaken op orde te krijgen, nl. het opstellen van het interne privacybeleid en het actualiseren van ons privacy statement op de website. De trainee zal fullttime met deze opdracht bezig zijn zodat dit over een aantal maanden is afgerond.

2. Tijdelijke aanstelling van een privacy Officer voor één jaar

Het aanstellen van een privacy Officer (PO) is noodzakelijk en onvermijdelijk, omdat:

- de [redacted] werkzaamheden uitvoert die niet tot zijn taken horen. Deze werkzaamheden moeten bij een PO belegd worden, zodat de [redacted] zijn wettelijke taken kan uitvoeren, namelijk het toetsen op de naleving van de AVG binnen de organisatie (zie hiervoor ook bijlage 1).
- Functiescheiding is belangrijk, zodat de [redacted] niet zijn eigen opgestelde adviezen 'moet' toetsen.
- De 10 uur per week die de [redacted] ter beschikking heeft om AVG vragen op te pakken, ruimschoots onvoldoende is.
- Bij uitval van de [redacted] de privacy werkzaamheden niet opgepakt kunnen worden door een collega.
- De werkzaamheden op privacy vlak de komende tijd alleen gaan toenemen. Denk bijvoorbeeld aan de GGD ambitie om 'data gedreven' te willen werken, alle technische ontwikkelingen waarbij steeds meer digitaal data wordt verzameld etc.

De inzet van de tijdelijke privacy officer is gericht om de taken van de [redacted] over ten nemen die niet bij de [redacted] horen te liggen (functiescheiding, onlasten [redacted] en de dagelijkse privacy vraagstukken GGD breed op te pakken (bijv. wettelijke veplichte DPIA's uitvoeren, vraagstukken datagedreven werken oppakken, toestemmingsvraagstukken, OGGZ/bemoeizorg AVG in kaart brengen, beoordelen verwerkersovereenkomsten etc).

3. Tijdelijke aanstelling van een (C)ISO voor één jaar

De functie van CISO/ISO zijn op dit moment binnen de GGD Hart voor Brabant niet ingevuld. De functie van CISO is, gezien de situatie rond het datalek en de reputatieschade als gevolg daarvan, belangrijk om in te vullen. Ook andere GGD 'en denken daar zo over. GGD BZO heeft een CISO aangesteld, GGD Utrecht gaat voor invulling van deze functie en GGD Gelderland-Zuid heeft een vacature opengesteld. Speerpunt voor de CISO zal in eerste instantie zijn alle ontwikkelingen rondom het programma Corona. Denk hierbij aan implementatie van GGD Contact en de uitfasering van HP Zone (Lite), ondersteuning en advisering bij DPIA's, veiligheid van de netwerken op de test- en vaccinatielocaties, opstellen van een informatiebeveiligingsbeleid voor programma Corona. Verder

kan de CISO een rol spelen in het oppakken van de acties die uit de Security Scan en het Risk Assessment naar voren komen om tot de implementatie van NEN7510 te komen.

De [redacted] kiest bewust voor beide functies voor een aanstelling van één jaar en niet voor korte tijdelijke externe inhuur van de medewerkers. Er speelt op dit moment zoveel, dat het niet verstandig is om dit door een tijdelijk externe kracht te laten oppakken. Uitgangspunt is niet het tijdelijk oplossen van een personeelstekort maar juist het oplossen van een structureel probleem en het zorgdragen voor het invullen van de diverse rollen conform de AVG.

De tijdelijke CISO, vallende onder programma corona, zal de urgente security vraagsukken bij het programma corona oppaken. Denk aan de implementatie van GGD Contact en de uitfasering van HP Zone (Lite), ondersteuning en advisering bij DPIA's, vragen veilig mailen, veiligheid van de netwerken op de test- en vaccinatielocaties, opstellen van een informatiebeveiligingsbeleid voor programma Corona etc. T.z.t. zal de CISO een belangrijke rol spelen in het oppakken van de acties die uit de Security Scan en het Risk Assessment naar voren komen om tot de implementatie van NEN7510 te komen.

Financiering

De [redacted] realiseert zich dat de invulling van alle hierboven genoemde functies op het gebied van privacy en informatiebeveiliging leidt tot een kostenpost, maar ziet dit als investering om te kunnen voldoen aan de eisen van de AVG (in control zijn). In afstemming met de concern controller wil de [redacted] de financiering als volgt vormgeven.

1. Masterstudent/trainee	30k (ten laste van discretionair MT budget)
2. 1,00 fte voor Privacy Officer	80-85 k (ten laste van huisvestingreserve)
3. 1,00 fte voor CISO/ISO	80-85 k (ten laste van programma Corona)

Bijlage 1: Organisatie van Privacy en informatiebeveiliging

Taken op het gebied van privacy en informatiebeveiliging dienen goed te worden gecoördineerd en uitgevoerd door medewerkers met verschillende disciplines binnen de organisatie. Doorgaans worden deze taken uitgevoerd door de Privacy Officer (PO), Chief Information Security Officer (CISO) en de Functionaris Gegevensbescherming (FG). Wie doet wat en hoe verhouden deze functies zich tot elkaar?

Privacy Officer (PO)

De Privacy Officer (PO) is de spin in het web op het gebied van privacy binnen de organisatie: de PO staat midden in de organisatie en is hét aanspreekpunt voor alle privacy gerelateerde vraagstukken.
De PO heeft voornamelijk uitvoerende taken, zoals het opstellen van een register voor gegevensactiviteiten, het opstellen van, en eventueel betrokken worden in de onderhandelingen van verwerkersovereenkomsten, een voorstel schrijven voor het privacy beleid en betrokken worden bij de integratie van privacy in de werkprocessen.

Zo kan de PO worden ingezet om privacy risico's in bepaalde werkprocessen in kaart te brengen, bijvoorbeeld door het uitvoeren van Privacy Impact Assessments (PIA's) of DPIA's. Het aanstellen van een PO met de juiste capaciteiten is voor grote organisaties met grootschalige en diverse verwerkingen van persoonsgegevens, een noodzaak.

Op allerlei vlakken moet de bewustwording omtrent privacy wordt vergroot, en moet de privacywet- en regelgeving juist worden toegepast. De PO speelt daarin een onmisbare rol, zeker bij de uitvoering van de adviezen van de FG vanuit diens toezichthoudende rol.

Een grote misvatting bij veel organisaties is dat de FG ook zorgt draagt voor de uitvoering en dus voor de implementatie van de AVG. De FG zal zich niet moeten bemoeien met de uitvoering van de AVG puur vanwege het feit dat de FG in dat geval later eigen werk moet gaan controleren. Vanwege de grote mate van juridische werkzaamheden die een PO moet verrichten, is het logisch en wenselijk dat de PO voldoende juridische kennis heeft.

Functionaris Gegevensbescherming (FG)

In tegenstelling tot de PO, zijn de positie, taken en bevoegdheden van de Functionaris Gegevensbescherming (FG) wettelijk geregeld in de AVG. De PO houdt zich bezig met uitvoering van de vereisten uit de AVG, de FG houdt toezicht op de naleving van de AVG (en andere privacywet- en regelgeving). Om dit te doen krijgt vanuit de AVG de nodige onderzoeks- en controlebevoegdheden

aangereikt. Daarnaast ziet de FG toe op ontwikkeling van bewustwording over privacy binnen de organisatie en staat hij in contact met de Autoriteit Persoonsgegevens. Bij complexe vraagstukken met grote risico's voor de bescherming van persoonsgegevens, kan de FG gevraagd en ongevraagd adviseren.

De FG vervult zijn werkzaamheden onafhankelijk en opereert bij uitoefening van zijn taken en bevoegdheden zelfstandig. Uiteindelijk rapporteert de FG aan het hoogste leidinggevende niveau binnen de organisatie.

Informatiebeveiliging: CISO

De Chief Information Security Officer (CISO) is de spil op het gebied van informatiebeveiliging binnen de organisatie. De CISO komt toe allerlei taken op het gebied van informatiebeveiliging zoals het opstellen en actualiseren van het informatiebeveiligingsbeleid, coördineren van de uitvoering van het informatiebeveiligingsplan en (gevraagd en ongevraagd) adviseren over informatiebeveiligings-vraagstukken. De CISO heeft voornamelijk adviserende en coördinerende taken en rapporteert ideaal gezien ook aan het hoogste leidinggevende niveau binnen de organisatie.

Samenwerking en combinatie van rollen

In de praktijk werken de FG, PO en de CISO nauw samen. Dat is ook aan te bevelen, aangezien de bescherming van persoonsgegevens niet los kan worden gezien van informatiebeveiliging. Door deze nauwe samenwerking zijn de medewerkers op de hoogte van elkaars werkzaamheden en kunnen ze de naleving van de AVG in de organisatie effectiever bewerkstelligen.

Voor veel organisaties is het verplicht om een FG aan te stellen, maar het is niet noodzakelijk om een fulltime FG te hebben. In de praktijk zie je vaak dat de rol van FG wordt gecombineerd met die van de PO of de CISO. Het combineren van de FG met de PO is echter niet aan te raden. De FG moet een onafhankelijke rol hebben binnen de organisatie en daarnaast kunnen uitvoering en toezicht niet samengaan.

Privacy- en Informatiebeveiligingsteam

Het beste is dus om bovenstaande rollen door verschillende personen in te laten vullen. In de praktijk is het gebruikelijk en wenselijk dat deze personen worden samengebracht in een privacy- en informatiebeveiligingsteam (PIT). Een PIT bestaat in ieder geval uit de PO en CISO.
De FG kan het team over bepaalde vraagstukken van advies voorzien en dus vaak aansluiten bij de overleggen. Daarnaast is het aan te bevelen om andere medewerkers deel uit te laten maken van dit

team (en weer andere medewerkers periodiek aan te laten sluiten, indien daarvoor aanleiding bestaat). Denk hierbij aan medewerkers van de afdelingen kwaliteit en klachten, HR en inkoop etc.
In het PIT worden privacy- en informatiebeveiligingsvraagstukken besproken, adviezen voor besluitvorming aangedragen en op de uitvoering van adviezen gestuurd.

Hart voor Brabant

Aan: het algemeen bestuur van GGD Hart voor Brabant

Datum: 5 februari 2021

Behandeld door: [redacted] E-mail: [redacted]@ggdhvb.nl

Onderwerp: Update datadiefstal

Geachte leden van ons algemeen bestuur,

Op 29 januari jl. heb ik u op hoofdlijnen per brief geïnformeerd over de datadiefstal uit GGD-systemen. In de media is hier momenteel veel aandacht voor. Wij kunnen ons voorstellen dat dit bij u vragen oproept en dat u behoefte heeft aan informatie om uw raad te kunnen informeren. Wij willen u dan ook graag nader informeren over de situatie en wat wij als GGD Hart voor Brabant hebben gedaan.

Landelijke reactie van GGD GHOR Nederland

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. 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.

Geen datadiefstal door medewerkers van GGD Hart voor Brabant

Geen van de gearresteerde vijf personen was werkzaam bij onze GGD. Wij hebben tot op heden ook geen aanwijzingen ontvangen van politie en justitie dat (vaste of ingehuurde) medewerkers van onze GGD worden verdacht. Ook hebben we zelf intern nadere checks uitgevoerd van onze 'logging-bestanden' op eventuele onregelmatigheden. We hebben geen onregelmatigheden aangetroffen. We

hebben dus ook op basis van eigen onderzoek op dit moment geen aanwijzingen dat door onze medewerkers data zouden zijn gestolen.

Het is evenwel nog niet duidelijk of door de gearresteerde medewerkers van het landelijk callcenter of medewerkers van andere GGD'en gegevens zijn gestolen en/of ten onrechte ingezien van inwoners uit ons werkgebied. Dit moet duidelijk worden uit het landelijke onderzoek van politie en justitie.

Welke maatregelen zijn vooraf genomen om gegevensmisbruik te voorkomen?
Als GGD'en werken we aan de virusbestrijding, met de benodigde functionaliteiten op een zo veilig mogelijke manier. De GGD'en hebben vooraf de volgende maatregelen genomen:

- Controle aan de poort. Mensen moeten een Verklaring Omtrent Gedrag (VOG) aanleveren en een geheimhoudingsverklaring ondertekenen. GGD Hart voor Brabant heeft zich er bij de aanname van personeel van verzekerd, dat altijd en voor iedereen een VOG en geheimhoudingsverklaring voor handen is.
- Autorisatieniveaus. De beide systemen die het betreft (CoronIT en HPZone) kennen verschillende rollen met bijbehorende autorisatieniveaus. Niet iedereen kan bij alle gegevens en kan alle functionaliteiten (zoals het downloaden van data-exports) gebruiken. Binnen GGD Hart voor Brabant hebben wij een autorisatiematrix gebaseerd op rol of functie van iedere medewerker. Medewerkers krijgen alleen die autorisatie, die nodig is voor zijn of haar functie. De autorisatiematrix wordt bijgehouden bij in-, door- en uitstroom van medewerkers. Er vindt hierop een maandelijkse check plaats.
- Controles op correct gebruik. De GGD'en controleren sinds de start het gebruik van de systemen door de medewerkers, hebben die controles steeds verder verbeterd en doen dat nog steeds. Vanwege het belang van de virusbestrijding en de gevraagde snelheid zijn de GGD'en – op diverse manieren – met steekproefsgewijze controles van start gegaan. De Autoriteit Persoonsgegevens had vóór het bekend worden van de datadiefstal geen aanvullende vragen gesteld over deze werkwijze. GGD Hart voor Brabant kan via de logging-functionaliteit van Microsoft 30 dagen terugkijken. De GGD gebruikt dit voor steekproeven en om terug te zoeken bij signalen en incidenten.

Welke maatregelen worden genomen sinds het bekend worden van de datadiefstal?
Landelijk is aangifte gedaan en wordt grootschalig onderzoek gedaan door politie en justitie. Binnen de organisatie hebben we continue aandacht voor kwaliteitsbevordering én -bewaking en worden de medewerkers regelmatig bijgepraat over de laatste stand van zaken rondom het incident. De eerder genomen maatregelen zijn gecontroleerd en geïntensiveerd:

- Controle aan de poort. GGD Hart voor Brabant heeft nogmaals een check uitgevoerd. We hebben vastgesteld dat alle door ons ingezette externe medewerkers een VOG en ondertekende geheimhoudingsverklaring hebben. Bij vaste, interne medewerkers is dit ook het geval voor zover ze bij ons zijn komen werken sinds het beleid omtrent VOG en geheimhoudingsverklaring is geïmplementeerd. Oudgedienden die al vele jaren bij ons werken hebben geen VOG, omdat dit

destijds nog niet bestond. Alle ambtenaren hebben echter sowieso een wettelijke geheimhoudingsplicht. Bij de invoering van de Wet normalisering rechtspositie ambtenaren hebben al onze vaste medewerkers digitaal moeten bevestigen dat zij zich houden aan de integriteitsregels, waaronder geheimhouding. We zoeken uit of het nodig is om oudgedienden alsnog te vragen om een VOG en/of geheimhoudingsverklaring.

- Autorisatieniveaus. Naar aanleiding van de datadiefstal is ter check nog een keer doorgelicht wie binnen GGD Hart voor Brabant geautoriseerd is tot grote downloads (datadump). Dit is een zeer beperkte groep van medewerkers die dit op grond van hun functie daadwerkelijk nodig hebben, bijvoorbeeld om dashboards te maken.
- Controles op correct gebruik. GGD Hart voor Brabant heeft een nadere check uitgevoerd van onze 'logging-bestanden' en geen onregelmatigheden aangetroffen. We zien geen afwijkingen in de IT-omgeving van onze GGD. Ons beeld is dat er binnen of door GGD Hart voor Brabant geen gegevens in verkeerde handen zijn gevallen. GGD Hart voor Brabant wil de periode van logging verlengen van 30 dagen naar 1 jaar, zodat we verder kunnen terugkijken. Verder verwacht GGD GHOR Nederland in maart systemen te implementeren die automatisch en continu zullen controleren op opvallend gebruik van de systemen (zoals grote downloads of onlogische inzage in dossiers).

Verder worden als aanvullende maatregelen genomen:

- Communicatie. GGD Hart voor Brabant vindt het van belang om de eigen inwoners gericht te informeren over de situatie, wat wij eraan doen en hoe mensen een verwijderingsverzoek kunnen indienen. We wijzen ons inwoners in eerste instantie op de landelijke lijst met veel gestelde vragen van GGD GHOR Nederland. Zit het antwoord op hun vraag er niet bij, dan adviseren wij hen om contact op te nemen met het landelijke nummer voor deze datadiefstal. Dit telefoonnummer (085-130 82 26) is dagelijks bereikbaar van 09.00 uur tot 21.00 uur. Daarnaast attenderen we inwoners uit onze regio op de mogelijkheid om hun eigen gegevens in te zien, te wijzigingen of te laten verwijderen.
- Verzoeken voor gegevensverwijdering. 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. De GGD heeft hiervoor al jaren een staand beleid en werkprotocol, conform de AVG. Vanuit GGD GHOR Nederland wordt op dit moment gewerkt aan de precieze invulling van het recht op gegevensverwijdering binnen CoronIT en HPZone. 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, die o.a. eisen stelt aan de bewaartermijn van medische gegevens. Op de website van GGD Hart voor Brabant (www.ggdhvb.nl) vindt men via het onderdeel Corona bij veel gestelde vragen de link naar privacy en corona. Daar is een formulier te downloaden, waarmee een aanvraag kan worden gedaan. Aanvragen worden binnen 4 weken behandeld. GGD Hart voor Brabant heeft sinds vorige week 60 inzage- en verwijderingsverzoeken ontvangen.

- Uitzetten van functionaliteiten in de systemen. Om het risico per direct te verminderen zijn landelijk in CoronIT en HPZone diverse functionaliteiten uitgezet. Het is niet meer mogelijk om downloads van gegevensbestanden te doen, prints van gegevensbestanden te maken (omdat dit als PDF kon) en om zoekopdrachten te doen (query's) op BSN en postcode. Het risico op verder misbruik is hiermee zoveel mogelijk gereduceerd.

Tot slot

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.

Als er nieuwe relevante ontwikkelingen zijn op dit dossier, dan stel ik u daar zo snel mogelijk van op de hoogte. Voor nu vertrouw ik erop u met dit schrijven voldoende geïnformeerd te hebben. Tijdens uw vergadering van 24 maart praten we u verder bij. Tot die tijd zal ik eventuele belangrijke en/of spoedeisende zaken steeds via een brief met u delen.

Met vriendelijke groet,

[redacted]

4.3

Zie onder. Ter info. De GGD doet mee. [redacted] is het aanspreekpunt.

Datum: DPG-overleg 15 april 2021

Betreft: Notitie Cultuuraudit

1. Aanleiding
   a. Motie TK + Toezegging M

   Kamerbrief 2 februari 2021, toezeggingen tijdens debat datalek 3 februari 2021.

   In reactie op het datalek bij GGD'en, waarbij persoonlijke gegevens van Nederlanders in handen van derden terecht zijn gekomen, heeft de minister van VWS verschillende maatregelen aangekondigd voor de korte en lange termijn, om de risico's in de toekomst te beperken en een volgend datalek te voorkomen.
   Eén van de aangekondigde maatregelen is de uitvoering van een IT-audit, waarbij de IT-systemen en procedures van de GGD'en onder de loep worden genomen. In aanvulling op de IT-audit heeft de minister van VWS toegezegd de cultuur van melden binnen de GGD'en en hun partners te laten onderzoeken (een cultuuraudit).

   b. Beperken scope -> van cultuur audit naar check op klachtenprocessen

   In het licht van de drukte die er is rond de Covid 19-bestrijding is het onderzoek zo min mogelijk belastend en richt zich op de functionarissen binnen de meldstructuur van de organisaties (en niet op bijvoorbeeld de medewerkers en leidinggevenden in de organisatie). Het onderzoek richt zich zowel op meldingen/klachten vanuit de organisatie zelf (door medewerkers) als op meldingen/klachten vanuit cliënten van de organisatie. Ook wel: interne klachten/meldingen en externe klachten/meldingen.
   Het onderzoek richt zich zowel op de GGD'en als op de partnerorganisaties.

   c. Besproken in DPG-overleg 26-02-2021

   In het DPG-overleg van 26 februari 2021 stond het onderwerp op de agenda en heeft [redacted] een mondelinge toelichting gegeven.

   d. DPG-overleg 9 april 2021

   Zoals afgesproken in het DPG-overleg van 9 april jl. geeft deze deze notitie meer informatie over deze audit.

2. Het onderzoek
   a. Onderzoek bij GGD GHOR Nederland, de GGD'en en onderaannemers

      Onderzoek naar opzet, bestaan en werking van voorzieningen voor het melden van signalen door medewerkers en cliënten van GGD'en en partnerorganisaties

      Is het melden van problemen (bij alle GGD-en en partnerorganisaties) op een goede manier geborgd, kunnen mensen bijvoorbeeld intern met signalen terecht en geven organisaties voldoende ruimte aan kritische geluiden?

   b. Naar de inrichting van klachtenprocedures waar medewerkers terecht kunnen (Arbeidsomstandigheden, ongewenst gedrag, maatschappelijk misstanden, medische fouten, en privacy gerelateerde vraagstukken)

      In de vragenlijst voor de GGD'en zal worden gevraagd (en getoetst/geverifieerd): of zij: een vertrouwenspersoon, een FONA-commissie, een klachtencommissie hebben en zijn aangesloten bij een Geschillencommissie Publieke Gezondheid.
      Of zij aan de wettelijke vereisten voldoen. Of zij op een aantal onderdelen informatie kunnen verstrekken die een beeld geeft over de werking van het systeem.

4.3

Zie onder. Ter info. De GGD doet mee. [redacted] is het aanspreekpunt.

De vragenlijsten voor de partnerorganisaties kunnen afwijken van die van de GGD-en, bijvoorbeeld op het punt van de FONA-commissies, geschillencommissies en andere verschillen omdat zij geen zorgorganisatie zijn.

c. Uitgevoerd door de Kwink groep
Aanpak bestaat uit 4 fases, bureauonderzoek, vragenlijsten uitzetten, check compleetheid en interview geschillencommissie, analyse en rapportage.

d. Middels vragenlijst die aan medewerker (klachtenfunctionaris) van iedere organisatie gestuurd wordt. Deze vragenlijst wordt getoetst bij de GGD Regio Utrecht.

e. Start eind april
Planning offerte is (in overleg met Kwink groep) 2 weken opgeschoven, fase 1 loopt, fase 2 start mogelijk eind april met een doorlooptijd van in totaal 8 weken.

f. Oplevering rapport met bevindingen
Rapport wordt eind mei opgeleverd.

3. Opdrachtgeverschap
   a. GGD GHOR (op aangeven van VWS)
   b. Uitgezet via enkelvoudige aanbesteding (bedrag onder 30k)
   c. Rapport wordt opgeleverd aan GGD GHOR en gedeeld met DPG'en
   d. Rapport of hoofdlijnen daaruit wordt vervolgens gedeeld met VWS na bespreking in DPG-overleg
   e. Zodat M bevindingen met TK kan delen

4. <u>Verzoek</u>
   a. Mee te werken aan de audit zodat integraal beeld branche ontstaat
   b. Indien er behoefte is aan aanvullende informatie dit aan te geven bij [redacted].
   c. Contactpersoon door te geven aan [redacted] ([redacted]@ggdghor.nl)

4.3

Zie onder. Ter info. De GGD doet mee. [redacted] is het aanspreekpunt.

4.4
Archived: donderdag 12 mei 2022 09:31:25
From: [redacted]
Sent: donderdag 4 februari 2021 08:37:42
To: [redacted]
Subject: FW: gevolgen datalek voor izb regulier
Importance: Normal
Sensitivity: None

Ter info.

Van: [redacted]
Verzonden: dinsdag 2 februari 2021 17:11
Aan: [redacted]
CC: [redacted]
Onderwerp: FW: gevolgen datalek voor izb regulier

Hoi [redacted],

Ik heb begrepen dat jij bezig bent om input op te halen voor de gevolgen van aanpassingen in rechten en functies HP Zone op het werk. Op verzoek van [redacted] heb ik met [redacted] ook gesproken over de gevolgen voor het reguliere IZB proces. [redacted] heeft hierop vervolgens een overzicht gemaakt van de gevolgen die we nu zien. Zou je dit ook mee kunnen nemen in dit traject?

Met vriendelijke groet,

[redacted]

GGD Hart voor Brabant

Pettelaarpark 10, Den Bosch
Postbus 3024, 5003 DA Tilburg
www.ggdhvb.nl

[redacted]
Aanwezig op: ma-di-wo-do
[redacted]

Gezond doet leven!

Van: [redacted]
Verzonden: dinsdag 2 februari 2021 16:50
Aan: [redacted]
Onderwerp: gevolgen datalek voor izb regulier

Hoi [redacted],

Heb input opgehaald vanuit IZB, hieronder beschreven wat de gevolgen zijn voor reguliere proces.

- **Exportfunctie**: verwijderd voor bepaalde rollen en bepaalde gegevens (bsn + postcode) kunnen niet meer geëxporteerd worden.

Gevolgen voor:

4.4
- collega's die geen administrator rol hebben kunnen geen exports meer draaien. Dit geldt dus voor bijna alle IZB artsen en IZB verpleegkundigen
- surveillance van legionella en Q-koorts. Hiervoor gebruiken wij de postcode om te kunnen plotten of indexen dicht bij waterzuiveringsinstallaties of veehouderijen wonen. Of om te traceren of er besmettingen zijn op één bepaalde plaats.
- Verwachting is dat ook geboortedatum verwijderd wordt uit de exportfunctie. In combinatie met de verwijderde gegevens van bsn en postcode betekend dit dat je niet meer goed je dubbelingen uit het systeem kan halen.

- **Printfunctie**: verwijderd in zijn totaliteit uit HPzone.

Gevolgen voor:

- Het doorsturen van een volledig dossier via zorgmail. Dit gebeurt bv bij een verhuizing van een index naar een andere GGD regio. Of bij uitbraakonderzoek waarbij meerdere GGD'en betrokken zijn.
- Het niet meer kunnen printen of doorsturen van iemand zijn dossier als deze via de officiële manier zijn dossier heeft verzocht op te vragen

- **Look up person** (zoeken op persoon): kan niet meer op postcode. Hierdoor is het erg lastig om een persoon op te zoeken waarvan je alleen een naam en geboortedatum hebt. Met een postcode erbij ben je specifieker

Met vriendelijke groeten,

[redacted]

Verpleegkundige

Team Infectieziekten & programma Corona

GGD Hart voor Brabant

Pettelaarpark 10, Den Bosch

Postbus 3024, 5003 DA Tilburg

www.ggdhvb.nl

[redacted]

Aanwezig op: ma-, di-, woe- en donderdag.

Gezond doet leven!

4.5
Archived: donderdag 12 mei 2022 09:31:32
From: [redacted]
Sent: dinsdag 23 maart 2021 09:54:48
To: [redacted]
Subject: FW: Update datadiefstal m.b.t. opsporing afwijkend gedrag van medewerkers in Corona ICT systemen
Importance: Normal
Sensitivity: None

Van: [redacted]
Verzonden: vrijdag 19 maart 2021 15:23
Aan: [redacted]
Onderwerp: FW: Update datadiefstal m.b.t. opsporing afwijkend gedrag van medewerkers in Corona ICT systemen

Ter info en evt ter verdere verspreiding

Van: [redacted]
Verzonden: vrijdag 19 maart 2021 15:19
Aan: Directie GGD GHOR Nederland <directie@ggdghor.nl>
Onderwerp: Update datadiefstal m.b.t. opsporing afwijkend gedrag van medewerkers in Corona ICT systemen

Beste DPG'en,

Zoals jullie weten, hebben we met elkaar naar aanleiding van de datadiefstal een aantal maatregelen genomen.

Die maatregelen betroffen het uitzetten van functionaliteiten in de systemen, maar ook het nader analyseren en beter monitoren van het gebruik van onze systemen. Voor de gebruikersanalyse ten tijde van de datadiefstal hebben we Fox-it en Hoffman opdracht gegeven om een onderzoek te doen en afwijkend gedrag op te sporen in respectievelijk CoronIT en HPzone(Lite). Voor de structurele monitoring hebben we een SOC team ingericht. Met deze mail informeren we je graag nader over deze twee maatregelen.

Onderzoek Fox-it en Hoffman

Het onderzoek van Fox-it bevindt zich in de afrondende fase. We verwachten hun definitieve bevindingen voor 1 april. Op basis van dit onderzoek zijn meldingen bij de politie gedaan van waaruit ook een deel van de arrestaties gedaan.

De eerste fase van het onderzoek van Hoffman is afgerond. Op basis van de analyse van de datadump is een longlist samengesteld met ruim 560 account waarop afwijkend gebruik van HPzone is waargenomen. De volgende stap is om nader onderzoek te doen naar deze 560 accounts om te bezien of het afwijkende gedrag te verklaren is, dan wel om maatregelen vraagt. Het is de bedoeling om eind volgende week de namen van medewerkers die uit het onderzoek van Hoffmann gekomen zijn door te geven aan de reeds door jullie doorgegeven HR-medewerkers.

Een aantal van jullie heeft aangegeven nog niet zover te zijn vanwege vragen op het gebied van privacy met betrekking tot deze werkwijze. We hebben deze vragen opgepakt en komen daar bij de DPG'en die het betreft over op de lijn. De overdracht van namen zal dan op een later moment plaatsvinden. We hopen zodoende dat ook Hoffman zijn onderzoek op korte termijn kan

afronden. 4.5

Continue monitoring

Bij GGD GHOR Nederland is naar aanleiding van de datadiefstal een SOC-team van start gegaan (Security Operations Center). Dat team monitort continu het gebruik van de ICT-systemen die gebruikt worden voor Corona. Er is al meerdere keren opvallend gebruik geconstateerd, waarbij dat gedrag in enkele gevallen dusdanig van aard was, dat er direct is ingegrepen en accounts zijn afgesloten. De medewerkers die daarbij in beeld komen (tot nu toe allemaal van [redacted]), kunnen zowel van een callcenter zijn als van een GGD. Momenteel werken we beleid uit hoe te handelen wanneer het SOC team onregelmatigheden bij één van jullie medewerkers constateert. Dit beleidsvoorstel zal begin april met jullie besproken worden.

Tot zover deze informatie. Mocht je hierover vragen hebben, laat het me dan weten.

Met vriendelijke groet,

[redacted]

[redacted]

GGD GHOR Nederland
Zwarte Woud 2
3524 SJ Utrecht

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

Dit bericht is uitsluitend bestemd voor de geadresseerde. Het bericht kan vertrouwelijke informatie bevatten. Als u dit bericht per abuis hebt ontvangen, wordt u verzocht het te vernietigen en de afzender te informeren. GGD GHOR Nederland is niet aansprakelijk voor onjuiste en onvolledige overbrenging van de inhoud van een verzonden e-mail bericht, of een te late ontvangst daarvan.

Rijksinstituut voor Volksgezondheid
en Milieu
*Ministerie van Volksgezondheid,
Welzijn en Sport*

> Retouradres Postbus 1 3720 BA Bilthoven

Aan de [redacted] van de Volksgezondheid
Ministerie van Volksgezondheid, Welzijn en Sport
[redacted]
Postbus 20350
2500 EJ DEN HAAG

Aan de [redacted] COVID-19
Ministerie van Volksgezondheid, Welzijn en Sport
mr. [redacted]
Postbus 20350
2500 EJ DEN HAAG

A. van Leeuwenhoeklaan 9
3721 MA Bilthoven
Postbus 1
3720 BA Bilthoven
www.rivm.nl

KvK Utrecht 30276683

T 030 274 91 11
F 030 274 29 71
info@rivm.nl

Ons kenmerk
0030/2021 LCI/JvD/rj

Behandeld door
LCI

T (030) 274 7000
F (030) 274 4455
lci@rivm.nl

Datum 2 februari 2021
Onderwerp Impact overgang nieuw ICT-systeem

Geachte mevrouw [redacted], geachte heer [redacted],

Als reactie op de vorige week bekend geworden datadiefstal wil GGD GHOR NL HPZone Lite vervangen door een ander registratiesysteem. Mogelijk zou dit op zeer korte termijn al het huidige HPZone Lite moeten gaan vervangen. Het RIVM-CIb maakt zich zorgen over de impact die dit zal gaan hebben op een van de pijlers van het kabinet: het zicht houden op en het inzicht hebben in de verspreiding van het virus.

Omdat het RIVM afhankelijk is van de datastromen die via HPZone en HPZone Lite naar het CIb komen, heeft een vervanging veel impact op de gegevens en adviezen die het RIVM kan bieden in het kader van de bestrijding van de COVID-19-pandemie. Ook het OMT benadrukt het belang van landelijke en regionale surveillance die zonder onderbreking en tijdig uitgevoerd dient te worden, en de afhankelijkheid hierin van het registratiesysteem van GGD GHOR. Mocht men daar overgaan op een ander systeem, dan moet tevoren niet alleen de veiligheid en privacy, maar ook de output voor de surveillance gewaarborgd zijn. Wij zullen bij een te snelle, onvoldoende geteste en volledige nieuwe datastroom, niet de rapportage en data kunnen leveren die benodigd is om het landelijke bestrijdingsbeleid te onderbouwen. We zetten in de bijlage uiteen wat de gevolgen zullen zijn van een (tijdelijke) stop van datatoevoer en wat de voorwaarden voor livegang zijn vanuit het oogpunt van de RIVM-taken in de surveillance en bestrijding van COVID-19.

De timing van overgaan naar een nieuw registratiesysteem is uiterst ongelukkig. We verkeren in een lockdown, er komen nieuwe virusvarianten op, en de vaccinatiecampagne is net opgestart. We staan daarnaast aan de vooravond van een periode dat er mogelijk nieuwe maatregelen dan wel versoepelingen komen. Dat alles dient gebaseerd te zijn op recente en complete data; en toegang hiertoe is nu in gevaar. Daarnaast zorgt een nieuw registratiesysteem voor de vele medewerkers bij de GGD' en bij de overgang tot extra werklast. Juist een invoering ten tijde van een 'derde golf' kan dit ertoe leiden dat het bron-en contactonderzoek eerder moet worden afgeschaald. Dit heeft een negatief effect op de bestrijding, en op het zicht houden op het virus.

Een nieuw systeem kent altijd opstartproblemen en dient daarom uiterst goed getest te worden. Ook het RIVM moet de tijd hebben de nieuwe aanvoer te

verwerken in analyses, rapportages, en aanmaak van open datasets (onder andere t.b.v. het Rijksoverheid-coronadashboard). Het is hierbij van belang dat alle GGD'en geheel over zijn op het nieuwe systeem en dat de data van alle 25 GGD'en via eenzelfde datastroom loopt. Verlies van historische data uit HPZone dient, zowel voor de GGD als voor het RIVM, voorkomen te worden door opname van deze data in het nieuwe systeem (datamitigatie).

Datum
2 februari 2021

Ons kenmerk
0030/2021 LCI/JvD/rj

We zijn graag bereid verdere toelichting te geven.

Hoogachtend,

Prof. dr. [redacted]

Bijlage bij brief "Impact overgang nieuw ICT-systeem"

Datum
2 februari 2021

Ons kenmerk
0030/2021 LCI/JvD/rj

Consequenties van een te vroege livegang van een nieuw ICT-systeem GGD'en

De datavoorziening vanuit HPZone – welke direct gekoppeld is aan Osiris, contactmonitoring en clusterinformatie – is nodig voor onderstaande processen. Hierin kan mogelijk (tijdelijk) geen inzicht meer in gegeven worden. Er zijn 3 datastromen vanuit HPZone die essentieel zijn voor landelijke surveillance door het RIVM, die weg kunnen vallen bij een te vroege livegang van een nieuw ICT-systeem als vervanging van HPZone Lite:

Osiris datastroom:

- Wettelijke meldingen van deze A-ziekte: geen zicht meer op de totalen, en alle achtergrondkarakteristieken van de meldingen; zie ook het epidemiologisch rapport (verdeling leeftijd, beroep, geslacht, comorbiditeit, setting van mogelijk bron, gelinkte bron etc.)
- Berekening reproductiegetal op basis van de meldingen (dit kan dan alleen nog op basis van stichting NICE-data over ziekenhuisopnames en IC-opnames; deze laten echter minder tijdig veranderingen zien en hebben een erg breed onzekerheidsinterval, wat interpretatie en communicatie over het effect van maatregelen moeilijk maakt)
- Kiemsurveillance: koppelen genetische uitslagen van virusvarianten aan epidemiologische data uit meldingen over de (reis)achtergrond van mensen met een virusvariant; dit is essentieel voor onderbouwen van internationale reisbeperkende maatregelen
- Epidemiologische weekrapportage: van de 12 hoofdstukken vallen 1 t/m 8, 10 en 12 weg
- Coronadashboard: uitval van data, in ieder geval de data weergegeven onder de kopjes Besmettingen en Kwetsbare groepen
- Surveillance van besmettingen en sterfte in verpleeghuizen en instellingen gehandicaptenzorg valt weg
- Surveillance van het effect van vaccinatie en vaccinfalen is niet meer mogelijk. De eerste effecten zijn te verwachten bij de groepen met de hoogste prioriteit voor vaccinatie (t.w. zij met de grootste ziektelast door COVID-19): de bewoners in verpleeghuizen en thuiswonende ouderen. Onderscheid tussen deze 2 groepen is niet meer mogelijk. Selectie van stammen voor genetische typering van degenen met vaccinfalen en daarmee opsporing van vaccinfalen als gevolg van circulatie van bepaalde virusvarianten is dan niet op te sporen

Contactmonitoring datastroom:

- Contactmonitoring data valt weg: percentage positief per type contact, aantal contacten per index op individueel niveau, tijdigheid van BCO
- Vaccinatiestatus van gemonitorde contacten valt weg: dit biedt zicht op vaccineffectiviteit

Cluster datastroom:

- Geen zicht meer op clusters (geen Cluster SitRep meer mogelijk, geen clusterinfo als basis voor specifieke OMT adviezen)
- Geen zicht op settings waarin verspreiding plaatsvindt; dit valt geheel weg: zie bij Osiris datastroom én cluster datastroom
- Inzicht in clusters wat betreft nieuwe varianten: epidemiologie en uitslag test niet te koppelen

- Selectie voor welke clusters sequencing moet plaatsvinden is niet meer mogelijk

Voorwaarden voor livegang

In het belang van de surveillance van COVID-19 en het monitoren van het effect van bestrijdingsmaatregelen en vaccinatie moet het RIVM mee kunnen beslissen over de datum dat het nieuwe systeem live kan gaan. Het RIVM heeft hiervoor de volgende voorwaarden opgesteld:

- Alle datastromen die nu naar het RIVM (Osiris, BCO, clusterrapportage) lopen, zijn geborgd.
- Deze nieuwe datastromen leveren identiek dezelfde variabelen, met alle zelfde kenmerken, vanuit 1 systeem.
- Het RIVM heeft minimaal 2 weken de tijd om het oude systeem naast het nieuwe systeem te laten lopen voor een controle op volledigheid, kwaliteit en nauwkeurigheid.
- Het systeem kent alle mogelijkheden die het huidige HPZone Lite ook kent op het gebied van aanmaken van contacten en het definiëren en aanmaken van clusters.
- Gegevens van eerder uitgevoerde BCO’s zijn beschikbaar van zowel de dossiers van indexcases, contacten, contexten, clusters en outbreaks (datamigratie).

4.7
Archived: donderdag 12 mei 2022 08:27:37
From: [redacted]
Sent: vrijdag 18 juni 2021 17:51:37
To: [redacted]
Subject: nog een paar dingen en tot over 3 weken
Importance: Normal
Sensitivity: None
Attachments:
Oplegnotitie DPG Raad - HPZone Information Officer V3.1 Definitief (003).pdf; FW_ TER INFO_ Gespreksverslag Vervolggesprek Toekomst BCO - Hart voor Brabant .msg; COVID-19_rapport_GGD_Hart_voor_Brabant_20210618_1727.pdf;

Hoi [redacted]

Hopelijk heb je een fijne dag gehad en hopelijk heeft vooral je zus de 'dag van haar leven' ervaren.

Ik wilde met jou bijgaande oplegnotitie bespreken die dinsdag in de DPG raad wordt behandeld.

Het gaat erover dat in ons systeem HPzone sinds de datadiefstal veel beperkingen zijn ingevoerd die tot problemen leiden. Het is namelijk niet mogelijk om exports te maken met gevoelige informatie (zoals BSN en adres). Deze exports zijn wel nodig voor een aantal activiteiten, zoals het declareren van verzekerde zorg, kwaliteitschecks (op dubbele of eerdere meldingen) en analyse op PC4 niveau. Dan ook niet allen bij COVID, maar juist bij de reguliere Infectieziektebestrijding

Het plan is nu om dit voor een beperkt aantal professionals wel mogelijk te maken (BIG geregistreerd, met VOG, met geheimhoudingsplicht en beroepsgeheim (!)), dus een paar van onze reguliere IZB professionals. De vraag binnen deze notitie is wie in de gaten gaat houden dat er geen rare dingen mee gebeuren. Naar mijn idee en dat van vele collega's kan je dat prima binnen de GGD zelf en moet je dit niet met allerlei vertragende regels en logboeken doen door een externe partij (GGDGHOR). Goede afspraken erover ((melden waarom en wanneer en -nog veel belangrijker- waar bewaar je ze (met wachtwoord of wat dan ook). Mijn pleidooi is dan ook om dit als GGD te regelene. Dat deden we al jaren.. Zijn mensen die je kent en vertrouwt. Onderbrengen bij anderen geeft een gevoel van wantrouwen en big brother.

Daarnaast heb ik je de notities gestuurd van het gesprek met de GGDGHOR over het BCO. [redacted] Ik heb geprobeerd er enige kaas van te maken. Reageer jij ook namens mij? De mail die ik stuurde heb ik voor de voolledigheid bijgesloten

Ik vind het jammer dat we al een tijd de 'benen op tafel' niet hebben gedaan. ik waardeer dat namelijk altijd erg. Na de vakantie moeten we misschien gewoon een keer naar het terras. [redacted], mag jij digitaal meedoen.

Als laatste de uitsmijter (voor ik voor 3 weken mijn computer dicht doe: we zijn (hieperdepiep) onder het landelijk gemiddelde (41,6) gezakt!!!! Wij Hvb 40,1. Of het tijdelijk is weet ik niet, maar dit doet mij deugt. In de schijnwerpers staan bovenaan de lijstjes is even interessant, maar soms niet meer leuk.

Ik ga wandelen, fietsen en veel lezen in Oostenrijk en Italie. Afkicken van werk en de batterij opladen

Ciao

4.7

11 Vergelijking met landelijke situatie

Tabel 23: Aantal meldingen van de afgelopen en vorige week.

GGD	Aantal meldingen afgelopen week	Aantal meldingen per 100000 afgelopen week	Aantal meldingen vorige week	Aantal meldingen per 100000 vorige week
Nederland-totaal	7244	41.6	11330	65.1
GGD Haaglanden	670	39.0	1080	89.5
GGD Amsterdam	598	56.9	575	53.7
Veiligheids- en Gezondheidsregio Gelderland-Midden	386	55.4	537	77.1
GGD Rotterdam-Rijnmond	678	51.2	1134	85.7
GGD Limburg-Noord	248	47.7	403	89.0
GGD Gelderland-Zuid	267	47.5	533	94.9
GGD Hollands-Midden	381	47.1	457	56.5
GGD Twente	296	46.9	473	75.0
GGD Gooi en Vechtstreek	148	45.9	93	30.2
GGD West-Brabant	317	44.7	537	75.7
GGD Regio Utrecht	378	42.7	360	61.4
Dienst Gezondheid & Jeugd ZHZ	187	40.7	286	62.3
GGD Hart voor Brabant	430	40.4	841	78.3
GGD Kennemerland	218	39.8	289	52.6
GGD Zeeland	148	38.6	182	47.5
GGD Zaanstreek/Waterland	125	36.9	203	59.8
GGD Brabant-Zuidoost	283	36.3	542	69.4
GGD IJsselland	175	32.0	327	61.2
GGD Flevoland	137	32.4	214	50.6
GGD Noord- en Oost-Gelderland	267	32.3	435	52.6
GGD Zuid-Limburg	191	32.0	367	61.5
GGD Hollands-Noorden	185	27.9	309	46.6
GGD Drenthe	123	24.0	232	47.0
GGD Fryslân	129	19.8	239	36.8
GGD Groningen	109	18.6	214	36.5

Met vriendelijke groet,

[redacted]

Arts Maatschappij & Gezondheid, infectieziektebestrijding

Regionaal Arts Consulent Zeeland-Brabant

GGD Hart voor Brabant

Pettelaarpark 10, 's-Hertogenbosch

Postbus 3024, 5003 DA Tilburg

www.ggdhvb.nl

[redacted]

Gezond doet leven!

4.8
Archived: donderdag 12 mei 2022 09:31:54
From: [redacted]
Sent: vrijdag 26 februari 2021 09:33:29
To: [redacted]
Subject: RE: Persoonsgegevens in te zien via dashboard GGDGHORNL
Importance: Normal
Sensitivity: None

Dag [redacted],

Is er een verslag of mailwisseling waarin die melding en toezegging begin december zwart op wit staat?

Groeten,

[redacted]

Van: [redacted]@ggdhvb.nl>
Verzonden: donderdag 25 februari 2021 15:07
Aan: [redacted]@ggdhvb.nl>; [redacted]@ggdhvb.nl>; [redacted]@ggdhvb.nl>; [redacted]@ggdhvb.nl>
Onderwerp: RE: Persoonsgegevens in te zien via dashboard GGDGHORNL

Nog wat extra achtergrond informatie/sum up:

- Vanuit deze landelijke rapportage omgeving die vanuit het performance dashboard te raadplegen is halen wij geen gegevens binnen voor dashboards;
- Dit dashboard is op dit moment voor 13 personen binnen HvB beschikbaar (onderzoekers, test coördinatoren en projectleider testen en vaccineren) en kan worden gebruikt om vaccinatie en test sturingsinformatie van HvB in te kunnen zien;
- De persoonsgelateerde gegevens die in de rapportage omgeving van het landelijk performance dashboard te vinden zijn mogen überhaupt niet beschikbaar zijn voor gebruikers ook al zijn het maar een beperkt aantal per GGD die toegang hebben
- Er is ons begin december al toegezegd dat deze gegevens er niet in thuis horen en zouden worden verwijderd. Dit is tot op heden niet gebeurd

Groet,

[redacted]

Met vriendelijke groet,

[redacted]

[redacted]

GGD Hart voor Brabant
Pettelaarpark 10,
5216 PD 's Hertogenbosch
[redacted]@ggdhvb.nl
Aanwezig op: ma-di-wo-do

www.ggdhvb.nl

[redacted]

Van: [redacted]
Verzonden: donderdag 25 februari 2021 09:56
Aan: [redacted]@ggdhvb.nl>; [redacted]@ggdhvb.nl>; [redacted]@ggdhvb.nl>
CC: [redacted]@ggdwestbrabant.nl>
Onderwerp: RE: Persoonsgegevens in te zien via dashboard GGDGHORNL

Het is een landelijk dashboard dat voor alle GGD'en op deze manier is ingericht.

[redacted] heeft contact gehad met [redacted] die aangeeft dat de GGD'en een kopie van hun eigen gegevens nodig hebben voor hun regionale dashboards. Voor WB, BZO, HvB en NOG is dit in ieder geval niet van toepassing en in een eerder stadium ook niet zo gecommuniceerd vanuit GGD GHOR. Het is gewoon zo ingericht.

Bij ons hebben de volgende personen toegang tot dit landelijke performance dashboard:

[redacted]@ggdhvb.nl
[redacted]@ggdhvb.nl
[redacted]@ggdhvb.nl
[redacted]@ggdhvb.nl
[redacted]@ggdhvb.nl
[redacted]@ggdhvb.nl
[redacted]@ggdhvb.nl
[redacted]@ggdhvb.nl

[redacted]@ggdhvb.nl

[redacted]@ggdhvb.nl

[redacted]@ggdhvb.nl

[redacted]@ggdhvb.nl

[redacted]@ggdhvb.nl

[redacted]@ggdhvb.nl = autorisatie is aangevraagd

Met vriendelijke groet,

[redacted]

[redacted]

GGD Hart voor Brabant

Pettelaarpark 10,

5216 PD 's Hertogenbosch

www.ggdhvb.nl

[redacted]@ggdhvb.nl

Aanwezig op: ma-di-wo-do

[redacted]

Van: [redacted]@ggdhvb.nl>
Verzonden: donderdag 25 februari 2021 09:35
Aan: [redacted]@ggdhvb.nl>; [redacted]@ggdhvb.nl>; [redacted]@ggdhvb.nl>
Onderwerp: RE: Persoonsgegevens in te zien via dashboard GGDGHORNL

Hallo,

Geldt dit voor alle GGD'en? Indien ja, wie heeft er toegang vanuit GGD Hvb?

Met vriendelijke groeten,

[redacted]

[redacted]

[redacted]

Hart voor Brabant

Postbus 3024, 5003 DA Tilburg

www.ggdhvb.nl

[redacted]@ggdhvb.nl

Aanwezig op: ma-di-wo-do

Gezond doet leven!

Van: [redacted]@ggdhvb.nl>
Verzonden: donderdag 25 februari 2021 09:27
Aan: [redacted]@ggdhvb.nl>; [redacted]@ggdhvb.nl>; [redacted]@ggdhvb.nl>
Onderwerp: RE: Persoonsgegevens in te zien via dashboard GGDGHORNL

Hoi,

Ik krijg net mail van [redacted] (WB) dat [redacted] hier ook van schrok en dit mee wil nemen naar de DPG raad dat morgen plaatsvindt.

@[redacted] kan jij dit ook bij [redacted] neerleggen? Lijkt me goed om dit signaal ook vanuit HvB te communiceren.

Groet,

[redacted]

Met vriendelijke groet,

[redacted]

[redacted]

Hart voor Brabant

Pettelaarpark 10,

5216 PD 's Hertogenbosch

www.ggdhvb.nl

[redacted]@ggdhvb.nl

Aanwezig op: ma-di-wo-do

[redacted]

Van: [redacted]@ggdhvb.nl>
Verzonden: dinsdag 23 februari 2021 12:17
Aan: [redacted]@ggdhvb.nl>; [redacted]@ggdhvb.nl>; [redacted]@ggdhvb.nl>
Onderwerp: RE: Persoonsgegevens in te zien via dashboard GGDGHORNL

[redacted] Vooral ook omdat HPZone/HPZLite op de 'slachtbank' wordt gelegd vanwege vergelijkbare redenen.

Groeten,

[redacted]

[redacted]

Hart voor Brabant

Ringbaan West 227 Tilburg

Postbus 3024, 5003 DA Tilburg

[redacted]@ggdhvb.nl

4.8 | www.ggdhvb.nl | Aanwezig op: di-wo-do-vr

Gezond? doet leven!

Van: [redacted]@ggdhvb.nl>
Verzonden: dinsdag 23 februari 2021 12:08
Aan: [redacted]@ggdhvb.nl>; [redacted]@ggdhvb.nl>; [redacted]@ggdhvb.nl>
Onderwerp: FW: Persoonsgegevens in te zien via dashboard GGDGHORNL
Urgentie: Hoog

Ter info.

Zojuist met [redacted] (WB) besproken; vanuit GGD GHOR 8 december jl. al de toezegging gekregen dat ze in de rapportages die in het landelijke performance dashboard te vinden zijn de persoonsgerelateerde velden zouden verwijderen. Dit is tot op heden nog niet gebeurd. Zie bijlage. Vanuit WB is dit nu nogmaals aangekaart bij [redacted] en [redacted].

Groet,

[redacted]

Met vriendelijke groet,

[redacted]

[redacted]

GGD Hart voor Brabant

Pettelaarpark 10,
5216 PD 's Hertogenbosch
www.ggdhvb.nl

[redacted]@ggdhvb.nl
Aanwezig op: ma-di-wo-do
[redacted]

Van: [redacted]@ggdwestbrabant.nl>
Verzonden: dinsdag 23 februari 2021 11:42
Aan: [redacted]@ggdghor.nl>; [redacted]@mxi.nl>
CC: [redacted]@ggdwestbrabant.nl>; [redacted]@ggdwestbrabant.nl>; [redacted]@ggdhvb.nl>; [redacted]@ggdnog.nl>; [redacted]@ggdbzo.nl>; [redacted]@ggdwestbrabant.nl>
Onderwerp: FW: Persoonsgegevens in te zien via dashboard GGDGHORNL
Urgentie: Hoog

Beste [redacted],

Zie onderstaande en bijgevoegde mails/print screens. Ik constateer dat deze rapporten nog steeds live staan, ondanks dat dit op 8 december vorig jaar in een gedeeld overleg (HvB, WB, NOG) door ons aan jou kenbaar is gemaakt en we van jou de toezegging hadden gekregen dat dit zo snel mogelijk aangepast zou worden. We hebben toen besproken dat in alle (operationele) rapporten minimaal de volgende velden verwijderd moeten worden: BSN nummer, Naw-gegevens, geboortedatum - en dat enkel het patiënt nr getoond wordt. [redacted] Ik wil je dringend verzoeken om deze rapporten aan te laten passen, conform

afgelopen december besproken.

Daarnaast zou ik je willen adviseren om alle door jullie opgeleverde en beschikbare rapportages na te (laten) lopen op mogelijke persoonsgegevens.

Hartelijke groet,

[redacted]

Van: [redacted]@ggdwestbrabant.nl>
Verzonden: dinsdag 23 februari 2021 11:19
Aan: [redacted]@ggdwestbrabant.nl>
Onderwerp: Persoonsgegevens in te zien via dashboard GGDGHORNL

Hoi [redacted],

Sinds vorige week heb ik toegang tot de dashboards van GGDGHORNL om live actuele cijfers te kunnen zien.

[redacted] zag ik na het klikken op Rapportages regionaal en vervolgens 'afspraken live' geen cijfers, maar een tabel met persoonsgegevens van mensen met een testafspraak. In de tabbladen die naast deze rapportage werden weergegeven, kon ik ook gegevens inzien van positief geteste personen.

[redacted] toen ik een Share-button en Download-button bovenaan dit scherm zag.

[redacted]

[redacted]

Zie bijlage voor een printscreen van wat ik op mijn scherm zie. Ik heb hierin de persoonsgegevens onleesbaar gemaakt, maar de kolomkoppen laten staan zodat je ziet welke gegevens er te lezen zijn.

Groeten [redacted]

Vriendelijke groeten,

[redacted]

[redacted]

GGD West-Brabant

Doornboslaan 225-227, Breda

Postbus 3024, 5003 DA Tilburg

www.ggdwestbrabant.nl

[redacted]

[redacted]@ggdwestbrabant.nl

Aanwezig op: ma, di, do, vr

Archived: donderdag 12 mei 2022 09:31:11
From: Programma Corona
Mail received time: Wed, 9 Jun 2021 13:49:36
Sent: woensdag 9 juni 2021 15:49:36
To: [redacted]
Subject: Update programma Corona | 09/06
Importance: Normal
Sensitivity: None

09/06/21

Lees deze email in jouw browser

\itap4Beste collega's,

\itap4Deze week bereiken we de piek met vaccineren en zetten we 90.000 vaccinaties per week. Een prestatie van formaat! Het harde werken werpt zijn vruchten af, want inmiddels zijn er landelijk 10 miljoen vaccinaties gezet. Reden voor RTL Nieuws om in gesprek te gaan met collega [redacted], prikker vanaf het eerste uur en werkzaam op de vaccinatielocatie in Den Bosch. Het verhaal van [redacted] lees je in deze nieuwsbrief. Uiteraard staan we stil bij de start van [redacted], vertellen de epidemiologen over hun werk en is er nieuws over GGD Contact.

\itap4[redacted] gestart als [redacted]

[redacted] heeft letterlijk en figuurlijk het stokje overgenomen van [redacted]. In een interview op Hartslag vertelt ze hoe ze het vindt om binnen het Programma aan de slag te zijn en deelt ze met ons hoe ze in balans blijft.

4.9

\itap4GGD Contact

Het uitvoeren van bron- en contactonderzoek (BCO) is een cruciaal onderdeel in de bestrijding van het coronavirus. Uit landelijk onderzoek is gebleken dat HP Zone Lite niet voldoet aan de eisen. Zoals eerder aangekondigd wordt er landelijk gewerkt aan een systeem om slimmer en efficiënter deze onderzoeken uit te voeren. Hiervoor is GGD Contact ontwikkeld. Het streven is om GGD Contact op woensdag 23 juni live te laten gaan. Allereerst in de zes praktijktestregio's. In de tweede stap volgen de andere GGD regio's. Hiertoe behoort ook GGD Hart voor Brabant. De BCO-medewerkers in de zes praktijktestregio's zullen in elk geval vanaf 23 juni gaan werken in het BCO-portaal van GGD Contact. Het is nog niet zeker of op deze datum de GGD Contact-app ook al ingezet kan worden. De stuurgroep beslist vrijdag 11 juni wanneer de GGD Contact-app wel in de praktijktestregio's in gebruik kan worden genomen. Voor GGD Hart voor Brabant is de voorlopige implementatiedatum 21 juli. Deze datum is nog niet definitief en kan nog veranderen.

\itap4Vaccineren uit spillage

Eerder berichten we op Hartslag over 'spillage'. Soms blijft er bij het vaccineren een klein aantal vaccins over, de zogenaamde spillage. Dit willen we natuurlijk niet weggooien. Tot op heden is deze spillage beschikbaar gesteld aan medewerkers op de vaccinatielocaties, de testlocaties en collega's met direct klantcontact. Omdat er steeds meer mensen zijn gevaccineerd, kunnen nu ook medewerkers die werkzaam zijn op kantoor worden gevaccineerd met spillage. Ook wanneer je al een afspraak hebt staan voor jouw eerste vaccinatie, kun je je aanmelden voor de spillagelijst. Heb je al 1 vaccinatie gehad? Dan kun je

je niet meer op de spillagelijst laten zetten. Kijk voor meer informatie op Hartslag.

\itap4Een kijkje achter de schermen bij epidemiologen [redacted] en [redacted]

Besmettingscijfers per gemeente. Coronagevallen per leeftijdsgroep. Clusters op basisscholen. Uitbraken in verpleeghuizen. Aantallen uitgevoerde coronatests. Percentages positieve tests. Hoeveelheden gezette vaccinaties. Voor epidemiologen zijn al deze gegevens goed voor analyses, duidingen, onderzoeken en adviezen die zij leveren. Omroep Brabant liep een dagje mee met epidemiologen [redacted].

\itap4Prikster [redacted] geïnterviewd door RTL nieuws

[redacted], een van onze priksters in de Brabanthallen, heeft tijdens haar werk via de telefoon RTL Nieuws te woord gestaan. Dat was naar aanleiding van de 10 miljoenste landelijke vaccinatie. Alsof ze nooit anders heeft gedaan, vertelt [redacted] via landelijke media aan Nederland over haar motivatie om bij te dragen. De journalist tevreden over [redacted] en [redacted] tevreden over de journalist: “Hij heeft het goed verwoord”. Lees hier het bericht op de website van RTL Nieuws.

\itap4Studenten Rooi Pannen trakteren op verse koeken

Donderdag 3 juni deelden studenten van de horecaopleiding van de Rooi Pannen verse koeken uit, als blijk van waardering voor alle inzet. De door de studenten zelfgebakken koeken waren bestemd voor alle medewerkers van de GGD die werken op de testlocatie aan

4.9 de Simon de Cockstraat in Tilburg. Het lekkers werd met open armen ontvangen en met smaak opgegeten. Bedankt Rooi Pannen voor deze leuke verrassing!

\itap4Deuren sluiten op Pettelaarpark Deuren sluiten op Pettelaarpark

Zoals jullie weten zit er een risico op datalekken in de toegankelijkheid van het gebouw aan het Pettelaarpark. Een datalek kan ook ontstaan als er printjes of een laptop worden meegenomen. Daarom is het belangrijk om alle deuren gesloten te houden. Dit geldt ook voor de glazen deuren op de eerste verdieping op het Pettelaarpark. Dat je niet zonder druppel heen en weer kan lopen is juist de reden van deze deuren. Dit is ter voorkoming van onbevoegden op de werkvloer. Graag vragen wij hier nogmaals jouw aandacht voor.

\itap4Gouden regels privacy

Binnen een grote organisatie als de GGD is het erg belangrijk om bewustwording te creëren over hoe om te gaan met persoonsgegevens. Om te werken aan deze bewustwording wordt elke week een gouden regel gepubliceerd. Iedere week komt er een regel bij en worden de eerdere regels herhaald om zo jullie geheugen op te frissen.

\itap4De veertiende 'gouden regel' luidt:

\itap4Wees je bewust van risico's van digitale opslag.

\itap4We voegen deze veertiende regel toe aan de eerdere privacyregels:

1. \itap4*\pn\pnlvlbody\pndec\pnstart1\pnindent360\pnql\pntxta.Je bent verplicht tot geheimhouding van alle vertrouwelijke informatie.

2. \itap4*\pn\pnlvlbody\pndec\pnstart2\pnindent360\pnql\pntxta.Deel wachtwoorden en toegangscodes nooit met anderen.
3. \itap4*\pn\pnlvlbody\pndec\pnstart3\pnindent360\pnql\pntxta.Schrijf je wachtwoorden niet op, onthoud deze of maak gebruik van een wachtwoordmanager.
4. \itap4*\pn\pnlvlbody\pndec\pnstart4\pnindent360\pnql\pntxta.Stel vragen als je niet zeker bent hoe en of je persoonsgegevens mag verwerken. Hiervoor kun je contact opnemen met de Privacy Officer of de Functionaris Gegevensbescherming binnen de organisatie.
5. \itap4*\pn\pnlvlbody\pndec\pnstart5\pnindent360\pnql\pntxta.Raadpleeg alleen de dossiers die op jouw naam staan of waartoe je gerechtigd bent om deze in te zien. Raadpleeg ook alleen dossiers die nodig zijn bij de uitvoering van je werkzaamheden.
6. \itap4*\pn\pnlvlbody\pndec\pnstart6\pnindent360\pnql\pntxta.Zorg ervoor dat onbevoegden niet mee kunnen kijken in dossiers en geen vertrouwelijke gesprekken kunnen meeluisteren.
7. \itap4*\pn\pnlvlbody\pndec\pnstart7\pnindent360\pnql\pntxta.Laat je geprinte documenten niet onbeheerd achter.
8. \itap4*\pn\pnlvlbody\pndec\pnstart8\pnindent360\pnql\pntxta.Gooi vertrouwelijke informatie in een versnipperaar of in daartoe bestemde containers.
9. \itap4*\pn\pnlvlbody\pndec\pnstart9\pnindent360\pnql\pntxta.Hanteer een clear desk/clear screen policy.
10. \itap4*\pn\pnlvlbody\pndec\pnstart10\pnindent360\pnql\pntxta.Laat digitale gegevensdragers nooit onbeheerd achter.
11. \itap4*\pn\pnlvlbody\pndec\pnstart11\pnindent360\pnql\pntxta.Maak alleen gebruik van een vertrouwd en beveiligd wifi-netwerk, gebruik geen gratis wifi-netwerk.
12. \itap4*\pn\pnlvlbody\pndec\pnstart12\pnindent360\pnql\pntxta.Ga zorgvuldig om met internet en e-mail, mijd onveilige situaties en open geen e-mail van onbekenden. Wanneer je een vreemde e-mail ontvangt, maak dan een incidentenmelding via Topdesk.
13. \itap4*\pn\pnlvlbody\pndec\pnstart13\pnindent360\pnql\pntxta.Sla geen vertrouwelijke informatie op op je privé apparatuur.

\itap4Cijfers

4.9

Testen

Vorige week (week 22) hebben 13.351 mensen zich laten testen bij onze GGD. Daarvan was 8,4% positief. De week daarvoor lieten meer mensen zich testen bij ons (15.165) en waren er procentueel gezien meer mensen positief: 10,2%.

Vaccineren

In week 22 hebben 36.316 mensen een eerste vaccinatie gekregen en 31.668 een tweede prik. De week daarvoor (week 21) kregen 30.925 mensen een eerste vaccinatie en 31.659 een tweede. Het verschil in cijfers heeft te maken met het verschil in aanbod van vaccins per week.

\itap4Dank weer voor jullie inzet,

4.9

[redacted] en [redacted]

[redacted]

Copyright © 2021 GGD Hart voor Brabant.
Je ontvangt deze email omdat je werkzaam bent voor het Programma Corona van de GGD Hart voor Brabant

Ons adres is:
\itap4GGD Hart voor Brabant
\itap4Reitseplein 3
Tilburg, 5037 AA
\itap4Netherlands

Add us to your address book

Wil je jouw voorkeuren voor onze nieuwsbrief aanpassen?
Voorkeuren aanpassen of afmelden

mailchimp

Archived: donderdag 12 mei 2022 09:29:31
From: [redacted]
Sent: dinsdag 26 januari 2021 09:13:20
To: [redacted]
Cc: [redacted]
Subject: RE: hpzone
Importance: Normal
Sensitivity: None

Hoi [redacted],

onderstaande foutmelding is inderdaad vanwege 'datalek'/diefstal. Vanuit infact bericht gekomen dat dit voor medewerkers met administrator rol of bco coordinator rol zo snel mogelijk hersteld zou worden.

Van: [redacted]
Verzonden: dinsdag 26 januari 2021 09:11
Aan: [redacted]
CC: [redacted]
Onderwerp: hpzone

Hi [redacted],

We gaan vandaag de exports overdragen aan [redacted]

Kun jij ervoor (laten) zorgen dat zij toegang heeft tot de juiste map (DWH Data import) om de exports op te plaatsen?

En natuurlijk de juiste authorisatie in HPzone.

Alvast dank

Met vriendelijke groet,

[redacted]

onderzoeker

GGD Hart voor Brabant

Vogelstraat 2 's-Hertogenbosch
Postbus 3024, 5003 DA Tilburg
www.ggdhvb.nl/onderzoek

[redacted]
Aanwezig op: ma-di-do-vr
9:30-14:30
[redacted]

Gezond doet leven!

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

Van: [redacted]
Verzonden: dinsdag 26 januari 2021 08:29
Aan: [redacted]
Onderwerp: hpzone

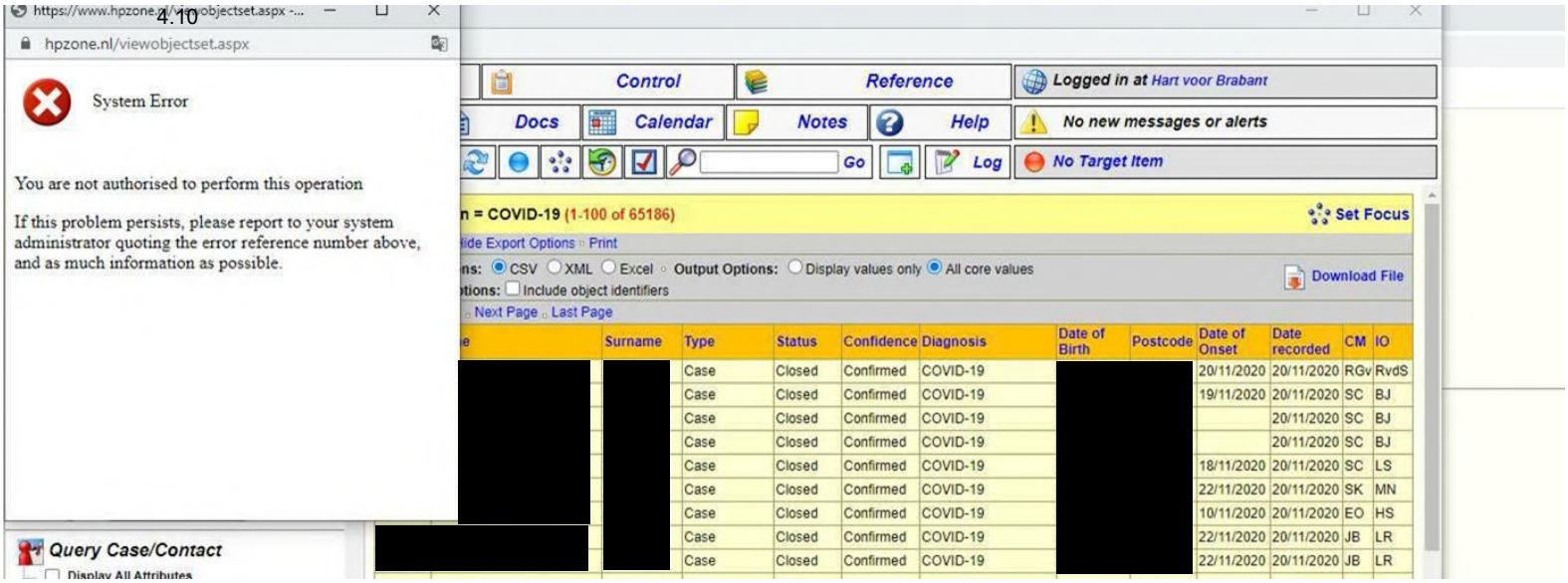
Hi,

Misschien ivm de datafraudes?

Ik was het niet hoor…

Maar goed, ik kom er nu dus niet in

Ik probeer nog een keer opnieuw en zal [redacted] waarschuwen..



Met vriendelijke groet,

[redacted]

onderzoeker

GGD Hart voor Brabant

Vogelstraat 2 's-Hertogenbosch

Postbus 3024, 5003 DA Tilburg

www.ggdhvb.nl/onderzoek

[redacted]

Aanwezig op: ma-di-do-vr

9:30-14:30

[redacted]

Gezond doet leven!

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

4.11
Archived: donderdag 12 mei 2022 09:29:00
From: [redacted]
Sent: maandag 25 januari 2021 13:32:55
To: [redacted]
Subject: RE: Overzicht FW: overdracht HPzone exports
Importance: Normal
Sensitivity: None

Hoi [redacted],

Vanuit de rapportageserver van CoronIT kunnen datadumps opgehaald worden door medewerkers met de autorisatierol "Onderzoeker (IZB/team onderzoek)". De volgende mensen hebben deze rol:

datum in behandeling	Achternaam	Tussen-voegsel	Voornaam	Pers.nr.	Inlognaam CoronIT
01-01-2020	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
01-01-2020					
01-01-2020					
14-10-2020					
06-10-2020					
25-01-2021					

Dezelfde onderzoekers hebben ook toegang tot HPZone om daar rapportages te maken. Daarnaast hebben onderstaande medewerkers dezelfde mogelijkheid:

Medewerkers met de rol "BCO Hoofdcoordinator"

datum in behandeling	Achternaam	Tussen-voegsel	Voornaam	Pers.nr.	Inlognaam CoronIT
18-09-2020	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
25-06-2020					
21-08-2020					
01-09-2020					
05-10-2020					
1-1-2020/25-09-2020					
10-8-2020/17-8-2020					
25-06-2020					
1-1-2020/23-07-2020					

En alle reguliere medewerkers van Team IZB plus de DIP'ers

Groeten,

[redacted]

[redacted]

Hart voor Brabant

Ringbaan West 227 Tilburg

Postbus 3024, 5003 DA Tilburg

www.ggdhvb.nl

[redacted]

Aanwezig op: di-wo-do-vr

Gezond doet leven!

Van: [redacted]
Verzonden: maandag 25 januari 2021 12:49
Aan: [redacted]
Onderwerp: Overzicht FW: overdracht HPzone exports

Hoi [redacted],

Heb jij een overzicht van medewerkers die een datadump kunnen maken voor beide systemen?

Met vriendelijke groeten,

[redacted]

[redacted]

[redacted]

Hart voor Brabant

Pettelaarpark 10 Den Bosch

Postbus 3024, 5003 DA Tilburg

www.ggdhvb.nl

[redacted]

Aanwezig op: ma-di-wo-do

Gezond doet leven!

Van: [redacted]
Verzonden: vrijdag 22 januari 2021 14:37
Aan: [redacted]
CC: [redacted]
Onderwerp: RE: overdracht HPzone exports

Hoi [redacted] en [redacted],

Kunnen jullie [redacted] meenemen in deze communicatie. Zij is op zoek naar inzicht omtrent de handelingen die voor dit proces moeten worden uitgevoerd en wil graag weten welke personen deze taak op gaan pakken. Ik heb haar in de cc gezet.

Dank je.

Groet,

[redacted] 4.11

Met vriendelijke groet,

[redacted]

[redacted]

GGD Hart voor Brabant

Pettelaarpark 10,

5216 PD 's Hertogenbosch

www.ggdhvb.nl

[redacted]

Aanwezig op: ma-di-wo-do

[redacted]

Van: [redacted]
Verzonden: vrijdag 22 januari 2021 11:42
Aan: [redacted]
Onderwerp: RE: overdracht HPzone exports

Voor zover ik weet hebben HP invoer medewerkers toegang tot N schijf, maar G schijf weet ik niet. Ik ben nog aan het overleggen bij wie we dit het beste kunnen leggen. Zit zelf ook te denken aan onze procescoordinatoren. Werk vandaag niet dus zal maandag nogmaals kijken en wanneer we weten wie het gaat doen meteen authorisatie aanvragen.

Van: [redacted]
Verzonden: vrijdag 22 januari 2021 08:27
Aan: [redacted]
Onderwerp: RE: overdracht HPzone exports

Beste [redacted],

Heel fijn!

He is wel belangrijk dat de personen die dit gaan doen toegang hebben tot HPzone en tot

onderstaande map waar zij het bestand in moeten wegschrijven.

Alvast dank!

Met vriendelijke groet,

[redacted]

onderzoeker 4.11

Vogelstraat 2 's-Hertogenbosch

Postbus 3024, 5003 DA Tilburg

www.ggdhvb.nl/onderzoek

[redacted]

Aanwezig op: ma-di-do-vr

9:30-14:30

[redacted]

Gezond doet leven!

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

Van: [redacted]
Verzonden: donderdag 21 januari 2021 12:18
Aan: [redacted]
Onderwerp: RE: overdracht HPzone exports

[redacted],

ik heb inderdaad begrepen dat jullie dit al geruime tijd doen, maar dat het een handeling is die ook elders belegd kan worden, dus fijn als we jullie daarmee kunnen ontlasten.

Ik zal het hier bespreken en dan stuur ik de uitnodiging door naar degene die dit op zich zal nemen.

Met vriendelijke groet,

[redacted]

[redacted]

Team Infectieziekten

Pettelaarpark 10, 5216 PD 's-Hertogenbosch

Postbus 3024, 5003 DA Tilburg

www.ggdhvb.nl

[redacted]

Ma,di,wo,do

Gezond doet leven!

Van: [redacted]
Verzonden: donderdag 21 januari 2021 12:15
Aan: [redacted]
Onderwerp: overdracht HPzone exports

Beste [redacted],

Wij hebben van [redacted] en [redacted] begrepen dat we met jou de overdracht van de HPzone exports t.b.v corona dashboard kunnen regelen.

Wij doen dit nu al ruim 9 maanden en dragen het graag over.

Ik heb een meeting in teams ingepland.

Als jij al weet wie de exports (iedere ochtend voor 8:45) gaan uitvoeren kunnen we die personen misschien ook al uitnodigen.

Dan kunnen we zo snel mogelijk overdragen.

Alvast dank!

Met vriendelijke groet,

[redacted]

onderzoeker

GGD Hart voor Brabant

Vogelstraat 2 's-Hertogenbosch

Postbus 3024, 5003 DA Tilburg

www.ggdhvb.nl/onderzoek

[redacted]

Aanwezig op: ma-di-do-vr

9:30-14:30

[redacted]

Gezond doet leven!

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

GGD Hart voor Brabant
[redacted]
Postbus 3024
5003 DA TILBURG

Behandeld door: [redacted] Datum: 14 oktober 2021
Onderwerp: Instemmingsaanvraag Logging CoronIT en HPzone(Lite) E-mail: [redacted]

Geachte mevrouw [redacted]

Deze brief bevat de reactie van de Ondernemingsraad (OR) op uw reeds genomen besluit over Logging CoronIT en HPzone(Lite). U verzoekt de OR hiermee in te stemmen.
Dit instemmingsverzoek komt voort uit Artikel 27 lid 1 sub l van de WOR.

De OR constateert dat controles op logbestanden al sinds februari 2021 worden uitgevoerd. Zonder de instemming van de OR hadden deze controles nooit ingevoerd mogen worden.
De OR begrijpt de noodzaak van de maatregelen. Desondanks stemt de OR niet in met dit besluit, om de volgende redenen:

- Het gaat hier niet meer om een voorgenomen besluit, maar om een reeds genomen besluit. De OR ziet er geen meerwaarde in om nu nog instemming te geven.
- Betrokken medewerkers hadden vooraf op de hoogte moeten worden gesteld van het besluit om te controleren én over onder welke voorwaarden dit gebeurt. Idealiter worden deze voorwaarden vastgelegd in een gedragscode, die ook ter instemming moet worden voorgelegd.
- Instemming met dit genomen besluit is voor de OR niet uit te leggen aan de achterban.
- De vereiste procedure is niet gevolgd; het voorgenomen besluit is nooit besproken in een overlegvergadering.

De OR heeft nog een aantal vragen over de door u toegestuurde documenten:

- Waarop heeft de DPG precies invloed?
- Waar valt het SOC onder? Wat is CISO? Wat is DPIA? (Zie bladzijde 2 aanvraag)
- Wat moet er voor onze GGD en onze medewerkers door de DPG geregeld worden?
- Welke medewerkers vallen precies onder deze regeling? Alleen medewerkers in dienst van de GGD of ook de medewerkers die via een andere constructie werkzaamheden verrichten voor de GGD?
- Waarover wordt dan precies instemming gevraagd aan de OR?

De OR vindt het van belang dat er een gedragscode wordt opgesteld, welke eveneens ter instemming aan de OR moet worden voorgelegd.

De OR vindt het belangrijk dat medewerkers worden geïnformeerd over de gang van zaken tot nog toe en dat er aandacht is voor de (nadelige) gevolgen die medewerkers hiervan hebben ondervonden.

De OR wil met u in gesprek over de verdere afhandeling van dit besluit.
Tevens wil de OR afspraken met u maken over de wijze waarop hij in de toekomst tijdig om instemming wordt gevraagd bij instemmingsplichtige onderwerpen.

De OR denkt dat er mogelijk meer systemen binnen de GGD gebruikt (gaan) worden waarbij controle mogelijk is. Denk hierbij aan het systeem dat binnen het KCC wordt gebruikt ter bevordering van de kwaliteit.
Wat heeft u daarvoor ingeregeld?

De OR wil met u in de overlegvergadering van dinsdag 19 oktober in gesprek over dit instemmingsverzoek en de vragen die de OR hierover nog heeft.

Met vriendelijke groet,

Voorzitter OR

4.13
Gearchiveerd: dinsdag 3 mei 2022 08:49:37
Van: [redacted]
Verzonden: donderdag 18 maart 2021 17:24:06
Aan: [redacted]
Onderwerp: FW: Toegang tot HP ZOne Lite door landelijke teams
Urgentie: Normal
Precisie: None

Ter informatie

Met vriendelijke groet,

[redacted]

[redacted]

Hart voor Brabant

Pettelaarpark 10, 5216 PD 's-Hertogenbosch

www.ggdhvb.nl

[redacted]

Aanwezig op: ma-di-do-vrij

Gezond doet leven!

Van: [redacted]
Verzonden: donderdag 18 maart 2021 15:04
Aan: [redacted]
Onderwerp: RE: Toegang tot HP ZOne Lite door landelijke teams

Hoi [redacted]

op dit moment hebben alleen SOS international toegang tot onze HP zone, dit zijn 1148 mensen.

We krijgen 2 wekelijks een active directory document. Aan de hand van dit document passen de procescoordinatoren de autorisaties aan.

Knelpunt is hierin dat we een totaal overzicht krijgen van alle medewerkers, het kost erg veel tijd om dit document door te nemen en vervolgens autorisaties in te trekken. Omdat ook de capacity planner nog niet gebruikt kan worden hebben de proces co's nog steeds niet veel tijd over. We hebben aangegeven dat administratieve ondersteuning in dit deel gewenst zou zijn.

Mvg [redacted]

Van: [redacted]ggdhvb.nl>
Verzonden: donderdag 18 maart 2021 14:48
Aan: Watervliet, Mandeley van de <m.vd.watervliet@ggdhvb.nl>
Onderwerp: Toegang tot HP ZOne Lite door landelijke teams

Hoi [redacted]

4.13

Hoe veel mensen van landelijke pool (SOS international, etc) hebben nu toegang tot onze lokale HP Zone omgeving via HP Zone Lite?

Is er een check op wie dat nu kan?

Moeten er weer autorisaties ingetrokken worden? Om dit aantal weer te beperken?

Met vriendelijke groet,

[redacted]

[redacted]

GGD Hart voor Brabant

Pettelaarpark 10, 5216 PD 's-Hertogenbosch

www.ggdhvb.nl

[redacted]

Aanwezig op: ma-di-do-vrij

Gezond doet leven!

Instemmingsverzoek

Conform artikel 27, eerste lid, onder l, van de Wet op de ondernemingsraden (WOR)

Datum	21 september 2021
Van	[redacted], directeur publieke gezondheid
Aan	Ondernemingsraad GGD Har voor Brabant (OR)
Onderwerp	Informatiebeveiliging: instemmingsverzoek logging CoronIT en HPZone(Lite)

Samenvatting

Het gebruik van de systemen CoronIT en HpZone(Lite) wordt bijgehouden in zogenoemde logfiles. Het Security Operation Center (SOC) voert sinds begin februari controles uit op die logbestanden. Het SOC signaleert afwijkend gedrag dat kan duiden op onrechtmatige toegang tot, onrechtmatige inzage of onrechtmatig gebruik van de persoonsgegevens in een dossier. Het is in het licht van artikel 32 AVG belangrijk dat dit gebeurt. Naast andere beveiligingsmaatregelen is het bijhouden van logfiles nodig om de dossiers van burgers – waarin ook gezondheidsgegevens staan – goed te beschermen door onrechtmatig gebruik van die informatie te voorkomen en op te sporen.
In juni staat de implementatie van de ´SIEM-oplossing´ (Security Information & Event Management) gepland, waarmee een deel van het werk van het SOC bij de controle op de logfiles geautomatiseerd zal plaatsvinden. Werknemers van GGD'en vallen, evenals werknemers van de partners, onder deze vorm van monitoring. Hiervoor is instemming van de OR vereist.

Instemmingsverzoek

De directeur vraagt de OR conform artikel 27, eerste lid, onder l van de WOR instemming op het besluit ten aanzien van informatiebeveiliging, namelijk:

- het door het SOC monitoren van logfiles van CoronIT en HPzone(lite) met als doel het voorkomen dat en te controleren of persoonsgegevens in die systemen onrechtmatig door medewerkers of partners van GGD-en worden verwerkt;
- het voeren van een triageproces, waarin wordt bepaald door wie en hoe wordt gehandeld in het geval afwijkend en mogelijk onrechtmatig gedrag wordt gesignaleerd.
- implementatie van de SIEM-oplossing per 30 juni 2021.

Gevraagde datum van instemming

Zo spoedig mogelijk.

Beweegredenen en uitwerking

Naar aanleiding van de datadiefstal eind januari zijn diverse maatregelen genomen om systemen en databestanden beter te beschermen. Eén van die maatregelen vormt de inzet van het SOC. Dit team bestaat uit data- en security analisten, identity- and access specialisten en compliance officers. Het SOC monitort de logfiles van CoronIT en HPzone(Lite) met als doel om te voorkomen dat en te controleren of persoonsgegevens in CoronIT en HPZone(Lite) onrechtmatig door medewerkers of partners van GGD'en worden verwerkt (bijvoorbeeld: ingezien, opgeslagen of geëxporteerd). Bij die monitoring kijkt het SOC naar verschillende indicatoren van onrechtmatige

verwerking, zoals naar het aantal schermen dat per account in een tijdvak bekeken wordt en naar het benaderen van specifieke dossiers (o.a. BN'ers). Momenteel gebeurt dit handmatig, eind juni is de implementatie van de SIEM-oplossing voorzien, waarmee een deel van de handmatige monitoring zal worden geautomatiseerd.

Bij signalen van mogelijk onrechtmatige verwerkingen gaat het SOC over tot nadere analyse van het account en het gedrag van de gebruiker daarachter. Dit triage proces is ingericht conform NEN 7510 en ISAE3402. Wanneer voor het afwijkende gedrag geen valide reden gevonden wordt, of wanneer het SOC ziet dat het om een onrechtmatige verwerking gaat, schakelt zij daar direct op met de betreffende werkgever en/of politie. Indien het een GGD-medewerker betreft, treedt de CISO van GGD GHOR of de Manager SOC in overleg met de vertrouwenspersoon en/of CISO bij de betreffende GGD. Maatregelen die dan genomen (kunnen) worden lopen uiteen van het (tijdelijk) blokkeren van het account van de betreffende tot aan aangifte bij de politie. De timing van het inlichten van de GGD en het inlichten van de politie wordt bepaald door de Manager SOC, al naar gelang de inschatting van de ernst van de situatie.

Waarborgen

De werking van het SOC (straks met behulp van de SIEM oplossing) en het acteren op onregelmatigheden in samenspel met de GGD of partner, is in lijn met de bepalingen hierover in de AVG. Om de privacy van medewerkers en burgers zo goed mogelijk te beschermen, zijn er zo min mogelijk SOC-medewerkers betrokken bij de controle op de logfiles. De logfiles bevatten niet de naam van medewerker die het dossier van een burger raadpleegt. In plaats daarvan wordt in CoronIT gewerkt met een medewerkernummer dat is gekoppeld aan een individuele medewerker en losstaat van diens personeelnummer. Ook de naam van de burger is in de logfiles niet opgenomen. In plaats daarvan wordt gewerkt met een uniek patiëntnummer. Voor Hpzone (Lite) geldt dat gewerkt wordt met een sessie-nummer. Pas bij de analyse van signalen die kunnen wijzen op onrechtmatige toegang tot, onrechtmatige inzage of onrechtmatig gebruik van de persoonsgegevens in een dossier wordt achterhaald welke medewerker en welke burger er gekoppeld zijn aan voormelde nummers/sessies. Bij deze analyse zijn maximaal twee analisten betrokken (de tweede analist fungeert als back-up). Zij volgen het in de bijlage bijgevoegde triageproces.

Op de monitoring van het SOC, het triageproces en de SIEM-oplossing zullen DPIA's worden uitgevoerd. Het proces om te komen tot de DPIA's is inmiddels gestart.
Van belang is, is dat medewerkers worden geïnformeerd over het SOC en de controle op logfiles met behulp van de SIEM-oplossing, en hoe hun persoonsgegevens in dit kader worden verwerkt. Informeren kan middels een privacy verklaring en/of door vermelding in de geheimhoudings-verklaring die door iedere medewerker getekend moet worden.

Proces

DPG'en zijn op 15 juni geïnformeerd over de huidige handmatige controle op de logbestanden van CoronIT en HPZone(Lite) en het voornemen om in juni 2021 SIEM-tooling te implementeren.

Gelet op het bredere maatschappelijke belang, waaronder het voorkomen van inbreuken op de grondrechten van betrokkenen wiens gegevens in de gegevens staan opgeslagen, wordt de reeds bestaande werkwijze van monitoring van logfiles en het daaraan gekoppelde triageproces in afwachting van de beslissing van de OR voortgezet.

Gevolgen voor personeel en communicatie

Na instemming van de OR informeert het team Personeel en organisatie (namens de directeur) de medewerkers over de ingebruikname van de SIEM-tooling en het bijbehorende proces rondom controle op logbestanden. Daarbij wordt tevens een privacyverklaring gevoegd, waarin onder meer wordt beschreven welke persoonsgegevens bij de controle op logbestanden worden verwerkt, voor welke doeleinden deze persoonsgegevens worden gebruikt en welke rechten medewerkers in dit verband hebben.

Bijlage

- Samenvatting Procesbeschrijving Triage CoronIT

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:

Hart voor Brabant

Gezond² doet leven!

Vergadering dagelijks bestuur

Datum **16 december 2021** DB 20211216-2-0
Onderwerp **Mededelingen**
Agendapunt **2**
Afzender **Directeur**
Portefeuille **Hillenaar**

Omschrijving

1. Rapport onderzoek datalekken

De Autoriteit persoonsgegevens (AP) heeft onderzoek naar datalekken gedaan bij GGD GHOR Nederland en twee GGD'en (niet de onze). Haar conclusie: er zij verbetermaatregelen waardoor het risico op datalekken is verminderd. Maar de AP ziet nog wezenlijke risico's voor de beveiliging van persoonsgegevens: er zijn geen duidelijke afspraken tussen organisaties over bepaalde beveiligingsaspecten, bijvoorbeeld rond het autorisatiebeheer en de controle van logbestanden. Verder leidt het vervangen van een systeem niet zonder meer tot een betere beveiliging.

2. Verslag gesprek Inspectie Gezondheidszorg en Jeugd

Op 22 september was er een gesprek tussen de IGJ en de GGD, zie bijgaand verslag. Het was een vooral een kennismaking met de volgende inspecteur, dat voor de GGD weinig nieuws opleverde. De meeste punten in het verslag zijn u al bekend.

3. Nieuwe landelijke stichting (COVID-19 bestrijding)

Vanaf het begin van de coronacrisis voert GGD GHOR Nederland een aantal taken uit voor de bestrijding ervan, in opdracht van de minister van VWS. Dit gebeurde door de Stichting Projectenbureau en zij besloot om deze taken af te splitsen in een aparte stichting, de *Stichting Landelijke Coördinatie COVID-19 Bestrijding.* De stichting beschrijft in haar statuten, zie bijlage …, ook de betrokkenheid van de directeuren publieke gezondheid. Zij zitten in een 'deelnemersraad' die een adviezen geeft en niet verantwoordelijk is voor het bestuur van de stichting. Het deelnemen in de raad bindt de gemeenten of de GGD 'en (dus) op geen enkele wijze en het past binnen de bevoegdheden die u aan uw directeur overdroeg via de organisatieverordening.

4.

5.1

Beslispunt(en)
1. Kennis nemen van de mededelingen.
2. Informeren van het algemeen bestuur over de mededelingen 4 tot en met 8.

Eerdere besluiten --

Gevolgen --

Besluit

De secretaris, de voorzitter,

T.H.I. Claassen W.A.G. Hillenaar

Bijlage(n)
1. Eindbrief onderzoek beveiliging persoonsgegevens GGD GHOR en GGD'en.
2. Verslag gesprek IGJ - GGD Hart voor Brabant 22-09-2021.
3. Statuten Stichting Landelijke Coördinatie COVID-19 Bestrijding.

.

Hart voor Brabant

Gezond² doet leven!

Vergadering dagelijks bestuur

Datum **16 december 2021** DB 20211216-2-0
Onderwerp **Mededelingen**
Agendapunt **2**
Afzender **Directeur**
Portefeuille [redacted]

Omschrijving

1. Rapport onderzoek datalekken

De Autoriteit persoonsgegevens (AP) heeft onderzoek naar datalekken gedaan bij GGD GHOR Nederland en twee GGD'en (niet de onze). Haar conclusie: er zij verbetermaatregelen waardoor het risico op datalekken is verminderd. Maar de AP ziet nog wezenlijke risico's voor de beveiliging van persoonsgegevens: er zijn geen duidelijke afspraken tussen organisaties over bepaalde beveiligingsaspecten, bijvoorbeeld rond het autorisatiebeheer en de controle van logbestanden. Verder leidt het vervangen van een systeem niet zonder meer tot een betere beveiliging.

2. Verslag gesprek Inspectie Gezondheidszorg en Jeugd

Op 22 september was er een gesprek tussen de IGJ en de GGD, zie bijgaand verslag. Het was een vooral een kennismaking met de volgende inspecteur, dat voor de GGD weinig nieuws opleverde. De meeste punten in het verslag zijn u al bekend.

3. Nieuwe landelijke stichting (COVID-19 bestrijding)

Vanaf het begin van de coronacrisis voert GGD GHOR Nederland een aantal taken uit voor de bestrijding ervan, in opdracht van de minister van VWS. Dit gebeurde door de Stichting Projectenbureau en zij besloot om deze taken af te splitsen in een aparte stichting, de *Stichting Landelijke Coördinatie COVID-19 Bestrijding.* De stichting beschrijft in haar statuten, zie bijlage …, ook de betrokkenheid van de directeuren publieke gezondheid. Zij zitten in een 'deelnemersraad' die een adviezen geeft en niet verantwoordelijk is voor het bestuur van de stichting. Het deelnemen in de raad bindt de gemeenten of de GGD 'en (dus) op geen enkele wijze en het past binnen de bevoegdheden die u aan uw directeur overdroeg via de organisatieverordening.

4.

5.1

Beslispunt(en)
1. Kennis nemen van de mededelingen.
2. Informeren van het algemeen bestuur over de mededelingen 4 tot en met 8.

Eerdere besluiten --

Gevolgen --

Besluit

De secretaris, de voorzitter,

[redacted] [redacted]

Bijlage(n)
1. Eindbrief onderzoek beveiliging persoonsgegevens GGD GHOR en GGD'en.
2. Verslag gesprek IGJ - GGD Hart voor Brabant 22-09-2021.
3. Statuten Stichting Landelijke Coördinatie COVID-19 Bestrijding.

.

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

Een screenshot van de verkennerpagina van map 6:

6.1

Versie 07-03-2022

			Programma					Testen					KCC Corona											BCO, Signalering en Advies													Vaccinaties									IDMS	Key-user		IZB/Infectiepreventie								
			Programma-manager	Arts Corona	Planning programma Corona	Projectleider	Programma-bureau	Testen Coördinator	Testen Projectondersteuner	Testen afnemer	Testen 1e verantwoordelijke teststraten	Logistiek Medewerker	KCC Corona 1e lijns medewerker	KCC Corona 2e lijns medewerker	KCC Corona 1e lijns chat medewerker	KCC Corona 2e lijns chat medewerker	KCC Corona Webcare medewerker	KCC Corona 1e lijns kwaliteitsmedewerker telefonie	KCC Corona 1e lijns kwaliteitsmedewerker chat	KCC Corona 2e lijns kwaliteitsmedewerker chat	KCC Corona 1e lijns coordinator	KCC Corona 2e lijns Coördinator	KCC Corona 2e lijns Aanspreekpunt	BCO Cluster Coordinator	BCO Cluster Medewerker	BCO Medewerker	BCO Medewerker Yource	BCO Medewerker Soleo	BCO Hoofdcoordinator	BCO Inhoudelijk coordinator	BCO Procescoordinator	BCO Coordinator Yource	BCO Coordinator Soleo	BCO Projectleider Yours	BCO Projectondersteuner	HP invoer medewerker	Vaccinatie medisch/arts	Vaccinatie Administrateur	Vaccinatie Administrateur Plus	Vaccinatie 1e verantwoordelijke	Vaccinatie Coordinator Vangnet	Vaccinatie Coordinator	Vaccinatie Projectondersteuner	GVKI	Logistiek medewerker	Onderzoeker (IZB/team onderzoek)	Key-user Corona	Funtioneel Beheer programma Corona	SELECTIE IZB totaal	Arts IZB	Arts AIOS/ANIOS IZB	Verplk. IZB Corona	Verplk.IZB	Epidemioloog IZB	Co-assistant Arts IZB	PPO IZB	DIP'er
		Alleen doorstroom →															x	x	x					x	x																			x													
Applicatie/Onderdeel ↓	Autorisatie ↓	Geregeld door ↓																																																					
Office	E3 CSP Licentie	Servicedesk ICA	x	x	x	x	x	x	x		x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x		x	x		x	x	x	x	x		x		x	x									
	Standaard licentie (Check s.v.p. of een medewerker een vaste GGD-medewerker is. Dan heeft hij/zij deze al, en moet die ook houden!)	Servicedesk ICA																																												x			x	x	x	x	x	x	x	x	x
Documenten	map n:\ Programma Corona	Servicedesk ICA																												x					x																				
	map l:\AGZ\IZB	Servicedesk ICA																																															x	x	x		x	x		x	
	Teams BCO (toegang door Corona Beheer)	Corona Beheer												x								x	x	x	x	x	x		x	x	x	x		x	x	x													x	x	x	x					
	Teams Test	Beheerder Teams site						x	x		x	x																																													
	Teams Corona Advies	Beheerder Teams site																				x																																			
	Teams Doelgroepen	Beheerder Teams site																																																							
	Teams ID&S	Beheerder Teams site																																												x											
	Teams Uitbraak opschaalteam	Beheerder Teams site																											x																												
	Teams P Corona Bereikbaarheid	Beheerder Teams site																				x	x																																		
	Teams Corona Artsen	Beheerder Teams site		x																									x																				x	x	x						
	Teams Programmasturing	Beheerder Teams site	x																																																						
	Teams HvB P ProgCorona	Beheerder Teams site	x	x	x	x	x	x	x													x	x	x					x									x	x										x	x							
	Teams Vaccinatie (HVB P Vaccinatie Corona)	Beheerder Teams site																																				x	x																		
Mailbox	Planning Corona HvB (planningcorona@ggdhvb.nl)	Servicedesk ICA			x																																																				
	Corona Declraties (corona.declaraties@ggdhvb.nl)	Servicedesk ICA			x																																																				
	Artsen IZB (artsenIZB@ggdhvb.nl)	Servicedesk ICA		x																																													x	x	x						
	Infectieziekten HvB (infectieziekten@ggdhvb.nl)	Servicedesk ICA		x																																													x	x	x		x	x		x	
	GGD Hart voor Brabant Klantcontactcentrum (contact@ggdhvb.nl)	Servicedesk ICA											x								x																																				
	Corona Bemonstering (corona.bemonstering@ggdhvb.nl)	Servicedesk ICA						x	x																																																
	Corona Testlocaties (corona.testlocaties@ggdhvb.nl)	Servicedesk ICA									x																																														
	Administratie Corona administratie.corona@ggdhvb.nl	Servicedesk ICA							x																																																
	Corona .2elijn (corona.2elijn@ggdhvb.nl)	Servicedesk ICA												x								x	x																																		
	Corona Advies (noreply) (corona.advies.noreply@ggdhvb.nl)	Servicedesk ICA												x								x	x																																		
	Digitaal corona certificaat GGD HVB (corona.dcc@ggdhvb.nl)	Servicedesk ICA																																										x													
	Corona 2elijn Coordinatoren (corona.2elijn.coordinatoren@ggdhvb.nl)	Servicedesk ICA																				x																																			
	Corona.vragenbco (corona.vragenbco@ggdhvb.nl)	Servicedesk ICA																											x	x	x																										
	Corona Contactonderzoek (corona.contactonderzoek@ggdhvb.nl)	Servicedesk ICA																								x	x	x	x	x	x	x	x																								
	BCOYource (bcoyource@ggdhvb.nl)	Servicedesk ICA																														x		x																							
	Coordinatie Soleo (coordinatiesoleo@ggdhvb.nl)	Servicedesk ICA																															x																								
	BCOVVT (bcovvt@ggdhvb.nl)	Servicedesk ICA																						x	x					x																											
	corona.IDMS (corona.idms@ggdhvb.nl)	Servicedesk ICA																																												x			x								x
	corona.clustermeldingen (corona.clustermeldingen@ggdhvb.nl)	Servicedesk ICA	x																																																						
	Corona Clusters (corona.clusters@ggdhvb.nl)	Servicedesk ICA																						x	x																																
	Corona Invoerhpzone (corona.invoerhpzone@ggdhvb.nl)	Servicedesk ICA																																		x																					
	PBM Landelijk Consortium Hulpmiddelen Bestellingen (logistiek@ggdhvb.nl)	Servicedesk ICA						x	x			x																																													
	FAX IZB (fax-izb@ggdhvb.nl)	Servicedesk ICA																																		x																					
	Programma Corona (programmacorona@ggdhvb.nl)	Servicedesk ICA	x			x	x																																																		
	Coronateam Ziekenhuizen (coronateam.ziekenhuizen@ggdhvb.nl)	Servicedesk ICA																																		x																					
	BCO Processcoördinatoren (processcoordinatorenBCO@ggdhvb.nl)	Servicedesk ICA																												x																											
	Corona Verzoek Persoonsgegevens (corona.verzoek.persoonsgegevens@ggdhvb.nl)	Servicedesk ICA																																																							
	ikwilhelpenmetvaccineren (ikwilhelpenmetvaccineren@ggdhvb.nl)	Servicedesk ICA																																																							
	Corona.2elijnscholen (corona.2elijnscholen@ggdhvb.nl)	Servicedesk ICA												x								x	x							x																											
	Vaccinatie HVB (vaccinatiehvb@ggdhvb.nl)	Servicedesk ICA																																							x	x															
HPZone	HPZone-L-HPZoneLite-G	Servicedesk ICA																																x										x													
	HPZone-L-HPZoneLite-S	Servicedesk ICA																																																							
	HPZone-L-HPZoneLite-P	Servicedesk ICA		x										x								x	x	x	x	x	x	x	x	x	x	x	x		x	x											x		x			x					
	HPZone-National-Role	Servicedesk ICA		x										x								x	x	x	x	x	x	x	x	x	x	x	x			x																					
	HPZone-Investigating-Officer	Servicedesk ICA												x								x	x	x	x	x	x	x	x	x	x	x	x	x	x	x								x		x			x	x	x	x	x	x	x	x	x
	HPZone-Case-Manager	Servicedesk ICA		x																																													x	x	x						x
	HPZone-Administrative-Officer	Servicedesk ICA																											x		x				x												x										
	HPZone-Information-Officer	Servicedesk ICA																																																							
	HPZone-L-HPZone-G	Servicedesk ICA																																																							
	HPZone-L-HPZone-S	Servicedesk ICA																																																							
	HPZone-L-HPZone-P	Servicedesk ICA																											x																	x	x		x	x	x	x	x	x	x	x	x
	HPZone-L-Administration-P	Servicedesk ICA																											x		x				x												x										
	HPZone-L-Dashboard-P	Servicedesk ICA																																												x											
	HPZone-Coordinator	Servicedesk ICA																													x															x			x	x	x						
CoronIT	Coronit-GGD-MW	Servicedesk ICA		x	x			x	x	x	x		x	x							x	x	x	x	x	x			x	x	x				x	x	x	x	x	x	x	x	x			x			x	x		x					
	Monsterafname	Corona Beheer			x			x	x	x	x																																					x									
	Roosterplanner	Corona Beheer			x			x	x																														x			x	x					x									
	Anamnese(en afspraken plannen)	Corona Beheer		x	x			x	x		x		x	x							x	x	x	x	x	x			x	x	x																	x	x	x		x					
	Inzien en terugkoppelen labresultaten	Corona Beheer		x				x					x	x							x	x	x	x	x	x			x	x	x				x	x												x	x	x		x					
	Importeren groep dossiers	Corona Beheer																																					x							x											
	Correspondentie	Corona Beheer											x	x							x	x	x	x					x																												
	GKVI-registratiemedewerker	Corona Beheer																																										x													
	Vaccinatie inplannen	Corona Beheer											x	x							x	x	x																																		
	Vaccinatie registratie	Corona Beheer												x								x	x															x	x																		
	Vaccinatie afhandeling	Corona Beheer												x								x	x																x	x	x	x	x														
	Vaccinatie medisch	Corona Beheer																																			x																				
GGD GHOR Academy	Moodle-Coach	Servicedesk ICA																											x																												
	Moodle-Cursist	Servicedesk ICA		x										x								x	x	x	x	x	x	x		x		x	x																x			x					
iWink-Lezer	iWink-Lezer	Servicedesk ICA		x										x								x	x	x	x	x	x	x	x	x	x	x	x	x	x	x																					
GGD contact	DBCO-Gebruiker	Servicedesk ICA																						x	x	x	x	x	x	x	x	x	x																								
	DBCO-Werkverdeler	Servicedesk ICA																						x					x	x	x	x	x																								
	BCO-GGD-Compliance	Servicedesk ICA																											x						x																						
	BCO-GGD-Dossierkwaliteit	Servicedesk ICA																												x	x		x																								
	BCO-GGD-MedischeSupervisie	Servicedesk ICA																																																							
	BCO-GGD-Gesprekscoach	Servicedesk ICA																																																							
	BCO-GGD-Contextbeheerder	Servicedesk ICA																						x	x					x																											
	AMZX-VPN	Servicedesk ICA																						x	x	x	x	x	x	x	x	x	x		x																						
	Eerstelijn	Corona Beheer													x						x																																				
	Tweedelijn	Corona Beheer														x																																									
	Beheer algemene snelle teksten	Corona Beheer																	x	x	x																																				

6.1

Serviant Chat Corona	Beheer chatmedewerkers	Corona Beheer																																													x									
	Bekijk live dashboard	Corona Beheer													x	x			x	x	x																																			
	Bekijk statistieken en exports	Corona Beheer																			x																																			
	Blokkeer deelnemers	Corona Beheer													x	x			x	x	x																																			
	Chat inrichting	Corona Beheer																			x																																			
	Deblokkeer deelnemers	Corona Beheer													x	x			x	x	x																																			
	Lees gesprekken voor eigen groep(en)	Corona Beheer																	x	x	x																																			
Foleon	Foleon-GGDContact-lezer	Servicedesk ICA	x	x		x								x								x	x	x	x	x	x	x	x	x	x	x	x																x			x						
	Foleon-BCOMagazine-lezer	Servicedesk ICA																																																								
Osiris AIZ	RIVM-OSIRIS-AIZ	Servicedesk ICA		x																									x																				x	x	x	x	x	x		x	
Clusterbuster	RIVM-GGD-Clusterbuster	Servicedesk ICA																																															x			x					
	RIVM-GGD-Clusterbuster	Corona Beheer																																															x			x					
Meldportaal	Meldportaal	Corona Beheer																																	x																					
Quandago	Quandago	Corona Beheer										x	x	x		x	x	x		x	x	x	x		x	x				x																										
Kennisbank Dialoogplatform	LIQ_Kennisbank_Corona	Servicedesk ICA												x				x		x																																				
GGDTOOLS	GGDTOOLS-Gebruiker	Servicedesk ICA																																																								
OBI4wan		Corona Beheer														x				x																																				
Coronadashboard GGD GHOR	Coronadashboard GGD GHOR	Corona Beheer				x		x	x													x							x		x				x						x	x			x											
ODBC koppeling datafeed	ODBC koppeling datafeed	Corona Beheer																																																								
Zorgmail Hosted Mail	ggdhartvoorbrabant.corona@zorgmail.nl	Mandeley van de Watervliet																																	x																					
	ggdhartvoorbrabantinfectieziekten@zorgmail.nl	?																																														x	x		x	x			x	
Inconto	Inconto	Corona Beheer				x			x			x																													x		x												
GKVI	GKVI-Registrant	Servicedesk ICA																																								x													
Corona Melder portaal	C19NA-Telefonist	Servicedesk ICA												x								x	x			x	x	x	x	x		x	x																							

6.2

Ministerie van Volksgezondheid,
Welzijn en Sport

De Basis op Orde

Verbeterplan fase 1 met betrekking tot

Digitale Ondersteuning Test- en Traceerketens

Voorzitter Regiegroep DOTT

15 februari 2021

6.2

Context | Relevante context uit kamerbrief van 12 februari 2021

Context Kamerbrief 12 februari 2021

- ***Onderzoek HPZone***
  GGD GHOR Nederland heeft extern onderzoek laten doen naar de kwaliteit van de software en de kwaliteit van de dienstverlening van de softwareleverancier van HPZone. De resultaten van dit onderzoek nopen GGD GHOR Nederland tot versnelde vervanging van HPZone (Lite). De urgente behoefte aan vervanging midden in de huidige pandemie vraagt om landelijke aansturing. Voor de vervanging van HPZone zijn bij GGD GHOR Nederland meerdere alternatieven (en combinaties van alternatieven) in beeld, waaronder go.data dat onder verantwoordelijkheid van de WHO is ontwikkeld. Een ander alternatief voor een deel van de functionaliteiten van HPZone is GGD Contact. Deze en overige alternatieven worden zo zorgvuldig en spoedig mogelijk nader onderzocht door de GGD'en en GGD GHOR Nederland. Een nieuwe voorziening zal bewijsbaar moeten voldoen aan alle standaarden en vereisten inzake privacy en veiligheid.
- ***Strakker sturen – Verbeterplan DOTT***
  Op basis van de risicoanalyse is er in de Regiegroep Digitale Ondersteuning Test- en Traceerketen (DOTT) met alle betrokken ketenpartners een verbeterplan opgesteld met daarin maatregelen om de eerder gesignaleerde risico's en kwetsbaarheden in de ketenbrede digitale ondersteuning en infrastructuur binnen de gehele test- en traceerketen te mitigeren. Dit verbeterplan is op 11 februari jl. in concept vastgesteld door de LCT. Het 'verbeterplan DOTT fase 1 – Basis op orde' bestaat uit deelplannen die elk belegd zijn bij de ketenpartners. Elke ketenpartij is zelf uitvoerder van haar eigen acties en projecten. In de Regiegroep vindt coördinatie, ondersteuning en sturing plaats. Het verbeterplan DOTT fase 1 gaat in op de acties met een korte horizon van zes weken (tot de audit) en drie maanden. Het streven is om eind maart het plan voor fase 2 op te leveren, dat zal bestaan uit acties met een horizon van zes maanden of langer. Deze acties zullen meer innovatief en duurzaam van aard zijn. Daarvoor is het nodig dat eerst de basis op orde is.
- ***Gateway***
  De LCT heeft de voorzitter van de Regiegroep DOTT verzocht een Gateway Review uit te laten voeren op het verbeterplan DOTT fase 1. Zo is besloten. De intake voor deze review vindt op korte termijn plaats.
- ***Aanvullend***
  Naast dit verbeterplan zijn er andere initiatieven die verbetering van de algehele situatie met betrekking tot informatiebeveiliging en privacybescherming voorstaan. Zo is het Red Team met ethische hackers inmiddels gestart. Ook adviezen vanuit het Nationaal Cyber Security Centrum, de CIO-Rijk en Z-CERT worden betrokken bij de door te voeren verbeteringen.

Aanleiding en doel | door actuele situatie rondom dataveiligheid doel om snel in control te komen in test- en traceerketen

Verhoogde aandacht voor dataveiligheid in de keten van COVID-19 bestrijding door aantal incidenten en analyses

- **Datadiefstal in januari 2021:** heeft urgentie en noodzaak verhoogd
- **Risicoanalyse als reactie op aantal incidenten:** verbeteracties als basis voor verbeterplan
- **IT audit van GGD GHOR Nederland door KPMG:** als aanvulling op de risicoanalyse
- **Kamerbrief van 2 feb en Tweede Kamer debat van 3 feb:** heeft de politieke verwachting scherp gesteld

Hoogste prioriteit gegeven aan verbeterplan om risico's aan te pakken en in control te komen in test / traceerketen

- **Kern van verbetering in de digitale ondersteuning van test en traceerketen:** algemeen en bij de GGD
- **Datalekken voorkomen dan wel zo snel mogelijk oplossen**
- **Informatie-uitwisseling betrouwbaar en snel laten verlopen**
- **Aansluitend op de uiteindelijke ketenoplossing**

Fase 1 | Basis op orde | drie verschillende werkpakketten om bevindingen uit o.a. risicoanalyse en IT-rapport in te richten

A. Herijken en –inrichten ICT landschap

Binnen dit werkpakket gaat het om de techniek. Hieronder vallen o.a.

- A2: Ten behoeve van de pandemiebestrijding z.s.m. overstappen van HPZone (Lite) op alternatieve voorziening
- A8: Ketenbreed incidentmanagement ontwerpen en versneld inrichten.
- A10: Keten start architectuur (KSA) gezamenlijk met ketenpartners opzetten en uitwerken

B. Informatiebeveiliging en privacy

Binnen dit werkpakket gaat het voornamelijk om het gebruik, de gebruikers en de beveiliging van de systemen. Hieronder vallen o.a.

- B2: Print- en exportfunctie van HPZone (Lite) uitschakelen
- B5: Geautomatiseerde controles op gebruik CoronIT en HPZone (Lite) inrichten, teneinde verdacht gedrag vroegtijdig te signaleren.
- B9: Afronden DigiD audit

C. Informatie-uitwisseling in de keten

Binnen dit werkpakket gaat het voornamelijk om de uitwisseling van informatie tussen verschillende systemen. Hieronder vallen o.a.

- C1: Beschrijf op welke wijze gegevens uit HPZone (Lite) in de huidige situatie digitaal worden uitgewisseld met Osiris, OMV en cluster output van het RIVM
- C2: Beschrijf op welke wijze gegevens uit HPZone (Lite) in de toekomstige situatie digitaal worden uitgewisseld met Osiris, OMV en cluster output van het RIVM
- C3: Realisatie nieuw (SOLL) koppelvlak voor de uitwisseling van gegevens tussen GGD (BCO-Portaal, HPZone, GGD-Contact) met Osiris, OMV en cluster output van het RIVM

Herijken en inrichten ICT landschap | verschillende activiteiten die gezamenlijk dit werkpakket vormen

A. Herijken en –inrichten ICT landschap

Doel werkpakket

Het creëren van een goede basis voor ketenbesturing van de Corona test- en traceerketens, waardoor de ketens 'in control' komen.

Randvoorwaarden werkpakket

- Alle ketenpartners committeren zich aan het resultaat.
- Binnen de keten wordt onderlinge transparantie de norm.

Fiches werkpakket | die als activiteiten bij verschillende partijen zijn belegd

A1 GGD GHOR Nederland neemt het beheer en het eigenaarschap over HPZone	**A2** Ten behoeve van de pandemiebestrijding z.s.m. overstappen van HPZone-Lite op alternatieve voorziening	**A3** Inrichten IT governance en ketenoverleg	**A4** Opschalen IT organisatie met primair interne collega's
A5 Leveranciers-management professionaliseren	**A6** Ketensamenwerking in pandemiebestrijding: Visieontwikkeling, inrichting en realisatie van de (keten-)samenwerking, samenwerkingsverbanden en keteninformatisering.	**A7** Opzet wekelijkse rapport ten behoeve van de minister van VWS	**A8** Ketenbreed incidentmanagent ontwerpen en versneld inrichten
A9 Regierol inregelen op naleving van wet- en regelgeving, standaarden en andere ketenafspraken	**A10** Keten Start Architectuur (KSA) gezamenlijk met ketenpartners opzetten en uitwerken	**A11** Onderzoeken in hoeverre beschikbare alternatieve BCO ICT-oplossingen aansluiten bij de eisen en wensen van het BCO-proces.	**A12** Changemanagement CoronIT rondom nieuwe testmethodes en testdoeleinden inrichten

Zie de bijlage voor een verdieping per fiche

X Verantwoordelijkheid DOTT X Verantwoordelijkheid GGD GHOR NL X Verantwoordelijkheid VWS X Verantwoordelijkheid RIVM

Informatiebeveiliging en privacy| verschillende activiteiten die gezamenlijk dit werkpakket vormen

B. Informatiebeveiliging en privacy

Doel werkpakket

- In de Corona test- en traceerketens wordt zorgvuldig omgegaan met wettelijke eisen rondom informatiebeveiliging en privacy.
- Burgers mogen ervan uit kunnen gaan dat hun gegevens veilig zijn.

Randvoorwaarden werkpakket

- Privacy by design is de norm.
- Ketenpartners voldoen aan relevante wet- en regelgeving en beveiligingsnormen zoals AVG, BIO en NEN-7510.

Fiches werkpakket | die als activiteiten bij verschillende partijen zijn belegd

B1 Gebruik en toegang van HPZone (Lite) beperken tot selecte groep specialisten (IZB-artsen en –verpleegkundigen)	**B2** Print- en exportfunctie van HPZone (Lite) uitschakelen	**B3** Printfunctie van CoronIT uitschakelen. Toegang en zoekmogelijkheden CoronIT beperken	**B4** Zoekmogelijkheden HPZone (Lite) beperken
B5 Geautomatiseerde controles op gebruik CoronIT en HPZone (Lite) inrichten, teneinde verdacht gedrag vroegtijdig te signaleren.	**B6** HPZone (Lite) wordt door externe IT-deskundigen verder doorgelicht. Preventieve maatregelen om datalekken te voorkomen	**B7** CoronIT wordt door externe IT-deskundigen verder doorgelicht. Preventieve maatregelen om datalekken te voorkomen	**B8** VOG administratie gebruikers CoronIT en HPZone (Lite) op orde brengen
B9 Afronden Digi-D audit	**B10** In kaart brengen welke initiatieven er zijn binnen de keten op gebied van AVG, BIO en NEN7510 en welke maatregelen nodig zijn	**B11** **B12** Informatiebeveiliging GGD Contact app conform Rijks- en NEN-normen, deel 1 en 2	**B13** Data Governance in de testketen inrichten

Zie de bijlage voor een verdieping per fiche

X Verantwoordelijkheid DOTT X Verantwoordelijkheid GGD GHOR NL X Verantwoordelijkheid VWS X Verantwoordelijkheid RIVM

Informatie-uitwisseling in de keten | verschillende activiteiten die gezamenlijk dit werkpakket vormen

C. Informatie-uitwisseling in de keten

Doel werkpakket

- Er ligt een helder en actueel model voor informatie-uitwisseling in de keten.
- Definities van onder meer gegevens- en berichtenverkeer zijn op orde.

Randvoorwaarden werkpakket

- Bij iedere ketenpartner is een aanspreekpunt voor dit onderwerp.
- Beheer van de informatie-uitwisselingsafspraken wordt onderdeel van de ketenbesturing.

Fiches werkpakket | die als activiteiten bij verschillende partijen zijn belegd

C1
Beschrijving op welke wijze gegevens uit HPZone en HPZone-Lite in de huidige situatie digitaal worden uitgewisseld met Osiris, OMV en cluster output van het RIVM

C2
Beschrijving op welke wijze gegevens van GGD (BCO-Portaal, HPZone, GGD-Contact) in de toekomstige situatie worden uitgewisseld met Osiris, OMV en cluster output van RIVM

C3
Realisatie nieuw (SOLL) koppelvlak voor de uitwisseling van gegevens tussen GGD (BCO-Portaal, HPZone, GGD-Contact) met Osiris, OMV en cluster output van het RIVM

Zie de bijlage voor een verdieping per fiche

X Verantwoordelijkheid DOTT X Verantwoordelijkheid GGD GHOR NL X Verantwoordelijkheid VWS X Verantwoordelijkheid RIVM

Ministerie van Volksgezondheid,
Welzijn en Sport

Bijlage

De Basis op Orde

Verbeterplan fase 1 met betrekking tot

Digitale Ondersteuning Test- en Traceerketen

Fase 1 - Basis op orde - DOTT | Fiche A1

A1	**GGD GHOR Nederland neemt het beheer en het eigenaarschap over HPZone.**
Werkpakket	*Herijken en -inrichten ICT landschap*
Actiehouder	**GGD GHOR Nederland**
Tijdslijn	Q1
Beoogd resultaat	Beter zicht op de informatiebehoefte, mogelijkheid om het wijzigingsproces beter te faciliteren en daarmee beter inzicht in het gebruik van HPZone

Actuele status	**15-02-2021** GGD'en hebben besloten om HPZone (Lite) uit te faseren. HPZone (Lite) blijft wel actief totdat vervanging definitief is. Beheer en eigenaarschap wordt bij het toekomstige alternatief voor de landelijke voorziening van digitale ondersteuning IZB bij GGD GHOR NL belegd.
Bijzonderheden	

Fase 1 - Basis op orde - DOTT | Fiche A2

A2	**Ten behoeve van de pandemiebestrijding z.s.m. overstappen van HPZone-Lite op alternatieve voorziening.**
Werkpakket	*Herijken en -inrichten ICT landschap*
Actiehouder	**GGD GHOR Nederland**
Tijdslijn	Q1
Beoogd resultaat	Ten behoeve van de pandemie BCO uitvoeren met een applicatie die voldoet aan de hedendaagse eisen o.a. op het gebied van veiligheid.

Randvoorwaarden	Privacy by design; Brief van Dissel: RIVM bezorgd om ketencontinuïteit
Bijzonderheden	De ontwikkeling van GGD Contact heeft hoge prioriteit en dit wordt erkend door VWS en GGD GHOR NL. Fit-Gap analyse op functionele en technische requirements gaat uitgevoerd worden door KPMG. Daarnaast heeft het RDO project GGD Contact uitgebreid werkprocessen geanalyseerd. KPMG voert second opinion uit op alternatieve voorzieningen voor het BCO-proces waaronder GGD Contact. Deze is 2e helft maart beschikbaar. Uitkomst QuickScan: GGD Contact is enige reële alternatief HPZone Lite.

6.2

Fase 1 - Basis op orde - DOTT | Fiche A3

A3	**Inrichten IT governance en ketenoverleg.**
Werkpakket	*Herijken en -inrichten ICT landschap*
Actiehouder	**GGD GHOR Nederland**
Tijdslijn	Q1
Beoogd resultaat	In control zijn wat betreft de informatievoorziening en -behoefte met de mogelijkheid om te faciliteren waar nodig.

Actuele status	**09-02-2021** Management reactie GGD GHOR NL: • Voorstel IT governance wordt uitgewerkt op basis van algehele governance Infectie Ziekte Bestrijding (IZB). • Inrichting contactnetwerk voor Monitoring, Digitalisering en ICT in oprichting.
Bijzonderheden	VWS zal samen optrekken met GGD GHOR Nederland bij het beantwoorden van de komende Kamervragen en de Kamerbrief.

Fase 1 - Basis op orde - DOTT | Fiche A4

A4	**Opschalen IT organisatie met primair interne collega's.**
Werkpakket	*Herijken en -inrichten ICT landschap*
Actiehouder	**GGD GHOR Nederland**
Tijdslijn	Q1
Beoogd resultaat	Het geconstateerde tekort aan capaciteit wordt weggewerkt. De focus tijdens de werving van vaste medewerkers komt het behoud en verspreiden van kennis ten goede.

Actuele status	**09-02-2021** Management reactie GGD GHOR NL: Dit heeft continue aandacht. Voorstel door manager IM a.i. opgesteld, gereed voor besluitvorming.
Bijzonderheden	

Fase 1 - Basis op orde - DOTT | Fiche A5

A5	**Leveranciersmanagement professionaliseren.**
Werkpakket	*Herijken en -inrichten ICT landschap*
Actiehouder	**GGD GHOR Nederland**
Tijdslijn	Q1
Beoogd resultaat	Afspraken met leveranciers over SLA's, beleid bij storingen en onder andere downtime om beter preventief te kunnen opereren. Dit verbetert tevens de samenwerking met ketenpartners.

Actuele status	**09-02-2021** VWS steunt de GGD GHOR in alle acties die zij noodzakelijk acht ten aanzien van HPZone (Lite) en de betrokken leverancier om op korte termijn de bedrijfsvoering veilig en overeind te houden (ook als dat betekent dat de leverancier wordt aangesproken).
Bijzonderheden	Brede keteninrichting wordt gefaciliteerd vanuit DOTT.

Fase 1 - Basis op orde - DOTT | Fiche A6

A6	**Ketensamenwerking in pandemiebestrijding: Visieontwikkeling, inrichting en realisatie van de (keten-)samenwerking, samenwerkingsverbanden en keteninformatisering.**
Werkpakket	*Herijken en -inrichten ICT landschap*
Actiehouder	**DOTT**
Tijdslijn	Q2 (start Q1)
Beoogd resultaat	Komen tot basisopzet (en keuzescenario's) voor: - Een ketenvisie die een referentiekader biedt voor het analyseren van ketenvraagstukken (zoals Ketenbehoeftestellingsproces en ketenwijzigingenproces). - Een governance structuur voor de ketensamenwerking (op strategisch, tactisch en operationeel niveau). - Een toetsingskader dat erop gericht is in ketens om onder meer risicovolle keteninformatiesystemen en ketenprojecten te identificeren. - Een sturingskader dat helpt de samenwerkingsdoelen te bereiken, door suggesties te geven voor effectieve keteninterventies.
Randvoorwaarden	
Bijzonderheden	Binnen de overheid zijn tal van voorbeelden van goed functionerende ketens; deze kenmerken zich allen door een duidelijke ketenorganisatie waarin het ketenbelang boven het kolombelang staat. NORA-katern "Ketens de Baas" geldt als leidraad.

Fase 1 - Basis op orde - DOTT | Fiche A7

A7	**Opzet wekelijkse rapport ten behoeve van de minister van VWS.**
Werkpakket	*Herijken en -inrichten ICT landschap*
Actiehouder	**DOTT**
Tijdslijn	Week 7 opzet voortgangsrapportage, vanaf week 8 wekelijkse rapportage
Beoogd resultaat	Strakke rapportagelijn vanuit de keten (VWS, GGD-GHOR, GGD'en en RIVM) richting regiegroep Digitale Ondersteuning van de Test- en Traceerketen (DOTT) en de stuurgroep Landelijke Coördinatiestructuur Testcapaciteit (LCT) om richting de minister te rapporteren.

Randvoorwaarden	Transparantie en validatie van gerapporteerde (tussen)resultaten
Bijzonderheden	De regiegroep wordt onder meer geadviseerd door het Nationaal Cyber Security Centre (NCSC), de chief information officer (CIO) van de Rijksoverheid, de informatiebeveiligingsorganisatie voor de zorg Z-CERT en andere experts.

6.2

Fase 1 - Basis op orde - DOTT | Fiche A8

A8	**Ketenbreed incidentmanagent ontwerpen en versneld inrichten.**
Werkpakket	*Herijken en -inrichten ICT landschap*
Actiehouder	**DOTT**
Tijdslijn	Q1-Q2 (Q1 opzet, Q2 ketenimplementatie)

Beoogd resultaat	Afgestemd Incident Management Proces:
	- Centrale coördinatie / 1 aanspreekpunt voor de keten en per ketenpartner een incident coördinator.
	- Incidentproces keten breed geeffectueerd (melding, analyse, oplossen).
	- Oplostijden en servicewindow afgestemd.
	- Processen in beeld met proceseigenaren.
	- Communicatie en escalatieprocessen zijn ingericht.
	- Voor ieder ketenonderdeel in beeld gebracht betrokken:
	  - Leveranciers
	  - Dienstverleners
	  - Medewerkers
	- Heldere, vastgelegde afspraken tussen keten-onderdelen over de te leveren diensten.
	- Maandelijkse rapportage over opvolging.

Actuele status	**09-02-2021** Management reactie GGD GHOR NL: SLA afspraken met Yenlo en Topicus worden herzien en aangescherpt op basis van response- en oplostijden. Inrichting van SIEM voor continue monitoring Projectleider servicemanagement richt incident- en changemanagement in.
Bijzonderheden	Afspraken maken m.b.t. verstoringen, uitval systemen en data-inconsistentie in de ketenprocessen als tijdelijke workaround.

Fase 1 - Basis op orde - DOTT | Fiche A9

A9	**Regierol inregelen op naleving van wet- en regelgeving, standaarden en andere ketenafspraken.**
Werkpakket	*Herijken en -inrichten ICT landschap*
Actiehouder	**DOTT**
Tijdslijn	Q1
Beoogd resultaat	Basisvoorwaarde voor inrichting van ketensamenwerking is inzicht in hoeverre vigerende wet- en regelgeving, standaarden (pas-toe-of-leg-uit) en andere ketenafspraken worden nageleefd door alle ketenpartijen.

Randvoorwaarden	Wens en bereidheid tot ketenbrede samenwerking en regie te komen
Bijzonderheden	Prioriteit Hoog: start met het maken van duidelijke afspraken over levering en gebruik van gegevens tussen (gegevens)-leverancier en afnemer en leg deze afspraken vast in een Gegevens Levering Overeenkomst (GLO). Inventariseer de overige ketenafspraken en formaliseer die waar nodig.

Fase 1 - Basis op orde - DOTT | Fiche A10

A10	**Keten Start Architectuur (KSA) gezamenlijk met ketenpartners opzetten en uitwerken.**
Werkpakket	*Herijken en -inrichten ICT landschap*
Actiehouder	**DOTT**
Tijdslijn	Eind Q1 (IST beschrijving, SOLL beschrijving volgt in Q2)
Beoogd resultaat	Door het ICT landschap te beschrijven (in de IST) komen tot herijken en herinrichten (naar de SOLL) met oog op ketenbrede inrichting van het ICT landschap ten behoeve van pandemiebestrijding (en/of reguliere processen).

Randvoorwaarden	Medewerking architecten ketenpartijen
Bijzonderheden	Een KSA biedt voor de ketenpartijen de kaders en hulpmiddelen vanuit de architectuur voor te realiseren functionele en technische projectresultaten.

Fase 1 - Basis op orde - DOTT | Fiche A11

A11	**Onderzoeken in hoeverre beschikbare alternatieve BCO ICT-oplossingen aansluiten bij de eisen en wensen van het BCO-proces.**
Werkpakket	*Herijken en -inrichten ICT landschap*
Actiehouder	**DOTT**
Tijdslijn	Q1
Beoogd resultaat	Fit-gap analyse rapport (quickscan) met als doel verkenning om een concreet beeld te krijgen van mogelijke ICT oplossingen voor het BCO proces. De op te leveren producten zijn o.a.: informatiebehoeften (functionele- en niet-functionele eisen) en inzicht in bestaande BCO ICT oplossingen.

Randvoorwaarden	In ieder geval betrekken van go.data (van WHO) en CoronaCare. Mogelijk andere oplossingen in quick scan meenemen.
Bijzonderheden	BCO = Bron- en contactonderzoek.

Fase 1 - Basis op orde - DOTT | Fiche A12

A12	**Changemanagement CoronIT rondom nieuwe testmethodes en testdoeleinden inrichten.**
Werkpakket	*Herijken en -inrichten ICT landschap*
Actiehouder	**VWS – DT (Dienst Testen)**
Tijdslijn	Q1-Q2
Beoogd resultaat	Komen tot gezamenlijke afspraken en afstemming over: Hoe beleidswijzigingen (zoals grootschalig testen) en nieuwe testmethodes (zoals ademtest) geregistreerd worden in CoronIT en ontsloten wordt in de keten.

Actuele status	**09-02-2021** Geen afspraken en/of overlegstructuur
Bijzonderheden	

Fase 1 - Basis op orde - DOTT | Fiche B1

B1	**Gebruik en toegang van HPZone (Lite) beperken tot selecte groep specialisten (IZB-artsen en –verpleegkundigen).**
Werkpakket	*Informatiebeveiliging en privacy*
Actiehouder	**GGD GHOR Nederland**
Tijdslijn	Q1
Beoogd resultaat	HPZone qua gebruik terug naar waar het oorspronkelijk voor bedoeld was. Kans op misbruik daardoor tot minimum beperkt.

Actuele status	**09-02-2021:** Procesvoorstel toegang HPZone (Lite) is in samenwerking met juristen opgesteld. Bevoegdheid over het ontstaan van nieuwe rollen ligt bij de voorzitter van de HPZone gebruikersgroep (in afstemming met Privacy Officer GGD GHOR NL). Het toekennen van rollen ligt bij individuele GGD'en. **15-02-2021:** Deze actie is inmiddels achterhaald door het besluit om HPZone (Lite) uit te faseren. In het alternatief voor HPZone (Lite) wordt deze actie opgepakt en als randvoorwaardelijk meegenomen.
Bijzonderheden	

Fase 1 - Basis op orde - DOTT | Fiche B2

B2	**Print- en exportfunctie van HPZone (Lite) uitschakelen.**
Werkpakket	*Informatiebeveiliging en privacy*
Actiehouder	**GGD GHOR Nederland**
Tijdslijn	Q1
Beoogd resultaat	Mogelijkheid voor datalek via print- en exportfuncties onmogelijk maken

Randvoorwaarden	AVG, i.s.m. HPZone gebruikersgroep
Bijzonderheden	• Printfunctie is reeds uitgeschakeld. • De exportfunctie is gewijzigd. BSN en NAW gegevens zijn eruit gehaald en de rol is alleen nog toegekend aan een beperkt aantal functionarissen. • Ook zijn de custom queries aangepast. Hier zijn ook BSN en NWW gegevens uitgehaald. • Rollen/rechten matrix wordt verder uitgewerkt.

Fase 1 - Basis op orde - DOTT | Fiche B3

B3	**Printfunctie van CoronIT uitschakelen. Toegang en zoekmogelijkheden CoronIT beperken.**
Werkpakket	*Informatiebeveiliging en privacy*
Actiehouder	**GGD GHOR Nederland**
Tijdslijn	Q1
Beoogd resultaat	Mogelijkheid voor datalek via printfuncties onmogelijk maken.

Actuele status	**09-02-2021** • De printfunctie is uitgeschakeld. • De zoekfunctie is aangepast en privacy vriendelijker gemaakt. Er is nu meer data nodig om personen te vinden.
Bijzonderheden	NOOT: Een exportfunctie heeft nooit bestaan in CoronIT

Fase 1 - Basis op orde - DOTT | Fiche B4

B4	Zoekmogelijkheden HPZone (Lite) beperken
Werkpakket	*Informatiebeveiliging en privacy*
Actiehouder	**GGD GHOR Nederland**
Tijdslijn	Q1
Beoogd resultaat	Alleen bevoegde personen mogen informatie zoeken waarvoor zij gerechtigd zijn.

Actuele status	**09-02-2021:** Mogelijkheden zoekfunctie worden momenteel in kaart gebracht op functioneel gebruik. Zoekmogelijkheden worden in week 6 beperkt. **15-02-2021:** Deze actie is inmiddels achterhaald door het besluit om HPZone (Lite) uit te faseren. In het alternatief voor HPZone (Lite) wordt deze actie opgepakt en als randvoorwaardelijk meegenomen.
Bijzonderheden	In Kamerbrief 2-2-21 aangegeven dat dit in week 5 gedaan wordt. Reactie GGD GHOR NL: is afgedaan.

Fase 1 - Basis op orde - DOTT | Fiche B5

B5	**Geautomatiseerde controles op gebruik CoronIT en HPZone (Lite) inrichten, teneinde verdacht gedrag vroegtijdig te signaleren.**
Werkpakket	*Informatiebeveiliging en privacy*
Actiehouder	**GGD GHOR Nederland**
Tijdslijn	Q1
Beoogd resultaat	Verdacht gedrag opsporen en aanpakken.

Actuele status	**09-02-2021** De technische oplossing (SIEM) is ingericht. Er wordt gewerkt aan het koppelen van de systemen. Eind maart is de omgeving klaar.
Bijzonderheden	Gespecialiseerde teams sporen dagelijks verdachte patronen en verdacht gedrag op. Dit blijven zij doen tot het moment dat het systeem geautomatiseerd is. In Kamerbrief 2-2-21 aangegeven dat dit nu loopt. Status actualiseren.

Fase 1 - Basis op orde - DOTT | Fiche B6

B6	**HPZone (Lite) wordt door externe IT-deskundigen verder doorgelicht. Preventieve maatregelen om datalekken te voorkomen.**
Werkpakket	*Informatiebeveiliging en privacy*
Actiehouder	**GGD GHOR Nederland**
Tijdslijn	Q1
Beoogd resultaat	Aanvullende kwetsbaarheden opsporen en aanpakken.

Actuele status	**09-02-2021** Voor HPZone zijn er twee onderzoeken uitgevoerd naar: - Software/software leverancier, - Database HP-Zone.
Bijzonderheden	

Fase 1 - Basis op orde - DOTT | Fiche B7

B7	**CoronIT wordt door externe IT-deskundigen verder doorgelicht. Preventieve maatregelen om datalekken te voorkomen.**
Werkpakket	*Informatiebeveiliging en privacy*
Actiehouder	**GGD GHOR Nederland**
Tijdslijn	Q1
Beoogd resultaat	Aanvullende kwetsbaarheden opsporen en aanpakken.

Actuele status	**09-02-2021** Herhalen van pentest. Tegelijk met reeds geplande pentest vaccinatie over paar weken.
Bijzonderheden	

Fase 1 - Basis op orde - DOTT | Fiche B8

B8	**VOG administratie gebruikers CoronIT en HPZone (Lite) op orde brengen.**
Werkpakket	*Informatiebeveiliging en privacy*
Actiehouder	**GGD GHOR Nederland**
Tijdslijn	Q1
Beoogd resultaat	Medewerkers zonder VOG krijgen geen toegang tot systemen met persoonsgegevens.

Actuele status	**09-02-2021** - Landelijke schil: alle medewerkers BCO landelijke schil hebben een VOG, of er is er een aangevraagd (ook voor nieuwe instroom). Mocht er geen VOG zijn, dan worden mensen niet ingezet op BCO. - Regionale GGD'en: alle medewerkers hebben een VOG. Vanuit Corona Programma Organisatie geadviseerd dat, mocht dit niet het geval zijn, deze mensen niet ingezet worden totdat VOG binnen is. Controle en verantwoordelijkheid hiervoor ligt bij de regionale GGD'en zelf. - Voor testen en vaccineren bij Teleperformance zullen mensen wel worden ingezet. Er wordt onderzocht of duur van hebben van een VOG van 6 naar 3 of 4 weken kan worden verkort.
Bijzonderheden	

Fase 1 - Basis op orde - DOTT | Fiche B9

B9	**Afronden Digi-D audit.**
Werkpakket	*Informatiebeveiliging en privacy*
Actiehouder	**GGD GHOR Nederland**
Tijdslijn	Q1
Beoogd resultaat	Voldoen aan de DigiD normen voor coronatest.nl

Actuele status	**09-02-2021** Op dit moment voldoen we aan zes normen nog niet, waarvan vier nog binnen de verbetertermijn. Vijf worden komende weken (tot 4/5 maart) opgepakt en opgeleverd (of eerdere gecommuniceerde realistische opleverdatums). één moet voor 5 mei worden opgeleverd.
Bijzonderheden	Er is hoog ambtelijk contact tussen BZK en VWS/GGD GHOR Nederland.

Fase 1 - Basis op orde - DOTT | Fiche B10

B10	**In kaart brengen welke initiatieven er zijn binnen de keten op gebied van AVG, BIO en NEN7510 en welke maatregelen nodig zijn.**
Werkpakket	*Informatiebeveiliging en privacy*
Actiehouder	**DOTT**
Tijdslijn	Q1
Beoogd resultaat	Overzicht per GGD, GGD GHOR, RIVM van: Voldoen aan AVG, BIO en/of NEN7510; Hoe geconstateerd; Status evt. verbeterplan als nog niet voldoen. Gecertificeerd NEN 7510 ja/nee. Door wie (NEN registratie etc.), wanneer, SCOPE. Planning voor blijvend voldoen aan normering. Als niet gecertificeerd voor scope IZB planning voor wanneer dan wel?
Randvoorwaarden	Iedereen behoort AVG na te leven. Zorgorganisaties moeten voldoen aan NEN7510, overheden moeten voldoen aan BIO.
Actuele status	**09-02-2021** GGD GHOR wil 2021 gecertificeerd zijn voor NEN 7510, scope is onbekend. Van alle overige partijen is vooralsnog onbekend of en waaraan zij voldoen.
Bijzonderheden	Moeten GGD niet aan gemeenten / Informatie Beveiligingsdienst (IBD) rapporteren over NEN7510 compliance? > IBD.

Fase 1 - Basis op orde - DOTT | Fiche B11

B11	**Informatiebeveiliging GGD Contact app conform Rijks- en NEN-normen, deel 1**
Werkpakket	*Informatiebeveiliging en privacy*
Actiehouder	**VWS**
Tijdslijn	Q1
Beoogd resultaat	In control zijn van Informatiebeveiliging van GGD Contact: - Data protection impact assessment (DPIA) uitgevoerd - Rol Functionaris gegevensbescherming (FG) regionale GGD'en Landelijke Referentie DPIA (LRDPIA) duidelijk - Aantoonbaar privacy by design
Randvoorwaarden	Bron- en contactonderzoek (BCO) proces is buiten scope van LRDPIA. Deze is noodzakelijk om privacy waarborgen in de keten inzichtelijk te krijgen.
Actuele status	**09-02-2021** Versie 1.0 van de Landelijke Referentie DPIA (LRDPIA) is opgesteld door GGD-GHOR (penvoerder), VWS en de FG's van de betrokken praktijktestregio's. Inhoud is afgestemd met landsadvocaat. Iedere beoogde functionele uitbreiding, inclusief eventuele vervanging HPzone, wordt daarna in een addendum verwerkt en afgestemd met de FG's van de praktijktestregio's. Lokale afwijkingen kunnen in de GGD-eigen DPIA worden opgenomen. Privacy/security informatiesessies over GGD contact hebben plaatsgevonden (+100 deelnemers). Wekelijkse updates voor FG's. Aandachtspunt: rechten van betrokkene over de keten (Onderzoek GGD-GHOR loopt) en dataminimalisatie/pseudonimisatie bij exports (samenwerking met RIVM loopt).

Fase 1 - Basis op orde - DOTT | Fiche B12

B12	**Informatiebeveiliging GGD Contact app conform Rijks- en NEN-normen, deel 2**
Werkpakket	*Informatiebeveiliging en privacy*
Actiehouder	**VWS**
Tijdslijn	Q1
Beoogd resultaat	In control zijn van Informatiebeveiliging van GGD Contact: - Inrichting applicatie volgens de normen die gelden voor systeem met medische informatie (NEN 7510, 7512, 7513). - Aangesloten op ketenbreed incidentmanagementproces en changeproces - Ge-audit door onafhankelijke derde
Actuele status	**09-02-2021** **Loopt:** Analyse op NEN 7510, 7512, 7513 in concept. Inrichting logging conform NEN 7513 loopt. Voor informatie-uitwisselingen worden NEN 7512 maatregelen gehanteerd. GGD-GHOR organiseert pentest op omgeving. Basis is dataminimalisatie: Elke rol heeft alleen noodzakelijke autorisaties/inzages voor een minimale looptijd (least privilige). **Gereed:** Hostingpartij is NEN 7510-gecertificeerd. Externe SOC monitort op kwetsbaarheden. Interne QA toets continu kwaliteit broncode. Externe source code review wordt uitgevoerd zodra code stabiel is. **Aandachtspunt** is autorisatieproces in de keten: Onbevoegde toegang kan door onterecht toekennen rol in systemen van GGD of landelijke partner. Afstemming loopt.
Bijzonderheden	

Fase 1 - Basis op orde - DOTT | Fiche B13

B13	**Data Governance in de testketen inrichten.**
Werkpakket	*Informatiebeveiliging en privacy*
Actiehouder	**VWS**
Tijdslijn	Q1-Q2
Beoogd resultaat	Data governance ingericht in de testketen met afspraken over: • (Data) definities, • (Data)uitwisseling en beheer, • Risicomanagement: beleid op rollen en toegang tot data, • Kwaliteitscontroles en monitoring.
Actuele status	**09-02-2021** Data Governance Plan DT is in de maak.
Bijzonderheden	Binnen de overheid is er een algemene aanpak op data governance, deze kan wellicht keten breed aangepakt worden.

6.2

Fase 1 - Basis op orde - DOTT | Fiche C1

C1	**Beschrijf op welke wijze gegevens uit HPZone en HPZone-Lite in de huidige situatie digitaal worden uitgewisseld met Osiris, OMV en cluster output van het RIVM.**
Werkpakket	*Informatie-uitwisseling in de keten*
Actiehouder	**RIVM**
Tijdslijn	Q1
Beoogd resultaat	Gedetailleerde beschrijving van het huidige (IST) koppelvlak in termen van POTI: Processen, organisatie, techniek en informatie (data).

Randvoorwaarden	
Bijzonderheden	DOTT kan helpen met ketenproces analyse.

Fase 1 - Basis op orde - DOTT | Fiche C2

C2	**Beschrijf op welke wijze gegevens van GGD (BCO-Portaal, HPZone, GGD-Contact) in de toekomstige situatie worden uitgewisseld met Osiris, OMV en cluster output van RIVM.**
Werkpakket	*Informatie-uitwisseling in de keten*
Actiehouder	**RIVM**
Tijdslijn	Q1-Q2
Beoogd resultaat	Gedetailleerde beschrijving van het nieuwe/gewenste (SOLL) koppelvlak in termen van POTI: Processen, Organisatie, Techniek en Informatie (data). De afspraken worden in de vorm van een Gegevens Levering Overeenkomst (GLO) vastgelegd conform de NORA Rijks standaard. (https://www.noraonline.nl/wiki/Gegevensleveringsovereenkomst).

Randvoorwaarden	Privacy by design; Information security by design; DPIA inclusief grondslagen voor verwerking(en); Datagovernance inclusief rechten en rollen.
Bijzonderheden	Nog te starten

Fase 1 - Basis op orde - DOTT | Fiche C3

C3	**Realiseer het nieuwe (SOLL) koppelvlak voor de uitwisseling van gegevens tussen GGD (BCO-Portaal, HPZone, GGD-Contact) met Osiris, OMV en cluster output van het RIVM.**
Werkpakket	*Informatie-uitwisseling in de keten*
Actiehouder	**RIVM**
Tijdslijn	nntb
Beoogd resultaat	Werkend koppelvlak. Het koppelvlak is getest, geaccepteerd door de gebruikers en beheerders, in beheer genomen door beheerders van RIVM en GGD (inclusief SIEM/SOC en wijzigingsproces).

Randvoorwaarden	Gedetailleerde beschrijving van het nieuwe/gewenste (SOLL) koppelvlak in termen van POTI: Processen, Organisatie, Techniek en Informatie (data).
Bijzonderheden	Te starten zodra aan randvoorwaarden is voldaan.

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

Geen documenten aanwezig.

Wob-verzoek SOLV/ICAM datalek 2021 coronasysteem

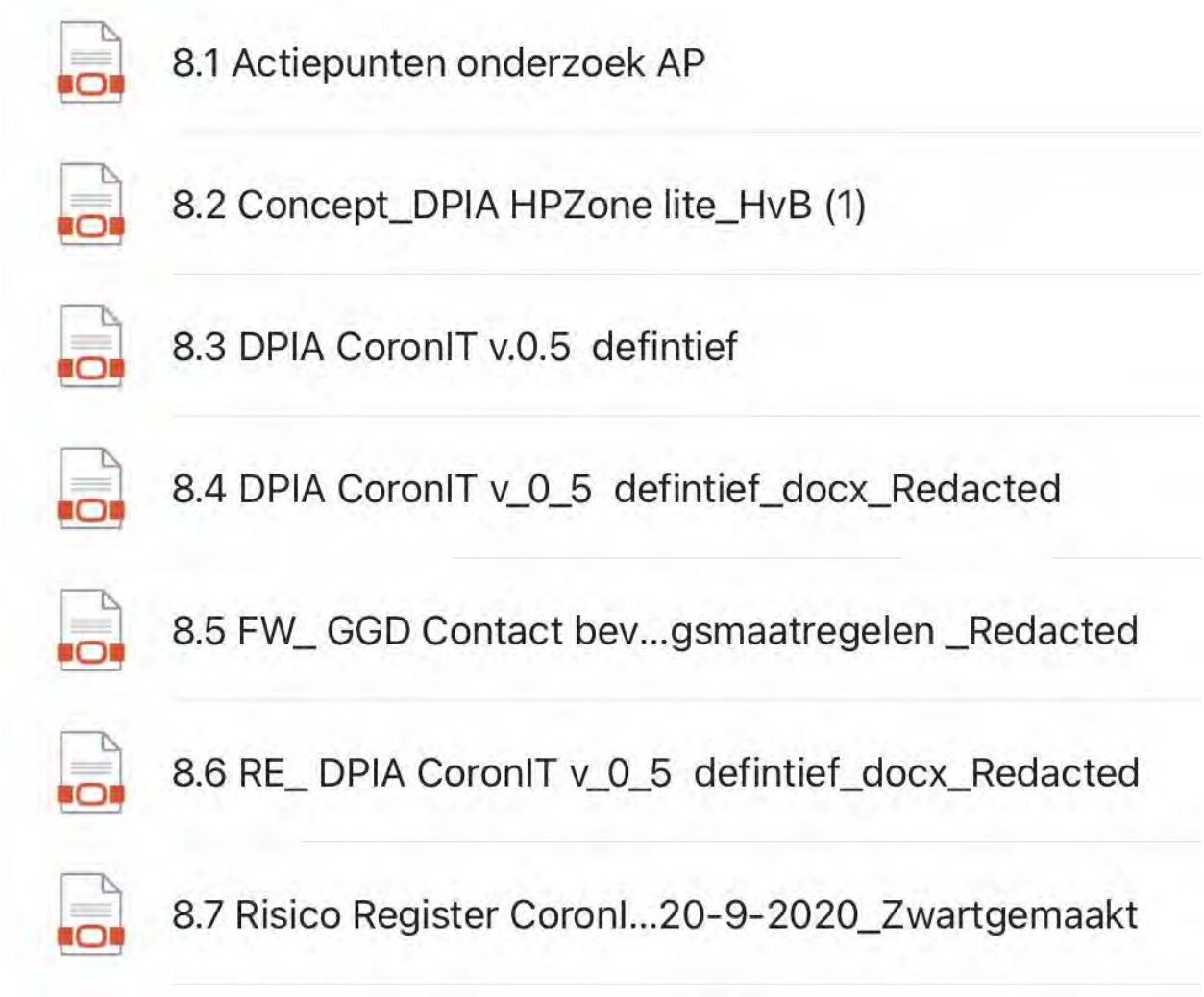
8.0 Tekst Wob-verzoek en register documenten

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:



Actiepunten onderzoek AP

- Voorgangsrapportage in maart 2022 → Actie voor GGD GHOR, met regionale input. Belangrijk om met GGD GHOR en GGD'en af te stemmen hoe deze terugkoppeling plaats zal vinden en in welke bewoording.

- Beleid gebruik eigen apparatuur opstellen als deze er nog niet is. – HSC
    - Indien gebruik eigen apparatuur toegestaan, mitigerende maatregel uitvoeren, zoals mogelijkheid tot inloggen alleen via een beveiligde werkomgeving.

- Autorisaties HP: Goed kijken naar een beleid van toekennen en intrekken van rechten. → daarbij moeten de verleende autorisaties regelmatig beoordeeld worden en hiervoor duidelijke afspraken worden gemaakt over wie in dit verband acties onderneemt.

    - Beleid opstellen
    - Controle op beleid

- Duidelijke schriftelijke afspraken maken met betrokken organisaties / landelijke partners voor toekennen rechten → hoe zitten onze afspraken met Yource?

- AP heeft geen autorisatiematrix aangetroffen met daarin specifieke rechten en functionaliteiten aan de verschillende rollen → Deze heeft Frank wel als het goed is toch?

- Logbestanden controleren: logging en de controle op logging moet vanaf begin af aan goed zijn ingericht bij GGD Contact → Hiervoor is dus OR goedkeuring vereist + informeren medewerkers. Overige maatregelen op dit gebied liggen bij GGD GHOR.

- Voor GGD Contact moeten in/exportfuncties goed worden ingericht. → actie voor GGD GHOR

- Zoekfunctionaliteiten: moeten in GGD Contact goed worden ingeregeld → actie voor GGD GHOR

- Duidelijke schriftelijke afspraken maken met betrokken partijen op het vlak van informatiebeveiliging (Governance) -> wie is voor welke technische en/of organisatorische maatregelen verantwoordelijk

- Controleren van afspraken met ketenpartners waarbij duidelijk moet zijn wie welke technische en/of organisatorische maatregelen moet nemen.

- Audits: deze moeten periodiek worden uitgevoerd t.a.v. informatiebeveiliging → Voor CISO een actiepunt m.b.t. regionale systemen.

Data Protection Impact Assessment (DPIA) HPZONE

Inleiding **2**
A. Beschrijving kenmerken gegevensverwerkingen **2**
1. Voorstel 2
2. Scope 3
3. Persoonsgegevens 3
4. Betrokken partijen en gegevensverwerking 4
6. Verwerkingsdoeleinden 10
7. Belangen bij gegevensverwerking 11
8. Verwerkingslocaties 12
9. Techniek en methode van gegevensverwerking 12
10. Juridisch en beleidsmatig kader 12
11. Bewaartermijn 12
12. Rechtsgrond 13
14. Doelbinding 14
15. Noodzaak en evenredigheid 14
16. Rechten van betrokkenen 15
B. Beschrijving en beoordeling risico's voor de betrokkenen **17**
17. Risico's 17
16. Maatregelen 23
Bijlage 1: Achtergrond Risiconiveaus 25

CONCEPT

Inleiding

Voor dit onderzoek, uitgevoerd voor GGD Hart voor Brabant is er gebruik gemaakt van een Data Protection Impact Assesment model gegevensbeschermingseffectbeoordeling Rijksdienst (PIA). Met behulp van dit format is een overzicht gecreëerd van het systeem en hierdoor kunnen de mogelijke risico's in beeld worden gebracht. Vervolgens wordt er een advies gegeven met mogelijke maatregelen om deze risico's verder te reduceren.

De DPIA speelt een belangrijke rol bij het in kaart brengen van risico's over verschillende systemen. Door gebruik te maken van een DPIA kan er vroegtijdig worden vastgesteld of er sprake zal zijn van risico's bij verwerken van persoonsgegevens.

A. Beschrijving kenmerken gegevensverwerkingen

DPIA: landelijke format voor GGD 'en

Het model gegevensbeschermingseffectbeoordeling Rijksdienst (PIA) is gebruikt als uitgangspunt voor het opstellen deze DPIA. GGD 'en kunnen de inhoud van deze DPIA gebruiken en, indien nodig, DPIA aanpassen en/of aanvullen op basis van de situatie binnen de lokale GGD.

1. Voorstel

Aanleiding

Door de opkomst van COVID-19 wordt er sinds maart 2020 op grootschalige wijze Bron- en Contactonderzoek uitgevoerd. Bron- en contactonderzoek (BCO) is een essentieel onderdeel van de bestrijding van de huidige COVID-19-epidemie. Effectief bron- en contactonderzoek verkort namelijk de duur tussen het ontstaan van klachten en het starten van isolatiemaatregelen, en reduceert daarmee transmissie.[1] Voor het uitvoeren van een effectief bron- en contactonderzoek is een applicatie voor de dossiervorming nodig. De GGD 'en werkte al met HPZone. Dit is een registratiesysteem voor infectieziekte bestrijding. Gezien de grootschaligheid van het Covid-19 virus is gekozen om een "aparte" omgeving te maken voor het registeren van positieve Covid-19 gegevens, genaamd HPZone Lite. Deze applicatie is een schil van de applicatie HPZone en maken gebruik van dezelfde infrastructuur en database.

Voorstel

Alle gegevens die nodig zijn en worden opgehaald bij een bron- en contactonderzoek en/of worden geregistreerd in HPZone Lite.

Registratie in HPZone Lite vindt pas plaats indien de GGD een melding ontvangt van een positief getest persoon. In de Wpg is vastgelegd dat Groep-A-infectieziekten, zoals COVID-19, onverwijld na vaststellingen gemeld moeten worden door de behandelend arts en het laboratorium (Art. 22-25).

[1] Bi Q, Wu Y, Mei S, Ye C, Zou X, Zhang Z, et al. Epidemiology and transmission of COVID-19 in 391 cases and 1286 of their close contacts in Shenzhen, China: a retrospective cohort study. Lancet Infect Dis. (27 April, 2020).

CONCEPT

Het doel van HPZone Lite is het faciliteren van dossiervorming voor het bron- en contactonderzoek.

2. Scope

In deze opdracht is voor de beoordeling van de beginselen van de AVG gekeken naar de praktische uitvoering aan de hand van interview(s) en enkele documenten. Deze zijn:

- Verwerkersovereenkomst
- Handleiding/werkinstructies
- Autorisatiematrix
- HPZone Lite Werkinstructies
- Stand van Zaken HPZone v06 (uitwerkingen audits)
- Diverse documenten onder Teams (inFact, HPZone)

Dit onderzoek betreft slechts de verwerkingen in en de mogelijkheden van de voornoemde applicatie HPZone Lite. Het gebruik van HPZone Lite hangt samen met het bron- en contactonderzoek. De aanvulling van het dossier gebeurt immers wanneer een bron- en contactonderzoek is verricht.

3. Persoonsgegevens

HPZone Lite bevat gegevens over iemands gezondheid, wat valt onder de categorie bijzondere persoonsgegevens in de AVG. Voor deze gegevens geldt dan ook de regel dat zij alleen mogen worden verwerkt op grond van een in art. 9 lid 2 AVG genoemde voorwaarde. De verwerking van deze persoonsgegevens door de GGD 'en is noodzakelijk om redenen van het algemeen belang op het gebied van de volksgezondheid (art. 9 lid 2 sub i AVG) en is wettelijk vastgelegd in art. 30 van de Wet publieke gezondheid (hierna Wpg genoemd). De voorzitter van de veiligheidsregio kan op grond van art. 30 Wpg een behandelend arts verzoeken om zo spoedig mogelijk de medische gegevens te verstrekken, die noodzakelijk zijn om vast te stellen hoe ernstig het verspreidingsgevaar is.

In HPZone Lite worden gegevens verwerkt van de geïnfecteerd persoon (hierna 'de betrokkene(n)'). De betrokkenen zijn in dit geval inwoners van de veiligheidsregio Midden en West-Brabant en Brabant-Zuidoost die een geconstateerde infectieziekte (of een sterk vermoeden hiervan) uit klasse A hebben of hebben gehad.

In de onderstaande tabel is per persoonsgegeven weergegeven om wat voor type persoonsgegevens (gewone, bijzondere of wettelijke identificerende) het gaat.

Informatie over index

Persoonsgegeven	**Gewoon persoonsgegeven**	**Bijzonder persoonsgegeven**	**Wettelijk identificerend persoonsgegeven**
BSN	Ja		Ja
BSN Gevalideerd	Ja		Ja
Voor- en achternaam	Ja		
Geslacht	Ja		

CONCEPT

Geboortedatum	Ja		
UZOVI-nummer		Ja	
Polisnummer	Ja		
Adres, woonplaats en gemeente	Ja		
Infectieziekte		Ja	
Beroep	Ja		
Etnische afkomst		Ja	
Geboorteland		Ja	
Telefoonnummer			
Mobiele telefoonnummer	Ja		
E-mailadres	Ja		

Tabel 1: persoonsgegevens HPZone Lite

HPZone Lite verstrekt bepaalde gegevens aan het RIVM. Deze gegevens worden verstrekt doormiddel van de applicatie Osiris. De verstrekken gebeurt handmatig. De gegevens die worden verstrek aan het RIVM middels Osiris staan hieronder beschreven.

Nadat een BCO-medewerker het HPZone-dossier zo volledig mogelijk heeft ingevuld, moet de Osiris melding worden voltooid. De volgende 'key details' en 'personal details' neemt Osiris over uit HPZone voor een melding aan het RIVM:

- Date of onset (eerste ziektedag)
- Personal details
- Geslacht
- Date of birth
- Postcode
- Melding aan GGD: oorspronkelijke bron van de melding
- Osiris-nummer
- Datum gefiatteerd in Osiris: datum van melding aan Osiris
- Status van melding: BCO-medewerkers moeten 'gefiatteerd' selecteren. Hierdoor telt de casus mee in de landelijke cijfers, maar kan de lokale GGD nog eventuele aanpassingen doen. De lokale GGD zal uiteindelijk de melding op definitief zetten.

4. Betrokken partijen en gegevensverwerking

Betrokken partijen en rolverdeling

In deze paragraaf wordt uiteengezet welke partijen betrokken zijn bij de applicatie HPZone Lite en onder welke rol.

CONCEPT

1. GGD GHOR Nederland en de regionale GGD

GGD GHOR Nederland neemt het beheer en het eigenaarschap over HPZone. Hieronder wordt het volgende verstaan[2]:

- Regie op Infrastructuur (KPN) – herontwerp in testfase. Project gestart voor aanbesteding infrastructuur
- Regie op inFact genomen n.a.v. datalek. Samenwerking tussen GGD 'en, GGD GHOR en inFact nog niet geformaliseerd. Advocatenbrief en vervolg
- Advies geformuleerd over toekomstbestendigheid HPZone/ HPZone Lite.
- NB: momenteel onduidelijk wat stand van zaken is t.a.v. Overdracht van FBEI -> GGD GHOR NL

2. GGD – Zelfstandig verwerkingsverantwoordelijke en tevens gezamenlijk verantwoordelijk

De regionale GGD 'en blijven verantwoordelijk voor het gebruik en regionaal beheer/autorisatie van HPZone Lite. De GGD 'en bepalen dus de vraag naar nationale BCO-medewerkers en verstrekken de autorisaties voor HPZone Lite. GGD GHOR coördineert het aanbod en neemt het beheer onder zich.

3. RIVM – Zelfstandig verwerkersverantwoordelijke

Osiris is het systeem van het RIVM waarin anoniem actuele infectie-en sterftecijfers bijgehouden worden. Osiris is gekoppeld aan HPZone Lite, maar de informatie moet wel actief naar het systeem verstuurd worden. Dagelijks wordt vanuit HPZone Lite informatie over contacten doorgegeven aan het RIVM. In HPZone Lite worden de volgende gegevens gerapporteerd per contact:

- Persoonskenmerken (geslacht, geboortejaar, postcode);
- Link aan index (Osiris-nummer) of situatie;
- Categorie contact;
- Eerste en laatste dag blootstelling;
- Monitoringsperiode;
- Belcontacten tijdens monitoringsperiode;
- Ontstaan van klachten inclusief eerste ziektedag en soort klachten;
- Afgenomen diagnostiek;
- GGD-regio.

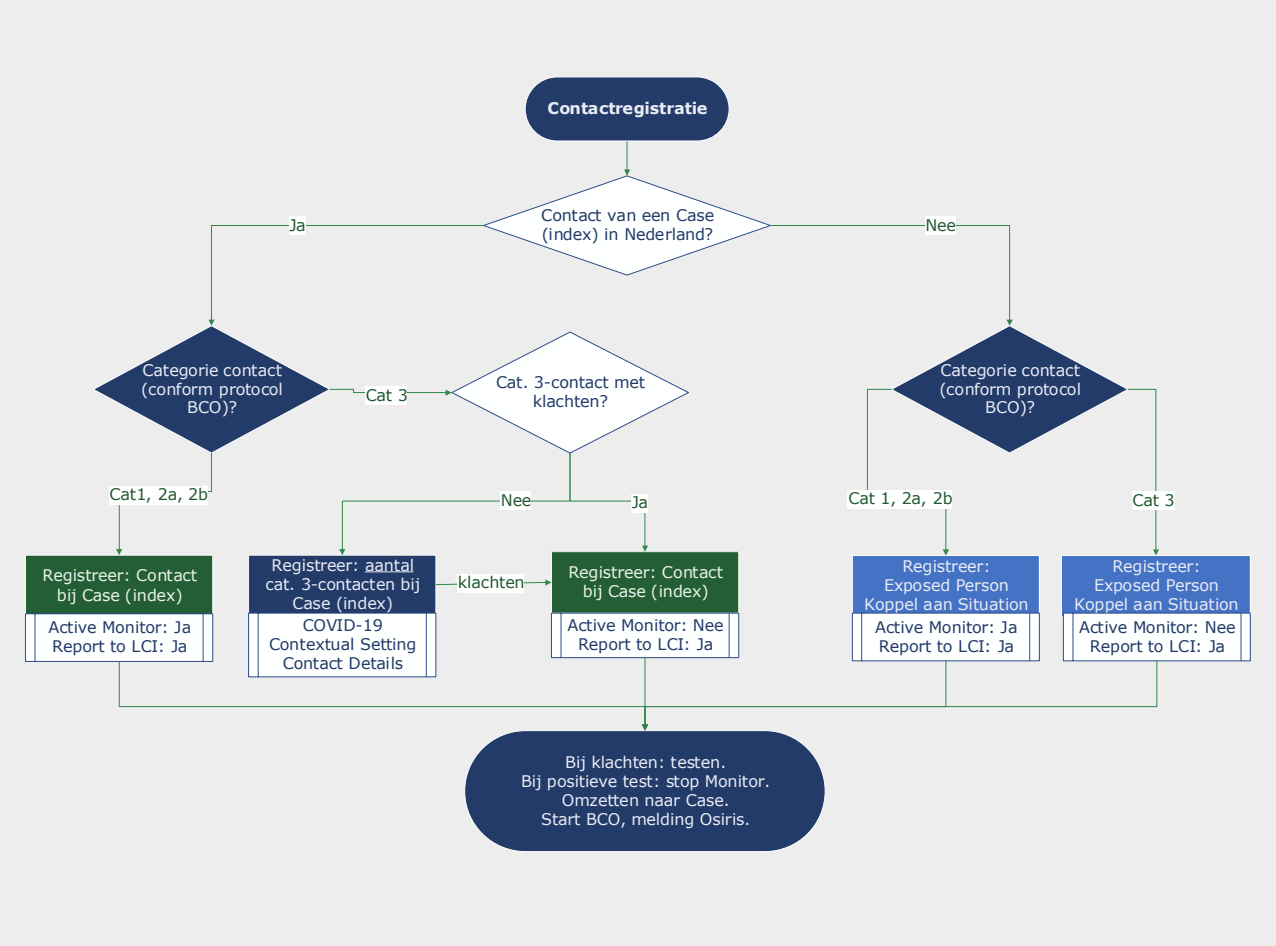
Het RIVM krijgt een geanonimiseerde lijst met data aangeleverd door GGD GHOR. Het RIVM gebruikt deze gegevens om rapportages op te kunnen stellen, die dient als stuurinformatie. Het RIVM bepaalt hoe deze gegevens worden geanalyseerd en gebruikt voor rapportages.

Gegevensverwerking

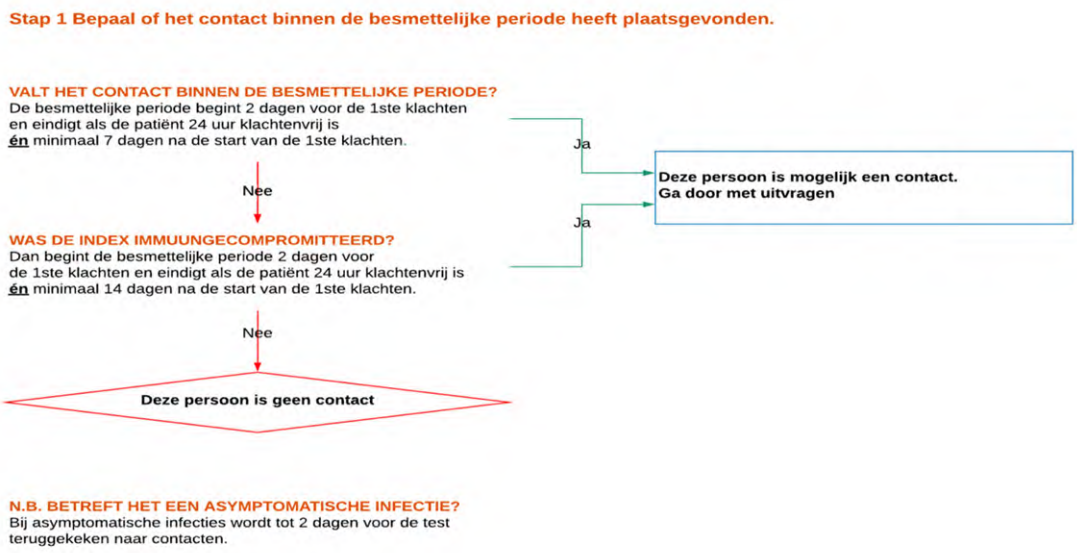
In deze paragraaf wordt de datastroom van de applicatie HPZone Lite weergegeven.

[2] CDPG20210212.05 - Presentatie NR -Acties ICT DATA def 12 feb 2021.

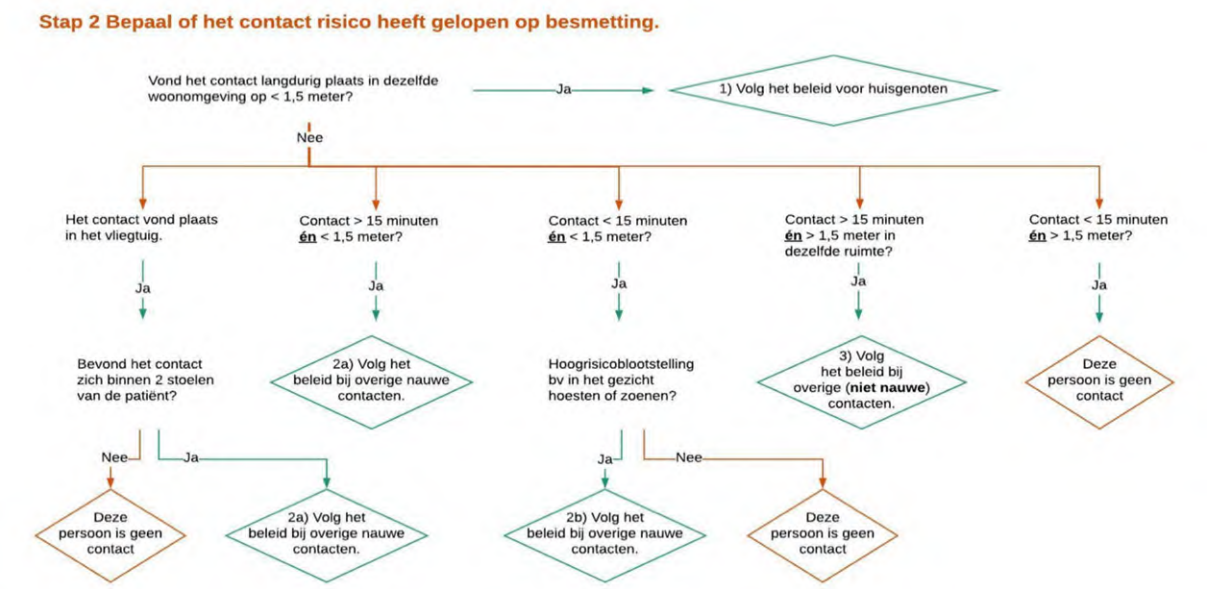
CONCEPT



Registratie HPZone Lite



Stap 1 BCO-protocol



Stap 2 BCO-protocol

1. Registratie aantal categorie 3-contacten

De lokale GGD ontvangt een melding via CoronIT van een behandelend arts en laboratorium bij een positieve COVID-19 test. Bij een positief getest persoon worden de aantal categorie 3-contacten gerapporteerd. De data wordt automatisch vanuit HPZone Lite naar het RIVM gestuurd.[3]

Start BCO
Bepalen en geven van advies op maat op basis van context en type contact. Versturen van e-mail met gemaakte afspraken (informatiepakket) naar index patiënt en contacten. Dit kan ook per post indien e-mail niet mogelijk is.

2. Categorie contact

De GGD maakt vervolgens een dossier voor de index-patiënt aan in HPZone. Werknemers van de landelijke schil van BCO maken gebruik van HPZone Lite, zodat zij enkel gegevens die betrekking hebben op COVID-19 in kunnen zien. In beginsel is de index al op de hoogte van zijn/haar positieve uitslag, maar landelijke BCO-medewerkers verifiëren dit aan het begin van het gesprek. Het is verder uiteraard van belang dat geverifieerd wordt of je de juiste persoon aan de lijn hebt. De index wordt ondervraagd aan de hand van een vragenformulier dat BCO-medewerkers kunnen vinden onder 'Events' in HPZone Lite en/of op GGD GHOR Kennisnet. In dit vragenformulier staat een opsomming van vragen omtrent o.a.: klachten, ziekteverloop, verblijfplaats index, mogelijke bron, verblijfplaats, setting, contacten.

Huisgenoten, nauwe contacten en overige contacten waarmee de index in de besmettelijke periode in worden in contact is geweest worden geïnventariseerd en gecategoriseerd. Deze besmettelijke

[3] C. 200806 Handleiding Contactregistratie HPZlite.

periode begint 2 dagen voor start van de klachten, en eindigt als de patiënt 24 uur klachtenvrij is en minimaal 7 dagen na start symptomen.

Als een huisgenoot klachten overeenkomstig COVID-19 heeft, moet worden vastgesteld wat voor klachten en wanneer de eerste ziektedag was. Wanneer de klachten overeenkomen met de indicaties tot testen van contacten, moet dit contact verwezen worden naar de lokale GGD voor het aanmaken van een testaanvraag. Het HP-zone nummer van de Index wordt dan verstrekt en het contact moet dat HPZone-nummer benoemen bij zijn/haar testaanvraag.

Tot slot, geven BCO-medewerkers voorlichting, instructies en advies op maat aan de Index-patiënt en huisgenoten.

Het is van belang om te controleren of het juiste e-mailadres is genoteerd om later de informatiebrieven naar te mailen. Van belang om in de instructies op te nemen dat een BCO-medewerkers het emailadres nog een keer herhaald ter verificatie.

2A. Informeren van index en huisgenoten en brieven sturen
De index ontvangt vanuit de BCO-medewerker een mail met te nemen maatregelen. De BCO-medewerker moet vervolgens de volgende stappen doorlopen:

- Informeren van de index dat een medewerker/de GGD-contact opneemt met de huisgenoten (als dat niet gelijk met de index kan) om passende maatregelen te bespreken. Deze worden ook per mail aan hun toegestuurd.
- Informeren van de index dat een medewerker/de GGD-contact opneemt met de overige nauwe contacten om passende maatregelen te bespreken. Deze worden ook per mail aan hun toegestuurd.
- Benoemen dat als men de brieven niet dezelfde dag hebben gekregen, ze mogen bellen met de eigen lokale GGD.
- De index verzoeken om de mail, bedoeld voor overige niet-nauwe contacten, door te sturen naar deze personen (afhankelijk wat er met de BCO-gesprekscoach is besproken).

2B. Bellen en informeren van nauwe en brieven versturen
BCO-medewerkers nemen telefonisch contact op met alle huisgenoten (>16 jaar) en nauwe contacten. Voor definities huisgenoten en nauwe contacten, zie ook https://lci.rivm.nl/COVID-19-bco. Nadat er telefonisch contact heeft plaatsgevonden, sturen ze ook nog een e-mail met daarin de besproken adviezen. Er is een standaard mail-format, maar het HPZone nummer en het telefoonnummer van de lokale GGD moeten handmatig worden ingevuld.

2C. Bellen en informeren van overige (niet nauwe) contacten en brieven versturen
BCO-medewerkers nemen tot slot telefonisch contact op met alle overige contacten. Nadat er telefonisch contact heeft plaatsgevonden, sturen ze ook nog een e-mail met daarin de besproken adviezen.

Ter ondersteuning van het doorlopen van stap 2 is in de landelijke werkinstructie BCO de volgende checklist opgenomen:

Informatievoorziening contacten	
Is de informatiemail verstuurd aan de index?	Let op: vul nummer lokale GGD in!!!
Zijn alle huisgenoten gebeld en is de informatiemail aan hen verstuurd?	
Zijn alle nauwe-contacten gebeld en is de informatiemail aan hen verstuurd?	
Is aan de index geadviseerd de informatiemail door te sturen aan zijn privé overige niet-nauwe contacten?	
Zijn de overige (niet nauwe) contacten buiten de privésfeer overgedragen aan de lokale GGD	
Vraag of de index zelf de huisarts wil informeren	

Vervolgens moet een BCO-medewerkers ook van alle huisgenoten (categorie 1) en nauwe contacten (categorie 2) een dossier aanmaken via het HPZone dossier van de index. Contactmomenten met deze contacten worden dan ook geregistreerd in het dossier van het contact. Overige contacten worden geregistreerd in 'COVID-19 Contextual Setting Contact Details' in de midden kolom van het HPZone dossier van de index. Als blijkt dat een contact al een bestaand dossier heeft (eventueel in een andere regio), dan worden BCO-medewerkers geïnstrueerd om te overleggen met een BCO-gesprekscoach voor verdere afhandeling van de monitoring.

Het monitortype van contacten behorend tot categorie 1 en 2 staat standaard op 'Active Monitoring'. BCO-medewerkers mogen het type monitoring enkel aanpassen naar een blanco veld (niet actief/passief) bij categorie 3-contacten. De status van monitoring wordt automatisch vanuit HPZone naar het RIVM verstuurd, zodat deze data gebruikt kan worden om een beeld te krijgen van blootstelling en besmettingen in specifieke omgevingen ('Settings').

3. Telefonische nazorg en instructies

De contacten die zelf bellen met een vraag komen binnen bij de lokale GGD, dus niet bij het landelijke BCO-team.

4. Individuele monitoring

Beantwoording van contacten die zelf bellen in verband met koorts of andere klachten (hoesten en/of neusverkouden) en eventuele doorverwijzing voor een test, wordt ook gedaan door de lokale GGD 'en.

Bij een negatieve uitslag wordt het dossier afgesloten. Keuze om huisarts in te lichten over de uitslag wordt bij contact neergelegd.

CONCEPT

5. Afronden BCO

Monitoring met index patiënt om BCO af te ronden voor index en huisgenoten. Betermelding van index-patiënt bij huisarts wordt bij de index neergelegd.

Er worden 3 vaste contactmomenten in HPZone Lite ingebouwd: dag van eerste gesprek, dag 5 en een gesprek ter afsluiting van de quarantaineperiode (dag 10):

- Het 1e gesprek is voor uitleg en instructie
- Het 2e gesprek op dag 5 is om te informeren hoe het gaat en of er klachten zijn
- Het 3e gesprek checkt of er reden is om de quarantaine te verlengen. Als dat niet het geval is, is dit een afsluitend gesprek, waarmee de monitoring beëindigd wordt.

6. Verwerkingsdoeleinden

Een infectieziekte is een ziekte bij mens of dier die wordt veroorzaakt door de aanwezigheid van een of meer micro-organismen, zoals een bacterie, een virus of een schimmel. Infectieziekten kunnen op verschillende manieren worden overgedragen, zoals door contact met besmette personen, lichaamsvloeistoffen, insecten, voorwerpen of inademing van besmette lucht. Covid-19 Valt hier ook onder. Gezien de grootschaligheid van deze infectieziekte is een apart registratiesysteem gecreëerd voor Covid-19 meldingen. Deze worden geregistreerd in HPZone Lite. Het proces begint bij en ontvangen van een melding van een positieve besmetting. Daarna wordt handmatig een dossier aangemaakt in HPZone Lite. Dit dossier wordt verder aangevuld door een bron- en contactonderzoek.

Om de verspreiding van infectieziekten te helpen voorkomen is er in de Wet publieke gezondheid een meldingsplicht geregeld.[4] Deze meldingsplicht schrijft voor dat artsen en medische laboratoria bepaalde infectieziekten aan de GGD melden. De GGD zal vervolgens de bron van de infectie opsporen en gaat na of contacten van de patiënt risico lopen op een besmetting. Er kunnen maatregelen worden genomen door de GGD ter bescherming van deze contacten en om te voorkomen dat de ziekte verder verspreid wordt.[5]

Melding plichtige infectieziekten zijn verdeeld over de groepen A, B1, B2 en C. De indeling van deze groepen is gebaseerd op de mate waarin (dwingende) maatregelen om de bevolking te beschermen opgelegd kunnen worden.[6] Zie bijlage 1 voor de indeling van de groepen infectieziekten.

Infectieziektes die mogelijk internationale consequenties hebben, worden geanonimiseerd door het RIVM aan de Wereld Gezondheidsorganisatie doorgegeven.

4

5 RIVM 2020

6 RIVM 2020

CONCEPT

Voor het bestrijden van het COVID-19 Virus en voor het uitvoeren van het uitvoeren van artikel 6, lid 1, sub c van de Wet Publieke Gezondheid (Hierna: WPG) is het noodzakelijk om de persoonsgegevens benoemd in §3 te verwerken. De desbetreffende persoonsgegevens zijn dus ter zake dienend en niet bovenmatig voor het beoogde doel, namelijk het registreren en monitoren van het aantal besmettingen, het delen van deze gegevens voor onder andere sturingsdata en het reduceren van transmissie door de tijd tussen het ontstaan van klachten en het starten van isolatiemaatregelen te verkorten.

7. Belangen bij gegevensverwerking

Samenleving als geheel

Indien een burger positief getest is, wordt dit geregistreerd in de applicatie HPZone Lite. Deze registratie heeft verschillende doeleinden zoals beschreven in §6. Door middel van deze applicatie kunnen verschillende belangen worden behartigd, zoals het bestrijden van verdere besmettingen. Dit wordt gerealiseerd door het bron en contactonderzoek en het registreren van deze data voor sturing op nationaal niveau. Het uitgebreid testen van mensen en het doen van bron- en contactonderzoek is een voorwaarde voor blijvende versoepeling van de maatregelen. De samenleving is er namelijk bij gebaat dat zo veel mogelijk mensen die mogelijk besmet zijn zichzelf isoleren, zodat zij andere mensen niet besmetten.

Betrokkenen

Een betrouwbare registratie van de positief geteste burgers is de basis van een effectieve bron- en contactonderzoek. Dit verkort de duur tussen het ontstaan van klachten en het starten van isolatiemaatregelen, en reduceert daarmee overdracht. Hoe eerder COVID-19 kan worden ingedamd, hoe sneller burgers terug kunnen keren naar het gewone maatschappelijke leven. Voor het realiseren succesvolle indamming is het cruciaal om zo snel mogelijk de bron van besmetting te achterhalen, contacten te identificeren, hen te informeren over de blootstelling en risico op besmetting, hen te wijzen op maatregelen die genomen moeten worden om verdere verspreiding te voorkomen en actuele sturingsdata te verzamelen en te delen. Hiervoor is op dit moment nog toegang nodig tot HPZone Lite. Hierin worden alle gegevens die zijn opgehaald verwerkt en verstrekt aan derde zoals het RIVM.

GGD GHOR Nederland

GGD GHOR heeft van het Ministerie van VWS de opdracht gekregen tot opschaling van onder andere het realiseren van voldoende capaciteit en het coördineren van de samenwerking met verschillende externe partners. Om alle data die wordt verzameld tijdens een bron- en contactonderzoek te registreren is er een registratiesysteem nodig. Door de aard en de omvang van de huidige COVID-19-epidemie, is gekozen om gebruik te maken van HPZone Lite (een schil van HPZone). GGD GHOR heeft hier het beheer en het eigenaarschap over genomen, nadat een grootschalig datalek heeft plaatsgevonden.

CONCEPT

GGD
De aard en de omvang van de huidige COVID-19-epidemie vereisen een flexibele aanpak waarbij men adequaat kan inspelen op regionale uitbraken en dit op regionaal niveau kunnen registreren en monitoren.

RIVM
In kaart brengen van de stand van zaken en ontwikkeling van de verspreiding van COVID-19 in Nederland. De informatie uit HPZone Lite wordt gepseudonimiseerd verstrekt aan het RIVM en dient om te voorzien in stuurinformatie.

Ministerie van Volksgezondheid
Het ministerie, vertegenwoordigd door de minister, is op basis van de Wet publieke gezondheid (Wpg artikel 7.1) verantwoordelijk voor het coordineren van de bestrijding van epidemieen van infectieziekenten categorie A (zoals corona). Het ministerie (en de minister) hebben derhalve belang bij het op een verantwoorde manier opschalen van de landelijke BCO-capaciteit.

8. Verwerkingslocaties
De infrastructuur, HP Zone Lite, waar BCO-medewerkers van de landelijke schil gebruik van maken in het kader van bron- en contactonderzoek wordt gehost op KPN-datacentra gesitueerd in Nederland. Er worden geen gegevens verwerkt buiten de Europese Unie. Bepaalde informatie wordt in gepseudonimiseerd verstrekt aan het RIVM middels Osiris. Osiris communiceert direct met HPZone Lite. De gegevens worden handmatig via een sent button verstuurt zodra het dossier is gesloten.

9. Techniek en methode van gegevensverwerking
Voor deze verwerking wordt gebruik gemaakt van:
- HPZone Lite
- Koppeling Osiris

10. Juridisch en beleidsmatig kader
Voor de verwerking van persoonsgegevens in HPZone Lite zijn de volgende wet- en regelgeving van toepassing:
- Algemene Verordening Gegevensbescherming (AVG);
- Uitvoeringswet AVG (UAVG);
- Wet publieke gezondheid (Wpg);
- Opdracht van Ministerie van VWS aan GGD GHOR;
- Mandaat GGD 'en aan GGD GHOR Nederland.

11. Bewaartermijn
De persoonsgegevens die geregistreerd staan in HPZone Lite, worden voor ten hoogste vijf jaar (art. 29 lid 1 en lid 2 Wpg) bewaard. Dit is afhankelijk van hoelang de pandemie duurt. Dit geldt voor in de meldplicht opgenomen persoonsgegevens (meldingsgegevens) zoals omschreven in artikel 24 lid 1 Wpg.

CONCEPT

Uit de memorie van toelichting van artikel 29 Wpg blijkt dat de gegevens verwijderd dienen te worden zodra de GGD 'en hebben vastgesteld dat deze niet langer noodzakelijk zijn, met een maximale bewaartermijn van 5 jaar. In het voorkomende geval is het bewaren van de betreffende persoonsgegevens in ieder geval noodzakelijk voor de gehele duur van de pandemie. Indien de pandemie minder lang duurt dan 5 jaar, zullen de gegevens dus eerder verwijderd worden.

Voor de persoonsgegevens die aanvullend op de hierboven vermelde gegevens worden verzameld, geldt dat deze voor dezelfde periode worden bewaard als de meldingsgegevens. Hiervoor is gekozen omdat dit gegevens betreft waarmee contact op kan worden genomen met betreffende personen (zoals telefoonnummer en e-mailadres). Tijdens de pandemie kan het voorkomen dat personen meerdere keren onderdeel uitmaken van een bron- en contactonderzoek. Ter voorkoming van het meermaals moeten uitvragen van de gegevens en het daarmee verkleinen van de kans op het verzamelen van onjuiste of dubbele gegevens, is ervoor gekozen alle tijdens het BCO verzamelde persoonsgegevens te bewaren zolang de pandemie duurt, met een maximum bewaartermijn van 5 jaar. Dit geldt ook voor alle persoonsgegevens die worden verzameld over contacten van de Index, aangezien deze niet vallen onder de meldplicht uit de Wpg.

Na deze bewaartermijn, worden de persoonsgegevens verwijderd of geanonimiseerd. De mogelijkheid bestaat dat gegevens in een geanonimiseerde vorm beschikbaar blijven om onderzoek mee te doen. In dat geval wordt gezorgd dat de gegevens niet herleidbaar zijn en op een adequate wijze worden afgeschermd.

Beoordeling rechtmatigheid gegevensverwerkingen

12. Rechtsgrond

De bestrijding van COVID-19 betreft een infectie behorend tot groep A waarvoor veiligheidsregio's verantwoordelijk zijn (art. 6 lid 2 Wpg). Het doel van de GGD is; Overzicht creëren van infectieziekten in de regio, om eventueel passende maatregelen te nemen in het belang van de volksgezondheid. De grondslag voor het verwerken van de gegevens zijn opgenomen in artikel 6, lid 1, sub c jo. artikel 30 WPG.

Het doel van de GGD is; Overzicht creëren van infectieziekten in de regio, om eventueel passende maatregelen te nemen in het belang van de volksgezondheid. Om deze feitelijke uitvoering door de GGD 'en te realiseren en zo te voldoen aan de wettelijke taak die voortkomt uit de Wet Publieke Gezondheid, is de verwerking van persoonsgegevens noodzakelijk. Het opvragen van persoonsgegevens door de GGD is derhalve noodzakelijk voor het vervullen van een taak van algemeen belang of een taak in het kader van de uitoefening van het openbaar gezag (art. 6 lid 1 sub e AVG). Deze noodzaak moet bij lidstatelijk recht zijn geregeld (art. 6 lid 3 sub b AVG) en in dit geval is deze wettelijke taak opgenomen in artikel 6, lid 1, sub c jo. artikel 30 Wpg.

CONCEPT

13. Bijzondere persoonsgegevens

Voor het verwerken van bijzondere persoonsgegevens, zoals gegevens over de gezondheid, is het noodzakelijk dat er een wettelijke uitzondering van toepassing is, zoals gesteld in art. 9 AVG. Het verbod op het verwerken van bijzondere persoonsgegevens kan worden doorbroken als de verwerking noodzakelijk is om reden van algemeen belang op het gebied van de volksgezondheid zoals bescherming tegen ernstige grensoverschrijdende gevaren voor de gezondheid als dit ook nog in lidstatelijk recht is geregeld (art. 9 lid 2 sub i AVG).

Art. 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, 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.

De Covid-19 pandemie is een grensoverschrijdende aanslag op onze volksgezondheid en valt dus te scharen onder de bovenstaande uitzondering. Het toepasselijke lidstatelijk recht waarin dit geregeld is, is de Wet publieke gezondheid. Deze specifieke wetgeving heeft daarnaast voorrang op algemene wetgeving zoals de UAVG.

14. Doelbinding

Het registreren en monitoren van de COVID-19 epidemie is noodzakelijk om de volksgezondheid te beschermen. Hiervoor dienen bepaalde gegevens te worden verwerkt. HPZone Lite is op dit moment nog het systeem waarin deze gegevens worden vastgelegd en waar dossiervorming plaatsvindt. De verwerking van persoonsgegevens is noodzakelijk om de bron van besmetting te achterhalen en mogelijk besmette contacten in kaart te brengen.

15. Noodzaak en evenredigheid

De AVG bepaalt dat alle verwerkingen van persoonsgegevens moeten voldoen aan de
Vereisten van proportionaliteit en subsidiariteit. Dit houdt kort gezegd in dat: het doel en de aard en omvang van de gegevens die voor dat doel worden verwerkt met elkaar in verhouding moeten zijn en dat altijd moet worden gekozen voor de minst ingrijpende verwerking van persoonsgegevens.

Bij het inrichten van de BCO-procedure is als volgt rekening gehouden met de beginselen proportionaliteit en subsidiariteit:

Proportionaliteit

De GGD heeft de wettelijke taak tot het doen van BCO. BCO is vormvrij en moet breed worden opgevat. De GGD moet immers kunnen differentiëren naar wat afhankelijk van de omstandigheden van het geval de beste aanpak is. Voor de bestrijding van de pandemie geldt dat het doel van BCO

CONCEPT

het beste kan worden bereikt als zoveel mogelijk mensen die risicovol in de nabijheid van een geïnfecteerde persoon zijn geweest zo snel mogelijk kunnen worden gewaarschuwd. Voor de uitvoering van het bron- en contactonderzoek wordt gebruikt gemaakt van HPZone Lite, om de gegevens die nodig zijn voor de uitvoering van deze taak te verwerken. Daarbij worden enkel gegevens geregistreerd die nodig zijn voor het uitvoeren van deze taak. De verwerking van persoonsgegevens door invoering in HPZone Lite tijdens het bron- en contactonderzoek is daarom noodzakelijk en proportioneel. Gezien de omstandigheden, de voortvarendheid en de aard en omvang van de COVID-19 epidemie, was dit de meest voor de hand liggende oplossing.

Deze wettelijke taak van de GGD dient een algemeen belang op het gebied van volksgezondheid. Het door de GGD registreren en monitoren is essentieel voor het doorbreken van de keten van infecties en het voorkomen van verdere infecties en levert daarmee een cruciale bijdrage aan de bestrijding van COVID-19. Dit sluit aan bij het uitgangspunt van de EDPB dat 'het rechtskader voor gegevensbescherming is ontworpen met flexibiliteit voor ogen en als zodanig een efficiënte respons mogelijk maakt die de pandemie indamt en de fundamentele mensenrechten en vrijheden beschermt'.[7]

Subsidiariteit
HPZone Lite is speciaal ontwikkeld zodat landelijke BCO-medewerkers in een applicatie werken die hen alleen inzicht verschaft in de relevante COVID-19 dossiers. Andere applicaties zijn daardoor overbodig in het BCO-proces, wat betekent dat een wildgroei aan applicaties en verscheidenheid aan gemelde informatie wordt vermeden. Dit zorgt ook voor rapportages die betrouwbaarder zijn en zorgen dat adequatere keuzes kunnen worden gemaakt.

De verwerking van (persoons)gegevens is beperkt tot het strikt noodzakelijke. Daarnaast zijn ook verschillende andere passende technische en organisatorische beveiligingsmaatregelen getroffen.

In dit proces is het van belang dat registratie adequaat wordt uitgevoerd, ook als de GGD zelf niet voldoende capaciteit heeft. Het structureren van deze extra inzet volgens eenzelfde training en landelijke werkinstructie, maakt dat de gegevens op een uniforme wijze worden verwerkt en dat wordt gezorgd dat de medewerkers worden gescreend en getraind. Dit voorkomt versnippering van werkwijzen van verschillende bureaus die anders op regionaal niveau zouden worden ingezet. Verwerking op landelijk niveau volgens de landelijke werkinstructie/richtlijnen door BCO-medewerkers is daarom subsidiair.

16. Rechten van betrokkenen
In HPZone Lite worden zowel gewone als bijzondere persoonsgegevens verwerkt. Omdat die persoonsgegevens worden verwerkt, hebben betrokkenen een aantal rechten, zoals bepaald in hoofdstuk III AVG. Het is de verantwoordelijkheid van GGD Hart voor Brabant om de verzoeken gebaseerd op art. 15 tot en met 21 AVG te beoordelen.

CONCEPT

Recht op informatie (art. 13/14 AVG):
De betrokkene heeft recht om informatie te ontvangen over de verwerking van zijn/haar persoonsgegevens. Op de website van GGD Hart voor Brabant, is een link naar de privacyverklaring geplaatst die informatie verstrekt over de gegevens die landelijke BCO-medewerkers uitvragen en verwerken.

Recht op inzage en afschrift (art. 15 AVG)
De betrokkene heeft het recht om de gegevens in te zien. Op de website van GGD Hart voor Brabant is een formulier geplaatst dat gebruikt kan worden om het verzoek in te dienen. Hiervoor dient de betrokkene een kopie van het legitimatiebewijs bij te voegen. Daarbij mag de pasfoto en het BSN worden afgeschermd en mag er een watermerk geplaatst worden op de kopie. De betrokkene wordt op deze mogelijkheid gewezen.

Recht op rectificatie (art. 16 AVG)
De betrokkene heeft het recht om gegevens die niet (langer) juist zijn, te laten rectificeren. Ook hiervoor kan gebruik worden gemaakt van het formulier.

Indien de aanpassing kleine aanpassingen betreft, zoals telefoonnummer en e-mailadres, dan kunnen betrokkenen dit ook telefonisch laten aanpassen. Dit moet worden opgenomen in de landelijke werkinstructie.

Recht op gegevenswissing (art. 17 AVG)
De betrokkene kan verzoeken persoonsgegevens te wissen. De GGD conformeert zich aan de werkinstructie gegevenswissing. Daarin staat de afweging beschreven welke gegeven wel en welke niet kunnen worden verwijderd i.v.m. de wettelijke bewaartermijn. Ook speelt de vraag of de WPG of WGBO van toepassing is. Indien uit later onderzoek duidelijk wordt dat de WBGO van toepassing is, dan dient deze werkinstructie te worden herzien. Om een verwijderverzoek in te dienen kan gebruik worden gemaakt van het formulier op de website van GGD Hart voor Brabant.

Recht op beperking van de verwerking (art. 18 AVG)
De betrokkene kan in de door de wet bepaalde gevallen verzoeken om de verwerking van zijn/haar gegevens te beperken. Dit is enkel het geval indien de gegevens mogelijk onjuist zijn. Ook hiervoor kan gebruik worden gemaakt van het formulier.

Recht op overdraagbaarheid van de gegevens (art. 20 AVG)
Dit recht is alleen van toepassing bij toestemming of contract, daarvan is in dit proces geen sprake.

Recht van bezwaar (art. 21 AVG)
De betrokkene heeft het recht om in bepaalde gevallen bezwaar te maken tegen de verwerking van persoonsgegevens, wanneer de individuele omstandigheden van het geval dit rechtvaardigen en de verwerking plaatsvindt op basis van het algemeen of gerechtvaardigd belang. Zo kan er bezwaar

CONCEPT

gemaakt worden tegen het gebruik van persoonsgegevens voor wetenschappelijk onderzoek. De betrokkene wordt op deze mogelijkheid gewezen in de privacyverklaring van GGD Hart voor Brabant.

Recht om niet te worden onderworpen aan geautomatiseerde individuele besluitvorming (art. 22 AVG)
Registratie en monitoring in HPZone Lite geschied handmatig er is geen sprake van geautomatiseerde individuele besluitvorming overeenkomstig art. 22 AVG.

B. Beschrijving en beoordeling risico's voor de betrokkenen

17. Risico's

In deze paragraaf worden de risico's voor betrokkenen uiteengezet, inclusief de risico's die door voorgenomen maatregelen reeds gemitigeerd zijn. Per risico wordt een inschatting gemaakt van het risiconiveau op basis van kans x impact. Vervolgens worden er verschillende mitigerende maatregelen voorgedragen en wordt ingeschat wat het risiconiveau betreft na toepassing van deze maatregelen. Aangezien er hier sprake is van een proces waarin veranderingen plaatsvinden, zullen eventuele nieuwe risico's in een register worden bijgehouden. Grote wijzigingen in het proces zullen in een addendum bij deze DPIA worden bijgevoegd.

1. Onvoldoende controle op Autorisaties leidt tot niet opsporen van onrechtmatige verwerkingen.

Voor HPZone Lite is een interne autorisatiematrix opgesteld in Excel. Deze worden toegepast bij het indienst treden, doorstromen en het uitstromen van medewerkers. Door de grote opschaling van het BCO en de huidige informatiestructuur van HPZone Lite, kost het veel inspanning om de matrix ook na te leven. Indien een (ingehuurde) BCO-medewerker toegang nodig heeft tot HPZone Lite dient de regionale GGD deze persoon te autoriseren. Dit gebeurt handmatig. Als het BCO moet opschalen dienen alle autorisaties dus handmatig te worden doorgevoerd. Ook bij doorstroom of indien downscaling plaatsvindt dienen de autorisaties handmatig weer te worden ingetrokken. Dit is tijdrovend en kost veel inspanning. Daarnaast is het proces ook zeer foutgevoelig. De applicatiebeheerders zijn namelijk afhankelijk van het doorgeven van wijzigingen vanuit de coördinatoren.

- Autorisatie landelijk schil van medewerkers krijgen toegang tot HPZone Lite. Maandelijks worden alle rechten ingetrokken van de (ingehuurde) BCO-medewerkers die niet hebben ingelogd om ongeautoriseerde toegang tegen te gaan. Het risico bestaat dat (ingehuurde) BCO-medewerkers geen werkzaamheden meer uitvoeren voor het callcenter waar ze voor werken, maar nog wel toegang kunnen hebben tot HPZone Lite
- De landelijke schil bepaalt welke rechten de inhuur medewerkers krijgen. HVB kan alleen toegang geven. Hierdoor bestaat het risico dat het landelijke schil medewerkers te veel rechten geeft waardoor ze meer bevoegdheden hebben dan nodig is;

CONCEPT

- Applicatiebeheerders zijn afhankelijk van de input van de coördinatoren. Kans bestaat dat dit niet altijd juist of tijdig wordt doorgegeven waardoor bepaalde autorisaties (langere tijd) blijven bestaan.
- De impact van het datalek is hoog. Als persoonsgegevens onrechtmatig worden verwerkt en uitlekken, lekken medische gegevens uit. Daarnaast kan uitlekken wie potentieel besmet is door wie. Dit kan gevolgen hebben voor alle betrokkenen.

Geadviseerd wordt om de volgende maatregelen te nemen:

- Autorisaties wekelijks controleren;
- Het invoeren van extra controle op de autorisaties;
- Extra aandacht besteden aan het belang van het verstrekken en het intrekken/wijzingen van autorisaties.;
- Extra aandacht te besteden bij de nieuwe applicatie aan de mogelijkheid om automatisch autorisaties in te trekken bijvoorbeeld na 3 dagen bij het niet inloggen van ingehuurde BCO-medewerkers;
- Nieuwe rollen voor ingehuurde BCO-medewerkers opstellen.

Risico voor Betrokkene (voor maatregelen)	Hoog
Risico voor Betrokkene (na maatregelen)	Laag

Restrisico: HPZone Lite wordt vervangen door een nieuwe applicatie. Op moment van schrijven is nog niet duidelijk wanneer deze wordt geïmplementeerd. Tot die tijd kunnen extra controles op de autorisaties het risico op datalekken en misbruik worden verkleind. Houdt bij de nieuwe applicatie rekening mee met het eventueel automatisch kunnen intrekken van bepaalde autorisaties nadat een bepaalde periode niet is ingelogd. Daarnaast zijn er verschillende partijen, waarbij het moeilijk is te controleren of zij doen wat is overeengekomen en fouten gemaakt kunnen worden in het verstrekken van autorisaties. Zorg ervoor dat de verantwoordelijkheden helder zijn en maak afspraken welke organisatie het beheer van autorisaties op zich neemt. Het meest praktisch is om dit te beleggen bij de organisatie die zicht het op het in- uit en doorstromen van de (ingehuurde) medewerkers.

2. Onvoldoende controle op en monitoring van logging leidt tot niet opsporen van onrechtmatige verwerkingen.

Voor de uitvoering van de werkzaamheden van de medewerkers is het noodzakelijk dat wordt gelogd wat de medewerkers in de dossiers doen. Dit betekent dat gecontroleerd wordt of de handelingen die zei uitvoeren met betrekking tot de persoonsgegevens rechtmatig zijn. Dit kan door controle van de logging. Indien deze controle niet wordt uitgevoerd, kunnen onrechtmatige verwerkingen niet worden opgespoord en afgehandeld.

- De kans dat het risico zich manifesteert is hoog. Medewerkers worden ingezet bij GGD 'en, die zelf moeten monitoren. Het is niet bekend of deze logging bij iedere GGD wordt

gecontroleerd en of wordt gekeken naar de BCO-medewerkers van de landelijke schil die worden ingezet.

- De impact van het datalek is hoog. Het aantal gegevens waar toegang toe wordt gekregen, bevatten gegevens die gevoelig zijn, zoals medische gegevens, maar ook gegevens die extra beschermd worden, zoals een BSN. Het uitlekken van deze persoonsgegevens kan grote gevolgen hebben, zoals fraude met deze persoonsgegevens.

Geadviseerd wordt om de volgende maatregelen te nemen:

- Zorg dat met iedere verwerker en met de GGD 'en wordt afgesproken dat de logging is ingeschakeld en periodiek wordt gecontroleerd. Controle van de logging is een verantwoordelijkheid van de GGD 'en. Voor de controle is een procedure nodig, waarbij rekening wordt gehouden met de omstandigheden waaronder wordt gewerkt, het aantal mensen dat werkt en het aantal persoonsgegevens dat wordt verwerkt.
- Zorg voor een uniforme werkwijze bij het opsporen van onrechtmatige activiteiten en indien opzettelijk, de sancties die worden gegeven.
- Maak medewerker bewust van het feit dat logging plaatsvindt en dat hierop wordt gemonitord. In sommige gevallen kan dit gezien worden als een personeelsvolgsysteem en dient goedkeuring nodig te zijn van de Ondernemingsraad.

Risico voor Betrokkene (voor maatregelen)	Hoog
Risico voor Betrokkene (na maatregelen)	Midden

Het restrisico is dat door de grote aantallen medewerkers, die constant wisselen en die thuis werken, de kans op fraude en onrechtmatig gebruik blijft bestaan. Er is geen controle op de werkvloer en met periodieke controle kan niet alles worden gecontroleerd. Zo kan een kwaadwillige medewerker niet worden opgemerkt.

3. Medewerkers werken vanuit huis met hun eigen apparaten, wat kan leiden tot situaties waarin persoonsgegevens onrechtmatig worden verwerkt.

Medewerkers werken thuis, wat betekent dat andere personen aanwezig kunnen zijn en gebruik kunnen maken van het thuisnetwerk. Dit betekent dat huisgenoten onrechtmatig gegevens kunnen horen of zien, indien de medewerker werkt op een locatie waar andere aanwezig zijn.
Daarnaast kunnen mensen die op hetzelfde netwerk werken, toegang krijgen tot de gegevens die via dat netwerk worden verstuurd. Hierdoor kan onrechtmatige inzage van gegevens mogelijk zijn.
Ten slotte gebruiken medewerkers eigen apparatuur om de werkzaamheden op uit te voeren. Medewerkers kunnen bestanden met vertrouwelijke informatie downloaden uit de beveiligde omgeving en niet/niet tijdig verwijderen. Indien deze apparatuur niet goed is beveiligd, kan worden meegekeken in de systemen van de medewerker of kunnen inloggegevens worden gestolen. Dit betekent dat fraude kan worden gepleegd met deze gegevens.

- De kans dat het risico zich manifesteert is hoog. Medewerkers werken thuis, maar vaak ook de huisgenoten. Dit betekent dat de medewerker zich altijd zal moeten afzonderen, wat voor sommige medewerkers niet mogelijk is. Ook kan een huisgenoot binnenlopen bij een gesprek. Vaak wordt door huisgenoten ook hetzelfde wifi-netwerk gebruikt, waardoor deze toegang kunnen krijgen tot de data-uitwisseling van de medewerker met het netwerk.
- De impact van het risico is hoog. Hoewel het gaat om huisgenoten, kunnen zij de persoonsgegevens opvangen. Hierdoor bestaat de kans dat wordt gesproken over de casus. Als een huisgenoot de data-uitwisseling kan volgen, betekent dat dat hij met de persoonsgegevens kan doen wat hij wenst, terwijl het hier gaat om gegevens die gevoelig zijn en die gebruikt/verkocht kunnen worden om fraude mee te plegen.

Geadviseerd wordt om de volgende maatregelen te nemen:

- Stel een landelijke procedure met gedragsregels bij thuiswerken en de beveiliging van een device en het netwerk. Leg deze aan de medewerker voor en laat de medewerker deze ondertekenen/hiermee akkoord gaan. Benadruk dat deze documenten grondig moeten worden gelezen.
- Besteed bij de training aandacht aan dit onderwerp en laat dit tijdens periodieke trainingen terugkomen.
- Breng de gedragsregels voor thuiswerken en beveiliging van de device en het netwerk periodiek aan de orde bij de dag start.
- Controleer of er opties bestaan om na te gaan of de medewerker zich aan de afspraken houdt.

Risico voor Betrokkene (voor maatregelen)	Hoog
Risico voor Betrokkene (na maatregelen)	Laag

4. Onvoldoende zicht op het in- uit en doorstroom proces leidt tot niet opsporen van onrechtmatige verwerkingen.

Voor het landelijke BCO-traject heeft de intentie bestaan een convenant te sluiten tussen GGD GHOR en de GGD ‘en om duidelijke afspraken te maken over de taken van GGD GHORNL en de GGD ‘en. De optie van het convenant is afgewezen, waardoor nu geen afspraken zijn gemaakt. Dit heeft een aantal nadelen. Zo is het niet duidelijk wie welke rollen heeft. Applicatiebeheerders bij GGD ‘en moeten medewerkers van de landelijke schil rechten geven om in de systemen van de GGD te kunnen werken. Dit wordt vaak wel gedaan, maar door de drukte wordt vergeten de rechten in te trekken als de medewerker niet meer werkt voor die GGD. Daarnaast wordt vergeten de rechten op inactief te zetten als de medewerker bij een andere GGD wordt ingezet, waardoor de medewerker actieve inloggegevens heeft bij meerdere GGD ‘en, terwijl deze maar bij een GGD werkt op dat moment. Verder is niet duidelijk waar de verantwoordelijkheid ligt voor het doorgeven dat iemand van rol veranderd of uit dienst treedt. Ook blijken medewerkers met gegevens van een andere GGD voor een GGD te werken. Hierdoor wordt het moeilijk na te gaan voor welke GGD is gewerkt en of de verwerkingen die de medewerker heeft uitgevoerd rechtmatig zijn, waardoor de kans op onder andere fraude toeneemt en fouten minder snel kunnen worden opgespoord.

CONCEPT

Dit geldt ook voor het geven van meerdere accounts aan een landelijke BCO-medewerker. Hierdoor hebben landelijke BCO-medewerkers toegang tot de omgevingen van meerdere GGD 'en, wat betekend dat ze altijd in al deze omgevingen in kunnen loggen. Dit verhoogt de kans op onrechtmatige toegang en fraude, en verkleint die kans op detectie van deze onrechtmatige toegang en fraude.

De applicatiebeheerder krijgen elke maand van HR een lijst met alle medewerkers die in dienst zijn. Deze wordt vergeleken met de autorisatielijst. Het resultaat is een lijst met gegevens van (oud) medewerkers die nog geautoriseerd zijn voor HPZone Lite. Applicatiebeheerders sturen maandelijks deze lijst met bevindingen naar alle projectleiders van team corona met de vraag of de lijst van medewerkers nog actueel is. Hier wordt door drukte en de onduidelijkheden wie verantwoordelijk is voor dit onderdeel van het proces niet altijd opvolging aan gegeven.

In het verleden werd ook het privéadres gebruikt. Deze worden op moment van schrijven nog opgeschoond.

- De kans dat het risico zich manifesteert is hoog. De medewerkers kunnen gewoon bij de gegevens tot de autorisaties worden ingetrokken of gewijzigd. Dit in combinatie met de maandelijkse monitoring en de onduidelijkheid omtrent de verantwoordelijkheden zorgt ervoor dat niet kan worden achterhaald dat er iets fout gaat en de kans op onrechtmatige toegang groot is. Met multipels accounts kunnen medewerkers gelijktijdig toegang krijgen tot de verschillende omgeving waarbij deze medewerkers toegang krijgen tot persoonsgegevens van verschillende omgevingen.
- De impact is hoog. Indien deze gegevens door verlies of fraude bekend worden gemaakt, ondervinden betrokkenen grote gevolgen.
- De kans dat het risico zich manifesteert is hoog. Door een gebrek aan afspraken is het onduidelijk wat de taken van de partijen zijn. Hierdoor kan verwarring bestaan in het verwerken van de persoonsgegevens.
- De impact van het risico is hoog. Onrechtmatige of onjuiste verwerking van de gegevens kan grote gevolgen hebben voor de persoonsgegevens van de betrokkene, maar ook de manier waarop zij op de hoogte worden gebracht over een eventuele besmetting.

Geadviseerd wordt om de volgende maatregelen te treffen:

- Stel eenduidige maatregelen rond het intrekken en op inactief zetten van accounts, zodat medewerkers geen toegang blijven houden tot een of meerdere omgevingen van de GGD.
- Maak GGD 'en bewust dat ook moet worden gezorgd voor voldoende capaciteit bij de functioneel beheerders die de activatie en de activatie van accounts verzorgen.
- Maak GGD 'en bewust van de risico's en promoot een adequate logging en monitoring daarvan.
- Maak key-users bewust van hun verantwoordlijkheden.
- Stel een overeenkomst op, bij voorkeur een convenant, waarin wordt geregeld wie welke rol heeft en welke taken de partijen hebben.

CONCEPT

- Maak bij het implementeren van de nieuwe applicatie duidelijke afspraken wie verantwoordelijk is voor de autorisatie.

Risico voor Betrokkene (voor maatregelen)	Hoog
Risico voor Betrokkene (na maatregelen)	Midden

Het restrisico is dat GGD 'en focussen op de bestrijding van corona, en daarbij vergeten in de haast en door het niet verhogen van de capaciteit van het aantal functioneel beheerders, accounts onrechtmatig op actief blijven staan. Dit geldt ook voor medewerkers en GGD 'en die medewerkers op een account laten werken. Hoe drukker het wordt met BCO, hoe hoger dit restrisico.

5. Betrokkenen worden onvoldoende geïnformeerd over de verwerking van persoonsgegevens in BCO.

Voor betrokkenen is een privacyverklaring opgesteld naar de stand van zaken op dat moment. Indien er wijzigingen zijn, zullen die worden doorgevoerd in de privacyverklaring. Betrokkenen in het BCO-traject worden echter gebeld, wat betekent dat ze vooraf niet weten of ze gebeld worden en dus niet vooraf kijken naar de privacyverklaring. Dit betekent dat betrokkenen in het gesprek op de hoogte moeten worden gebracht over de verwerking van hun persoonsgegevens en indien nodig toestemming moet worden gevraagd voor het opnemen van het gesprek en wat dit betekent voor de verwerking van de opname. Dit zal voor iedere GGD gelijk moeten zijn, zodat geen verwarring ontstaat in de uitleg.

Indien de betrokkene niet wordt geïnformeerd, wordt niet voldaan aan de verplichtingen uit de AVG. Indien de verwerking op toestemming berust en de betrokkene de toestemming niet geïnformeerd is gegeven, dan is de verwerking onrechtmatig.

- De kans dat het risico zich manifesteert is hoog. De callscripts zijn niet doorgenomen op de eisen de gesteld worden met betrekking tot de informatieplicht, waardoor het aannemelijk is dat de benodigde informatie niet wordt verstrekt.
- De impact van het risico is hoog. De persoonsgegevens van de betrokkene zullen worden verwerkt zonder dat de betrokkene op de hoogte is wat deze verwerking inhoudt. Dit betekent dat ze niet de keuze kunnen maken wat ze wel en niet verstrekken. Daarnaast geven ze toestemming voor een opname waarvan ze niet weten wat daarmee gebeurt.

Geadviseerd wordt om de volgende maatregelen te nemen:

- Stel callscripts op en laat ze controleren op de informatieverstrekking en de wijze waarop toestemming wordt gevraagd.
- Bespreek de callscripts met een aantal GGD 'en en stel deze vast.
- Laat wijzigingen checken op de informatie en de verdeel deze aan de regionale GGD 'en.

Risico voor Betrokkene (voor maatregelen)	Hoog

CONCEPT

Risico voor Betrokkene (na maatregelen)	Laag

6. BCO-medewerkers verwerken bijzondere persoonsgegevens, waarbij de gegevens niet op de meest adequate wijze worden verwerkt.

BCO-medewerkers verwerken bijzondere en gevoelige gegevens. Hieronder vallen het BSN en medische gegevens, namelijk een besmetting met corona van de index en een potentiële besmetting van de contacten. BSN wordt door de BCO-medewerkers actief uitgevraagd in outbound gesprekken. Dit is niet in lijn met de fraude bestrijdende richtlijn dat overheden niet om BSN vragen als de overheid zelf belt. Voor de medische gegevens geldt dat normaal een arts infectieziekten betrokken is bij het proces. Door de grote hoeveelheden van besmettingen, kan niet al het BCO door artsen of medewerkers die weten wat verwacht wordt worden uitgevoerd. Daarom is gezorgd voor training en het ondertekenen van geheimhoudingsverklaringen.

- De kans dat het risico zich voordoet is hoog. Medewerkers blijven BSN uitvragen, tegen de richtlijn in, waardoor gemakkelijk door een kwaadwillende fraude kan worden gepleegd. Daarnaast zijn medewerkers zich niet altijd bewust van de risico's van het verwerken van medische gegevens. Hierdoor kunnen de persoonsgegevens onrechtmatig worden verwerkt.
- De impact van het risico is hoog. Indien fraude wordt gepleegd, kan, met de gegevens die in het BCO-traject normaal worden gebruikt, behoorlijk wat schade worden toebrengen aan de betrokkene. Dit geldt ook als de medewerker de persoonsgegevens onrechtmatig verwerkt.

Geadviseerd wordt om de volgende maatregelen te nemen:

- Vraag geen BSN bij het outbound bellen.
- Indien geverifieerd moet worden met het BSN, zorg dan dat enkel wordt geverifieerd met de laatste drie cijfers van het BSN en communiceer dit ook helder in communicatie rond de uitvoering van BCO, zowel naar de medewerkers als de betrokkenen.
- Zorg voor periodieke training van medewerkers en heldere werkinstructies over de verwerking van de persoonsgegevens in het kader van BCO.

Risico voor Betrokkene (voor maatregelen)	Hoog
Risico voor Betrokkene (na maatregelen)	Laag

16. Maatregelen

Ter beveiliging van de persoonsgegevens, zijn verschillende maatregelen genomen. Deze zijn onder te verdelen in technische en organisatorische maatregelen.

Organisatorische maatregelen:

- Training van callcentermedewerkers door GGD GHOR Nederland om mensen correct te informeren over de verwerking en toestemming vast te leggen. Daarnaast organiseert GGD GHOR Nederland webinars voor medewerkers van verschillende organisaties om

CONCEPT

verschillende facetten van het proces in kaart te brengen. GGD'en en andere partijen zijn daarnaast zelf verantwoordelijk voor het trainen van medewerkers en het creëren van awareness met betrekking tot de verwerking van persoonsgegevens.

- GGD GHOR Nederland heeft afspraken met alle aangesloten partijen die persoonsgegevens verwerken om vast te leggen hoe en waarom de verwerkers de persoonsgegevens mogen verwerken.
- Afstemming met CISO en privacy specialisten om het proces zo veilig mogelijk te maken bij de verwerking van persoonsgegevens. Deze zijn betrokken bij het proces en analyses die op worden geleverd. Daarnaast is tijdens het proces telkens om adviezen gevraagd indien nodig.
- Monitoring van de logging is ingericht.
- Autorisatiematrix voor toegang tot de verwerkte gegevens.
- Indienstproces aangepast (VOG administratie)

Technische maatregelen:

- Een ketentest is uitgevoerd om te controleren of het proces loopt zoals het is beoogd te werken. Op deze wijze stroopt het proces niet op en komen gegevens niet op andere plaatsen dan waar ze moeten komen.
- In de testomgeving wordt gewerkt met testgegevens. Dit betekent dat tijdens het testen geen persoonsgegevens worden gebruikt, puur om te controleren of het systeem werkt.
- Autorisaties zijn ingericht zodat enkel bevoegde medewerkers toegang krijgen tot de persoonsgegevens.
- Externe audits zijn uitgevoerd.
- Wordt gewerkt aan een nieuwe applicatie.
- Printfuncties zijn uitgeschakeld en zoekfuncties zijn aangeoast.

CONCEPT

Bijlage 1: Achtergrond Risiconiveaus

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 de kwetsbaarheid; en
- Aanwezig zijn van bestaande maatregelen en hun effectiviteit

De kans dat een potentiele kwetsbaarheid kan worden uitgebuit door een actor zal worden omgeschreven als hoog, midden, of laag. De onderstaande tabel beschrijft deze drie lagen.

Kans	Kans beschrijving
Hoog	De actor is zeer gemotiveerd en bekwaam en maatregelen ter preventie van de uitbuiting van de kwetsbaarheid zijn ineffectief.
Midden	De actor is zeer gemotiveerd en bekwaam, maar er zijn maatregelen geïmplementeerd die de uitbuiting van de kwetsbaarheid belemmeren.
Laag	De actor mist motivatie of bekwaamheid, of maatregelen zijn geïmplementeerd om de uitbuiting van de kwetsbaarheid te voorkomen of significant te belemmeren.

Impact

De impact van een geëffectueerd risico wordt beschreven in termen van verlies of beperking van beschikbaarheid, integriteit of vertrouwelijkheid van gegevens op een schaal van laag, midden en hoog. De onderstaande beschrijvingen geven een korte omschrijving van deze aspecten en de consequentie (of impact) die daaraan verbonden is als dit doel niet behaald wordt.

Verlies van integriteit – Systeem en data integriteit verwijst naar de eis dat de juistheid en volledigheid van informatie geborgd moet zijn. De integriteit is verloren als incorrecte wijzigingen zijn aangebracht in de informatie door opzettelijk of onopzettelijk handelen. Als verlies van integriteit niet (tijdig) verholpen wordt kan verder gebruik van het gecompromitteerde systeem of data resulteren in onnauwkeurigheid, fraude of beveiligingsincidenten. Verlies van integriteit kan een eerste stap zijn in een aanval op systemen met verlies van beschikbaarheid of vertrouwelijkheid tot gevolg.

Verlies van Beschikbaarheid – Als een dienst (of gegevens aangeboden door een dienst) niet beschikbaar is voor de eindgebruikers, raakt dit mogelijk de missie van de organisatie. Verlies van systeemfunctionaliteit en operationele effectiviteit kunnen leiden tot beveiligingsincidenten of verlies van productiviteit.

Verlies van Vertrouwelijkheid – Systeem en data vertrouwelijkheid verwijst naar de bescherming tegen ongeautoriseerde openbaarmaking van gegevens (o.a. verlies van bedrijfsgeheimen, intellectueel eigendom (software, protocollen, documenten, etc.), of persoonsgegevens). Ongeautoriseerde, onverwachte, of onopzettelijk openbaarmaking van persoonsgegevens kan leiden tot het schenden van wet en regelgeving.

CONCEPT

Impact niveau	Impact Beschrijving
Hoog	Misbruik van een kwetsbaarheid: 1. Kan resulteren in het kostbare verlies van kritische assets of middelen; 2. Kan de missie, reputatie of belang van de organisatie of Betrokkene significant schaden, compromitteren of belemmeren; 3. Kan een schending van wettelijke richtlijnen veroorzaken; 4. Kan resulteren in sterfte of ernstig letsel; 5. Kan een grote inbreuk opleveren in de fundamentele rechten en vrijheid van Betrokkene
Midden	Misbruik van een kwetsbaarheid: 1. Kan resulteren in het kostbare verlies van materiële assets of middelen; 2. Kan de missie, reputatie of belang van de organisatie of Betrokkene schaden, compromitteren of belemmeren; 3. Kan resulteren in persoonlijk letsel. 4. Kan een inbreuk opleveren in de fundamentele rechten en vrijheid van Betrokkene
Laag	Misbruik van een kwetsbaarheid: 1. Kan resulteren in het verlies van bepaalde assets of middelen; 2. Kan de missie, reputatie of belang van de organisatie of Betrokkene schaden 3. Kan een kleine inbreuk opleveren in de fundamentele rechten en vrijheid van Betrokkene

Risico Calculatie

Deze stap gebruikt de kans en impact 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 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

CONCEPT

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.

CONCEPT

Data Protection Impact Assessment (DPIA) CoronIT

- Landelijke referentie DPIA voor GGD'en -

Inleiding **2**
1. Voorstel 3
2. Persoonsgegevens 4
3. Betrokken partijen en gegevensverwerking 6
4. Verwerkingsdoeleinden 11
5. Belangen bij gegevensverwerking 12
6. Verwerkingslocaties 13
7. Techniek en methode van gegevensverwerking 13
8. Juridisch en beleidsmatig kader 13
9. Bewaartermijn 13
A. Beoordeling rechtmatigheid gegevensverwerkingen **14**
10. Rechtsgrond 14
11. Bijzondere persoonsgegevens 15
12. Doelbinding 16
13. Noodzaak en evenredigheid 16
14. Rechten van betrokkenen 17
B. Beschrijving en beoordeling risico's voor de betrokkenen **19**
15. Risico's 19
C. Beschrijving voorgenomen maatregelen **28**
16. Maatregelen 28
D. Bijlagen **36**
Bijlage 1: Advies Functionaris Gegevensbescherming GGD Hart voor Brabant 36
Bijlage 2: Achtergrond Risiconiveaus 37

Inleiding

CoronIT is een webapplicatie die is ontwikkeld in opdracht van GGD GHOR Nederland door Topicus om het testproces van COVID-19 te centraliseren, automatiseren, versnellen en vereenvoudigen. Hierdoor kan de testcapaciteit ten volle worden benut en kan de verspreiding van COVID-19 beter worden gecontroleerd en bestreden. De opdracht tot het ontwikkelen van CoronIT is gegeven door ministerie van Volksgezondheid, Welzijn en Sport (VWS) aan GGD GHOR Nederland en het implementeren van deze webapplicatie is door VWS uitdrukkelijk gevraagd aan alle GGD'en. Daarnaast dient CoronIT als basis voor statistieken om de verspreiding van COVID-19 te monitoren en stuurbeslissingen te nemen om de verspreiding van COVID-19 onder controle te houden.

CoronIT is een registratiesysteem en geen medisch dossier, waarin het testproces van COVID-19 wordt gecentraliseerd, geautomatiseerd, versneld en vereenvoudigd. In CoronIT worden slechts die persoonsgegevens verzameld die noodzakelijk zijn om te bepalen of iemand klachten heeft en getest kan worden, de test uit te laten voeren en het resultaat terug te kunnen koppelen. CoronIT is geen medisch dossier in de zin van de Wet geneeskundige behandelovereenkomst (Wgbo) en zal ook niet als zodanig worden gebruikt. Dientengevolge is de Wpg van toepassing.

Aanvulling lokale GGD:

Inmiddels is vastgesteld dat het testproces wel een medische handeling betreft en er dus sprake is van een medisch dossier in de zin van de WGBO, zie rapport 'De Wgbo en (grootschalig) testen op COVID-19 door de GGD', opgesteld 2-7-2021.

Overal conclusie uit het rapport:

Er is sprake van samenloop tussen de (bestuursrechtelijke) Wet publieke gezondheid (Wpg)en de (privaatrechtelijke) Wet op de geneeskundige behandelingsovereenkomst (Wgbo). Als iemand zich bij de GGD (vrijwillig) laat testen, is de Wgbo naast de Wpg van toepassing. Dit geldt ook als iemand (vrijwillig) meewerkt aan bron- en contactopsporing en/of zich (vrijwillig) laat vaccineren bij de GGD.

Dit betekent dat de basis voor de verwerking in de webapplicatie de Wet publieke gezondheid (Wpg) en de Wet geneeskundige behandelingsovereenkomst (Wgbo) is. De te nemen maatregelen & aanbevelingen n.a.v. van deze wijziging worden meegenomen in de lokale DPIA Testproces, die afzonderlijk opgesteld zal worden.

In CoronIT worden de gegevens verwerkt met betrekking tot de infectieziekte die verplicht zijn gesteld te melden aan de GGD door de arts die de infectieziekte vermoed of vaststelt. Dit betekent dat in CoronIT persoonsgegevens worden verwerkt, en daarbij ook bijzondere persoonsgegevens. De autoriteit Persoonsgegevens heeft een lijst gepubliceerd[1] van soorten verwerkingen waarvoor

[1] https://autoriteitpersoonsgegevens.nl/nl/zelf-doen/data-protection-impact-assessment-dpia#voor-welke-soorten-verwerkingen-is-het-uitvoeren-van-een-dpia-verplicht-6667

een DPIA verplicht is[2]. In deze lijst wordt gesteld dat voor gezondheidsgegevens een DPIA dient te worden uitgevoerd. Dientengevolge wordt voor de webapplicatie CoronIT een DPIA uitgevoerd.

Lokale aanvulling:

In een later stadium is door VWS en GGD GHOR besloten dit registratiesysteem, CoronIT, ook te gebruiken voor het vaccinatieproces.

Out of scope

Deze DPIA ziet sec op de webapplicatie CoronIT en de registratie in deze webapplicatie t.b.v. het (landelijke) testproces. Voor een uitgebreide risicoanalyse van het lokale GGD testproces (dus daadwerkelijke afname van testen / lokale proces) en het vaccinatieproces en de daarbij behorende verwerking van persoonsgegevens wordt verwezen naar de opgestelde DPIA's voor het uitvoeren van het testproces en het lokale vaccinatieproces. Het callcenter en de opzet van het portaal zijn tevens geen onderdeel van deze DPIA. Deze onderdelen zullen in een aparte DPIA worden uitgewerkt door de GGD GHOR.
De referentie DPIA CoronIT van GGD GHOR is gebruikt als basis voor deze DPIA. Er worden aanvullingen gedaan ten opzichte van de elementen waar het regionale proces afwijkt van de landelijke instructies.

DPIA: landelijke format voor GGD'en

Het model gegevensbeschermingseffectbeoordeling Rijksdienst (PIA) is gebruikt als uitgangspunt voor het opstellen deze DPIA.

Beschrijving kenmerken gegevensverwerkingen

1. Voorstel

Voorstel

Verwerking van persoonsgegevens in CoronIT

Om te zorgen dat het testproces van COVID-19 en de verstrekking van de daaruit volgende uitslag centraal, automatisch, versneld en eenvoudig verloopt, is CoronIT (een webapplicatie) ontwikkeld. In de webapplicatie worden door de aanvrager (bedrijfsarts, instellingsarts, GGD medewerker) of de betrokkene zelf via een callcenter of portaal) de persoonsgegevens die noodzakelijk zijn voor het testen van de betrokkene ingevuld en wordt vervolgens een afspraak gepland. Aanvullende gegevens worden ingevuld als de betrokkene dit wenst. De gemaakte afspraak wordt automatisch bevestigd aan de betrokkene en voor de afspraak plaatsvindt via e-mail, het plan bestaat om de betrokkene een herinnering per SMS, indien de betrokkene dit wenst. De betrokkene wordt getest bij een teststraat van de GGD. Hier worden de door de aanvrager ingevulde gegevens gecontroleerd, waarna bij de betrokkene een monster wordt afgenomen. Het afgenomen monster

[2] Zie hiervoor ook: "Besluit inzake lijst van verwerkingen van persoonsgegevens waarvoor een gegevensbeschermingseffectbeoordeling (DPIA) verplicht is, Autoriteit Persoonsgegevens" in de Staatscourant 2019 nr. 64418 van 27 november 2019.

van de betrokkene wordt door de GGD naar het laboratorium gestuurd. Het betreft hier laboratoria waarmee de GGD afspraken heeft gemaakt inzake het opsturen van monsters. Na ontvangst, worden de monsters door het laboratorium getest en worden de daaruit volgende uitslagen in CoronIT geladen. De aanvrager krijgt een melding via e-mail dat de uitslag bekend is en kan zich inloggen in de webapplicatie CoronIT om de uitslag te raadplegen. De betrokkene krijgt de uitslag van de test telefonisch via het callcenter of de aanvrager. Daarnaast zal een beveiligd portaal worden opgezet, waar betrokkenen zich kunnen aanmelden voor een test en waar ze de uitslag in kunnen zien.

VWS heeft GGD GHOR Nederland de opdracht gegeven om het proces te stroomlijnen en CoronIT te ontwikkelingen. GGD GHOR Nederland treedt voor CoronIT op als opdrachtgever voor de ontwikkeling van de applicatie, contactpersoon met Topicus en verantwoordelijke voor het functioneel beheer.

Aanleiding
VWS heeft GGD GHOR Nederland de opdracht gegeven om een webapplicatie te laten ontwikkelen en deze door alle GGD'en te laten implementeren om zo het testproces van COVID-19 en het communiceren van de uitslag te centraliseren en te zorgen voor een gelijke handelswijze. Daarnaast wordt de data uit CoronIT gebruikt als stuurdata tegen de verspreiding van COVID-19 en, wellicht, voor wetenschappelijk onderzoek.

2. Persoonsgegevens
Binnen CoronIT worden persoonsgegevens verwerkt. De gegevens die optioneel zijn, worden enkel gevuld als dit de wens van de betrokkene is. In de onderstaande tabel is per persoonsgegeven weergegeven om wat voor type persoonsgegevens (gewone, bijzondere of wettelijke identificerende) het gaat.

Persoonsgegeven	**Gewoon persoonsgegeven**	**Bijzonder persoonsgegeven**	**Wettelijk identificerend persoonsgegeven**
Voornaam en achternaam	Ja		
Geboortenaam partner (optioneel)	Ja		
Voorletters/roepnaam (optioneel)	Ja		
Postcode	Ja		
Huisnummer	Ja		
Straatnaam	Ja		
Woonplaats	Ja		
Gemeente	Ja		

Land	Ja		
Gekoppelde GGD	Ja		
Telefoonnummer (optioneel)	Ja		
E-mail	Ja		
Geslacht	Ja		
BSN			Ja
Barcode buisje	Ja		
Documentnummer	Ja		
Patiëntnummer	Ja		
Huisarts	Ja		
Adres huisarts	Ja		
Apotheek betrokkene	Ja		
Of de persoon de laatste 2 weken heeft gewerkt en zo ja, waar	Ja		
Checklist klachten		Ja	
Aantal afgenomen tests			
Testuitslag		Ja	

De checklist met klachten wordt door de aanvrager doorgenomen met de betrokkene. De checklist wordt doorgenomen en als er sprake is van de klacht, wordt deze aangekruist. De klachten zijn de volgenden:

- Koorts/verhoging
- Hoesten
- Keelpijn
- Benauwdheid of kortademigheid
- Heftige spierpijn
- Neusverkouden
- Reukverlies
- Smaakverlies
- Geen van deze

Indien er sprake is van andere klachten, wordt gevraagd contact op te nemen met de huisarts.
Daarnaast wordt gevraagd:

- Sinds wanneer de betrokkene de klachten heeft;
- Of de betrokkene direct intensief contact heeft gehad met mensen die besmet waren met corona (minder dan 1,5 meter, meer dan 15 minuten);
- Of de betrokkene de afgelopen 2 weken heeft gewerkt;
- Als de betrokkene in de afgelopen 2 weken heeft gewerkt: waar dat dan was (keuze uit een lijst).

3. Betrokken partijen en gegevensverwerking

Betrokken partijen en rolverdeling
In deze paragraaf worden de betrokken partijen inclusief hun rol binnen de verwerking beschreven. Indien er tussen partijen een verwerkersovereenkomst nodig is, staat dat aangegeven in deze paragraaf.

1. Ministerie van Volksgezondheid - *opdrachtgever*
   Het Ministerie van Volksgezondheid (in de vorm van de minister) is verantwoordelijk voor het leiding geven aan de bestrijding van epidemieën van infectieziekten categorie A (art. 7.1 Wpg). In dat kader zijn ze opdrachtgever aan GGD GHOR Nederland met betrekking tot het ontwikkelen van een efficiënt en gecoördineerd testproces, dat is uitgewerkt in CoronIT.

2. GGD GHOR Nederland – G*ezamenlijk verwerkingsverantwoordelijke met GGD'en*
   GGD GHOR Nederland is de landelijke koepel van de GGD'en en heeft de opdracht van VWS gekregen om een applicatie te laten bouwen en landelijk binnen alle GGD'en te implementeren om het testproces van COVID-19 te centraliseren, automatiseren, versnellen en vergemakkelijken, om zo ervoor te zorgen dat meer mensen kunnen worden getest. Omdat GGD GHOR Nederland vanuit de coördinerende rol invloed heeft op de verwerking van persoonsgegevens door GGD'en, is GGD GHOR Nederland samen met alle GGD'en (voor de eigen gegevens van de GGD) verantwoordelijk voor de verwerking van de persoonsgegevens in CoronIT. De verantwoordelijkheden van GGD GHOR Nederland en de GGD'en zijn vastgelegd in het 'Convenant gegevensuitwisseling gezamenlijk verantwoordelijken'. GGD GHOR Nederland heeft daarbij enkel inzage voor het ondersteunen bij het functioneel beheer, als inzage in gegevens noodzakelijk is voor dit functioneel beheer. Daarnaast hebben medewerkers van het callcenter toegang tot CoronIT, maar dat is geen onderdeel van deze DPIA.

   GGD GHOR Nederland is verwerker voor het aanleveren van rapportages naar het RIVM en de GGD´en. De GGD´en vragen databestanden uit CoronIT op en deze worden opgesteld naar de wensen van de GGD´en. Daarnaast worden rapportages opgemaakt voor het RIVM, zodat de GGD´en deze niet apart aan hoeven te leveren.

   GGD GHOR Nederland is daarnaast verantwoordelijk voor de helpdeskfunctie in het kader van het functioneel beheer en de verwerking van persoonsgegevens in het kader van deze functie. GGD GHOR Nederland zou voor deze taken gekwalificeerd kunnen worden als verwerker.

   De verantwoordelijkheden van GGD GHOR Nederland en de GGD'en zijn vastgelegd in het 'Convenant gegevensuitwisseling gezamenlijk verantwoordelijken'.

3. De lokale GGD'en – *zelfstandig verwerkingsverantwoordelijken en tevens gezamenlijk verantwoordelijk*

De GGD'en zijn zelfstandig verantwoordelijk voor de verwerking van de persoonsgegevens van de geteste personen in hun regio in CoronIT. GGHD GHOR Nederland zal deze gegevens niet verwerken zonder dat hiervoor aanleiding is. Die aanleiding kan een probleem in de applicatie zijn die wordt gemeld vanuit een GGD of een vraag van een GGD waarbij het noodzakelijk is dat de gegevens kunnen worden ingezien.

De GGD'en zijn gezamenlijk verantwoordelijk met GGD GHOR Nederland voor ontwikkelingen in de applicatie, waarbij GGD GHOR Nederland het enkele aanspreekpunt is naar Topicus, zoals is vastgesteld in het convenant. Op deze wijze komen verzoeken via GGD GHOR Nederland binnen en kan worden dat Topicus indien nodig op de hoogte wordt gebracht en dubbele vragen worden voorkomen.

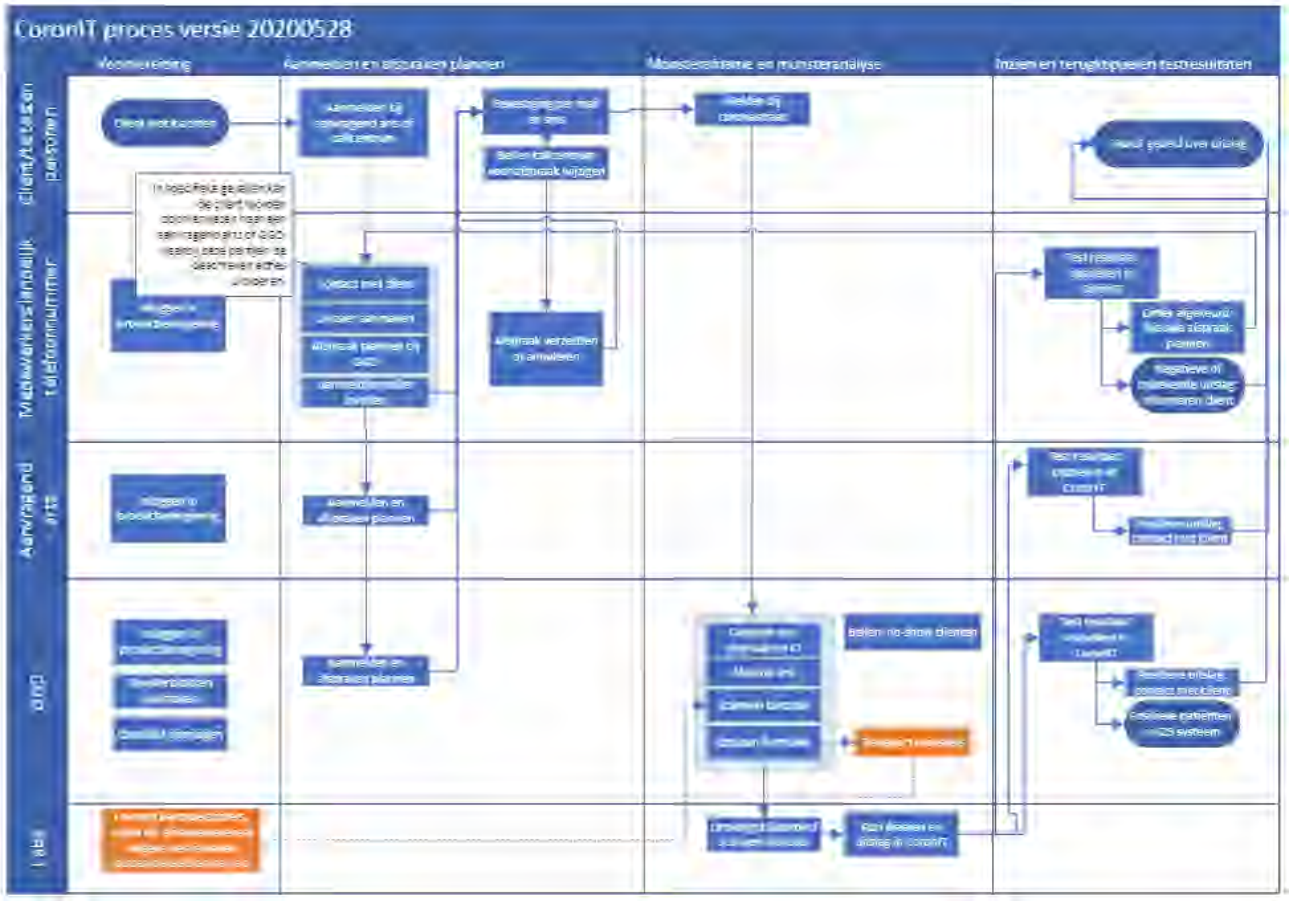
4. RIVM – *zelfstandig verwerkingsverantwoordelijke*
   Het RIVM krijgt een gepseudonimiseerde lijst met data aangeleverd door GGD GHOR Nederland op basis van art. 28 Wet publieke gezondheid. Het RIVM gebruikt deze gegevens om rapportages op te kunnen stellen, die dienen als stuurinformatie tijdens de COVID-19 pandemie voor VWS. Het RIVM bepaalt hoe deze gegevens worden geanalyseerd en gebruikt voor rapportages.

5. Topicus – *verwerker*
   Topicus heeft de applicatie in opdracht van GGD GHOR Nederland ontwikkeld en zorgt voor het technisch beheer. Om de applicatie technisch te kunnen beheren, hebben ze toegang tot de data, die zij enkel in kunnen zien als dit noodzakelijk is voor het technisch beheer. Tussen Topicus en GGD GHOR Nederland (als vertegenwoordiger van de GGD'en zoals vastgesteld in het convenant) is een verwerkersovereenkomst gesloten.

6. Externe aanvragers – *Zelfstandig verwerkingsverantwoordelijke*
   Externe aanvragers zijn in dit geval alle externen die gegevens invoeren voor de betrokkene. Zij krijgen allen inloggegevens om de betrokkene aan te melden voor een test en om de afspraak in de plannen. Vervolgens krijgen zij de uitslag ook teruggekoppeld. Zij zijn verantwoordelijk voor de gegevens die zij verwerken in dit proces. Hier zijn externe aanvragers arbo- en instellingsartsen.

7. Laboratoria – *Zelfstandig verwerkersverantwoordelijke*
   Laboratoria ontvangen van de GGD'en monsters om te analyseren op besmetting met COVID-19. Er zijn verschillende labs in de keten, namelijk de labs die al voor de GGD'en werkten, maar ook labs die zijn bijgeschakeld om de hoge aantallen monsters te kunnen analyseren. Het landschap en de afspraken met de labs zijn daarom verspreid. Dat geldt ook voor de gegevens die naar de labs gaan. Landelijke labs ontvangen vaak enkel een barcode, soms aangevuld met een geboortedatum, terwijl labs bij GGD'en meer informatie over de persoon kunnen ontvangen.

Gegevensverwerking en rolverdeling
In deze paragraaf wordt weergegeven welke stappen worden genomen in het testproces in CoronIT en wie deze stappen uitvoert. Hieronder wordt grafisch weergegeven welke partijen welke stappen uitvoeren. De voorbereiding van de teststraat is niet meegenomen, omdat dit proces niet binnen CoronIT valt, maar wel illustreert hoe het testproces verloopt.



<u>Voorbereidingen teststraat</u>
De medewerkers van de GGD zorgen dat het rooster van de medewerkers van de teststraat het rooster uploaden in CoronIT. Hierbij wordt gezorgd dat de capaciteit in de teststraat overeenkomt met het rooster in CoronIT.

Daarnaast wordt gezorgd dat alle juiste afnamematerialen beschikbaar zijn op de teststraat. Het betreft hier:

- Buisjes met een barcode;
- Correcte swabs;
- PBM;
- Laptops en scanners.

Op locatie zijn mensen beschikbaar voor het aanmelden van de betrokkene en het koppelen van de betrokkene aan het correctie buisje via de scanners op locatie.

Voor het transport zijn transportafspraken gemaakt, waarin is vastgesteld wanneer en door wie de buisjes worden opgehaald voor analyse in het laboratorium (MML's en landelijke labs).

De medewerkers hebben, voordat zij in de teststraat zullen werken, instructies gekregen en een korte training gevolgd om de werkzaamheden correct uit te kunnen voeren.

De betrokkene komt op afspraak en heeft ook informatie gehad over wie moet worden gebeld om de afspraak te verzetten.

Stap 1: Verzoek betrokkene tot testen

De aanvraag tot testen kan op verschillende manieren worden ingediend. De volgende opties zijn beschikbaar:

- De betrokkene kan een verzoek indienen om een test te laten uitvoeren bij een aanvrager (arts, bedrijfsarts, GGD). De betrokkene dient het verzoek in en zal contact op moeten nemen met een aanvrager om te verzoeken te worden getest. Deze route is de minst gebruikte route voor testen bij de GGD.
- De betrokkene kan bellen naar het landelijke callcenter. Een medewerker zal eerst een boodschap horen over wanneer ze getest mogen worden en wat aanvullende informatie, waarna en medewerker de betrokkene te woord zal staan. De medewerker controleert of de betrokkene voldoet aan de in het beleid vastgestelde testeisen. Deze optie is verder uitgewerkt in de DPIA callcenter.
- De betrokkene kan een afspraak maken via het burgerportaal. Hierbij vult de betrokkene eerst een aantal vragen in met betrekking tot de mogelijkheid om de teststraat te bereiken en de klachten, waarbij vervolgens wordt beoordeeld of de betrokkene zelf de afspraak kan inplannen door in te loggen met DigiD en de testlocatie en tijd te kiezen. Deze optie is verder uitgewerkt in de DPIA burgerportaal.

Stap 2: Checklist klachten en plannen van de afspraak

Indien de betrokkene contact opneemt met een aanvrager, zal de aanvrager starten met het doornemen van een checklist met klachten. Aan de hand daarvan wordt besloten of de betrokkene mag worden getest. Indien uit de checklist blijft dat er klachten zijn en dat de betrokkene mag worden getest, zal de aanvrager in CoronIT de persoonsgegevens van de betrokkene invoeren in een dossier (zoals benoemd in 2. Persoonsgegevens), alsook de gegevens uit de anamnese die is afgegeven en overeenkomen met de gegevens gesteld in art. 24 Wpg. Vervolgens opent de aanvrager het rooster van de GGD waar de persoon zal worden getest en een afspraak inplannen.

Indien de betrokkene zich aanmeld via het callcenter, zal de medewerker de gegevens van de betrokkene registreren en de checklist met klachten met de betrokkene doornemen. Indien er klachten zijn, zal de medewerker een afspraak inplannen. In sommige gevallen wordt de betrokkene direct doorverwezen naar de GGD, waar het proces verder wordt afgehandeld. De medewerker van het callcenter plant een test in voor de betrokkene.

De betrokkene ontvangt per mail een bevestiging van de afspraak met daarin de datum, tijd en locatie van de test. Tevens wordt in deze mail ook verwezen naar de privacyverklaring, zodat de betrokkene kan lezen wat met zijn/haar gegevens wordt gedaan.

Indien gewenst, krijgt de betrokkene ook een SMS-herinnering vlak voor de afspraak.

Indien de betrokkene een afspraak maakt in het burgerportaal, wordt ook een e-mail verstuurd met de afspraakbevestiging, met daarin de datum, tijd en locatie van de test. Indien gewenst, krijgt de betrokkene ook een SMS-herinnering vlak voor de afspraak.

Stap 3: Betrokkene meldt zich voor de test

De betrokkene meldt zich bij de receptie of de teststraat van de testlocatie. De medewerker van de receptie of testraat van de testlocatie controleert of de betrokkene aangemeld is in het systeem en controleert het ID.

Stap 4: Afname van het monster

De betrokkene meldt zich bij de ruimte waar het monster zal worden afgenomen. De bemonsteraar neemt het monster af en stopt dit in de buis met de streepjescode. De barcode wordt gescand en wordt in CoronIT geladen. Vervolgens wordt deze klaargelegd bij de andere monsters voor transport naar het lab.

Als de buis wordt gescand en deze is van een MML-lab, dan ontvangt de MML een laborder. Als de buis van een pandemielab is, dan wordt er niet gewerkt met lab orders. Bij de pandemielabs wordt enkel de barcode meegestuurd, op basis waarvan het monster wordt getest en de uitslag in het systeem wordt geladen.

Stap 5: Ophalen van het monster door transportdienst

De transportdienst zal, volgens afspraak met de betreffende GGD, de monsters ophalen om te worden vervoerd naar het lab dat het monster zal analyseren.

Stap 6: Aankomst in het laboratorium

Het monster wordt geregistreerd in het lab. Het MML heeft een laborder ontvangen en heeft daarbij de gegevens van de betrokkene. Een pandemielab heeft enkel de barcode.

Stap 7: Draaien run

Het lab analyseert de monsters.

Stap 8: Uitslag beschikbaar

Na analyse is de uitslag beschikbaar en wordt via een koppeling tussen de labsystemen en CoronIT in CoronIT geladen.

Stap 9: Terugkoppelen

De wijze waarop de uitslag wordt teruggekoppeld, is afhankelijk van de manier waarop de test is aangevraagd en de uitslag.

- De uitslag wordt teruggekoppeld aan de aanvrager van de test, indien deze door een aanvrager is aangevraagd. Hiervoor krijgt de aanvrager een mail waarin staat dat uitslagen bekend zijn. De aanvrager kan vervolgens inloggen in CoronIT om de uitslagen in te zien en zal vervolgens de uitslag terugkoppelen aan de betrokkene.
- Indien de aanvraag is gedaan via het callcenter, zijn er twee opties afhankelijk van de uitslag:
    - Negatief resultaat: een callcenter medewerker geeft de uitslag door;
    - Positief resultaat: de GGD van de regio waar de betrokkene is getest geeft de uitslag door.
- Indien de aanvraag is gedaan via het portaal, wordt de uitslag in het portaal geladen. Bij een positieve uitslag zal een medewerker van de GGD van de regio waar de betrokkene is getest de uitslag doorgeven.

Rapportage

Uit CoronIT worden verschillende rapportages aangeleverd. De gegevens helpen de partijen om een overzicht te houden van de pandemie en de ontwikkelingen daarin in hun werkveld. Deze rapportages zijn geanomiseerd. Voor de GGD en het RIVM zijn de gegevens gepseudonimiseerd, omdat een kans bestaat dat iemand herleid zou kunnen worden door de aangeleverde gegevens. De partijen ontvangen de volgende gegevens:

- De GGD ontvangt een rapportage met geslacht, leeftijd, postcode, uitslag, klachten. De rapportage wordt gepseudonimiseerd aangeleverd.
- Het RIVM ontvangt een rapportage met alle records van testen met geanonimiseerde patiëntgegevens (geen BSN of adres), PC3, klachten en testuitslag, op basis van art. 28 Wpg. Dit is een gespeundonimiseerde set, aangezien deze niet direct herleidbaar is.
- Het LCDK ontvangt productiecijfers, namelijk aantal (positieve) testuitslagen per dag, GGD, Laboratorium, beroepsgroep, leeftijdscategorie, geslacht en gemeente. Deze set is gepseudinimiseerd, echter lijkt de kans op herleiding zeer klein.
- LOTC
- Teleperformance, leverancier van het klantcontactcentrum ontvangt lijsten met betrokkenen die negatief zijn getest en moeten worden gebeld door medewerkers van Teleperformance.

4. Verwerkingsdoeleinden

Het doel van de verwerking is het centraliseren, automatiseren, versnellen en vergemakkelijken van het COVID-19 testproces en het geven van inzicht in de ontwikkeling van de pandemie. Met CoronIT kan het aanvragen van een test, het maken van een afspraak, het testen en het melden van de uitslag worden vergemakkelijkt en versnelt. Daarnaast krijgt de GGD direct de gegevens die verplicht gemeld moeten worden zoals beschreven in art. 24 Wpg. Ten slotte worden de gegevens zo ook op een gelijke wijze gemeld aan het RIVM conform art. 28 Wpg, op basis waarvan

stuurbeslissingen kunnen worden gemaakt. Door middel van deze stuurinformatie en stuurbeslissingen kan de verspreiding van COVID-19 worden beheerst.

5. Belangen bij gegevensverwerking

Samenleving als geheel

De samenleving als geheel heeft een aantal belangen bij het gebruik van CoronIT. Het centraliseert, automatiseert, vesnelt en vereenvoudigt het testproces, waardoor de volgende zaken gemakkelijker en betrouwbaar verlopen:

- Het testen van betrokkenen en het delen van de uitslag van de test zodat betrokkenen weten of ze maatregelen moeten nemen of niet;
- Melden van infectieziekten bij de GGD, zodat kan worden gestart met bron- en contactonderzoek indien dit nodig is;
- Het verstrekken van rapportages die inzicht geven in de verspreiding van COVID-19 en zo dienen om te sturen op het bestrijden van COVID-19;
- Door het snelle testen, weten mensen of ze kunnen blijven werken (bij een negatief resultaat) of maatregelen moeten nemen (bij een positief resultaat). Dit komt ten goede aan de volksgezondheid en de economie.

Betrokkenen

Door CoronIT kan snel en eenvoudig een betrokkene worden aangemeld en getest. De uitslag kan vervolgens snel worden teruggekoppeld aan de betrokkene, zodat deze de juiste maatregelen kan treffen om zijn/haar gezondheid te beschermen en verspreiding van COVID-19 te voorkomen. Het snelle testen kan de betrokkene ook geruststellen over de gezondheid.

GGD GHOR Nederland

Verzorgen van functioneel beheer van de applicatie, coördineren van de implementatie en het functioneren van de applicatie en het creëren van voldoende testcapaciteit. Daarnaast wordt ervoor gezorgd dat rapportages worden opgemaakt voor de GGD'en en het RIVM. Zij hebben een belang om de applicatie goed te laten lopen en de testen effeciënt te kunnen laten verlopen via CoroniT, samen met de GGD'en.

GGD

Door het inplannen van afspraken door het callcenter, een aanvrager of via het portaal, kan de GGD efficiënt testen in de teststraten en wordt het maken van afspraken uit handen genomen. De GGD zorgt voor teststraten en het doorsturen van monsters naar laboratoria, zodat de monsters snel geanalyseerd kunnen worden en de uitslagen kunnen worden gecommuniceeerd Daarnaast ontvangt de GGD snel de testresulaten van positief geteste betrokkenen, zodat ze snel kunnen starten met het bron- en contactonderzoek. Zij hebben er baat bij dat voldoende testcapaciteit bestaat om te weten wie besmet is met COVID-19 en aan de hand daarvan gericht Bron- en Contactonderzoek te kunnen doen.

RIVM

In kaart brengen van de stand van zaken en ontwikkeling van de verspreiding van COVID-19 in Nederland. De informatie uit CoronIT wordt gepseudonimiseerd verstrekt aan het RIVM en dient om te voorzien in stuurinformatie.

Ministerie van Volksgezondheid

Het ministerie, vertegenwoordigd door de minister, is op basis van de Wet publieke gezondheid (Wpg artikel 7.1) verantwoordelijk voor het coordineren van de bestrijding van epidemieen van infectieziekenten categorie A (zoals corona). Het ministerie (en de minister) hebben derhalve belang bij het op een verantwoorde manier uitbreiden van de capiciteit om testafspraken te maken.

6. Verwerkingslocaties

De gegevens die in CoronIT worden verwerkt, worden verwerkt in Nederland, dus binnen de Europese Unie.

Verwerkers is gesteld dat gegevens niet buiten de EER mogen worden verwerkt.

7. Techniek en methode van gegevensverwerking

Voor deze verwerking wordt gebruik gemaakt van:

- CoronIT (webapplicatie, geleverd door Topicus);
- Synaps (platform waarop CoronIT is gebouwd, geleverd door Topicus);
- Bemonsteringsbuisjes met barcode;
- Servers (Previder);
- Labkoppelingen (MIPS, Bodego, Philips, CompuGroup Medical);
- Tableau (tijdelijke oplossing voor oplevering rapportages, geleverd door Topicus);
- The Identity Hub (Authenticatie platform, in beheer van GGD GHOR);

8. Juridisch en beleidsmatig kader

Voor de verwerking in CoronIT is de volgende wet- en regelgeving van toepassing:

- Algemene Verordening Gegevensbescherming (AVG);
- Uitvoeringswet AVG (UAVG);
- Wet publieke gezondheid (Wpg);
- Wet op de geneeskundige behandelingsovereenkomst (WGBO) -> **aangevuld nav rapport testen GGD GHOR 2-7-2021.**

9. Bewaartermijn

Voor gegevens van een melding van een infectieziekte, is in art. 29 Wpg een bewaartermijn bepaald van 5 jaar. Dit is een maximale termijn. In praktijk zullen gegevens dus niet langer bewaard worden dan noodzakelijk is voor het in kaart brengen en bestrijden van de pandemie, met een maximum van 5 jaar. Periodiek zal worden bekeken of de gegevens nog noodzakelijk zijn.

Aanvulling lokaal:

De bewaartermijn vanuit de WGBO is 20 jaar voor medische gegevens. De uitwerking van de diverse bewaartermijnen zijn terug te vinden in de lokale DPIA Testen.

A. Beoordeling rechtmatigheid gegevensverwerkingen

10. Rechtsgrond

Het proces in CoronIT verloopt tweeledig. Ten eerste is er een aanmelding door een arts. Deze arts vermoed een COVID-19 besmetting en wil de persoon graag aanmelden voor een test. De arts plant een afspraak in CoronIT en de betrokkene krijgt daar een afspraakbevestiging. De betrokkene meldt zich vervolgens bij de GGD en daar wordt een monster afgenomen. Het monster wordt geanalyseerd door het lab, en de arts krijgt de uitslag, die aan de betrokkene wordt gemeld. COVID-19 is gekwalificeerd als een infectieziekte in categorie A.

De arts is volgens art. 21 Wet Publieke gezondheid (Wpg) verplicht een melding te maken aan de GGD indien er sprake is van een vermoeden of een vaststelling van een infectieziekte bij een patiënt. Als een arts een betrokkene aanmeldt, wordt deze getest, waarna de testuitslag aan de GGD wordt doorgegeven, om zo verder te kunnen handelen. CoronIT is op zichzelf dus geen meldsysteem, maar vanuit de testresultaten wordt wel gemeld bij de GGD wat de uitslagen waren van de test. De arts meldt daarbij alle zaken in CoronIT als anamnese zoals gesteld in art. 24 Wpg.

De tweede route voor het aanmelden voor een test, is via een callcenter of een online portaal. Hierbij kan een betrokkene zichzelf aanmelden. Via de telefoon zal door een callcenter medewerker worden gevraagd welke klachten er zijn, zodat kan worden bepaald of een test noodzakelijk is. Als de betrokkene staat op een test, zal deze worden afgenomen. Via het portaal moet de betrokkene een formulier invullen met de klachten, gelijk aan de vragen die worden gesteld door het callcenter. Als er geen klachten zijn, wordt de betrokkene verzocht het callcenter te bellen.

Het hele proces in CoronIT is gericht op het snel kunnen testen en verstrekken van de uitslag van een COVID-19 test. In het proces worden daarna de resultaten gemeld aan de GGD, zodat zij kunnen voldoen aan de wettelijke plicht die uit de Wpg op hen rust, namelijk de bestrijding van infectieziekten.

De verwerking van niet-bijzondere persoonsgegevens is toegestaan o.b.v. minimaal één van de zes grondslagen van de AVG [3]. Voor de verwerking van (gewone) persoonsgegevens in CoronIT wordt een beroep gedaan op art. 6 lid 1 sub c en e AVG:

- De verwerking is noodzakelijk om te voldoen aan een wettelijke verplichting die op de verwerkingsverantwoordelijke rust. Dit geldt voor het waar de exacte gegevens zijn bepaald, namelijk art. 24 en 28 Wpg.

[3] Artikel 6 AVG.

- De verwerking is noodzakelijk voor de vervulling van een taak van algemeen belang of van een taak in het kader van de uitoefening van het openbaar gezag dat aan de verwerkingsverantwoordelijke is opgedragen.

Er is sprake van een verplichting tot het bestrijden van de pandemie, vastgelegd in de Wet publieke gezondheid (Wpg), waarin wordt gesteld hoe moet worden gehandeld bij bestrijding van een infectieziekte. Deze bestrijding is in het algemeen belang. De Wpg biedt echter niet een specifieke handelwijze voor infectieziekten in de categorie A, waardoor niet alle verwerkingen binnen CoronIT direct beschreven zijn in de wet. De Wpg biedt echter de mogelijkheid aan de minister en veiligheidsregio's om maatregelen te nemen, waaronder de opdrachtverstrekking tot ontwikkeling van een landelijk testsysteem.+

Aanvulling lokaal:
Tevens is de WGBO van toepassing, zoals al eerder benoemd in dit rapport. Derhalve is ook art. 6 lid 1 sub b een grondslag (overeenkomst) voor de verwerking van de persoonsgegevens.

11. Bijzondere persoonsgegevens
Voor het verwerken van bijzondere persoonsgegevens is het noodzakelijk dat er een wettelijke uitzondering van toepassing is, zoals gesteld in art. 9 AVG. De verwerking valt onder de uitzondering zoals bepaald in art. 9 lid i AVG:

Art. 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, 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.

De Wpg is een lex specialis, de UAVG een lex generalis. Dit betekent dat de Wpg, die de mogelijkheid geeft tot het verwerken van (medische) persoonsgegevens voorrang heeft op de UAVG. Het is daarom niet noodzakelijk dat de UAVG een uitzondering biedt voor de verwerking in CoronIT, omdat de Wpg deze grondslag als lex specialis biedt.

De uitzonderingen in de AVG vereisen een grond in unierecht of lidstatelijk recht. Deze grond is te vinden in de Wpg en voor CoronIT in art. 6 lid 2 en 4 Wpg. Daarin is gesteld dat de veiligheidsregio zorg draagt voor de voorbereiding op de bestrijding en de bestrijding van een infectieziekte. Daarbij is door VWS besloten dat, om de bestrijding te stroomlijnen, GGD GHOR Nederland dit proces op te laten pakken en CoronIT te ontwikkelen.

In de memorie van toelichting is opgenomen dat *'de medewerking van de bevolking op vrijwillige basis aan te treffen noodzakelijke maatregelen staat immers voorop bij de infectieziektebestrijding'*. Gesteld kan worden dat dit ook geldt voor het vrijwillig aanmelden voor een coronatest.

In het kader daarvan kan worden gesteld dat in het kader van het algemeen belang (zoals gesteld in art. 9, lid 2 sub i AVG en art. 6 lid 1 sub e AVG) en op basis van de Wpg, kan worden gesteld dat het testen van de betrokkene en de registratie van eventuele symptomen wordt uitgevoerd in het algemeen belang in het kader van de bestrijding van een infectieziekte. Voor het testen en registratie is het echter noodzakelijk de betrokkene goed te informeren over de verwerking van de persoonsgegevens.

De persoonsgegevens die worden verwerkt in CoronIT, zijn enkel de gegevens die verplicht zijn om te worden opgenomen in de registratie van de GGD'en, zoals deze zijn bepaald in art. 24 Wpg als een arts een melding doet van een infectieziekte. Andere persoonsgegevens zijn optioneel, indien de betrokkene wenst dat deze gegevens ook worden opgenomen. Deze gegevens worden in de registratie opgenomen, omdat de GGD'en vanuit CoronIT de positieve uitslagen gemeld krijgen en zo de juiste informatie verstrekt krijgen. Daarnaast stelt de Wpg stelt dat een (vermoeden van) een besmetting van een infectieziekte moet worden geregistreerd. Aangezien enkel wordt getest op basis van symptomen die overeen kunnen komen met een COVID-19 besmetting, mogen deze worden geregistreerd in CoronIT.

12. Doelbinding

CoronIT is een registratiesysteem waarin een betrokkene kan worden aangemeld voor een coronatest. De betrokkene wordt geregistreerd, een afspraak kan worden gemaakt voor een test, de gegevens kunnen worden ingezien door de afnemer van de test bij het afnemen van het monster ter verificatie en de uitslag van de test kan worden geregistreerd, om zo weer te worden gemeld aan de betrokkene of de arts, indien de aanvraag door een arts is gedaan. Dit versnelt het proces en stroomlijnt de data. Het doel van de verwerking van gegevens in CoronIT is dus het uniform en efficïent testen van mensen, door het hele proces in één systeem uit te voeren.

Daarnaast worden de gegevens verstrekt aan het RIVM volgens art. 28 Wpg, dat rapportages opstelt voor VWS. Hierdoor kan VWS adequatere beslissingen nemen in de bestrijding van COVID-19.

13. Noodzaak en evenredigheid

Bij de start van het ontwikkelen van CoronIT is nagedacht hoe de COVID-19 pandemie het best kan worden bestreden. Een van de oplossingen is het stroomlijnen van het testproces, waarbij tevens direct een melding bij de GGD wordt gedaan zoals verplicht is gesteld door de Wpg. Enkel het snel kunnen testen via een landelijk systeem, zorgt ervoor dat gecentraliseerd en snel inzicht

wordt verkregen in de situatie rondom COVID-19 en dat adequate beslissingen kunnen worden genomen rond de bestrijding van COVID-19 door VWS.

Bij het ontwikkelen van CoronIT is rekening gehouden met de beginselen proportionaliteit ('Staat het belang in verhouding tot de inbreuk?') en subsidiariteit ('Is dit de beste/minst ingrijpende manier om het te bereiken?').

Wat betreft de proportionaliteit: de applicatie is opgebouwd om te zorgen dat testen op een snelle en gecentraliseerde wijze worden afgenomen. Verder worden op deze wijze de GGD'en ontlast, waardoor zij zich kunnen richten op de andere taken die zij hebben in het kader van de bestrijding van de pandemie.

Daarnaast wordt gezorgd dat de gegevens op een eenduidige wijze worden doorgezet naar de laboratoria en wordt zo het testproces versneld, zodat de betrokkene snel de uitslag van de test krijgt. CoronIT zorgt dat het hele proces gestroomlijnd wordt omdat heel duidelijk is gesteld welke persoonsgegevens per stap nodig zijn en dit de enige manier is om de persoonsgegevens te melden voor een test en dus ook voor een wettelijk verplichte melding aan de betrokkene.
Voor elk gegeven dat wordt gevraagd is er of een wettelijke grondslag in art. 24 Wpg, of is er een afweging gemaakt waarvoor deze gegevens worden verwerkt en wat de impact is van het uitvragen van dit gegeven op de persoonlijke levenssfeer van de betrokkene. Daarnaast is de betrokkene niet verplicht deze gegevens te verstrekken als hij/zij dat niet wenst.

Wat betreft de subsidiariteit: deze applicatie is gemaakt zodat het proces wordt gestroomlijnd en de gegevens snel en uniform worden gemeld. Andere applicaties zijn daardoor overbodig in het meld- en testproces, wat betekent dat een wildgroei aan applicaties en verscheidenheid aan gemelde informatie wordt vermeden. Dit zorgt ook voor rapportages die betrouwbaarder zijn en zorgen dat adequatere keuzes kunnen worden gemaakt. Daarnaast gaan er geen persoonsgegevens verloren, omdat alles in een systeem wordt verwerkt en niet overal en nergens in verschillende systemen worden verwerkt.

14. Rechten van betrokkenen

In CoronIT worden zowel gewone als bijzondere persoonsgegevens verwerkt. Omdat die persoonsgegevens worden verwerkt, hebben betrokkenen een aantal rechten, zoals bepaald in hoofdstuk III AVG. Verzoeken tot het uitoefenen van een van de rechten kunnen worden ingediend bij de GGD waar de betrokkene zich heeft laten testen. GGD'en beslissen zelf over het wel of niet uitvoering geven aan het verzoek van de betrokkene. Indien een verwijderingsverzoek is ingediend en de GGD besluit aan dit verzoek te voldoen, dan kan aan GGD GHOR Nederland worden gevraagd deze gegevens te verwijderen.

Recht op informatie (art. 13 AVG):

De betrokkene heeft recht om informatie te ontvangen over de verwerking van zijn/haar persoonsgegevens. Om deze informatie te verstrekken, wordt in de afspraakbevestiging en disclaimer vermeld dat in het kader van het testproces in CoronIT persoonsgegevens worden verzameld, waarbij wordt gelinkt naar de privacyverklaring van de gegevensverzameling in CoronIT.

Daarnaast is een privacyverklaring over de verwerking van gegevens in CoronIT online gepubliceerd op de website van GGD GHOR Nederland, waar GGD''en naar kunnen verwijzen op hun website.

Recht op inzage en afschrift (art. 15 AVG)
De betrokkene heeft het recht om zijn/haar gegevens in te zien. De gegevens kunnen worden opgevraagd bij de GGD waar de test is afgenomen en daar kan ook een afschrift worden verkregen.

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 GGD waar de test is afgenomen.

Recht op gegevenswissing (art. 17 AVG)
De betrokkene kan verzoeken persoonsgegevens te wissen. De GGD zal daar een zorgvuldige afweging voor moeten maken. Indien de GGD beslist dat de persoonsgegevens kunnen worden verwijderd, wordt een verzoek ingediend bij GGD GHOR Nederland om de gegevens te wissen.

Recht op beperking van de verwerking (art. 18 AVG)
De betrokkene kan in de door de wet bepaalde gevallen verzoeken om de verwerking van zijn/haar gegevens te beperken. Dit is enkel het geval indien de gegevens mogelijk onjuist zijn.

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 in een gangbare vorm. Indien de GGD dit direct kan doorsturen naar de gewenste ontvanger, zal dit worden verzorgd. Indien dit niet mogelijk is, zal de GGD de gegevens in een technisch gangbaar formaat aan de betrokkene overhandigen.

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 behandelen.

Recht om niet te worden onderworpen aan geautomatiseerde individuele besluitvorming (art. 22 AVG)

Er is geen sprake van geautomatiseerde besluitvorming in de zin van art. 22 AVG.

B. Beschrijving en beoordeling risico's voor de betrokkenen

15. Risico's

Uit bovenstaande analyse van de voorgestelde verwerking van persoonsgegevens zijn enkele risico's gedistilleerd. Hieronder is per risico kort uiteengezet wat het risico voor betrokkenen is en hoe dit risico gekwalificeerd dient te worden.

De kwalificatie wordt gemaakt op basis van kans x impact = risiconiveau. In bijlage 3 is een uitgebreide omschrijving opgenomen van de berekening en definities van kans, impact en risiconiveaus. Hieronder is aangegeven hoe de uiteindelijke risico calculatie plaatsvindt.

Risico Calculatie

We gebruiken de kans en impact 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.

1. *Geen logging van inzage afsprakenoverzicht*

Binnen CoronIT is geen logging aangezet op de inzage van het afsprakenoverzicht. In het afsprakenoverzicht is de naam, geboortedatum, geslacht, testlocatie, testdatum en testtijd te zien. Medewerkers kunnen zich hierdoor onrechtmatig inzage verschaffen in afspraakgegevens van betrokkenen.

- De kans dat dit risico zich manifesteert zonder maatregelen is hoog. Immers is het afsprakenoverzicht voor medewerkers toegankelijk en bijvoorbeeld snel worden gecontroleerd wanneer de afspraak van iemand is gepland.
- De impact van dit risico zonder maatregelen is middel. De gegevens bevatten geen medische gegevens, maar wel waar iemand op een exact moment te vinden is.

Geadviseerd wordt om de volgende maatregelen te nemen:

- Activeer logging op het afsprakenoverzicht, zodat duidelijk is wie zich wanneer toegang heeft verschaft tot het afsprakenoverzicht. **-> actiepunt GGD GHOR**;

Risico voor Betrokkene (voor maatregelen)	Hoog
Risico voor Betrokkene (na maatregelen)	Laag

2. *Geen controle op de logging*

Binnen CoronIT is logging ingeregeld, maar de logging wordt niet actief op periodieke wijze en automatisch gecontroleerd. Voor deze controle is geen beleid opgezet, zodat niet is vastgelegd hoe en door wie deze controle zal worden uitgevoerd. Hierdoor is de kans groot dat misbruik wordt gemaakt van de gegevens in CoronIT, maar dat dit niet wordt opgemerkt.

- De kans dat het risico zich manifesteert zonder maatregelen is hoog. Er zijn veel autorisaties uitgegeven voor toegang tot CoronIT, waarbij medewerkers en externen toegang hebben tot (een bepaald deel van) de gegevens. Bij de aantallen medewerkers die in dienst zijn en zijn ingehuurd, is de kans groot dat iemand, kwaadwillend of niet, onrechtmatig dossiers opent.

- De impact van het risico is hoog. In CoronIT zijn medische gegevens en het BSN opgenomen, alsook contactgegevens. Hier kan op verschillende wijze misbruik van worden gemaakt.

Geadviseerd worden om de volgende maatregelen te nemen:

- Stem met de GGD'en af wie verantwoordelijk is voor welke deel van de controle van de logging. Dit kan worden opgenomen in het convenant/een addendum bij het convenant. **Actie GGD Hart voor Brabant**
- Stel een beleid/procedure op voor de controle van de logging, dat voldoet aan de toepasselijke norm, de NEN 7513.
- Implementeer het beleid/de procedure in de organisatie en controleer zo snel mogelijk de logging. Indien dit niet met software kan, stel dan medewerkers aan die dit controleren tot de software wel beschikbaar is. Als met software wordt gecontroleerd, moet alsnog een menselijke controle worden uitgevoerd op een steekproef van de door de software gecontroleerde logbestanden.
- Zorg voor een sanctiebeleid waarin is opgenomen wat met de medewerker gebeurt indien hij niet werkt volgens de gestelde regels en zorg dat de medewerkers hiervan op de hoogte zijn.

Risico voor Betrokkene (voor maatregelen)	Hoog
Risico voor Betrokkene (na maatregelen)	Middel

Het restrisico na genomen maatregelen is dat de controle van logging niet iedere medewerker en iedere inzage van het dossier kan controleren. Hierdoor blijft een risico bestaan dat medewerkers toch onrechtmatig dossiers inzien en de gegevens misbruiken. De medewerkers werken in een groot deel van de gevallen thuis, waardoor ook geen onderling toezicht op de werkvloer bestaat.

3. Geen scheiding van toegang tussen regio's

Voor medewerkers van GGD'en is geen scheiding aangebracht tussen de regio's in CoronIT. Dit betekent dat medewerkers van de ene regio gegevens van betrokkenen in een andere regio kunnen opzoeken. Deze keuze is gemaakt op vraag van een aantal GGD'en, omdat mensen zich buiten hun regio kunnen laten testen en voor toegang tot die gegevens dan telkens een aanvraag moet worden ingediend, wat het proces vertraagd. Hierdoor is het echter mogelijk om onrechtmatig inzage te verkrijgen in de gegevens van alle inwoners van Nederland.

- De kans dat het risico zich manifesteert is groot. Er zijn veel medewerkers van GGD'en en ingehuurd personeel die gehele of beperkte toegang hebben tot CoronIT. De kans dat een van deze medewerkers zich, kwaadwillend of niet, toegang verschaft tot de gegevens.
- De impact van het risico is hoog. In CoronIT zijn medische gegevens en het BSN opgenomen, alsook contactgegevens. Hier kan op verschillende wijze misbruik van worden gemaakt.

Geadviseerd wordt om de volgende maatregelen te nemen:

- Besloten is dat het niet mogelijk is om CoronIT enkel voor de regio beschikbaar te stellen, omdat mensen zich ook regelmatig buiten de regio laten testen. Regel daarom dat, indien een dossier van iemand buiten de regio wordt geopend, breaking-the-glass is ingevoerd waarbij een reden moet worden ingegeven waarom de medewerker zich toegang wil verschaffen tot het dossier.
- Stel logging in op de breaking-the-glass inzages en controle elke toegang die via breaking-the-glass is verkregen. Op deze wijze kan worden beoordeeld of een medewerker rechtmatig inzage heeft gehad in de gegevens.
- Indien wordt gekozen breaking-the-glass niet in te stellen, dient strenge logging te worden toegepast op de verwerkingen in CoronIT.

Risico voor Betrokkene (voor maatregelen)	Hoog
Risico voor Betrokkene (na maatregelen)	Middel

Het restrisico na genomen maatregelen is dat als breaking-the-glass niet wordt aangezet en gecontroleerd, medewerkers toch onrechtmatig dossiers inzien en de gegevens misbruiken. De medewerkers werken in een groot deel van de gevallen thuis, waardoor ook geen onderling toezicht op de werkvloer bestaat. Logging kan daarbij niet iedere medewerker en iedere toegang tot de gegevens controleren.

4. *Medewerkers worden snel opgeleid en werken daarna thuis, waardoor niet adequaat kan worden gecontroleerd of ze begrijpen wat van hen wordt verwacht*

Medewerkers die extern worden ingehuurd, krijgen voor de start van de inhuur een training. Hierin wordt ook een stuk over privacy en informatiebeveiliging opgenomen. Ook krijgen ze een geheimhoudingsovereenkomst waar een en ander in wordt beschreven. Vervolgens beginnen ze met werken, in veel gevallen thuis. Hierdoor bestaat geen snelle controle of de medewerker alles begrijpt. Daarnaast is geen structuur opgezet, buiten de webinars als dit nodig blijkt, om periodiek kort het onderwerp privacy en informatiebeveiliging en dus de juiste omgang met gegevens aan te stippen. Hierdoor kunnen medewerkers, onbewust gegevens onrechtmatig verwerken.

- De kans dat het risico zich manifesteert is groot. Als enkel bij het begin van de inhuur een training wordt verzorgd, wordt in korte tijd veel informatie gegeven. Vervolgens wordt gestart met het nieuwe werk op de thuislocatie, waardoor het niet mogelijk is snel zaken na te vragen. Indien dit wel kan, kan dit gebeuren via digitale wegen, waar ook informatie kan worden meegestuurd over betrokkenen.
- De impact van het risico is hoog. Gegevens van betrokkenen kunnen op een verkeerde en/of onrechtmatige wijze worden verwerkt. Dit betekent dat er fouten in de gegevens kunnen ontstaan of gegevens onrechtmatig worden verwerkt. Hierdoor kunnen gegevens ook uitlekken, inclusief medische gegevens van de betrokkene.

Geadviseerd wordt om de volgende maatregelen te treffen: **-> actie GGD HvB**

- Stel een plan op om periodiek medewerkers te informeren over wat van hen wordt verwacht. Dit kan bestaan uit een korte presentatie, maar ook een vragenrondje. Dit moet in principe iedere organisatie zelf opstellen, echter kan ook worden gekeken in welke mate GGD GHOR Nederland hierin kan faciliteren. De vragenrondjes kunnen het best in het team worden georganiseerd.
- Stel duidelijke regels op waarin wordt gemeld wat medewerkers wel en niet mogen met de gegevens. Dit kan in de vorm van een korte lijst met gouden regels. Daarin kan bijvoorbeeld worden gemeld dat geen screenshots mogen worden gemaakt van de gegevens en dat gegevens niet via digitale media mogen worden gestuurd.
- Stel duidelijk waar medewerkers terecht kunnen met vragen en als wordt gemerkt dat een medewerker iets niet begrijpt, snel contact op wordt genomen.

Risico voor Betrokkene (voor maatregelen)	Hoog
Risico voor Betrokkene (na maatregelen)	Laag

5. *Medewerkers worden snel aangenomen en werken vaak thuis, waardoor het risico op fraude en onrechtmatige verwerking van gegevens verhoogd.*

Medewerkers worden gecontroleerd, maar werken daarna thuis en zijn nooit op locatie geweest. Ook wordt de werkplek niet gecontroleerd. Omdat geen controle op de werkplek of locatie van de werknemer/opdrachtgever bestaat, kan de medewerker sneller ongemerkt fraude plegen of de gegevens onrechtmatig verwerken. Een voorbeeld hiervan is dat huisgenoten mee kunnen kijken/luisteren met de medewerker.

- De kans dat dit risico zich manifesteert is hoog. Nadat de medewerker is aangenomen, worden weinig tot geen controles uitgevoerd over hoe de medewerker werkt en hoe zijn werkplek is ingericht.
- De impact van het risico is hoog. Gegevens van de betrokkene kunnen worden gebruikt voor fraude of op andere wijze onrechtmatig worden verwerkt. Dit kan ook door huisgenoten worden gedaan die de gegevens inzien/horen.

Geadviseerd wordt om de volgende maatregelen te treffen:

- Laat de medewerker een verklaring ondertekenen waarbij deze stelt een werkplek te hebben die aan in die verklaring opgenomen eisen voldoet.
- Laat de medewerker de juiste maatregelen treffen voor de beveiliging van zijn/haar systemen.
- Plan periodieke gesprekken met de medewerker om te vragen hoe het gaat en controleer daarbij of de medewerker werkt in een rustige ruimte zonder mensen in de buurt.
- Stel een sanctiebeleid op waarin wordt bepaald wat de sanctie is als niet aan de regels wordt voldaan en maak dit bekend bij de medewerkers.

- Voer de maatregelen met betrekking tot logging in.

Risico voor Betrokkene (voor maatregelen)	Hoog
Risico voor Betrokkene (na maatregelen)	Middel

Het risico blijft bestaan dat, zelfs met alle maatregelen, medewerkers zaken doen die niet mogen/wenselijk zijn. Als bovengenoemde maatregelen worden genomen, is de kans klein. Toch blijft de impact voor de betrokkene bij een kleine kans hoog, waardoor het risico voor de betrokkene als een medewerker toch iets onwettigs doet, bestaan.

6. *Uitwisseling van gegevens met verschillende partijen kan leiden tot onrechtmatige uitwisseling van gegevens*

De gegevens uit CoronIT zijn voor verschillende partijen interessant of van belang. Daarom vinden verschillende uitwisselingen plaats. Sommigen daarvan zijn in de wet bepaald, voor anderen wordt een grondslag gezocht. De snelle ontwikkelingen en drukte kan leiden tot onzorgvuldige afweging van de uitwisseling, waardoor gegevens onrechtmatig kunnen worden uitgewisseld.

- De kans dat dit risico zich manifesteert is middel. Over het algemeen worden de uitwisselingen op landelijk niveau aangevraagd, omdat dit voordelen oplevert. Binnen organisaties is vaak ook een lijn afgesproken om te beoordelen of de uitwisseling rechtmatig is. Er kunnen echter, door de drukte of door een medewerker die niet op de hoogte is dat een toetsing nodig is, gegevens worden uitgewisseld waar geen toetsing op is uitgevoerd.
- De impact van het risico is hoog. Vaak worden veel gegevens opgevraagd en daarbij ook de medische gegevens. Hier wordt vaak geen naam bij gegeven, maar sets kunnen naar personen worden herleid. Hoe meer informatie wordt gegeven, hoe sneller iemand kan worden herleid.

Geadviseerd wordt om de volgende maatregelen te treffen: **-> actie GGD HvB**

- Stel duidelijke richtlijnen op over de uitwisseling van data en neem daarin op dat eerst een toetsing moet plaatsvinden door iemand die daar in het kader van privacy een advies op kan geven.
- Wissel niet meer uit dan in het advies van de privacyspecialist is opgenomen. Extra gegevens kunnen namelijk leiden tot een ander advies.

Risico voor Betrokkene (voor maatregelen)	Hoog
Risico voor Betrokkene (na maatregelen)	Laag

7. *Wisselingen in partijen en verwerkingen kan leiden tot het niet maken van de juiste afspraken of onvoldoende grondslag*

CoronIT is gemaakt om te ondersteunen in het bestrijden van de coronapandemie. Dit betekent dat de verspreiding sneller of trager kan gaan, waardoor veranderingen in het beleid, de verwerking en

de partijen die meewerken ontstaan. Deze veranderingen kunnen snel gaan. Voor nieuwe partijen kan dit betekenen dat ze snel gaan meewerken, maar dat daardoor geen afspraken worden gemaakt over de verwerking van de persoonsgegevens. Wijzigingen in het beleid en/of de verwerking kunnen leiden dat snel gehandeld moet worden, waardoor een onjuiste of geen grondslag bestaat voor de verwerking.

- De kans dat het risico zich manifesteert is hoog. Continue verandering is vaak onder tijdsdruk, waardoor niet altijd kan worden nagedacht over de gevolgen van de veranderingen. Daarnaast is het snel aansluiten van partijen om het proces vlot te kunnen laten verlopen vaak belangrijk. Het opstellen van de juiste documenten en de onderhandeling daarover, vooral met betrekking tot privacy, kan daardoor worden vergeten.
- De impact van het risico is hoog. Onjuiste afspraken en geen of onvoldoende grondslag kan leiden tot onrechtmatige verwerking en/of het uitlekken van (medische) gegevens.

- Geadviseerd wordt om de volgende maatregelen te treffen: Stel een duidelijke communicatielijn in over uitwisselingen en het aansluiten van nieuwe partijen, zodat kan worden of een grondslag bestaat of kan worden bekeken of, en zo ja welke, afspraken moeten worden gemaakt.
- Controleer periodiek of er wijzigingen zijn in partijen, de verwerking of nieuw beleid/nieuwe inzichten.

Risico voor Betrokkene (voor maatregelen)	Hoog
Risico voor Betrokkene (na maatregelen)	Laag

8. *Door toename van medewerkers, tijdelijke inzet en wisseling van taken kunnen autorisaties verkeerd worden toegekend en vergeten worden in te laten trekken*

Door de grote vraag aan testen, is er een stijging in medewerkers, zowel eigen medewerkers als inhuur. Velen van hen moeten in meerdere of mindere mate rechten hebben om in te loggen in CoronIT. Door de drukte kan worden vergeten de juiste rechten voor CoronIT te verlenen, de rechten te laten wijzigen of de rechten te laten intrekken. Hierdoor kan onrechtmatige toegang worden verkregen tot de gegevens in CoronIT.

- De kans dat het risico zich voordoet is hoog. Organisaties staan onder grote druk en de medewerkers wisselen snel, waardoor een juiste administratie van autorisaties kan worden vergeten en medewerkers over het hoofd kunnen worden gezien, vooral als de rollen wisselen of iemand niet meer hoeft te werken met CoronIT.
- De impact van het risico is hoog. Medewerkers die niet in (bepaalde delen van) het dossier hoeven, kunnen zich alsnog toegang verschaffen tot de gegevens.

Geadviseerd wordt om de volgende maatregelen te treffen**:-> actie GGD Hart voor Brabant**

- Stel een regeling op waarbij wordt bepaald wie wijzigingen in rechten moet melden en waar dit moet worden gemeld in de organisatie.
- Meldt de wijzigingen zo snel mogelijk bij GGD GHOR Nederland zodat deze kunnen worden aangepast.

Risico voor Betrokkene (voor maatregelen)	Hoog
Risico voor Betrokkene (na maatregelen)	Laag

9. *Processen veranderen snel waardoor procesbeschrijvingen snel (kunnen) verouderen*

Het beleid rond testen verandert heel snel en is afhankelijk van ontwikkelingen rond de bestrijding van corona. Hierdoor kunnen processen en de daarbij behorende procesbeschrijving snel verouderen, waardoor het risico bestaat dat medewerkers niet zeker weten hoe ze moeten handelen of de update niet hebben gekregen van een verandering in het proces. Dit kan leiden tot fouten in de verwerking van persoonsgegevens.

- De kans dat dit risico zich manifesteert is hoog. Dit door de snelle wijzigingen, die niet altijd direct kunnen worden gecommuniceerd naar alle medewerkers en niet altijd direct kunnen worden omgezet in nieuwe/aangepast procesbeschrijvingen.
- De impact van het risico is middel. De aanpassingen kunnen klein zijn, waardoor de handeling vaak geen grote gevolgen hebben voor de verwerking van persoonsgegevens. Grote wijzigingen worden vaak ook via andere kanalen bekend gemaakt en zullen ook sneller en met meer aandacht door de organisatie worden gecommuniceerd.

Geadviseerd wordt om de volgende maatregelen te treffen: **-> actie GGD HvB**

- Stel een systeem op waarbij medewerkers direct op de hoogte worden gesteld van een verandering van werkwijze en dat daarbij ook dat medewerkers die thuis werken en/of medewerkers die op de dag geen dienst hebben alsnog hiervan op de hoogte worden gebracht als zij weer aan het werk gaan.

Risico voor Betrokkene (voor maatregelen)	Middel
Risico voor Betrokkene (na maatregelen)	Laag

10. *Een overzicht van alle partijen, datastromen en uitwisselingen is niet opgesteld, waardoor gegevensstromen niet in kaart zijn, persoonsgegevens onrechtmatig worden verwerkt en uitlekken.*

CoronIT is gelinkt met veel systemen. Daarnaast lopen nog processen langs CoronIT. Binnen GGD GHOR is geen totaaloverzicht van waar alle data wordt verwerkt en waar dat naar wordt uitgewisseld. Dit kan leiden tot het missen van stromen en onrechtmatige uitwisselingen, maar ook van het ontbreken van afspraken met partijen die de persoonsgegevens verwerken.

- De kans dat het risico zich voordoet is hoog. Er is geen totaal overzicht en daarom kan niet worden gezegd of alles is getoetst en of alles rechtmatig wordt uitgewisseld.

- Het impact van het risico is hoog. Gevoelige persoonsgegevens kunnen uitlekken, wat grote gevolgen heeft voor de betrokkene van wie de data is gelekt.

Geadviseerd wordt om de volgende maatregelen te nemen: **-> actie GGD GHOR**

- Breng de datastromen en afhankelijkheden rond de corona-applicaties in kaart.
- Toets na het in kaart brengen alle uitwisselingen en controleer of alle koppelingen zijn getoetst op beveiliging.

Risico voor Betrokkene (voor maatregelen)	Hoog
Risico voor Betrokkene (na maatregelen)	Laag

11. *Verschillende laboratoria zijn in de keten betrokken en gecontracteerd door verschillende partijen. Hierdoor wordt met ieder lab andere gegevens uitgewisseld en bestaat geen overzicht in de afspraken en potentiële onrechtmatigheid van de uitwisseling van persoonsgegevens.*

Aan CoronIT zijn diverse laboratoria met diverse koppelingen gelinkt. De ontwikkeling hierin is snel gegaan. GGD'en hebben vaak eigen afspraken, die van elkaar verschillen. Hierdoor kunnen de betrokkenen niet adequaat worden geïnformeerd, omdat andere afspraken, termijnen en voorwaarden worden gehanteerd. Daarnaast is niet duidelijk of met alle labs afspraken zijn gemaakt over de verwerking, wat resulteert in onrechtmatige verwerking van persoonsgegevens. Ten slotte is geen compleet overzicht van koppelingen en welke gegevens daarbij worden uitgewisseld. Dit resulteert in onrechtmatige verwerking.

- De kans dat dit risico zich voordoet is hoog. De koppelingen worden volgens standaard gemaakt en de persoonsgegevens die worden uitgewisseld zijn met de laboratoria besproken door de ontwikkelaars, maar het gebrek aan afspraken leidt ertoe dat laboratoria niet zijn gebonden aan afspraken met betrekking tot de verwerking.
- De impact van het risico is midden. De persoonsgegevens worden uitgewisseld met de laboratoria. Als de persoonsgegevens verder worden gebruikt, is dat vaak voor wetenschappelijk onderzoek en door de eigen verantwoordelijkheid van de laboratoria zullen zij dat ook volgens de regels uitwisselen.

Geadviseerd wordt de volgende maatregelen te nemen**: -> actie GGD GHOR / VWS Dienst Testen**

- Stel een algemeen convenant op voor COVID-19 analyse, zodat persoonsgegevens op een eenduidige wijze worden verwerkt en betrokkene op een eenduidige wijze kunnen worden geïnformeerd.

Risico voor Betrokkene (voor maatregelen)	Hoog
Risico voor Betrokkene (na maatregelen)	Laag

C. Beschrijving voorgenomen maatregelen

16. Maatregelen

Ter bescherming van de persoonsgegevens, zijn een aantal maatregelen genomen. Deze kunnen worden opgedeeld in technische en organisatorische maatregelen.

Organisatorische maatregelen

Informatiebeveiligingsbeleid

Binnen GGD GHOR Nederland is een informatiebeveiligingsbeleid opgesteld.

Topicus heeft een Informatiebeveilgingsbeleid, waarin 27 beleidspunten zijn opgenomen en waarin de ISO 27001 en NEN 7510 worden benoemd.

Privacybeleid

GGD GHOR Nederland heeft een privacybeleid. Dit is in 2018 opgesteld.

Geheimhoudingsverklaring

Geheimhoudingsverklaringen zijn ondertekend door personeel van GGD GHOR en externen die zijn ingehuurd door GGD GHOR Nederland voor het functioneel beheer. De geheimhoudingsverklaring wordt voorgelegd als een medewerker in dienst treedt. Voor externe medewerkers wordt de geheimhoudingsverklaring voorgelegd voor inhuur.

Van verwerkers wordt geëist dat medewerkers een geheimhoudingsverklaring hebben getekend voor hun dienstverband.

Lokale aanvulling:

Alle medewerkers van GGD HvB en of ingehuurde medewerkers ondertekenen de geheimhoudings- en integriteitsverklaring.

Bewustwording

Voor medewerkers van GGD GHOR Nederland die worden ingezet voor Corona, worden bij de start van het dienstverband trainingen georganiseerd. Daarnaast worden periodiek webinars gehouden over de werkwijze binnen CoronIT, waar telkens een ander deel uit de keten of nieuws wordt besproken. Daarbij wordt ook aandacht besteed aan hoe met de gegevens moet worden omgegaan.

Bij Topicus wordt in het onboardingstraject al bewustwording gecreëerd voor privacy en informatiebeveiliging. Daarnaast worden bewustwordingspresentaties gehouden en wordt minimaal eens per jaar een activiteit ingepland in het kader van bewustwording.

Lokale aanvulling:
Via de nieuwsbrief Corona zijn de 20 Gouden Regels gecommuniceerd naar de medewerkers van het programma Corona.

Autorisatiematrix
Een autorisatiematrix is opgesteld waarin de rollen en rechten zijn bepaald. Deze rollen en rechten zijn opgesteld voor de volgende organisaties:

- **GGD GHOR Nederland**
  Een kleine groep medewerkers van de servicedesk hebben toegang tot CoronIT. Zij mogen geen gegevens inzien tenzij dit absoluut noodzakelijk is om de vraag die hen wordt gesteld op te kunnen lossen. Daarnaast zijn er twee medewerkers die brede rechten hebben in CoronIT, waarbij ze bij alle gegevens kunnen en zaken kunnen wijzigen/verwijderen. Zo kan bijvoorbeeld worden gezorgd dat voor GGD'en gegevens kunnen worden verwijderd als ze een verwijderingsverzoek toekennen.
- **Callcenter**
  Medewerkers van het callcenter hebben toegang tot de gegevens in CoronIT om de gegevens van betrokkenen in te vullen die een afspraak willen maken en voor het terugbellen van betrokkenen, waarbij controle kan worden uitgevoerd op de juistheid van de gegevens en het resultaat. Dit is verder uitgewerkt in de DPIA callcenter.
- **Topicus**
  Medewerkers van Topicus hebben enkel toegang tot CoronIT als ze daar door GGD GHOR Nederland rechten voor hebben gekregen. Deze mogen alleen worden gebruikt om problemen op te kunnen lossen.

  Voor het synaps platform, waar CoronIT op is gebouwd, is wel toegang voor een aantal medewerkers als superuser om schermen te kunnen definiëren.
- **GGD**
  Voor medewerkers van de GGD zijn verschillende rollen gedefinieerd. Deze zijn uitgewerkt in een autorisatiematrix. De GGD heeft deze ontvangen. Als mensen toegang nodig hebben tot het systeem, kan de GGD bij GGD GHOR Nederland de autorisaties aanvragen die de nieuwe medewerker nodig heeft.

  Als een medewerker niet meer in CoronIT hoeft te werken of uit dienst gaat, moet de GGD dit melden bij GGD GHOR Nederland, zodat de autorisaties worden ingetrokken.

Overeenkomsten
Met de verschillende partijen zijn passende afspraken gemaakt over de verwerking van gegevens, zodat de gegevens niet onrechtmatig worden gebruikt. Daarnaast is, waar nodig, bepaald welke beveiligingsmaatregelen moeten worden genomen.

Met **verwerkers** zijn verwerkersovereenkomsten gesloten waarin duidelijk is gesteld welke gegevens zij mogen verwerken en hoe deze gegevens mogen worden verwerkt. Daarnaast is bepaald welke beveiligingsmaatregelen worden vereist.

Met **gezamenlijk verantwoordelijken** is een convenant gesloten waarin is bepaald welke verwerkingen worden uitgevoerd en wie verantwoordelijk is voor welke verwerkingen.

Procedure datalekken
GGD GHOR Nederland beschikt over een datalekkenprocedure.

Met de verwerkers is afgesproken dat datalekken of beveiligingsincidenten waarbij twijfel bestaat of persoonsgegevens betrokken zijn bij het beveiligingsincident altijd moeten worden gemeld aan GGD GHOR Nederland.

Met de GGD'en is afgesproken in het convenant dat GGD'en GGD GHOR Nederland op de hoogte brengen als zich een datalek (of beveiligingsincident waarbij (vermoedelijk) persoonsgegevens zijn betrokken) heeft voorgedaan. In onderling overleg wordt dan besloten wie het datalek meldt en welke maatregelen worden getroffen.

Logging en monitoring
Voor de controle van logging is geen procedure opgesteld. Controle vindt ad hoc plaats, na een vermoed of vastgesteld incident.

Wel zijn plannen opgesteld voor hoe logging dient te worden gecontroleerd voor ten minste medewerkers van het callcenter. Daarbij wordt onderzocht hoe dit geautomatiseerd kan worden.

Lokale aanvulling:
Inmiddels is het SOC – SIEM team binnen de GGD GHOR ingericht. Zij zijn verantwoordelijk voor de periodieke controle op de logging.

Gedragscodes
In de coronatijd is het niet altijd mogelijk om op een werklocatie te werken. Daarom zijn gedragscodes opgesteld over hoe moet worden omgegaan met thuiswerken en waar de beveiliging van de gebruikte computer aan moet voldoen, evenals de netwerkverbinding die wordt gebruikt.

Daarnaast zijn gedragscodes opgesteld over het gebruik van IT-middelen die zijn uitgegeven door GGD GHOR Nederland.

Van de verwerkers is geëist dat zij gedragscodes hebben opgesteld met betrekking tot IT-middelen en correct gebruik daarvan. Daarnaast wordt geëist dat afspraken zijn gemaakt met medewerkers over thuiswerken. De aanwezigheid van stukken hieromtrent bij Topicus is gecontroleerd. De

verbinding voor thuiswerken verloopt via VPN. In coronatijd is herhaald wat wordt verwacht bij thuiswerken.

Rechten van de betrokkenen en verwijdering van dossiers

Binnen CoronIT kunnn betrokkenen hun rechten uitvoeren. De verzoeken moeten worden ingediend bij de GGD waar de betrokkene is getest. De GGD maakt de afweging om het verzoek toe te kennen of af te wijzen. De GGD kan zelf inzage geven en gegevens wijzigen. De gegevens kunnen echter niet door de GGD verwijderd worden. Indien een verwijderingsverzoek wordt ingediend, moet de GGD een afweging maken of de gegevens verwijderd kunnen worden en vervolgens opdracht geven aan GGD GHOR Nederland om deze te verwijderen. Dit kan via de servicedesk. GGD'en zijn daarom zelf verantwoordelijk voor het hebben van een beleid of richtlijn met betrekking tot de rechten van betrokkenen.

Voor de verwijdering van dossiers, zijn er twee opties:

- Het dossier inactiveren: het dossier wordt dan op inactief gesteld, maar dat kan ongedaan worden gemaakt.
- Het dossier verwijderen: in dit geval is het dossier echt verwijderd.

Synaps maakt elke dag een snapshot. Deze blijven 7 dagen bewaard. Daarnaast blijven gegevens nog in de back-up bewaard tot deze worden vervangen. Pas daarna zijn de gegevens echt verwijderd.

Na de bewaartermijn moeten dossiers worden verwijderd. Dit is nog niet geautomatiseerd, maar de automatisering staat wel op de ontwikkellijst.

Procedures en plannen

Topicus heeft verschillende procedures en plannen opgezet. Dit zijn de volgenden:

- **CMDB**
  Is aanwezig.
- **Uitgifte werkmiddelen en bijbehorende gedragsregels**
  Is aanwezig. Dit wordt gedaan door facilitair beheer. Voor gebruik van de werkmiddelen worden op dat moment ook de gedragsregels verstrekt. De apparatuur wordt periodiek vervangen. Elke 3 jaar wordt een nieuwe laptop verstrekt en elke 2 jaar een nieuwe telefoon.
- **Classificatiebeleid.**
  Is aanwezig.
- **Wijzigingenbeheer.**
  Is aanwezig en opgenomen in de DAP.
- **Capaciteitsmanagement.**
  Is opgesteld en opgenomen in de DAP.

- **Continuïteitsregeling.**
  Is opgesteld en deels opgenomen in de DAP. Voor continuïteit is gezorgd voor een redundant datacenter. Als er iets bij een datacenter gebeurt, kan het andere datacenter het direct overnemen. Hierdoor is er geen down time in de applicatie.

  Voor business continuity is een bankgarantie opgesteld bij Previder. Als er iets misgaat, hebben klanten een half jaar om op zoek te gaan naar een andere oplossing.
- **Problem management**
  Is opgesteld en opgenomen in de DAP.
- **Calamiteitenplan**
  Is opgesteld.
- **Vulnerability management en patch en release management**
  Is opgesteld. Er zijn periodieke updates en er zijn bouwomgevingen voor dead code. Op deze wijze kan de dead code weg worden gehaald.

  Indien uit testen toch kwetsbaarheden blijken, worden plannen opgesteld om de kwetsbaarheden op te lossen.

  Daarnaast worden in bouwstraten testen op de code uitgevoerd en wordt gekeken of de componenten nog up-to-date zijn.
- **Procedure uitwisseling data**
  Voor personeel wordt duidelijk gemaakt dat data niet zomaar mag worden uitgewisseld. Er wordt beschreven welke data wel mag worden uitgewisseld, op welke wijze en hoe dit beveiligd dient te worden. Dit wordt vastgelegd in een interne norm, die wordt opgesteld op basis van opdrachten van de labs en GGD'en. Voorbeeld hiervan is de uitlagenlijst.
- **Hardening**
  Is aanwezig op het platform. Wordt gebouwd op basis van standaard.
- **Procedure risico analyse**
  Risico-analyses worden uitgevoerd in een cyclus van 3 jaar. Dat bestaat uit:
  - Distant risk assessments
  - Interne en externe audits
  - Continue risicobeheersing als onderdeel van de wijzigingsprocedure
- **Test management**
  Is aanwezig. Hierin is uitgeschreven hoe, welke tooling, visie en strategie. Daarnaast wil Topicus nog meer automatisch geen testen. Dat wordt nu uitgeschreven. Verder wordt bij elke release automatisch een test uitgevoerd op de code en is er een testmiddag waarbij allerlei scenario's worden doorlopen in de modules. Ook is er een smoketest waarbij de app op hoog niveau wordt doorlopen. Bij elke release krijgt GGD GHOR Nederland vervolgens 2 weken om de release te testen.
- **Leveranciersmanagement**
  Is opgenomen in een interne norm.

- **Beheersmaatregelen**
  Er wordt gewerkt naar een interne en externe norm, bovenop de certificering. Hiervoor worden action plans opgesteld. Dit is ook voor externe audits of pen-testen. Alles wordt centraal geregeld en aan acties worden deadlines gehangen. Dit wordt opgevolgd via een ticket dat wordt gekoppeld aan een team.

  Een corrective action plan is ook aanwezig.
- **Netwerkdiagram**
  Is opgesteld.

Technische maatregelen

Inregelen van autorisaties
De rechten en rollen die zijn bepaald in de autorisatiematrix, zijn ingeregeld in het systeem. Voor GGD´en is geregeld dat GGD GHOR Nederland het beheer van het systeem voert en dat GGD´en aan GGD GHOR Nederland de opdracht kunnen geven autorisaties te geven of in te trekken.

Normen
GGD GHOR Nederland tracht voor de systemen in eigen beheer te voldoen aan de voor hun toepasselijke normen, NEN 7510, 7512 en 7513.
Met verwerkers wordt overeen gekomen dat deze minstens werken volgens de NEN 7510, 7512 en 7513. De leverancier van CoronIT en het platform waarop dit draait, heeft een certificering voor de NEN 7510 en ISO 270001. Deze certificeringen zijn ingezien. Verder is met Topicus afgesproken dat zij werken volgens de NEN 7512 en 7513.

Logging
Op CoronIT wordt logging toegepast. Daarbij worden twee soorten logging bijgehouden:

- **Functionele logging (of audit trail).**
  In deze logging is te zien wat in het dossier is gebeurt. Dit betekent dat kan worden gezien welke delen van het dossier zijn geopend, door wie en wanneer. Daarnaast is te zien of er wijzingen of andere bewerkingen zijn geweest in de gegevens.

  Deze logging kan door GGD GHOR Nederland zelf worden ingezien.

  Op deze logging worden geen signalen gegeven bij afwijkingen. Er zijn hiervoor geen afwijken gedefinieerd.

  De functionele logging wordt nooit verwijderd.

- **Technische logging**

De techinsche logging geeft weer wat de applicatie wegschrijft. In principe worden hier geen persoonsgegevens in opgeslagen. Bij uitzondering kunnen echter wel zaken als een IP-adres worden opgeslagen.

De technische logging is bij Topicus op te vragen indien GGD GHOR Nederland deze in wil zien.

Op de technische logging is signalering ingericht, die in werking treedt als een drempelwaarde wordt bereikt.

Op de logging wordt logging toegepast. Deze wordt beveiligd middels keyhub.
GGD'en

Scheiding tussen systemen

Tussen de regio's van GGD'en is geen scheiding aangebracht tussen de omgevingen. Deze keuze is gemaakt omdat mensen zich buiten de regio kunnen laten testen en het dus noodzakelijk kan zijn om snel toegang te hebben tot de gegevens van een betrokkene. Er is voor gekozen geen breaking-the-glass procedure in te zetten, omdat door GGD'en is aangegeven dat dit belemmerend werkt.

PEN-test

Om te controleren of het systeem veilig is en niet kan worden gehackt of op een andere manier kan worden gecompromitteerd, zijn PEN-testen uitgevoerd. Deze test heeft zowel gecontroleerd of de omgeving zonder credentials niet kan worden gehackt, als met (gedeeltelijke) credentials. Daarnaast zijn alle aangesloten applicaties en koppelingen getest om te controleren of daar ook geen kwetsbaarheden bestaan waarmee toch toegang kan worden gekregen tot CoronIT.

Daarnaast voert Topicus periodiek PEN-testen uit om te controleren of de omgeving up-to-date en veilig blijft.

Back-up en restore

Van CoronIT worden back-ups gemaakt. Hiervoor is een procedure vastgesteld door Topicus, waarbij back-ups over verschillende periodes worden gemaakt.

Voor CoronIT is point in time recovery mogelijk, waarbij uit de database de transactielogging wordt gehaald en waarmee de back-up wordt aangevuld, om zoveel mogelijk te kunnen herstellen als dat nodig is.

De datacenters voor CoronIT zijn redundant. Als een datacanter uitvalt, kan het andere datacenter dit overnemen. Beide datacenters zijn gevestigd op een andere plaats in Nederland en worden geleverd door Previder.

Beveiliging
Ter beveiliging van het systeem is gezorgd voor een Firewall en anti-malware software, die up-to-date wordt gehouden.

Het webverkeer is encrypted met een HTTPS-protocol. Voor data in transit wordt SSL gebruikt. Op schijfniveau wordt alles geëncrypt, wat betekent dat dit ook op file niveau gebeurt.

Zaken die worden aangeleverd door Topicus, worden standaard geëncrypt, zoals bitlocker op windows laptops die worden uitgegeven.

Multifactor authenticatie
Voor CoronIT is tweefactor authenticatie ingericht. Dit is gedaan door een gebruikersnaam en wachtwoord en een authenticatie applicatie. Er kan worden ingelogd via de app Zorgportaal of de active directory van GGD GHOR Nederland. Om de authenticatie uit te voeren, wordt daarbij The Identity Hub gebruikt.

Bij Topicus is ook tweefactor authenticatie ingericht, wat verloopt via keycloack. Daarbij wordt ook gelogd wie, wanneer heeft ingelogd en waarom moet worden ingelogd. Deze logging is voor het hele team van de medewerker inzichtelijk, waardoor deze kan worden aangesproken bij onregelmatigheden. Verder is er een noodprocedure ingericht.

Scheiding met schema's op database applicaties Synaps platform

CoronIT is gebouwd op het Synaps-platform. Op dit platform draait ook de applicatie iTBC. Op de databases zijn daarom schema's ingesteld, zodat de data mensen met een autorisatie voor een applicatie geen toegang krijgen tot de gegevens in de andere applicatie.

Laboratoria en koppelingen
Labonline koppelt met de labsystemen en is onderdeel van synaps. De communicatie met laboratoria verloopt altijd via een VPN verbinding.

Er is een lijst opgesteld met de laboratoria, de koppelingen en het type data. Er zijn namelijk verschillende koppelingen met de verschillende labs. Ook is er een verschil tussen labs die enkel het nummer van het testbuisje van het monster krijgen en er zijn labs die een laborder krijgen met informatie over de geteste persoon, zoals dat bij regulier onderzoek ook gebeurt. De inrichting verandert echter elke dag. Via de labkoppeling en Labonline wordt de uitslag vervolgens weer in CoronIT geladen.

D. Bijlagen

Bijlage 1: Advies Functionaris Gegevensbescherming GGD Hart voor Brabant

GGD GHOR Nederland heeft een referentie DPIA uitgevoerd op de gegevensverwerkingen in CoronIT. Alhoewel er tot op heden alleen een conceptversie door de GGD GHOR is gepubliceerd, ben ik van mening dat deze DPIA met zorg is opgesteld. Als we kijken naar de verwerking in CoronIT is van begin af aan een discussie ontstaan of deze verwerking sec onder de WPG valt of ook onder de WGBO. Dit is van wezenlijk belang, aangezien de WGBO andere eisen stelt voor oa. Bewaartermijn, rechten betrokken, beveiligingseisen etc.

Op 2-7-2021 is het rapport Testen door de GGD GHOR gepubliceerd waarin onderstaande conclusie is getrokken:
Er is sprake van samenloop tussen de (bestuursrechtelijke) Wet publieke gezondheid (Wpg)en de (privaatrechtelijke) Wet op de geneeskundige behandelingsovereenkomst (Wgbo). Als iemand zich bij de GGD (vrijwillig) laat testen, is de Wgbo naast de Wpg van toepassing. Dit geldt ook als iemand (vrijwillig) meewerkt aan bron- en contactopsporing en/of zich (vrijwillig) laat vaccineren bij de GGD.

De te nemen maatregelen/aanbevelingen voor de lokale GGD zijn reeds gedeeld met het team testen en worden meegenomen in het uitwerken van de lokale DPIA Testproces. Deze DPIA zit in de afrondende fase.

<u>De Functionaris Gegevensbescherming adviseert de verwerkingsverantwoordelijke als volgt:</u>

1. Informatiebeveiliging

- <u>Controle op logging</u>
  GGD GHOR heeft inmiddels een SOC/SIEM team ingericht die de controle op de logging uitvoert voor o.a. CoronIT. Stem met de GGD GHOR af wie verantwoordelijk is voor welke deel van de controle van de logging. Dit kan worden opgenomen in het convenant/een addendum bij het convenant.

- <u>Zorg voor een goede registratie van autorisaties</u>
  Stel een regeling (beleid) op waarbij wordt bepaald wie wijzingen in rechten moet melden en waar dit moet worden gemeld in de organisatie. Zorg voor een sluiten in- door en uitstroomproces en zorg voor monitoring op dit proces.

2. Medewerkers

- <u>Informeren nieuwe medewerkers</u>
  Stel een plan op om periodiek medewerkers te informeren over wat van hen wordt verwacht en waar ze met vragen terecht kunnen. Dit kan bestaan uit een korte presentatie, maar ook een vragenrondje. Stel duidelijke regels op waarin wordt gemeld wat medewerkers wel en niet mogen met de gegevens.

  Stel een systeem op waarbij medewerkers direct op de hoogte worden gesteld van een verandering van werkwijze en dat daarbij ook dat medewerkers die thuis werken en/of medewerkers die op de dag geen dienst hebben alsnog hiervan op de hoogte worden gebracht als zij weer aan het werk gaan.

Bijlage 2: Achtergrond Risiconiveaus

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 de kwetsbaarheid; en
- Aanwezig zijn van bestaande maatregelen en hun effectiviteit

De kans dat een potentiele kwetsbaarheid kan worden uitgebuit door een actor zal worden omgeschreven als hoog, midden, of laag. De onderstaande tabel beschrijft deze drie lagen.

Kans	Kans beschrijving
Hoog	De actor is zeer gemotiveerd en bekwaam en maatregelen ter preventie van de uitbuiting van de kwetsbaarheid zijn ineffectief.
Midden	De actor is zeer gemotiveerd en bekwaam, maar er zijn maatregelen geïmplementeerd die de uitbuiting van de kwetsbaarheid belemmeren.
Laag	De actor mist motivatie of bekwaamheid, of maatregelen zijn geïmplementeerd om de uitbuiting van de kwetsbaarheid te voorkomen of significant te belemmeren.

Impact

De impact van een geëffectueerd risico wordt beschreven in termen van verlies of beperking van beschikbaarheid, integriteit of vertrouwelijkheid van gegevens op een schaal van laag, midden en hoog. De onderstaande beschrijvingen geven een korte omschrijving van deze aspecten en de consequentie (of impact) die daaraan verbonden is als dit doel niet behaald wordt.

Verlies van integriteit – Systeem en data integriteit verwijst naar de eis dat de juistheid en volledigheid van informatie geborgd moet zijn. De integriteit is verloren als incorrecte wijzigingen zijn aangebracht in de informatie door opzettelijk of onopzettelijk handelen. Als verlies van integriteit niet (tijdig) verholpen wordt kan verder gebruik van het gecompromitteerde systeem of data resulteren in onnauwkeurigheid, fraude of beveiligingsincidenten. Verlies van integriteit kan een eerste stap zijn in een aanval op systemen met verlies van beschikbaarheid of vertrouwelijkheid tot gevolg.

Verlies van Beschikbaarheid – Als een dienst (of gegevens aangeboden door een dienst) niet beschikbaar is voor de eindgebruikers, raakt dit mogelijk de missie van de organisatie. Verlies van systeemfunctionaliteit en operationele effectiviteit kunnen leiden tot beveiligingsincidenten of verlies van productiviteit.

Verlies van Vertrouwelijkheid – Systeem en data vertrouwelijkheid verwijst naar de bescherming tegen ongeautoriseerde openbaarmaking van gegevens (o.a. verlies van bedrijfsgeheimen, intellectueel eigendom (software, protocollen, documenten, etc.), of persoonsgegevens). Ongeautoriseerde, onverwachte, of onopzettelijk openbaarmaking van persoonsgegevens kan leiden tot het schenden van wet en regelgeving.

Impact niveau	Impact Beschrijving
Hoog	Misbruik van een kwetsbaarheid: 1. Kan resulteren in het kostbare verlies van kritische assets of middelen; 2. Kan de missie, reputatie of belang van de organisatie of Betrokkene significant schaden, compromitteren of belemmeren; 3. Kan een schending van wettelijke richtlijnen veroorzaken; 4. Kan resulteren in sterfte of ernstig letsel; 5. Kan een grote inbreuk opleveren in de fundamentele rechten en vrijheid van Betrokkene
Midden	Misbruik van een kwetsbaarheid: 1. Kan resulteren in het kostbare verlies van materiële assets of middelen; 2. Kan de missie, reputatie of belang van de organisatie of Betrokkene schaden, compromitteren of belemmeren; 3. Kan resulteren in persoonlijk letsel. 4. Kan een inbreuk opleveren in de fundamentele rechten en vrijheid van Betrokkene
Laag	Misbruik van een kwetsbaarheid: 1. Kan resulteren in het verlies van bepaalde assets of middelen; 2. Kan de missie, reputatie of belang van de organisatie of Betrokkene schaden 3. Kan een kleine inbreuk opleveren in de fundamentele rechten en vrijheid van Betrokkene

Risico Calculatie

Deze stap gebruikt de kans en impact 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 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.

8.4
Archived: donderdag 12 mei 2022 09:33:23
From: [redacted]
Sent: woensdag 17 november 2021 15:50:08
To: [redacted]
Cc: [redacted]
Subject: DPIA CoronIT v.0.5 defintief.docx
Importance: Normal
Sensitivity: None
Attachments:
DPIA CoronIT v.0.5 defintief.docx;

Hallo allen,

De DPIA van CoronIT kent een lange doorlooptijd. De oorzaak hiervoor is tweeledig:

- GGD GHOR heeft tot op heden nog geen definitieve referentie DPIA afgegeven;
- Er is landelijk heel veel discussie geweest of de verwerking in CoronIT wat betreft testen een WPG (wet publieke gezondheid) en/of een WGBO (wet geneeskundige behandelingsovereenkomst) is. In juli is een rapport door de GGD GHOR gepubliceerd waarin de conclusie is getrokken dat het 'testen' (= afname test/wattenstaafje in de neus) een medische handeling is en dus ook de WGBO van toepassing is. Wat dit betekent voor de gegevensverwerking is in het landelijk rapport 'Rapport testen' nader uitgewerkt. De aanbevelingen/acties worden binnen de GGD Hart voor Brabant meegenomen in onze lokale DPIA testen die we aan het opstellen zijn. We zijn daar in de afrondende fase.

Ik wil deze DPIA afronden en heb in het rapport lokale aanvullingen gedaan, toelichting gegeven en verwijzingen opgenomen. In mijn [redacted] advies richt ik mij met name op een aantal maatregelen die opgepakt kunnen worden of mogelijk al zijn uitgevoerd. Kijk daar met name na en ga na of er nog acties uitgezet moeten worden.

Zijn er vragen, laat het mij weten.

Met vriendelijke groeten,

[redacted]

[redacted]

[redacted]

GGD Hart voor Brabant

Pettelaarpark 10 Den Bosch

Postbus 3024, 5003 DA Tilburg

www.ggdhvb.nl

[redacted]

[redacted]@ggdhvb.nl

Aanwezig op: ma-di-wo-do

Gezond doet leven!

8.5
Archived: donderdag 12 mei 2022 09:32:23
From: [redacted]
Sent: woensdag 24 februari 2021 10:58:32
To: [redacted]
Subject: FW: GGD Contact beveiligingsmaatregelen
Importance: Normal
Sensitivity: None
Attachments:
Factsheet Privacy GGD Contact 1.0.pdf; Beveiligingsmaatregelen GGD voor gebruik van webapplicatie met medische informatie v3.1.pdf; Bijlage IV - 08_12_2020 Def. DPIA GGD Contact v1.0.docx;

Ha [redacted], ter kennisname onderstaande. Dit is een actie die loopt in het kader van de projectgroep verbeterplan gegevensbescherming.

Van: [redacted]@ggdhvb.nl>
Verzonden: woensdag 24 februari 2021 10:19
Aan: [redacted]@ggdhvb.nl>; [redacted]@hetservicecentrum.nl>; [redacted]@ggdhvb.nl>
CC: [redacted]@ggdhvb.nl>; [redacted]@ggdhvb.nl>; [redacted]@ggdhvb.nl>
Onderwerp: GGD Contact beveiligingsmaatregelen

Hallo collega's,

Zoals afgesproken heb ik op onze teamsite 'Implementatie GGD Contact' de veilig werken documenten vanuit de GGD GHOR geplaatst. Bijgaand een tweetal documenten die specifiek ingaan op de beveiliging en de DPIA.

Belangrijk hierbij is dat de opgenomen beveiligingsmaatregelen vereisten bevat waar GGD GHOR NL en de GGD aan moet voldoen voor ingebruikname BCO Portaal (een uitgebreidere checklist/self-assesmenent voor de NEN7510 zal binnenkort verschijnen en met jullie gedeeld worden).

Aan jullie drieën het verzoek om deze maatregelen intern te toetsen en jullie bevindingen in de DPIA op te nemen bij de opgesomde risico's vanaf pagina 41.

Met vriendelijke groeten,

[redacted]

[redacted]

[redacted]

GGD Hart voor Brabant
Pettelaarpark 10 Den Bosch
Postbus 3024, 5003 DA Tilburg
www.ggdhvb.nl
[redacted]
[redacted]@ggdhvb.nl
Aanwezig op: ma-di-wo-do

8.6
Archived: donderdag 12 mei 2022 09:39:45
From: [redacted]
To: [redacted]
Cc: [redacted]
Subject: RE: DPIA CoronIT v.0.5 defintief.docx
Importance: Normal
Sensitivity: None
Attachments:
DPIA CoronIT v.0.5 defintief.docx; Actiepunten onderzoek AP.docx;

Bedankt voor de toelichting [redacted]. Jouw adviezen uit de DPIA en de actiepunten uit het AP-onderzoek zullen door het programma en regulier samen moeten worden opgepakt. We hebben overigens eerder afgesproken dat Treja hierop primair de regie heeft.

[redacted], [redacted] en [redacted], kunnen jullie in jullie vaste afstemmingsoverleg procesafspraken maken over hoe deze adviezen en actiepunten het beste uitgezet kunnen worden?

Groeten,

[redacted]

De [redacted] adviseert de verwerkingsverantwoordelijke als volgt:

1. Informatiebeveiliging

- Controle op logging
  GGD GHOR heeft inmiddels een SOC/SIEM team ingericht die de controle op de logging uitvoert voor o.a. CoronIT. Stem met de GGD GHOR af wie verantwoordelijk is voor welke deel van de controle van de logging. Dit kan worden opgenomen in het convenant/een addendum bij het convenant.

- Zorg voor een goede registratie van autorisaties
  Stel een regeling (beleid) op waarbij wordt bepaald wie wijzingen in rechten moet melden en waar dit moet worden gemeld in de organisatie. Zorg voor een sluiten in- door en uitstroomproces en zorg voor monitoring op dit proces.

2. Medewerkers

- Informeren nieuwe medewerkers

Stel een plan op om periodiek medewerkers te informeren over wat van hen wordt verwacht en waar ze met vragen terecht kunnen. Dit kan bestaan uit een korte presentatie, maar ook een vragenrondje. Stel duidelijke regels op waarin wordt gemeld wat medewerkers wel en niet mogen met de gegevens.

Stel een systeem op waarbij medewerkers direct op de hoogte worden gesteld van een verandering van werkwijze en dat daarbij ook dat medewerkers die thuis werken en/of medewerkers die op de dag geen dienst hebben alsnog hiervan op de hoogte worden gebracht als zij weer aan het werk gaan.

Van: [redacted]@ggdhvb.nl>
Verzonden: donderdag 18 november 2021 09:44

Aan: [redacted]@ggdhvb.nl>
Onderwerp: RE: DPIA CoronIT v.0.5 defintief.docx

Goedemorgen [redacted],

Een DPIA hoeft niet officieel vastgesteld te worden. Dit is een risico analyse op privacy aspecten, waar verbeterpunten uit komen. Binnen onze organisatie is de afspraak dat de DPIA naar de sectormanager gaat. Voor programma Corona zie ik jou als 'opperhoofd' samen met [redacted] en [redacted].

Belangrijk is naar het [redacted] advies te kijken en de adviespunten op te pakken of na te gaan of dit al goed is ingeregeld. Indien het [redacted] advies niet wordt opgevolgd, dient dit beargumenteerd vastgelegd te worden.

Deze actiepunten en de actiepunten uit de DPIA GGD Contact liggen in lijn met de brief van de Autoriteit Persoonsgegevens. Had jij die brief al gezien? Bijgaand de stukken en een samenvatting van de actiepunten. Deze actiepunten dienen tevens opgepakt te worden door de lokale GGD. Vervolgens moet de status in de voortgangsrapportage in maart 2022 aan de AP teruggekoppeld moeten worden.

Belangrijk is om met GGD GHOR af te stemmen hoe deze terugkoppeling plaats zal vinden en in welke bewoording. -> misschien een onderwerp voor een overleg DPG Raad ?

Met vriendelijke groeten,

[redacted]

[redacted]

[redacted]

GGD Hart voor Brabant

Pettelaarpark 10 Den Bosch

Postbus 3024, 5003 DA Tilburg

www.ggdhvb.nl

[redacted]

[redacted]@ggdhvb.nl

Aanwezig op: ma-di-wo-do

Gezond doet leven!

Van: [redacted]@ggdhvb.nl>
Verzonden: woensdag 17 november 2021 17:49
Aan: [redacted]@ggdhvb.nl>; [redacted]@ggdhvb.nl>; [redacted]@ggdhvb.nl>; [redacted]@ggdhvb.nl>; [redacted]@ggdhvb.nl>; [redacted]@ggdhvb.nl>
CC: [redacted]@ggdhvb.nl>
Onderwerp: RE: DPIA CoronIT v.0.5 defintief.docx

Dag [redacted], dank voor de stukken. Wie moet de DPIA definitief vaststellen?

Van: [redacted]@ggdhvb.nl>
Verzonden: woensdag 17 november 2021 15:50
Aan: [redacted]@ggdhvb.nl>; [redacted]@ggdhvb.nl>; [redacted]@ggdhvb.nl>; [redacted]@ggdhvb.nl>; [redacted]@ggdhvb.nl>

[redacted]@ggdhvb.nl>
CC: [redacted]@ggdhvb.nl>
Onderwerp: DPIA CoronIT v.0.5 defintief.docx

Hallo allen,

De DPIA van CoronIT kent een lange doorlooptijd. De oorzaak hiervoor is tweeledig:

- GGD GHOR heeft tot op heden nog geen definitieve referentie DPIA afgegeven;
- Er is landelijk heel veel discussie geweest of de verwerking in CoronIT wat betreft testen een WPG (wet publieke gezondheid) en/of een WGBO (wet geneeskundige behandelingsovereenkomst) is. In juli is een rapport door de GGD GHOR gepubliceerd waarin de conclusie is getrokken dat het 'testen' (= afname test/wattenstaafje in de neus) een medische handeling is en dus ook de WGBO van toepassing is. Wat dit betekent voor de gegevensverwerking is in het landelijk rapport 'Rapport testen' nader uitgewerkt. De aanbevelingen/acties worden binnen de GGD Hart voor Brabant meegenomen in onze lokale DPIA testen die we aan het opstellen zijn. We zijn daar in de afrondende fase.

Ik wil deze DPIA afronden en heb in het rapport lokale aanvullingen gedaan, toelichting gegeven en verwijzingen opgenomen. In mijn FG advies richt ik mij met name op een aantal maatregelen die opgepakt kunnen worden of mogelijk al zijn uitgevoerd. Kijk daar met name na en ga na of er nog acties uitgezet moeten worden.

Zijn er vragen, laat het mij weten.

Met vriendelijke groeten,

[redacted]

[redacted]

[redacted]

GGD Hart voor Brabant

Pettelaarpark 10 Den Bosch

Postbus 3024, 5003 DA Tilburg

www.ggdhvb.nl

[redacted]

[redacted]@ggdhvb.nl

Aanwezig op: ma-di-wo-do

Gezond doet leven!

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.	Openstaand	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 appspraken (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.	Openstaand	Volledige technische documentatie is nog niet beschikbaar. Met Topicus vindt in augustus een Q&A sessie plaats om de technische informatie te bespreken.
		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	

DRAFT Risk Register Van Geloven

		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 persoonsgegevens. 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 [redacted] - 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 vastgelegd in een procedure specifiek voor CoronIT.
		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 [redacted]	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, waaruit een aantal bevindingen zijn gekomen. Deze bevindingen bevatten risico's voor het proces.				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 op dit moment niet (tot in detail) bekend. De hertest is pas mogelijk als alles getest is en de kwetsbaarheden zijn verholpen.
		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.
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	

DRAFT Risk Register Van Geloven

		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 geimplementeerd, 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	

DRAFT Risk Register Van Geloven

		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

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:

9.1 1.1 Verwerkers...Hart voor Brabant

9.10 Vacatureteks...Hart voor Brabant

9.11 terugkoppeling MT_Redacted

9.2 10629 Verwer...t Hart voor Brabant

9.3 FW_ Gegeven...rt voor Brabant (41)

9.4 FW_ Gegeven...Hart voor Brabant

9.5 FW_ SPOED_...dsvragen over AVG

9.6 Genomen maa...tal_Zwartgemaakt

9.7 HvB Overeenk...len_Zwartgemaakt

9.8 Beleidsplan inf...SC_Zwartgemaakt

9.9 Privacystatement medewerkers

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
Artikel 12. Aansprakelijkheid 5
Bijlage 1. De Verwerking van Persoonsgegevens 7
Bijlage 2. Passende technische en organisatorische maatregelen 8
Bijlage 3: Afspraken betreffende Inbreuken in verband met Persoonsgegevens 9

Verwerkersovereenkomst ARVODI-2018

De ondergetekenden:

1. De Gemeentelijke Gezondheidsdienst Hart voor Brabant, gevestigd te 's-Hertogenbosch aan het Pettelaarpark 10, ingeschreven in het handelsregister onder KvK nummer 17247544, rechtsgeldig vertegenwoordigd door mevrouw [redacted], 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, de [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 /datum/.

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,

's-Hertogenbosch, datum:	Den Haag, datum:
GGD Hart voor Brabant	DE MINISTER/STAATSSECRETARIS Volksgezondheid, Welzijn en Sport
namens deze, de directeur publieke gezondheid	namens deze, de directeur Informatiebeleid
Mevrouw T. Claassen	De heer R. Roozendaal

Bijlage 1. De Verwerking van Persoonsgegevens

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 GGD Contact is op een goede, veilige en efficiënte manier uitvoeren van bronnen- en contactonderzoek.
Het soort Persoonsgegevens	• Bijzondere categorieën van gegevens als bedoeld in artikel 9 AVG • Wettelijk voorgeschreven identificatienummers • Overige persoonsgegevens.
Beschrijving categorieën Persoonsgegevens	• Gegevens die de Opdrachtgever nodig heeft voor bron- en contactopsporing. Dit zijn gezondheidsgegevens. Bijvoorbeeld: netwerk/relatie-gegevens, gegevens over contacten van index, contactgegevens, besmettingsrisico, klachten, door de index in een open veld zelf ingevulde gegevens • Gegevens van medewerkers die het bronnen- en contactonderzoek uitvoeren, waaronder ook de logging van het gebruik van de applicatie.
Beschrijving categorieën Betrokkenen	• Met infectieziekte besmette personen ('index') • Contacten die mogelijk besmet zijn ('contacten') • Medewerkers die bronnen en contactonderzoek uitvoeren
Beschrijving categorieën ontvangers van Persoonsgegevens	Medewerkers van Opdrachtnemer en door Opdrachtnemer ingeschakelde (sub)verwerkers die vanuit hun rol bij de verwerking betrokken zijn.

Bijlage 2. Passende technische en organisatorische maatregelen

Het vereiste beveiligingsniveau is vastgelegd in de DVO in hoofdstuk 3 (Beveiliging) en in de daarbij behorende bijlage Beveiliging GGD Contact (zie de verwijzing in artikel 1.3 van de DVO).

Bijlage 3: Afspraken betreffende Inbreuken in verband met Persoonsgegevens

Inbreuken in verband met Persoonsgegevens moeten worden gemeld bij de servicedesk van GGD GHOR en worden afgewikkeld volgens het door GGD GHOR gehanteerde incidentproces.

Betreft het een incident dat zich voordoet bij Opdrachtnemer, dan worden bij de melding van het incident alleen die persoonsgegevens verstrekt die noodzakelijk zijn voor de afwikkeling van het incident, waaronder een beschrijving van

Aard van de Inbreuk in verband met Persoonsgegevens
De Persoonsgegevens en Betrokkene (voor zover noodzakelijk)
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

De wijze waarop incidenten kunnen worden aangemeld zal door GGD GHOR aan Opdrachtgever en Opdrachtnemer worden gecommuniceerd. Partijen zijn hierbij zelf verantwoordelijk voor de beveiliging van de henzelf verzonden berichten.

Op verzoek van de Privacy Lead van GGD GHOR of de FG van de GGD kan bij de opvolging van incidenten ondersteuning gevraagd worden van Opdrachtnemer. In dat geval wordt in een intake bepaald welke gegevens Opdrachtnemer hiervoor nodig heeft.

Verwerkingsovereenkomst GGD GHOR – GGD'en inzake datamutaties CoronIT

De ondergetekenden:

De Gemeentelijke Gezondheidsdienst Hart voor Brabant, gevestigd te 's-Hertogenbosch aan de Vogelstraat 2, ingeschreven in het handelsregister onder KvK nummer 17247544, ten deze rechtsgeldig vertegenwoordigd door mevrou [redacted] verder te noemen: '**Verwerkingsverantwoordelijke**';

En

GGD GHOR Nederland gevestigd te 3524SJ Utrecht aan de Zwarte Woud 2 ingeschreven zijnde in het register van de Kamer van Koophandel onder het nummer van 40478156, ten deze rechtsgeldig vertegenwoordigd door [redacted] verder te noemen: '**Verwerker**';

De hierboven genoemde partijen, hierna gezamenlijk ook aan te duiden als "**Partijen**" en ieder afzonderlijk als "**Partij**".

Nemen in overweging dat:

a) Verwerkingsverantwoordelijke aan Verwerker opdracht heeft verstrekt tot de levering van de diensten en/of producten van Verwerker, tussen Partijen contractueel vastgelegd in de "**Opdrachtverlening gegevensverwerking datamutaties**";

b) Verwerker in het kader van de uitvoering van de opdrachtverleningdata van de Verwerkingsverantwoordelijke verwerkt. Deze data omvat ook **"Persoonsgegevens"** in de zin van artikel 4 sub 1 Algemene Verordening Persoonsgegevens ("**AVG**");

c) Partijen conform artikel 28 lid 3 AVG de wederzijdse rechten en plichten betreffende de verwerking van Persoonsgegevens wensen vast te legen in deze Verwerkingsovereenkomst (hierna: de "**Verwerkingsovereenkomst").**

Komen overeen als volgt:

Artikel 1: Definities

De hieronder met een hoofdletter weergegeven woorden hebben de daaraan gekoppelde definitie, tenzij uit de Verwerkingsovereenkomst ondubbelzinnig anderszins blijkt.

- Betrokkene : een geïdentificeerde of identificeerbare natuurlijke persoon op wie de Persoonsgegevens betrekking hebben

- Bijlage : een bijlage bij de Verwerkingsovereenkomst welke onlosmakelijk onderdeel daarvan uitmaakt

- Data : een digitaal en/of fysiek opgeslagen set aan gegevens al dan niet omvattend Persoonsgegevens

- Derde : een natuurlijk persoon, een rechtspersoon, een overheidsinstantie, een dienst of een ander orgaan, niet zijnde de Betrokkene, noch de Verwerkingsverantwoordelijke en Verwerker, noch de personen die onder rechtstreeks gezag van de Verwerker gemachtigd zijn om de Persoonsgegevens te verwerken

- Opdrachtverlening :de Opdrachtverlening gegevensverwerking datamutaties d.d. 24 juni 2021 alsmede alle daaraan verbonden bijlagen tussen Partijen betreffende het onderwerp gegevensverwerking datamutaties.

- 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 (Artikel 4(12) AVG).

- Verwerking : een bewerking of een geheel van bewerkingen 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, verspreiden of op andere wijze ter beschikking stellen, aligneren of combineren, afschermen, wissen of vernietigen van gegevens

Artikel 2: Onderwerp

2.1 De Verwerkingsovereenkomst regelt de wederzijdse rechten en plichten van Partijen betreffende de Verwerking van Persoonsgegevens die voortvloeit uit de Hoofdovereenkomst en het daarin omschreven doel.

2.2 Partijen hebben in Bijlage 1 de aard, het soort Persoonsgegevens en de categorieën van Betrokkenen omschreven.

2.3 Partijen verplichten zich tot naleving van de geldende wet- en regelgeving met betrekking tot de Verwerking van Persoonsgegevens. Verwerker dient Verwerkingsverantwoordelijke te informeren indien een handelswijze van laatstgenoemde strijdig is met dergelijke wet- en regelgeving.

Artikel 3: Ingangsdatum en duur

3.1 De Verwerkingsovereenkomst treedt in werking op de datum waarop deze door Partijen is ondertekend.

3.2 Met inachtneming van hetgeen is bepaald in dit artikel, eindigt de Verwerkingsovereenkomst zodra de Hoofdovereenkomst is geëindigd.

3.3 Geen van Partijen kan deze Verwerkingsovereenkomst los van de Hoofdovereenkomst tussentijds opzeggen.

Artikel 4: Verplichtingen Verwerker

4.1 De Verwerking van Persoonsgegevens door Verwerker vindt uitsluitend plaats op basis van schriftelijke instructies van Verwerkingsverantwoordelijke.

4.2 Verwerker is niet gerechtigd om Persoonsgegevens voor eigen doeleinden of die van Derden te verwerken, tenzij Verwerkingsverantwoordelijke daartoe ondubbelzinnig voorafgaand toestemming voor heeft gegeven. De Verwerking vindt plaats op basis van het doel als vastgelegd in de opdrachtverlening.

4.3 Tenzij Verwerkingsverantwoordelijke ondubbelzinnig toestemming heeft verleend, zal de Verwerking van Persoonsgegevens niet plaatsvinden buiten de Europese Economische Ruimte (EER).

4.4 Verwerker betracht volledige vertrouwelijkheid betreffende de
Data en de daarin aanwezige Persoonsgegevens en draagt er zorg voor dat zijn medewerkers eveneens op een adequate wijze door een passende rechtsgeldige verplichting eveneens tot geheimhouding zijn gebonden.

4.5 Verwerker kan, na voorafgaande schriftelijke goedkeuring van Verwerkingsverantwoordelijke, een subverwerker inschakelen om ten behoeve van Verwerkingsverantwoordelijke verwerkingsactiviteiten te verrichten mits aan deze subverwerker dezelfde verplichtingen inzake gegevensbescherming worden opgelegd als die welke in de Verwerkingsovereenkomst zijn opgenomen voor Verwerker. In bijlage 1 zijn de reeds ingeschakelde subverwerkers opgenomen.

4.6 Verwerker assisteert en ondersteunt Verwerkingsverantwoordelijke indien de Verwerking onderwerp van onderzoek is door bevoegde autoriteiten. Daarnaast verleent Verwerker ondersteuning bij het uitvoeren van een ‘Data Protection Impact Assessment’ (DPIA) door Verwerkingsverantwoordelijke betreffende het onderwerp van de opdrachtverlening.

4.7 Verwerker maakt geen Persoonsgegevens openbaar, tenzij zij daartoe is gehouden op grond van een gerechtelijke uitspraak dan wel een wettelijke verplichting. In een dergelijk geval zal Verwerker eerst Verwerkingsverantwoordelijke gemotiveerd informeren alvorens uitvoering te geven aan een dergelijke verplichting.

4.8 Verwerker informeert Verwerkingsverantwoordelijke over wijzigingen in wet- en regelgeving welke van invloed zijn op de Verwerking als omschreven in de Verwerkingsovereenkomst.

4.9 Verwerker informeert Verwerkingsverantwoordelijke onmiddellijk over omstandigheden die een correcte naleving van de relevante wet- en regelgeving door Verwerker negatief beïnvloeden.

Artikel 5: Beveiligingsmaatregelen en controle

5.1 Rekening houdend met de stand van de techniek, de uitvoeringskosten, alsook de aard, omvang, context en verwerkingsdoeleinden alsmede de qua waarschijnlijkheid en ernst uiteenlopende risico's voor de rechten en vrijheden van Betrokkenen treft Verwerker, evenals Verwerkingsverantwoordelijke, passende technische en organisatorische maatregelen (Bijlage 2) om een op het risico afgestemd beveiligingsniveau te borgen. Verwerker handelt daarbij conform artikel 32 AVG. Verwerker zal Verwerkingsverantwoordelijke op eerste verzoek inzage geven in het bestaan, de opzet alsmede de werking van de in dit artikellid genoemde technische en organisatorische maatregelen.

5.2 Partijen erkennen dat het waarborgen van een passend beveiligingsniveau voortdurend kan dwingen tot het treffen van aanvullende beveiligingsmaatregelen. Verwerker waarborgt een op het actuele risico afgestemd beveiligingsniveau.

5.3 Verwerkingsverantwoordelijke is te allen tijde gerechtigd de verwerking van Persoonsgegevens te controleren. Verwerker is verplicht Verwerkingsverantwoordelijke, of de onafhankelijke onder geheimhouding controlerende instantie, in opdracht van Verwerkingsverantwoordelijke toe te laten en medewerking te verlenen, zodat de controle daadwerkelijk uitgevoerd kan worden.

5.4 Verwerkingsverantwoordelijke zal de controle slechts (laten) uitvoeren na een voorafgaande schriftelijke melding aan Verwerker.

5.5 Verwerker staat ervoor in, de door Verwerkingsverantwoordelijke, gegeven aanbevelingen ter verbetering binnen de daartoe door Verwerkingsverantwoordelijke te bepalen redelijke termijn uit te voeren.

Artikel 6: Inbreuk in verband met persoonsgegevens

6.1 Verwerker verleent Verwerkingsverantwoordelijke voortvarend bijstand bij het doen nakomen van de verplichtingen uit hoofde van artikel 32 tot en met 36 AVG en draagt er zorg voor dat haar organisatie daartoe technisch en organisatorisch is toegerust. In dat kader zal Verwerker onder andere ieder Inbreuk in verband met persoonsgegevens onverwijld aan Verwerkingsverantwoordelijke melden.

6.2 In geval van een datalek zal de afhandeling en de eventuele melding van het datalek bij de toezichthoudende autoriteit van het datalek worden overgelaten aan GGD GHOR Nederland voor zover het een datalek betreft die op landelijk niveau heeft plaatsgevonden. Dit is conform de huidige werkwijze in geval van een inbreuk in verband met persoonsgegevens. Enkel wanneer het een regionaal datalek betreft zal de melding worden overgelaten aan de Verwerkingsverantwoordelijke.

6.3 De Verwerker houdt een gedetailleerd logboek bij van alle (vermoedens van) inbreuken op de beveiliging, evenals de maatregelen die in vervolg op dergelijke inbreuken zijn genomen, en geeft daar op eerste verzoek van de Verwerkingsverantwoordelijke inzage in.

Artikel 7: Rechten van betrokkene

7.1 De rechten van betrokkene zullen uitgevoerd worden via de huidige procedures. Dit houdt in dat de betrokkene een verzoek indient bij de regio waar hij/zij getest of gevaccineerd is. Voor zover bij de afhandeling van het verzoek informatie van Verwerker vereist is, geldt hetgeen in dit artikel bepaald is.

7.2 De Verwerkerdient te handelen volgens alle redelijke instructies van de Verwerkingsverantwoordelijke met inachtneming van een verzoek van een Betrokkene met betrekking tot de Persoonsgegevens van die Betrokkene.

7.3 De Verwerker stelt de Verwerkingsverantwoordelijke te allen tijde in staat om binnen de wettelijke termijnen te voldoen aan de verplichtingen op grond van de AVG, meer in het bijzonder de rechten van Betrokkenen, zoals, maar niet beperkt tot een verzoek om informatie, inzage, verbetering, aanvulling, verwijdering, overdraagbaarheid of afscherming van Persoonsgegevens en het uitvoeren van een gehonoreerd aangetekend verzet.

7.4 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 hij de toepasselijke (privacy) wetgeving naleeft.

7.5 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 wanneer deze ziet op een verwerking bij een van de regio's. Wanneer het een klacht betreft ten aanzien van het landelijke proces, zal Verwerker de afhandeling van de klacht door Verwerker geschieden.

7.6 Indien Verwerker op grond van een wettelijke verplichting gegevens dient te verstrekken, zal Verwerker de grondslag van het verzoek en de identiteit van de verzoeker verifiëren en zal Verwerker Verwerkingsverantwoordelijke onmiddellijk, voorafgaand aan de verstrekking, ter zake informeren, tenzij wettelijke bepalingen dit verbieden.

Artikel 8: Wijziging en beëindiging

8.1 Wijziging van deze Verwerkingsovereenkomst kan slechts schriftelijk plaatsvinden middels een door Partijen geaccordeerd voorstel.

8.2 De artikelen 4.2, 4,4, en 1 van de Verwerkingsovereenkomst blijven, gezien hun aard, ook nadat de Verwerkingsovereenkomst is geëindigd van kracht.

8.3 Na afloop van de Verwerkingsovereenkomst draagt Verwerker, naar gelang de keuze van Verwerkingsverantwoordelijke, zorg voor het terugbezorgen aan Verwerkingsverantwoordelijke of het wissen van alle Persoonsgegevens. Verwerker verwijdert kopieën, behoudens afwijkende wettelijke voorschriften.

Artikel 9: Overige

9.1 Partijen verbinden zich om minimaal een keer per kalenderjaar de Verwerkingsovereenkomst en de daaruit voortvloeiende werkzaamheden te evalueren. Daarbij verklaren Partijen zich bereid om de Verwerkingsovereenkomst 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 de Verwerkingsovereenkomst te allen tijde ten minste aan de wettelijke vereisten ter zake de bescherming van Persoonsgegevens dient te voldoen.

Artikel 10: Slotbepalingen

10.1 De overwegingen maken onderdeel uit van deze Verwerkingsovereenkomst.

10.2 De nietigheid van enige bepaling van deze Verwerkingsovereenkomst tast de geldigheid van de overige bepalingen niet aan.

10.3 Het is Verwerker niet toegestaan om zonder uitdrukkelijke en schriftelijke toestemming van Verwerkingsverantwoordelijke deze Verwerkingsovereenkomst en de rechten en plichten die samenhangen met deze Verwerkingsovereenkomst over te dragen aan een Derde partij.

Artikel 11: Rechts- en forumkeuze

11.1 Eventuele conflicten zullen eerst met elkaar besproken worden, waarbij beide partijen zich inspannen om het geschil in goed overleg met elkaar op te lossen.

11.2 Op de Verwerkingsovereenkomst is Nederlands recht van toepassing.

11.3 Tenzij in de Hoofdovereenkomst anderszins is overeengekomen, worden geschillen die voortvloeien uit de Overeenkomst, in eerste aanleg uitsluitend voorgelegd aan de bevoegde rechter van de rechtbank Midden-Nederland locatie Utrecht.

Aldus opgemaakt en ondertekend in tweevoud te ……., op …….. 2021

De Gemeentelijke Gezondheidsdienst

Hart voor Brabant

…….

mevrouw T. Claassen

GGD GHOR Nederland

……..

Mw. N. Rigter, directeur Corona Programma Organisatie

Bijlage 1
Beschrijving verwerkingsactiviteiten

1. Persoonsgegevens

Het onderwerp/aard en doel van de Verwerking:
Binnen CoronIT kunnen test- en vaccinatiegegevens verkeerd worden geregistreerd, waardoor het niet mogelijk is om een test- en vaccinatiebewijs te krijgen voor toegang tot evenementen of reizen. Deze foute gegevens moeten worden gecorrigeerd, niet alleen om praktische redenen, zoals het juist versturen van communicatie, maar ook om te voldoen aan de wetgeving omtrent test- en vaccinatiebewijzen. Het is daarbij praktisch dat deze mutaties op een centrale plek worden uitgevoerd.

De GGD' en geven GGD GHOR Nederland de opdracht/machtiging voor het uitvoeren van mutaties in CoronIT ten behoeve van de test- en vaccinatiegegevens. Deze mutaties bevatten de volgende werkzaamheden:

- Identificeren van de burger
- Verifiëren van de identiteit van de burger
- Inzien van gegevens in CoronIT waaronder:
    - NAWTE
    - Vaccinatieverklaring
    - Positieve testverklaring
    - Negatieve testverklaring
    - Laborders
    - Labuitslagen
- Uitvoeren van correcties in:
    - NAWTE-gegevens;
    - Laborderformulieren (toestemmingsvinkjes);
    - Intakeformulieren (toestemming + positieve test in het verleden);
    - Vaccinatieregistraties (batchnummer en vaccinnaam), voor zover die eenvoudig te achterhalen zijn. Anders controleren en neerleggen bij de burger.
    - Ontbrekende data inzake BSN
- Afhandelen van contact (via ticket, mail, telefonie) met betrokken partijen, waaronder
    - Ministerie van Buitenlandse Zaken
    - Ministerie Volksgezondheid, Welzijn en Sport
    - Rijksinstituut voor Volksgezondheid en Milieu
    - Burger
    - Regionale GGD
- Opnamen telefoongesprekken ten behoeve van klachtafhandeling, in geval van aansprakelijkheidsstelling

Indien andere mutaties noodzakelijk zijn en uitgevoerd kunnen worden door GGD GHOR Nederland, is GGD GHOR Nederland daar tevens voor gemachtigd.

Het soort Persoonsgegevens:

- NAWTE-gegevens;
- Laborderformulieren (toestemmingsvinkjes);
- Intakeformulieren (toestemming + positieve test in het verleden);

o Vaccinatieregistraties (batchnummer en vaccinnaam), voor zover die eenvoudig te achterhalen zijn. Anders controleren en neerleggen bij de burger. o Ontbrekende data inzake BSN o Vaccinatieverklaring o Positieve testverklaring o Negatieve testverklaring o Laborders o Labuitslagen
Beschrijving categorieën Persoonsgegevens: 'Gewone persoonsgegevens' en 'bijzondere persoonsgegevens': gegevens over de gezondheid. Burgerservicenummer.
Beschrijving categorieën Betrokkenen: Burgers die zich hebben laten testen en/of vaccineren (Corona) en een test- of vaccinatiebewijs willen verkrijgen en hun gegevens hiervoor opvragen, welke in CoronIT staan en/of bij één van de GGD'en.
Beschrijving categorieën ontvangers van Persoonsgegevens: Subverwerker: Teleperformance voor klantcontact en het uitvoeren van datamutaties.
Bewaartermijn: De mutaties vinden plaats in het dossier van de betrokkene in CoronIT, waardoor de bewaartermijnen van CoronIT gelden. Hierdoor zijn de bewaartermijnen maximaal 20 jaar vanaf laatste wijziging in dossier, behoudens uitzonderingen. Opname telefoongesprekken: 4 weken.

2. Ingeschakelde subverwerkers

Naam en contactgegevens subverwerker	Uitbestede verwerkingen
Subverwerker: Teleperformance voor klantcontact en het uitvoeren van datamutaties.	Zie punt 1 van deze bijlage

Bijlage 2
Beveiligingsmaatregelen

Rekening houdend met de stand van de techniek, de uitvoeringskosten, alsook de aard omvang, context en verwerkingsdoeleinden alsmede de qua waarschijnlijkheid en ernst uiteenlopende risico's voor de rechten en vrijheden van Betrokkenen treft Verwerker, evenals Verwerkingsverantwoordelijke, passende technische en organisatorische maatregelen (Bijlage 2) om een op het risico afgestemd beveiligingsniveau te borgen. Verwerker handelt daarbij conform artikel 32 AVG. Verwerker zal Verwerkingsverantwoordelijke op eerste verzoek inzage geven in het bestaan, de opzet alsmede de werking van de in dit artikellid genoemde technische en organisatorische maatregelen.

Voor de genomen beveiligingsmaatregelen wordt verwezen naar de DPIA die is uitgevoerd ten aanzien van de gegevensuitwisseling die plaatsvindt in het kader van test-vaccinatie en herstelbewijzen middels CoronaCheck of andersoortige applicaties die hiervoor gebruikt worden.

9.3
Archived: donderdag 12 mei 2022 09:34:37
From: [redacted]
Sent: donderdag 18 maart 2021 22:54:46
To: [redacted]
Subject: FW: Gegevens datalek GGD Hart voor Brabant
Importance: Normal
Sensitivity: None

Ter info over de datadiefstal. Ik stuur deze info ook naar [redacted] door. Graag jullie advies of we dit bericht delen met ons bestuur en op welke wijze we dat dan doen…

Hartelijke groet,

[redacted]

Van: Directiesecretariaat GGD GHOR Nederland <Directiesecretariaat@ggdghor.nl>
Verzonden: donderdag 18 maart 2021 17:06
Aan: [redacted]@ggdhvb.nl>
CC: [redacted]@ggdghor.nl>; [redacted]@ggdghor.nl>; [redacted]@ggdghor.nl>
Onderwerp: Gegevens datalek GGD Hart voor Brabant

Beste DPG,

Bij deze geef ik graag een update over het informeren van de gedupeerden van de datadiefstal.

Gistermiddag 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 37 gedupeerden.

Wij 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.

De brieven worden vanmiddag gepost en zullen morgen (vrijdag) bij de gedupeerden worden bezorgd.

Uiterlijk 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.

Mocht je nog vragen hebben, dan kun je contact zoeken met [redacted]@ggdghor.nl) of met ondergetekende.

Met vriendelijke groet,

[redacted]

[redacted]

GGD GHOR Nederland
Zwarte Woud 2
3524 SJ Utrecht

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

Dit bericht is uitsluitend bestemd voor de geadresseerde. Het bericht kan vertrouwelijke informatie bevatten. Als u dit bericht per abuis hebt ontvangen, wordt u verzocht het te vernietigen en de afzender te informeren. GGD GHOR Nederland is niet aansprakelijk voor onjuiste en onvolledige overbrenging van de inhoud van een verzonden e-mail bericht, of een te late ontvangst daarvan.

9.4
Archived: donderdag 12 mei 2022 09:34:43
From: [redacted]
Sent: vrijdag 19 maart 2021 09:12:03
To: [redacted]
Cc: [redacted]
Subject: FW: Gegevens datalek GGD Hart voor Brabant
Importance: Normal
Sensitivity: None
Attachments:
20210315 - brief gedupeerden datadiefst GGD_def in sjabloon - getekend.docx;

Oeps. Ik zie dat [redacted] een schrijfdag heeft. [redacted], zou jij even contact kunnen leggen met [redacted] of ze akkoord is met onderstaande advies en zou je dan voor haar een kort bericht kunnen opstellen?

Van: [redacted]
Verzonden: vrijdag 19 maart 2021 09:08
Aan: [redacted]@ggdhvb.nl>; [redacted]@ggdhvb.nl>
CC: [redacted]@ggdhvb.nl>
Onderwerp: RE: Gegevens datalek GGD Hart voor Brabant

Ha [redacted], ik adviseer inderdaad om dit te delen met de bestuurders, omdat het hun eigen inwoners betreft, het mogelijk hernieuwde media-aandacht en raadsvragen oplevert en we eerder hebben toegezegd hen te informeren bij nieuwe ontwikkelingen in dit dossier. Mijn voorstel is om het te doen in de vorm van een korte mail van jou aan het AB. De kern:

- Refereren aan eerdere brief/mails over de datadiefstal, waarin we uiteen hebben gezet wat wij doen aan dat onderwerp
- Melden dat vandaag 37 van onze inwoners (en in de rest van Nederland) een brief krijgen die door GGD GHOR NL namens de GGD is verstuurd
- Dat in de brief mensen worden gewezen op de risico's van identiteitsfraude
- Procesinfo: dat wij de gedupeerden informeren waar ze terecht kunnen met vragen

[redacted] is vandaag vrij. Ik eigenlijk ook. [redacted], ik durf het bijna niet te vragen, maar kun jij dit vandaag oppakken?

Van: [redacted]@ggdhvb.nl>
Verzonden: donderdag 18 maart 2021 22:55
Aan: [redacted]@ggdhvb.nl>; [redacted]@ggdhvb.nl>
Onderwerp: FW: Gegevens datalek GGD Hart voor Brabant

Ter info over de datadiefstal. Ik stuur deze info ook naar [redacted] door. Graag jullie advies of we dit bericht delen met ons bestuur en op welke wijze we dat dan doen…

Hartelijke groet,

[redacted]

Van: Directiesecretariaat GGD GHOR Nederland <Directiesecretariaat@ggdghor.nl>
Verzonden: donderdag 18 maart 2021 17:06
Aan: [redacted]@ggdhvb.nl>
CC: [redacted]@ggdghor.nl>; [redacted]@ggdghor.nl>; [redacted]@ggdghor.nl>
Onderwerp: Gegevens datalek GGD Hart voor Brabant

Beste DPG,

Bij deze geef ik graag een update over het informeren van de gedupeerden van de datadiefstal.

Gistermiddag 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 37 gedupeerden.

Wij 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.

De brieven worden vanmiddag gepost en zullen morgen (vrijdag) bij de gedupeerden worden bezorgd.

Uiterlijk 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.

Mocht je nog vragen hebben, dan kun je contact zoeken met [redacted]@ggdghor.nl) of met ondergetekende.

Met vriendelijke groet,

[redacted]

[redacted]

GGD GHOR Nederland
Zwarte Woud 2
3524 SJ Utrecht

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

Dit bericht is uitsluitend bestemd voor de geadresseerde. Het bericht kan vertrouwelijke informatie bevatten. Als u dit bericht per abuis hebt ontvangen, wordt u verzocht het te vernietigen en de afzender te informeren. GGD GHOR Nederland is niet aansprakelijk voor onjuiste en onvolledige overbrenging van de inhoud van een verzonden e-mail bericht, of een te late ontvangst daarvan.

9.5
Archived: donderdag 12 mei 2022 09:33:29
From: [redacted]d
Sent: maandag 8 februari 2021 16:45:24
To: [redacted]
Subject: FW: SPOED: Gemeenteraadsvragen over AVG
Importance: Normal
Sensitivity: None
Attachments:
NEN7510-HvB.PDF;

Van: [redacted]@ggdhvb.nl>
Verzonden: maandag 8 februari 2021 16:26
Aan: [redacted]@ggdhvb.nl>; [redacted]@ggdhvb.nl>; [redacted]@ggdhvb.nl>; [redacted]@ggdhvb.nl>
Onderwerp: Re: SPOED: Gemeenteraadsvragen over AVG

Hoi [redacted],

Hieronder onze opmerkingen. Bijgevoegd ook het NEN certificaat.

Met vriendelijke groet,

[redacted]

[redacted]

GGD Hart voor Brabant

Pettelaarpark 10 Den Bosch

Postbus 3024, 5003 DA Tilburg

www.ggdhvb.nl

[redacted]

Gezond doet leven!

Van: [redacted]@ggdhvb.nl>
Datum: maandag 8 februari 2021 om 13:51
Aan: [redacted]@ggdhvb.nl>
Onderwerp: FW: SPOED: Gemeenteraadsvragen over AVG

Zoals nu aangevuld door [redacted] . Graag samen doorspreken

Met vriendelijke groeten,

[redacted]

[redacted]

[redacted]

GGD Hart voor Brabant

Pettelaarpark 10 Den Bosch

Postbus 3024, 5003 DA Tilburg

www.ggdhvb.nl

[redacted]

[redacted]@ggdhvb.nl

Aanwezig op: ma-di-wo-do

Gezond² doet leven!

Van: [redacted]@ggdhvb.nl>
Verzonden: maandag 8 februari 2021 11:30
Aan: [redacted]@ggdhvb.nl>; [redacted]@ggdhvb.nl>
CC: [redacted]@ggdhvb.nl>; [redacted]@ggdhvb.nl>; J[redacted]@ggdhvb.nl>
Onderwerp: RE: SPOED: Gemeenteraadsvragen over AVG

Dag [redacted],

[redacted] is zeker wel aangehaakt bij de acties omtrent privacy. Sterker nog, zij neemt al veel acties voor haar rekening. Om 11.30 hebben wij weer een oploopje datadiefstal en zullen we afstemmen hoe we vandaag tot beantwoording komen.

Omwille van de snelheid geef ik alvast input van mijn kant. Dit moet absoluut nader worden gecheckt door [redacted] en naar ik eerder begreep ook [redacted]. Daarna moet communicatie ook meekijken.

1. In hoeverre is sprake van toepassing van de AVG -richtlijnen binnen de huidige reguliere bedrijfsvoering? Zijn er Aantoonbare certificaten en/of gehanteerde systemen?

Binnen de reguliere bedrijfsvoering van de GGD Hart voor Brabant worden vanzelfsprekend de AVG-richtlijnen gehanteerd. We beschikken over werkprotocollen in lijn met de AVG. Specifiek voor inzage- en verwijderingsverzoeken hebben we voor burgers een aanvraagformulier op onze website gepubliceerd. Vast en tijdelijk personeel dat toegang heeft tot databestanden met persoonsgegevens wordt bij aanstelling gevraagd om een Verklaring Omtrent Gedrag en getekende geheimhoudingsverklaring. Naar aanleiding van de datadiefstal heeft GGD Hart voor Brabant nogmaals een check uitgevoerd. We hebben vastgesteld dat alle door ons ingezette externe medewerkers een VOG en ondertekende geheimhoudingsverklaring hebben. Bij vaste, interne medewerkers is dit ook het geval voor zover ze bij ons zijn komen werken sinds het beleid omtrent VOG en geheimhoudingsverklaring is geïmplementeerd. Oudgedienden die al vele jaren bij ons werken hebben geen VOG omdat dit destijds nog niet bestond. Alle ambtenaren hebben echter sowieso een wettelijke geheimhoudingsplicht. Bij de overgang van oude Ambtenarenwet naar de Wet normalisering rechtsposities ambtenaren hebben al onze vaste medewerkers digitaal moeten bevestigen dat zij zich houden aan de integriteitsregels, waaronder geheimhouding. We zoeken uit of het nodig is om oudgedienden alsnog te vragen om een VOG en/of geheimhoudingsverklaring.

Daarnaast is de datalekprocedure opnieuw geoptimaliseerd en onder de aandacht gebracht bij de medewerkers. Dit heeft onderdeel uitgemaakt van communicatie richting de medewerkers met trekking tot bewustwording. Hierbij worden medewerkers regelmatig gewezen worden op de het belang van privacy en de wijze waarop zij zorgvuldig met persoonsgegevens om moeten gaan. Dit zal ook in de toekomst regelmatig onder de aandacht worden gebracht bij de medewerkers. Ook zijn er op landelijk werkinstructies opgesteld, welke regionaal op maat worden gemaakt in geval van regionale afwijkingen. Bij het opstellen van deze werkinstructies is rekening gehouden met de rechten en plichten uit de AVG.

GGD Hart voor Brabant is ten aanzien van het onderdeel bedrijfsvoering, belegd bij het Servicecentrum, gecertificeerd conform NEN7510.

3. Is er een risicotoets op actuele processen – gegeven de uiterste onzorgvuldigheid waarmee we te maken hebben gekregen tijdens de coronapandemie ten aanzien van het lekken van persoonlijke gegevens. Dit zorgt voor een enorme deuk in het vertrouwen. Hoe gaat de GGD hiermee om in de toekomst om dit te voorkomen? @[redacted] en @[redacted], willen jullie het eerste deel van de vraag voor jullie rekening nemen? @[redacted] en @[redacted], kunnen jullie al iets zeggen over de veronderstelde 'deuk in het vertrouwen'. @[redacted], kun jij iets zeggen over 'de toekomst'?

Op grond van de AVG is het verplicht voor systemen waarin gezondheidsinformatie wordt verwerkt een Data Protection Impact Assessments (DPIA) op te stellen. Zoals alle overheden zijn wij sindsdien druk aan de slag om op basis van een prioriteitenlijst DPIA's voor verschillende systemen op te stellen, daar waar deze voorheen nog niet bestonden. Door de coronacrisis zijn we daarmee nog niet zover mee als we zouden willen. Voor het landelijk ontwikkelde systeem CoronIT is sinds vorig jaar mei landelijk door GGD GHOR Nederland een Data Protection Impact Assessment (DPIA) in ontwikkeling. Deze wordt op zeer korte termijn definitief landelijk vastgesteld. Hierna zullen wij deze op korte termijn verwerken in een nadere regionale DPIA. De GGD brengt momenteel versnelling in het opstellen van alle benodigde DPIA's voor verschillende systemen.

Wij stellen ipv de tekst hierboven het volgende voor:

Een van de wijze waarop risico's inzichtelijk worden gemaakt, is door het uitvoeren van een DPIA. Vanuit landelijk (GGD GHOR Nederland) worden er DPIA's opgesteld voor de verschillende processen/systemen. Deze worden vervolgens voorgelegd aan de GGD'en in de regio's. De GGD dient de DPIA aan te vullen ten aanzien van het regionale proces. Voor het landelijk ontwikkelde systeem CoronIT is door GGD GHOR Nederland een Data Protection Impact Assessment (DPIA) in ontwikkeling. Deze wordt op zeer korte termijn definitief landelijk vastgesteld. Hierna zullen wij deze op korte termijn verwerken in een nadere regionale DPIA. Voor het vaccinatieproces is er tevens een DPIA in ontwikkeling. De GGD brengt momenteel versnelling in het opstellen van alle benodigde DPIA's voor verschillende systemen.

De processen die worden uitgevoerd in het kader van de bestrijding van het Coronavirus zijn 'ongoing processen'. Dit gezien de snelheid waarop de processen worden uitgevoerd en de frequentie waarin processen wijzigen. Het is daarom niet voldoende om eenmalig een risicotoetst uit te voeren. Daarom worden de processen doorlopend gemonitord, waarbij regelmatig verbeterpunten/risico's naar boven komen. Deze risico's worden beoordeeld en indien nodig gemitigeerd.

Op basis van de DPIA's en de monitoring van de processen kunnen waar nodig gericht nadere beveiligingsmaatregelen worden genomen. Op dit moment heeft de GGD al diverse beschermingsmaatregelen, die waar nodig worden verbeterd:

- Controle aan de poort. Mensen moeten een Verklaring Omtrent Gedrag (VOG) aanleveren en een geheimhoudingsverklaring ondertekenen. GGD Hart voor Brabant heeft zich bij de aanname van personeel ervan verzekerd dat altijd en voor iedereen een VOG en geheimhoudingsverklaring voor handen is.

- Autorisatieniveaus. Onze systemen kennen verschillende rollen met bijbehorende autorisatieniveaus. Niet iedereen kan bij alle gegevens en kan alle functionaliteiten (zoals het downloaden van data-exports) gebruiken. Binnen GGD Hart voor Brabant hebben wij een autorisatiematrix gebaseerd op rol of functie van iedere medewerker. Medewerkers krijgen alleen die autorisatie die nodig is voor zijn of haar functie. De autorisatiematrix wordt bijgehouden bij in-, door- en uitstroom van medewerkers. Er vindt hierop een maandelijkse check plaats. Naar aanleiding van de datadiefstal is ter check nog een keer doorgelicht wie binnen GGD Hart voor Brabant geautoriseerd is tot grote downloads (datadump). Dit is een zeer beperkte groep van medewerkers die dit op grond van hun functie daadwerkelijk nodig hebben, bijvoorbeeld om dashboards te maken.

- Controles op correct gebruik. De GGD'en controleren het gebruik van systemen door de medewerkers, en hebben de controles steeds verder verbeterd en doen dat nog steeds. Vanwege het belang van de virusbestrijding en de gevraagde snelheid zijn de GGD'en – op diverse manieren – met steekproefsgewijze controles van start gegaan. ~~De Autoriteit Persoonsgegevens had vóór het bekend worden van de datadiefstal geen aanvullende vragen gesteld over deze~~

~~werkwijze.~~ GGD Hart voor Brabant kan via de logging-functionaliteit van Microsoft 30 dagen terugkijken. De GGD gebruikt dit voor steekproeven en om terug te zoeken bij signalen en incidenten. GGD Hart voor Brabant gaat de periode van logging verlengen van 30 dagen naar 1 jaar, zodat we verder kunnen terugkijken. Verder verwacht GGD GHOR Nederland in maart systemen te implementeren die automatisch en continu zullen controleren op opvallend gebruik van de systemen (zoals grote downloads of onlogische inzage in dossiers). → hier een duidelijker onderscheid maken tussen wat er landelijk gebeurt en wat regionaal. Dat lijkt nu door elkaar te lopen, zie volgende voorstel:

De GGD'en (is dit niet GGD GHOR?) controleren het gebruik van systemen door de medewerkers, en hebben de controles steeds verder verbeterd en doen dat nog steeds. Vanwege het belang van de virusbestrijding en de gevraagde snelheid zijn de GGD'en (GGD GHOR?) – op diverse manieren – met steekproefsgewijze controles van start gegaan. Deze controles worden gebruikt voor steekproeven en om terug te zoeken bij signalen en incidenten. Verder verwacht GGD GHOR Nederland in maart systemen te implementeren die automatisch en continu zullen controleren op opvallend gebruik van de systemen (zoals grote downloads of onlogische inzage in dossiers.

GGD Hart voor Brabant kan via de logging-functionaliteit van Microsoft 30 dagen terugkijken (waar kunnen zij in terugkijken?). GGD Hart voor Brabant gaat de periode van logging verlengen van 30 dagen naar 1 jaar, zodat we verder kunnen terugkijken

Het geschonden vertrouwen willen wij herstellen door transparant te zijn over onze verbeterpunten en hoe wij deze oppakken. Naast voornoemde punten analyseren we momenteel of nog andere verbeteracties nodig zijn. Hierover communiceren wij transparant.

Tot slot willen we benadrukken dat geen van de gearresteerde vijf personen werkzaam was bij onze GGD. Wij hebben tot op heden ook geen aanwijzingen ontvangen van politie en justitie dat (vaste of ingehuurde) medewerkers van onze GGD worden verdacht. Ook hebben we zelf intern nadere checks uitgevoerd van onze 'logging-bestanden' op eventuele onregelmatigheden. We hebben geen onregelmatigheden aangetroffen. We hebben dus ook op basis van eigen onderzoek op dit moment geen aanwijzingen dat door onze medewerkers data zouden zijn gestolen. Het is evenwel nog niet duidelijk of door de gearresteerde medewerkers van het landelijk callcenter of medewerkers van andere GGD'en gegevens zijn gestolen en/of ten onrechte ingezien van inwoners uit ons werkgebied. Dit moet duidelijk worden uit het landelijke onderzoek van politie en justitie.

Van: [redacted]@ggdhvb.nl>
Verzonden: maandag 8 februari 2021 10:56
Aan: [redacted]@ggdhvb.nl>
CC: [redacted]@ggdhvb.nl>; [redacted]@ggdhvb.nl>; [redacted]@ggdhvb.nl>
Onderwerp: SPOED: Gemeenteraadsvragen over AVG
Urgentie: Hoog

Hi [redacted] (en overige collega's in de CC),

Onze agenda's stemmen even niet lekker op elkaar af, dus ik had liever gebeld maar nu alvast maar per email. Als je vragen hebt, bel me en ik bel z.s.m. terug.

In de bijlage tref je een aantal vragen die gesteld zijn door een gemeenteraadslid van de gemeente Dongen. In eerste instantie had ik [redacted] gevraagd om vraag 1 te beantwoorden en vraag 3 in samenwerking met een aantal collega's. Inmiddels begrijp ik van [redacted] dat jij en [redacted] bezig zijn op het privacy dossier en dat [redacted] daar nog niet helemaal op aangehaakt is, terwijl dat wel relevant is voor de beantwoording van de vragen.

Mag ik jou vragen om de beantwoording van vraag 1 en vraag 3 in samenwerking met in ieder geval [redacted] en [redacted] op te

pakken? Vraag 2 is beantwoord door [redacted]. Vraag 4 hoeven wij niet te beantwoorden. Nota bene, aan vraag drie kleeft ook een communicatie- / imagokant. Willen jullie ervoor zorgen dat ook die kant van de vraag beantwoord wordt?

Ik ontvang het antwoord graag uiterlijk eind deze dag, zodat ik ze met [redacted] kan afstemmen voordat ik de antwoorden aan de gemeente terugstuur.

Heel veel dank!!!

Hartelijke groet,

[redacted]

[redacted]

GGD Hart voor Brabant

Pettelaarpark 10

5216 PD, 's-Hertogenbosch

Postbus 3024, 5003 DA Tilburg

www.ggdhvb.nl

[redacted]@ggdhvb.nl

Aanwezig op: ma t/m vr

[redacted]

[redacted]

Gezond? doet leven!

Genomen maatregelen na bekend worden landelijke datadiefstal

Eind januari zijn wij allemaal opgeschrikt door het bericht over het onzorgvuldig omgaan met bijzondere persoonsgegevens en het stelen van data uit de landelijke GGD-systemen CoronIT en HPZone Lite. Landelijk is aangifte gedaan, zijn er mensen in deze zaak gearresteerd en wordt grootschalig onderzoek gedaan door politie en justitie. Binnen GGD Hart voor Brabant hebben we continue aandacht voor kwaliteitsbevordering én -bewaking. We hebben een aantal bestaande maatregelen gecontroleerd en geïntensiveerd. Welke dat zijn lees je hier.

- **Controle aan de poort**. GGD Hart voor Brabant heeft nogmaals een check uitgevoerd. We hebben vastgesteld dat alle door ons ingezette externe medewerkers een VOG (Verklaring Omtrent Gedrag) en ondertekende geheimhoudingsverklaring hebben. Bij vaste, interne medewerkers is dit ook het geval voor zover ze bij ons zijn komen werken sinds het beleid omtrent VOG en geheimhoudingsverklaring is geïmplementeerd. Oudgedienden die al vele jaren bij ons werken en toegang hebben tot een van deze systemen zijn op basis van landelijk beleid verzicht om alsnog een VOG aan te vragen.
- **Autorisatieniveaus**. Naar aanleiding van de datadiefstal is nog een keer doorgelicht wie binnen GGD Hart voor Brabant geautoriseerd is tot grote downloads (datadump). Dit is een zeer beperkte groep van medewerkers die dit op grond van hun functie daadwerkelijk nodig hebben, bijvoorbeeld om dashboards te maken.
- **Controles op correct gebruik**. GGD Hart voor Brabant heeft een nadere check uitgevoerd van onze ‘logging-bestanden’ en geen onregelmatigheden aangetroffen. We zien geen afwijkingen in de

  ITomgeving van onze GGD. Ons beeld is dat er binnen of door GGD Hart voor Brabant geen gegevens in verkeerde handen zijn gevallen. GGD Hart voor Brabant wil de periode van logging verlengen van 30 dagen naar 1

9.6 voor Brabant wil de periode van logging verlengen van 30 dagen naar 1 jaar, zodat we verder kunnen terugkijken. Verder verwacht GGD GHOR Nederland in maart systemen te implementeren die automatisch en continu zullen controleren op opvallend gebruik van de systemen (zoals grote downloads of onlogische inzage in dossiers).

Verder hebben we de volgende aanvullende maatregelen genomen:

- **Communicatie**. GGD Hart voor Brabant vindt het belangrijk om eigen inwoners gericht te informeren over de situatie, wat wij eraan doen en hoe mensen een verwijderingsverzoek kunnen indienen. We wijzen ons inwoners in eerste instantie op de landelijke lijst met veel gestelde vragen van GGD GHOR Nederland. Zit het antwoord op hun vraag er niet bij, dan adviseren wij hen om contact op te nemen met het landelijke nummer voor deze datadiefstal. Dit telefoonnummer (085- 130 82 26) is dagelijks bereikbaar van 09.00 uur tot 21.00 uur. Daarnaast attenderen we inwoners uit onze regio op het recht om hun eigen gegevens in te zien, te wijzigingen of te laten verwijderen.
- **Verzoeken voor gegevensverwijdering.** 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. De GGD heeft hiervoor al jaren een staand beleid en werkprotocol, conform de AVG. GGD GHOR Nederland heeft aangegeven dat verwijderingsverzoeken voor CoronIT in principe kunnen worden gehonoreerd. Alleen de gegevens in HPZone (Lite) van positief geteste personen mogen op grond van wetgeving niet worden verwijderd. Op onze website kunnen burgers via het onderdeel Corona bij veel gestelde vragen de link naar privacy en corona vinden. Daar is een formulier te downloaden, waarmee een aanvraag kan worden gedaan. GGD Hart voor Brabant heeft sinds vorige week 60 inzage- en verwijderingsverzoeken ontvangen.
- **Uitzetten van functionaliteiten in de systemen.** Om het risico per direct te verminderen zijn landelijk in CoronIT en HPZone diverse functionaliteiten uitgezet. Het is niet meer mogelijk om downloads van gegevensbestanden te doen, prints van gegevensbestanden te maken (omdat dit als PDF kon) en om zoekopdrachten te doen (query's) op BSN en postcode. Het risico op verder misbruik is hiermee zoveel mogelijk

  gereduceerd. Inmiddels is het onze collega's van het datawarehouse team en onderzoek weer gelukt om onze regionale dashboards in de lucht te krijgen. Complimenten!

9.6 krijgen. Complimenten!

Landelijk wordt op dit moment gewerkt aan de vervanging van HPZone lite door de GGD Contact app met bijbehorend BCO-portaal. Nadere informatie volgt over wat dit voor ons gaat betekenen.

9.7

Overeenkomst gebruik ter beschikking gestelde bedrijfsapparatuur

Versie 5: februari 2020

De GGD Hart voor Brabant *(*verder te noemen *"De werkgever")* stelt aan haar medewerker bedrijfsapparatuur inclusief toebehoren in bruikleen ter beschikking:

de heer/mevrouw : [redacted]
(verder te noemen *"De medewerker"*)
Personeelsnummer : 108011

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 van bedrijfseigendommen
   - *"De medewerker"* wordt geacht de e-mail (aangeboden door *"De werkgever"*) voor zakelijke doeleinden te gebruiken.
   - Indien *"De werkgever"* *"De medewerker"* een computer, laptop, mobiele telefoon of andere apparatuur ter beschikking heeft gesteld, wordt *"De medewerker"* geacht deze voornamelijk te gebruiken voor zakelijke doeleinden. Afspraken hierover worden vastgelegd in een 'gebruikersovereenkomst'. Incidenteel en beperkt gebruik voor persoonlijke doeleinden van deze elektronische communicatiemiddelen is toegestaan. Hierbij dienen wel de regels van zorgvuldigheid, redelijkheid, integriteit en goede naam in acht te worden genomen.
   - Ter beschikking gestelde apparatuur blijft ten allen tijde eigendom van *"De werkgever"*.
   - *"De medewerker"* verplicht zich om na afloop van het dienstverband alle ter beschikking gestelde apparatuur in goede staat bij *"De werkgever"* in te leveren.
   - *"De medewerker"* wordt geacht als een goed huisvader om te gaan met ter beschikking gestelde apparatuur.
   - Kosten voor vervanging of reparatie van ter beschikking gestelde apparatuur komen voor rekening van de GGD Hart voor Brabant. In het geval kosten voor vervanging of reparatie veroorzaakt door nalatigheid van *"De medewerker"*, worden deze kosten verhaald op *"De medewerker"*.
   - Tussentijds te vervangen apparatuur wordt vervangen door eenzelfde of gelijkwaardige apparatuur, ook indien deze kosten voor rekening van *"De medewerker"* komen.

- Medewerkers van GGD Hart voor Brabant gaan veel om met vertrouwelijke gegevens. Het is niet toegestaan om zonder toestemming van *"De werkgever"*, computerprogrammatuur of andere auteursrechtelijk beschermde werken te kopiëren en/of te vermenigvuldigen.
- Indien afspraken uit de gebruikersovereenkomst niet nagekomen worden, is *"De werkgever"* bevoegd een geschil betreffende de teruggave van de apparatuur aan het oordeel van de President van de arrondissementsrechtbank te 's-Hertogenbosch of Tilburg (rechtsprekende in kort geding) te onderwerpen.

4. 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"*.

5. 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.

6. 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.

7. 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"*

8. 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 Servicecentrum.
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;
- 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.

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
[redacted]
Datum: 8 januari 2021

Informatieveiligheidsbeleid

2018 - 2022

Het Service Centrum

Versie: 1.0

Datum: 22-03-2018

Alleen voor intern gebruik

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

Alleen voor intern gebruik

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

Alleen voor intern gebruik

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.

Alleen voor intern gebruik

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.

Alleen voor intern gebruik

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.

Alleen voor intern gebruik

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)

Alleen voor intern gebruik

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.

Alleen voor intern gebruik

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 /

Alleen voor intern gebruik

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.

Alleen voor intern gebruik

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.

Alleen voor intern gebruik

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.

Alleen voor intern gebruik

Privacystatement voor de medewerkers van de GGD Hart voor Brabant

Uitgangspunten:

1. Wij verwerken jouw persoonsgegevens op een rechtmatige, behoorlijke en transparante manier.
2. Wij verwerken jouw persoonsgegevens alleen voor het doel waarvoor we ze verzamelden.
3. Wij verwerken niet meer persoonsgegevens dan nodig voor de beschreven doeleinden.
4. Wij spannen ons in voor de juistheid en volledigheid van de verwerkte en te verwerken persoonsgegevens.
5. Wij bewaren persoonsgegevens niet langer dan nodig is voor het doel van de verwerking.
6. Wij gaan vertrouwelijk om met persoonsgegevens en zorgen voor adequate beveiliging ervan.

We vinden het belangrijk om jou als werknemer uitgebreid te informeren over ons privacystatement en vragen je om ons privacystatement goed door te lezen.

Privacystatement voor de medewerkers van de GGD Hart voor Brabant

De GGD wil voldoen aan de eisen van de Algemene verordening gegevensbescherming (AVG). Ook vinden we het belangrijk om jou als werknemer uitgebreide informatie te geven over ons privacystatement. Daarnaast willen we je via dit statement informeren over je rechten. Tot slot willen we je laten weten bij wie je terecht kunt met vragen, verzoeken of klachten.
We vragen je deze informatie goed door te lezen.

Een ***persoonsgegeven*** is elke informatie die te herleiden is naar een persoon. Voor jou betekent dit dat die informatie direct over jou gaat of deze informatie naar jou te herleiden is. Dit kan bijvoorbeeld over je naam, geboortedatum en adres gaan, maar ook je personeelsnummer, zakelijke e-mailadres of zakelijke telefoonnummer is een persoonsgegeven.

Het ***verwerken van persoonsgegevens*** betreft alle handelingen die we kunnen uitvoeren met jouw persoonsgegevens, van verzamelen tot en met vernietigen. Dit is dus een heel ruim begrip. Handelingen die er in ieder geval onder vallen, zijn: het verzamelen, vastleggen, bewaren, wijzigen, opvragen, raadplegen, gebruiken, doorsturen, verspreiden, beschikbaar stellen, samenbrengen, met elkaar in verband brengen, afschermen, uitwissen en vernietigen van gegevens.

Gronden waarop wij jouw gegevens mogen verwerken

We verwerken je gegevens om een of meer van de volgende redenen. Deze staan in de wet:

- de gegevens zijn nodig voor het besluiten tot en/of uitvoeren van je aanstelling;
- de gegevens zijn voor ons nodig om te voldoen aan een wettelijke plicht (denk bijvoorbeeld aan het correct afdragen van belastingen en premies of de identificatieplicht);

- de gegevens zijn nodig omdat we daar als organisatie een gerechtvaardigd belang bij hebben (denk bijvoorbeeld aan de situatie waarin er een juridische procedure speelt of dreigt en wij verweer moeten kunnen voeren), of;
- een situatie van levensbelang (bijvoorbeeld in een noodsituatie, zoals bij een ongeval of bij een aandoening waarbij er voor jou acute zorg nodig is). Dan is het voor ons nodig om over je persoonsgegevens te kunnen beschikken om bijvoorbeeld medicijnen toe te dienen (denk aan gezondheidsinformatie bij een ernstige allergie, epilepsie of suikerziekte), hulp te kunnen regelen of anderen te kunnen informeren (zoals je familieleden);
- we hebben je toestemming voor bepaalde handelingen nodig.

Verplichting om gegevens te verstrekken

Je bent verplicht ons de gevraagde gegevens te verstrekken als het voor ons nodig is die gegevens te verwerken om bijvoorbeeld tot een aanstelling te besluiten, deze uit te voeren en/of om te voldoen aan een wettelijke verplichting. Je kunt ook denken aan gegevens die nodig zijn om je aan te kunnen melden voor een pensioenregeling, collectieve verzekering of leaseregeling. Je kunt in die gevallen niet weigeren om de gegevens te verstrekken. Doe je dat wel, dan kan dat betekenen dat wij je niet in dienst nemen of dat je geen gebruik kunt maken van bepaalde voorzieningen.

De gegevens die wij van jou verwerken

We verwerken in de ***personeels- en salarisadministratie*** de volgende *gegevens*:

- naam, voornamen, roep- en geboortenaam, voorletters, eventuele titel, geslacht, geboortedatum, adres, postcode, woonplaats, telefoonnummer(s) en andere gegevens die wij nodig hebben om met jou te communiceren, zoals je e-mailadres;
- bankrekeningnummer;
- burgerservicenummer;
- een kopie van je paspoort/identiteitskaart;
- burgerlijke staat;
- pensioenoverzicht;
- een personeels- en registratienummer dat geen andere informatie bevat dan bedoeld onder het eerste bolletje;
- sollicitatiebrief, CV;
- registratiegegevens BIG of Kwaliteitsregister V&VN;
- gegevens over door jou gevolgde en nog te volgen opleidingen, cursussen en stages;
- gegevens over je dienstverband; uren, werktijden, vast/tijdelijk, functiebenaming, plaats in de organisatie, datum in- en uitdienst, werklocatie;
- gegevens met het oog op de administratie van je afwezigheid in verband met verlof, arbeidsduurverkorting, bevalling of ziekte, maar geen gegevens over de aard van de ziekte;
- partner- en kindgegevens; voorletters, naam, geboortedatum, burgerlijke staat;
- contactpersoonsgegevens bij nood; naam, telefoonnummer, relatie tot medewerker;
- gegevens die nodig zijn voor een overeengekomen arbeidsvoorwaarde;
- gegevens die we in jouw belang opnemen rond je arbeidsomstandigheden;

- gegevens over tot je functioneren en eventuele loopbaanbegeleiding, voor zover die gegevens bij jou bekend zijn;
- gegevens voor het berekenen, vastleggen en betalen van je salaris, vergoedingen en andere geldsommen en beloningen in natura aan jou of voor jou;
- gegevens voor het berekenen, vastleggen en betalen van belasting en premies voor jou;
- gegevens die nodig zijn voor de uitvoering of toepassing van een wet.

We verwerken uit beveiligings- en integriteitsoogpunt de volgende gegevens:

- de logbestanden: informatie over welke medewerker een bepaald dossier heeft geraadpleegd, wanneer en hoe vaak medewerkers dossiers raadplegen;
- call logs: welke medewerker met wie een telefoongesprek heeft gehad.

Met opmaak: Met opsommingstekens + Niveau: 1 + Uitgelijnd op: 0,63 cm + Inspringen op: 1,27 cm

De verwerking van bovenstaande gegevens gebeurt alleen voor één of meer van deze ***doelen***:

- het geven van leiding aan je werkzaamheden;
- het behandelen van personeelszaken;
- het vaststellen en (laten) uitbetalen van je salaris;
- het regelen van aanspraken op uitkeringen in verband met de beëindiging van je aanstelling;
- je opleiding en ontwikkeling;
- de bedrijfsmedische zorg die voor jou van toepassing is;
- het bedrijfsmaatschappelijk werk;
- de verkiezing van de leden van een ondernemingsraad of personeelsvertegenwoordiging;
- de interne controle en de bedrijfsbeveiliging;
- de uitvoering van een voor jou geldende arbeidsvoorwaarde;
- het opstellen van een lijst van data van verjaardagen van werknemers en andere feestelijkheden en gebeurtenissen;
- het verlenen van ontslag;
- de administratie van de personeelsvereniging;
- het innen van vorderingen. Dit is ook: het uit handen geven van een vordering aan bijvoorbeeld een incassobureau of een deurwaarder;
- het berekenen, vastleggen en betalen van je salaris, vergoedingen en andere geldsommen en beloningen in natura aan jou of voor jou;
- het voor jou berekenen, vastleggen en betalen van belasting en premies;
- de personeelsadministratie;
- het behandelen van geschillen en het doen uitoefenen van accountantscontrole;
- de uitvoering of toepassing van een andere wet.
- Voor beveiligings- en integriteitsdoeleinden: te voorkomen dat en te controleren of persoonsgegevens onrechtmatig door medewerkers of partners van GGD'en worden verwerkt.

Doorgifte van jouw persoonsgegevens

We gebruiken je persoonsgegevens alleen voor de eigen bedrijfsvoering, in het kader van een (intern) sollicitatietraject en (de uitvoering van) de aanstelling. We gebruiken deze gegevens alleen voor de doelen waarvoor we deze gegevens kregen.

Het kan in sommige gevallen nodig zijn om je gegevens door te geven aan anderen, zoals aan een partij die namens ons gegevens verwerkt. Een paar voorbeelden:

- salarisverwerking: we verstrekken gegevens aan onze salarisverwerker;
- ziekte en re-integratie: we verstrekken gegevens aan de bedrijfsarts en/of UWV;
- een loonbeslag: we verstrekken gegevens aan de deurwaarder;
- pensioenfonds;
- Belastingdienst.

Met partijen die namens ons persoonsgegevens verwerken (de 'verwerkers'), sluiten we (voor zover dit nodig is) verwerkersovereenkomsten. Dit doen we zodat, wanneer we gegevens aan hen verstrekken, onder meer vaststaat dat zij deze gegevens ook goed beveiligen en ze tijdig melding bij ons doen bij een (vermoeden van een) datalek.

Het bewaren van jouw persoonsgegevens

Bij het bewaren van persoonsgegevens is ons uitgangspunt dat we gegevens niet langer bewaren dan nodig is voor het doel waarvoor wij ze verwerkt hebben. Voor zover die er zijn nemen we de wettelijke bewaartermijnen in acht.

We kunnen gegevens langer bewaren wanneer we daar een gerechtvaardigd belang bij hebben (bijvoorbeeld wanneer er een juridische procedure loopt of is aangekondigd en we ons moeten kunnen verweren).

De bewaartermijn is:

- fiscaal relevante gegevens (documenten in/van de salarisadministratie): 7 jaar na uitdiensttreding;
- loonbelastingverklaring en kopie identiteitsbewijs: 5 jaar na uitdiensttreding;
- overige gegevens uit personeelsdossier: 2 jaar na uitdiensttreding;
- sollicitatiegegevens: 4 weken na het einde van de procedure.
- Loggegevens: niet lange dan noodzakelijk.

Als de bewaartermijn is verstreken, vernietigen we de gegevens.

Het beveiligen van jouw persoonsgegevens

De beveiliging van je persoonsgegevens is bij ons goed geregeld door organisatorische en technische maatregelen. Alleen medewerkers die daartoe van ons een bevoegdheid kregen, hebben toegang tot de gegevens en zijn gehouden aan geheimhouding, behalve als ze moeten voldoen aan wet- en regelgeving. We kennen daardoor een passend beschermingsniveau. We stellen dit ook periodiek bij wanneer dit nodig is.

Jouw rechten

Je hebt op grond van de AVG het recht rond de persoonsgegevens die we van jou verwerken te vragen om:

- inzage in je gegevens, zoals je personeelsdossier (behalve eventuele persoonlijke werkaantekeningen van je leidinggevenden en anderen);

- een kopie van je gegevens (behalve persoonlijke werkaantekeningen van je leidinggevende(n) of anderen binnen onze organisatie);
- informatie te ontvangen over de verwerking van je gegevens (hiertoe dient ook dit privacystatement, maar misschien heb je nog vragen die we hiermee niet beantwoorden);
- informatie te laten corrigeren die feitelijk niet klopt (let wel: je kunt niet een functionerings- of beoordelingsverslag laten corrigeren als je het daarmee oneens bent. Je kunt dan wel een verklaring opstellen die je aan je personeelsdossier kunt laten toevoegen);
- onvolledige informatie compleet te maken wanneer dat nodig is voor het doel waarvoor we de gegevens verwerken;
- in bepaalde gevallen om je gegevens te laten verwijderen (let wel: we hoeven hier geen gehoor aan te geven wanneer we bij het (langer) bewaren van je gegevens nog een gerechtvaardigd belang hebben, wanneer dit nodig is bij de uitvoering van je aanstelling of om te voldoen aan een wettelijke plicht of op basis van een andere in de wet genoemde reden;
- in bepaalde gevallen om de gegevens te laten 'beperken' (let wel: we streven ernaar zo min mogelijk data te verzamelen);
- in bepaalde gevallen om bezwaar te maken tegen het gebruik van je gegevens;
- als je toestemming hebt gegeven voor het gebruik van je gegevens (zoals voor het gebruik van je foto op een 'wie-is-wie' pagina of op onze website), die toestemming weer in te trekken. De intrekking geldt dan voor toekomstig gebruik van jouw gegevens;
- al je digitaal verwerkte gegevens in een gangbaar format mee te krijgen en (als dat technisch mogelijk is) deze gegevens op die manier aan een andere partij over te dragen.

Met vragen, verzoeken of klachten over de verwerking van je persoonsgegevens of als je een beroep wilt doen op je rechten, kun je contact opnemen met de Servicedesk HR (servicedesk.hr@hetservicecentrum.nl of 0800 3 666 666)**.** We beantwoorden je vraag, verzoek of klacht in beginsel binnen 4 weken. Als het antwoord toch meer tijd kost, informeren we je hierover binnen 4 weken. Als we goede redenen hebben om je verzoek te weigeren, lichten we toe waarom dat zo is.

Als een klacht niet of slechts gedeeltelijk op te lossen is, kun je een klacht indienen bij de Autoriteit persoonsgegevens in Den Haag.

Voor nadere informatie en vragen over privacybescherming kun je je wenden tot onze functionaris gegevensbescherming: [redacted]

heeft verwijderd: [redacted]

Datum en aanpassing van het privacystatement

We behouden ons het recht voor dit privacystatement aan te passen. Als het om een belangrijke wijziging gaat zullen we je daarvan op de hoogte brengen.

heeft verwijderd: ¶
¶

9.9

De GGD Hart voor Brabant

Als GGD Hart voor Brabant hebben we hart voor de inwoners in onze regio. De veranderingen in onze omgeving vragen een andere manier van werken. We willen buiten gebaande paden treden. Voor onze inwoners en klanten oplossingen bedenken die echt een toegevoegde waarde hebben. We willen dat onze burgers zelfstandig en vanuit eigen kracht de uitdagingen in hun leven aangaan.

Je komt te werken in een innovatieve, dynamische, klantgerichte organisatie die er écht toe doet in de samenleving. Dat betekent voor ons allemaal dat we zelf onze verantwoordelijkheid nemen, initiatief tonen, lef hebben, met goede en vernieuwende ideeën komen. Dit doen we vanuit vakmanschap, talenten en passie! In een zelfstandig team werk je resultaatgericht aan gezondheid en veiligheid wat past binnen modern werkgeverschap. Bekijk ons filmpje om meer van ons te zien.

Voor de sector Bedrijfsontwikkeling zijn wij per direct op zoek naar een

Privacy Officer

32 tot 36 uur per week

Wat ga je doen?

De Privacy Officer is verantwoordelijk voor het vormgeven, uitvoeren en bewaken van de privacy maatregelen op operationeel en tactisch niveau binnen de GGD Hart voor Brabant. Je zorgt voor bewustwording over de AVG binnen de hele organisatie en zorgt dat ons verwerkingsregister up-to-date blijft. Je bent het eerste aanspreekpunt voor medewerkers met betrekking tot privacyvraagstukken.

Samen met de Functionaris Gegevensbescherming en de CISO zorg je ervoor dat de informatieveiligheid en privacy binnen de GGD Hart voor Brabant is geborgd. De volgende werkzaamheden vallen onder het takenpakket van de Privacy Officer:

- Adviseert medewerkers en management als eerste aanspreekpunt over verwerking van persoonsgegevens en adviseert medewerkers en (keten)partners over de te nemen maatregelen op het gebied van privacy;
- Stimuleert het bewustzijn op het gebied van privacy binnen de organisatie en volgt nieuwe ontwikkelingen en wetgeving op het gebied van privacy;
- Voert Data Protection Impact Assessments (DPIA’s) uit of ondersteunt hierbij;
- Ziet toe of de uitvoering van de DPIA’s in overeenstemming is met de wet- en regelgeving;
- Zorgt dat het verwerkingsregister actueel is en dat nieuwe verwerkingen worden opgenomen in het register;

- Coördineert, inventariseert en meldt de datalekken bij de Autoriteit Persoonsgegevens (AP) in samenwerking met de Functionaris Gegevensbescherming;
- Coördineert de afhandeling van rechten van betrokkenen;
- Actualiseert en implementeert het Privacy beleid;
- Adviseert over het aangaan van verwerkersovereenkomsten en beoordeelt bestaande verwerkersovereenkomsten;
- Levert een bijdrage aan de vorm en opzet van kwaliteitsonderzoeken met betrekking tot verwerken persoonsgegevens.

Je maakt het verschil als je…

- effectief en enthousiast de praktische doorvertaling van de AVG kan maken;
- minimaal 2 jaar werkervaring hebt als Privacy Officer, of als adviseur op het gebied van privacy- en gegevensbescherming;
- minimaal een afgeronde HBO/WO opleiding op het gebied van Rechten hebt;
- actuele kennis van de AVG en aanverwante wetgeving onder andere met betrekking tot (publieke) gezondheidszorg hebt;
- resultaatgericht bent, organisatiesensitief handelt en uitstekend kunt adviseren;
- pragmatisch bent ingesteld en mogelijkheden en oplossingen vanuit verschillende invalshoeken benadert;
- je breed georiënteerd bent waardoor je een weg kan vinden in een grote organisatie met veel verschillende taken.
- een klantgerichte instelling hebt, goed samenwerkt en flexibel bent.

Privacy certificering is een pré. Daarnaast ook een pluspunt als je kennis van toepasselijke wetgeving (Wmo, Jeugdwet) en gemeentelijke regelgeving meebrengt.

Voldoe je aan bovenstaande criteria en zie jij jezelf als onze nieuwe collega? Dan nodigen we je graag uit om te solliciteren!

Wat wij jou bieden…

- een tijdelijke aanstelling als vakspecialist B vallend onder de cao sgo, voor de duur van in eerste instantie één jaar. Verlenging van de aanstelling bij goed functioneren behoort tot de mogelijkheden. De aanstelling gaat in eerste instantie via een door ons geselecteerd bureau.
- een bruto maandsalaris van minimaal € 2.973,- en maximaal € 4.494,- (salarisschaal 10) bij een dienstverband van 36 uur per week. Inschaling is afhankelijk van je opleiding en ervaring. Daarboven op komt een Individueel Keuzebudget van 17,05% (inclusief vakantiegeld en eindejaarsuitkering).
- goede secundaire arbeidsvoorwaarden en een stimulerend werkklimaat met volop kansen voor ontwikkeling.

- werken bij een organisatie die er écht toe doet in de samenleving.

Ja, ik wil deze baan!

Via de knop ‘Solliciteer direct’ kun je jouw motivatiebrief samen met je CV uiterlijk 12 september 2021 uploaden. Wij zijn vooral geïnteresseerd om te lezen wie je bent en waarom jij bij ons past.

In verband met de vakantieperiode vindt de eerste en tweede gespreksronde plaats op vrijdag 17 september.

Vragen of meer informatie? Neem dan contact op met [redacted], via [redacted]

Acquisitie naar aanleiding van deze advertentie stellen wij niet op prijs.

9.11

From: [redacted]
Sent: maandag 10 mei 2021 15:02:17
To: [redacted]
Subject: terugkoppeling MT
Importance: Normal
Sensitivity: None
Attachments:
2.5.1 Advies inrichting privacy en informatiebeveiliging GGD Hart voor Brabant.pdf; 4.2 RI&E.pdf; 4.5 Cultuuraudit.pdf;

In het MT is het volgende besproken/besloten wat direct relevant is voor ons:

- **2.5.1 CISO**. Op advies van [redacted] en [redacted] worden enkele functionarissen aangesteld om de gegevensbescherming op orde te krijgen: een trainee die op korte termijn beleid opzet voor gegevensbescherming, een privacy officer die moet gaan werken aan privacybeleid en een Chief Information Security Officer (CISO) voor o.a. implementatie van GGD Contact en de uitfasering van HP Zone (Lite), ondersteuning en advisering bij DPIA's, veiligheid van de netwerken op de test- en vaccinatielocaties en opstellen van een informatiebeveiligingsbeleid voor programma Corona. De CISO komt ten laste van de Compensatieregeling en wordt functioneel aangestuurd door ons vanuit het programma i.s.m. [redacted].
- **4.2 RI&E**. De GGD gaat een RI&E doen, waarin ook het programma Corona wordt meegenomen. Ik heb verzocht om de bezoeken aan test- en vaccinatielocaties in goed overleg met ons te plannen, zodat het niet belastend is tijdens onze piekinzet. Ook heb ik aangegeven dat we druk bezig zijn met luchtkwaliteit op de testlocaties en dat dit niet dubbel moet worden gedaan.
- **4.5 check klachtenprocessen**. N.a.v. een Tweede Kamermotie over het datalek wordt de GGD'en gevraagd een check te doen op klachtenprocessen. [redacted] is daarbij aangesloten.
- **AB-brief update Corona.** Het MT heeft gevraagd om weer een updatebrief over Corona naar het AB te sturen.

Met vriendelijke groeten,

[redacted]

[redacted]

GGD Hart voor Brabant

Pettelaarpark 10

's-Hertogenbosch

www.ggdhvb.nl

[redacted]

[redacted]@ggdhvb.nl

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:

10.1

VERBETERPLAN GEGEVENSBESCHERMING & GEVOLGBESTRIJDING DATADIEFSTAL

MT
8 februari 2021

Gezond² doet leven!

10.1

Doel bespreking

Gezamenlijke beeldvorming en meningsvorming over:

1. Huidige situatie
2. Verbetersporen gegevensbescherming
3. Specifiek: aanpak informatievoorziening (DD en structureel)
4. Extra personele behoefte

Inrichting projectorganisatie staat nu niet op de agenda.
Dit wordt na deze bespreking verder uitgewerkt.

Huidige situatie

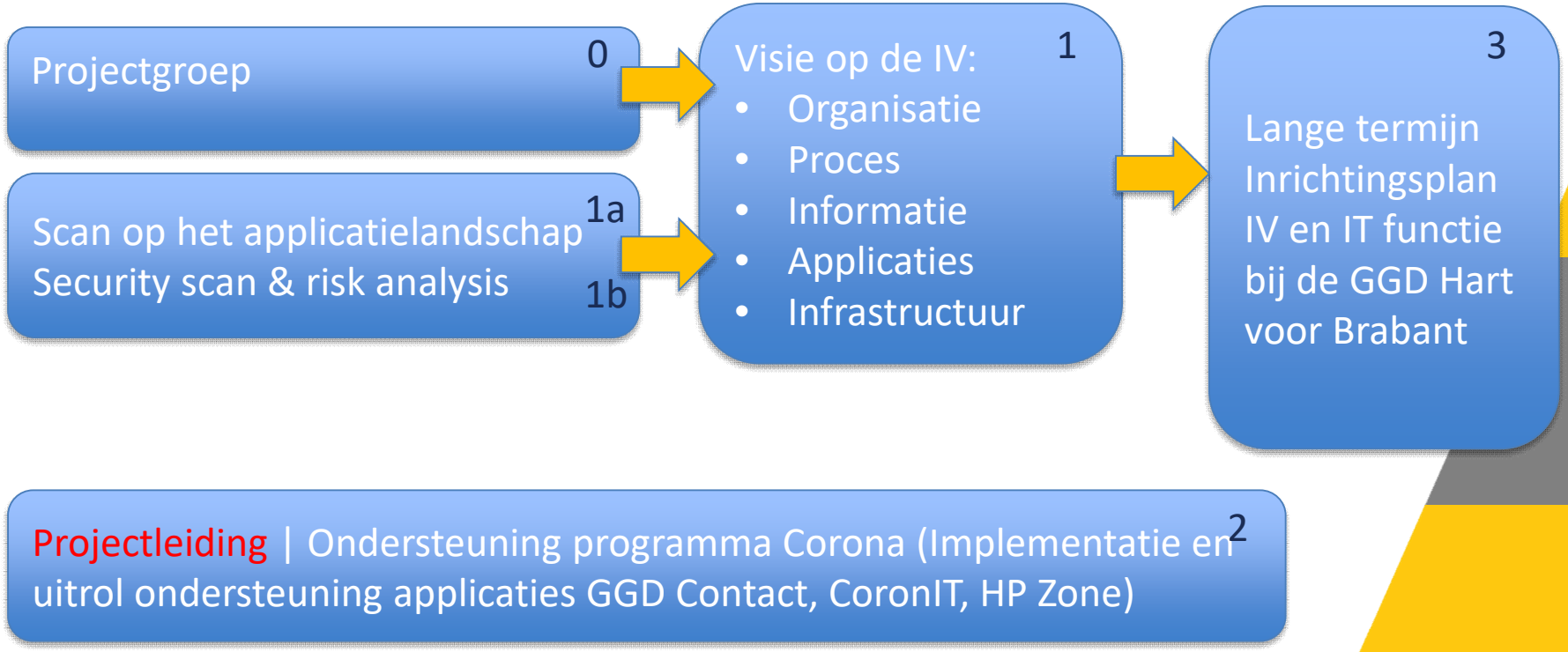
- 25 januari bekend geworden (vandaag 2 weken geleden)
- Sindsdien 6x vergaderd in 'stand-up' (BOB) met kernspelers om acties uit te zetten
- 29 januari: algemene brief aan AB, intern nieuwsbericht
- 3 februari: nadere brief aan DB
- 4 februari: DB-bespreking
- 5 februari: nadere brief aan AB
- Onderzoek AP aangekondigd

Verbetersporen *gegevensbescherming en gevolgbestrijding datadiefstal*

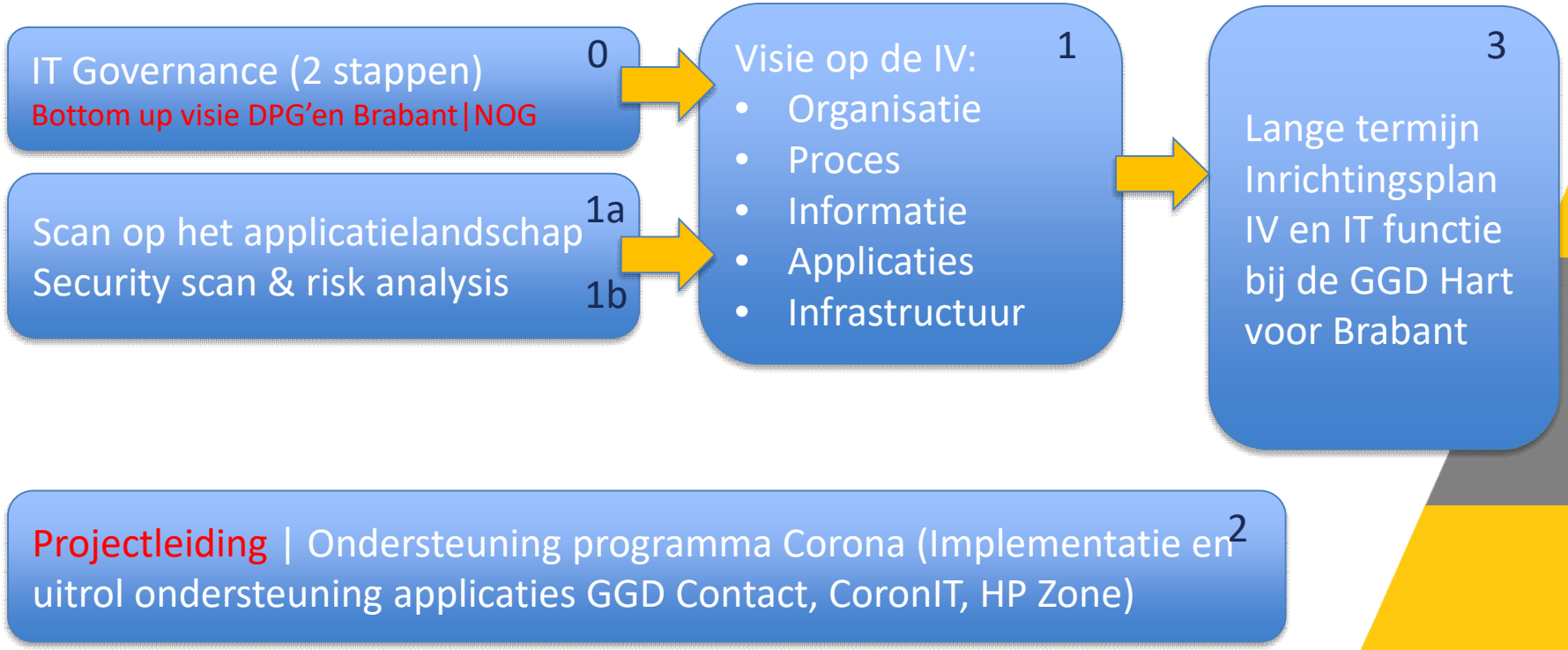
10.1

Hoofdspoor	Actielijnen
AVG	• Werkprotocollen AVG • Inzage- en verwijderingsverzoeken
Informatievoorziening	0. Standpuntbepaling landelijke-regionale governance 1. Visie informatievoorziening 1a. Applicatielandschap 1b. Security scan & risk analysis 2. Implementatie IT-wijzigingen testen, BCO, vaccinatie, IZB 3. Inrichtingsplan IV en overdracht programma
Personeel	• VOG & geheimhoudingsverklaringen • Trainingen & instructies 'omgaan met persoonsgegevens'
Werkprocessen	• Werkprocessen programma Corona • Werkprocessen sectoren (IZB, onderzoek)
Stakes	• Juridisch • Onderzoeksbegeleiding Autoriteit Persoonsgegevens • Financiën
Communicatie	• Externe communicatie & persvoorlichting • Interne communicatie • Informeren bestuur

10.1 Organisatie verbetersporen



Actielijnen informatievoorziening



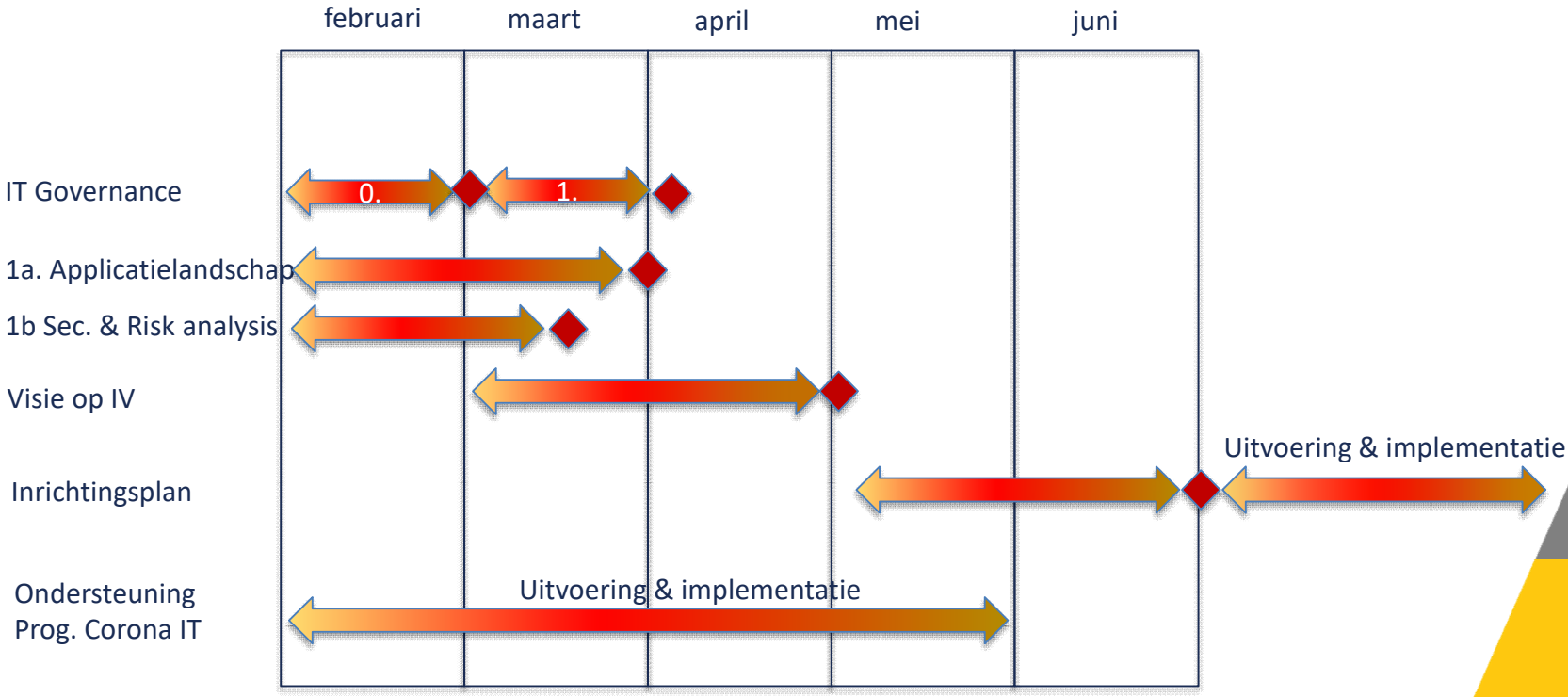
10.1

Actielijnen informatievoorziening

Actielijnen	Deliverable	Opdrachtgever	Opdrachtnemer
0. IT Governance	Fase 0: werksessie(s) modellen van IT Governance | bottom up visie	GGD HvB, i.s.m. WB, ZOB, NOG	
1. Visie informatievoorziening	Fase 1: uitwerking onderdeel organisatie	GGD HvB	
	1a. Totale applicatielandschap in kaart	Sector BO HvB Sector BO WB	HSC ism business, IM en extern bureau, [redacted]?
	1b. Risico analyse inclusief IT security scan	Sector BO HvB Sector BO WB	IM ism extern bureau, [redacted]?
	Document lange termijn visie op IV en IT functie bij de GGD HvB	Sector BO HvB	Extern bureau, IM?
2. Ondersteuning programma	Ondersteuning bij implementatie en uitrol CoronIT, HPZone, GGD Connect en andere apps	Programma Corona	Extern bureau
3. Inrichtingsplan IV en IT functie	Inrichtingsplan van de informatievoorziening en IT functie bij de GGD Hart voor Brabant	Sector BO HvB	Extern bureau, IM?

10.1

Sporen informatievoorziening planning



10.1

Extra personele behoefte

t.b.v. verbeterplan gegevensbescherming en gevolgbestrijding datadiefstal

Functie	Huidige uren	Uitbreiding	Periode	Invulling
Functionaris persoonsgegevens	10	+10	Februari-open einde	zzp (opzegbaar)
Privacy officer programma Corona	16	+20	Februari-open einde	[redacted] = zzp Evt. extra zzp
Projectleider IT Corona	- (regulier: Frank)	+32	Februari-juni	Inhuur adviesbureau
Communicatie	64	NTB	Februari-structureel	Structureel binnen regulier team comm.
Juridisch adviseur	-	NTB	NTB	Nu: juridische zaken gemeenten Wellicht nodig: AKD
Begeleiding AP onderzoek	-	NTB	NTB	?
Financiën	32	NTB	NTB	?

10.2
Archived: donderdag 12 mei 2022 09:38:15
From: [redacted]
To: [redacted]
Subject: Agendapunten bila 17 maart
Importance: Normal
Sensitivity: None

Ha [redacted],

Ik heb voor morgen de volgende bespreekpunten:

1. **Buitenwereld**

- Bestuurlijke dialoog herstelfase (RBT)
- Verbeteracties Twm-advies demonstraties

2. **Richten: strategie**

- Vervolgproces voor verkenning "hoe verder in 2021"

3. **Inrichten: PIOFACH**

- Opties opvolging [redacted]
- Uitkomsten OR-medewerkersbijeenkomsten
- Resultaten verkenning archivering & hotspot

4. **Verrichten: projecten**

- Landelijke schil BCO
- Spoor 2 testen

Verder de vraag of je er prijs op stelt dat ik de afspraken ook steeds aan je terugkoppel, of niet. Hieronder ter illustratie de terugkoppeling zoals ik die na de vorige bila's heb gegeven aan de stuurgroep Corona.

Bila 10 maart

1. **Buitenwereld**

- **Terugblik discussie governance tussen voorzitters VR, voorzitters GGD en DPG'en.** [redacted] neemt de feedback op zijn rol mee. [redacted] gaat in het iRBT maandag de boodschap aan de voorzitters VR geven dat als zij beter gevoed willen worden, we vooraf de stukken van het Veiligheidsberaad moeten krijgen. [redacted] stelt overigens de rol van de voorzitter VR in de governance ter discussie.
- **Procesafspraken voorbereiding DB-heisessie governance**. Heisessie met alleen het DB (niet MT) over alle vier de onderwerpen uit de position paper. De heisessie opdelen in blokjes: stukje inleiding en stukje discussie. [redacted] is [redacted]. Voorbereiding stemmen we af in het begeleidingsclubje governance. De position paper is overigens door [redacted] gedeeld met de andere 2 GGD-voorzitters. **Actie [redacted]:** eerste voorstel voor aanpak doen.
- **Standpunt Raad van DPG'en over testen spoor 2**. We houden vast aan het landelijke beleid dat we alleen testen in

spoor 1 en communiceren dat ook naar het DB. **Actie [redacted]:** in de Raad van DPG'en de vraag blijven herhalen of we vanuit maatschappelijk oogpunt wellicht meer zouden moeten willen.

- **Position paper governance IZB crisis**. Blijft zwak verhaal. Advies aan [redacted] is om in de Raad van DPG'en aan te geven: stuk is één van de bouwstenen in de governance-discussie, maar geen definitief standpunt of opdracht, dus bouw er geen PR-campagne op en geef ook nog niet de opdracht om een inrichtingsplan te maken.
- **Update Corona in AB 24 maart.** Vooral richten op het beeld en de kerngetallen: de omvang van de operatie, hoeveel mensen hebben we ingezet, aantal FTE, gehaalde opschaling. Voor wat betreft verbinding met de reguliere processen: refereren aan eerdere ambitie dat vanaf 1 september iedereen weer zoveel mogelijk terug zou gaan naar reguliere organisatie (nu nog max. XX eigen medewerkers ingezet). Ik pak technische vragen en [redacted] pakt politiek-bestuurlijke. Volgende week vrijdag voorbereidend overleg [redacted]- [redacted] **Actie [redacted]:** vraag formuleren aan [redacted] over hoe diep we in AB ingaan op datadiefstal.

2. **Richten: strategie**

- **Procesafspraken regionaal meedenken met landelijke exitstrategie. Actie [redacted]:** over een week bij [redacted] vragen hoe dit landelijk procesmatig wordt aangevlogen en hoe wij vanuit de werkvloer daaraan kunnen bijdragen.
- **Terugkoppeling standpunt [redacted] over scan evaluaties door afdeling onderzoek**. Wij kunnen meeliften. [redacted] geeft aan bij [redacted] dat dit voor beide GGD'en geldt. [redacted] doet het voor beide GGD'en.

3. **Inrichten: PIOFACH**

- **Landelijke opdracht i.r.t. arbeidscontracten. Actie [redacted]:** [redacted] vragen om bij VWS aan te dringen op snelle helderheid over duur van opdrachten en compensatieregeling. **Actie [redacted]:** [redacted] verzoeken aan het MT aan procesvoorstel te doen voor proactief arbeidsmarktbeleid, waaronder:
    - vooruit kijken naar toekomstige personeelstekorten in GGD-specialismen en dit matchen met mogelijke pareltjes in het programma
    - exitbeleid vanuit goed werkgeverschap: nazorg, evaluatie en feedbackgesprekken voor belangrijkste sleutelposities om medewerkers uit het programma met een goed gevoel over de GGD de wereld in te sturen, zodat goede mensen in de toekomst ook solliciteren bij ons.
- **Datalek landelijk dashboard**. **Actie [redacted]:** [redacted] rappelleren over brief van 4 DPG'en aan GGD GHOR NL.
- **Archivering & hotspot**: nog geen reactie ontvangen van GGD GHOR NL

4. **Verrichten: projecten**

- Vaccinatie:
    - **Spillage**. We wachten het landelijk voorstel voor de prioritaire groepen af.
    - **Standpunt verlengde arm**. Arts op locatie is wel degelijk nodig, kan wel eventueel minder zijn (1 per locatie ipv 1 per 5 priklijnen)
    - **Prikevents.** Weinig enthousiasme onder de DPG'en. **Actie [redacted]:** via Regiegroep VWS verzoeken om snelle helderheid over het gat tussen 1,75 miljoen en 2,5 miljoen.
- **Gezond leven met Corona.** Het is eigenlijk geen project meer, maar een beweging om collega's bewust te maken van de impact van Corona op het reguliere werk. Eigenlijk moet je dan een hele andere nadruk leggen: niet op de taken/diensten, maar op de bewustwording en dialoog. Je zou bijvoorbeeld een extra communicatiemedewerker kunnen aannemen die zich helemaal richt op bewustwording, gesprekken aanjagen binnen teams (ieder team laten nadenken over de eigen corona-opgave, middels een huiswerkopdracht, kernvragen laten beantwoorden) en veel interne glossy aandacht voor de beweging. Een dergelijke cultuuromslag is feitelijk breder dan alleen gezond leven c.q. gezondheidsbevordering en gaat over alle taken van de GGD. Dit gaat dus over de hele dialoog die door het programma Corona kan worden aangezwengeld over overdracht van taken, cultuur, innovaties etc. We moeten het risico onderkennen dat het nooit concreet wordt als we dit niet slim aanvliegen. We moeten concrete resultaten benoemen en het niet alleen een vage

beweging laten worden. Dat blijkt ook uit de reactie van het DB op het voorstel. **Actie** [redacted]: gesprek aangaan met [redacted] en [redacted] over de opdracht van het 'project' versus deze beweging.

Bila 4 maart

1. **Buitenwereld**

- Nabespreking DB:
  - Update Corona: de vraag van wethouders omtrent testen ging niet over officiële fieldlabs, maar over eigen evenementen. **Actie**: [redacted] vraagt in de Raad van DPG'en of de GGD'en toch niet meer willen bijdragen aan spoor 2 van de roadmap i.v.m. het maatschappelijk belang heropenen samenleving
  - Aanbesteding: DB is akkoord met verlengen tot 31 december, tenzij we de enige GGD zijn die dat doen. Kortom, als VWS geen vrijbrief geeft en veel andere GGD'en tóch ook gaan aanbesteden, dan moeten we het alsnog gaan doen (voor BCO). **Actie:** [redacted] benadrukt in Raad van DPG'en dat we VWS heel snel om duidelijkheid moeten vragen. We moeten uiterlijk 1 april weten of we alsnog moeten beginnen met aanbesteden of niet.
  - Position paper PG: [redacted] was erg blij met ons stuk. DB heeft verzocht om heisessie hierover te beleggen. **Actie:** [redacted] bereiden voor.
  - Gezond leven met Corona: DB sloeg aan op het woord accentverschuiving. In plaats van het plan vast te stellen, hebben ze er kennis van genomen. Er is geen financiële dekking afgesproken. **Actie:** [redacted] vraagt [redacted] en [redacted] om toelichting in MT op hoe nu verder.
  - Machtiging melden datadiefstal aan slachtoffers: we hebben eerst antwoorden nodig van GGD GHOR NL voordat we besluiten. Vragen zijn al door [redacted] en [redacted]h uitgezet.
- Datalek derde partij (daar gaan we weer; dit is weer een andere): **Actie:** [redacted] bespreekt standpunt met [redacted], koppelt terug naar [redacted].
- Ambitie voor evalueren Corona. **Actie:** [redacted] bespreekt met [redacted] of GHOR MWN hun onderzoeksvraag niet zowel bij WB als HvB kan uitzetten. **Actie:** stuurgroep corona start zelf met nadenken na over verdere interne evaluatie, slimme onderzoeksopdracht.

2. **Richten: strategie**

- Nabespreking begeleidingsgroep governance PG: in de begeleidingsgroep houden we de focus op het annoteren van [redacted] op de landelijke stukken. De verdere bespreking van onze eigen (concept) position paper koppelen we aan de voorbereiding van de DB-heisessie. **Actie:** [redacted] bedenken aanpak voor het voorbereiden van de heisessie (wie betrekken, interne subgroepjes).
- Governance informatievoorziening: interview is geweest. GGD GHOR NL past concept notitie aan. Na gehele interviewronde komt er een schriftelijke consultatieronde op de nieuwe versie. **Actie:** [redacted] checkt wanneer dat is.

3. **Inrichten: PIOFACH**

- Archivering & hotspot. **Actie:** [redacted] stuurt voorstel [redacted] naar Raad van DPG'en. Stemt dit eerst af met [redacted].
- Werkplekken Pettelaarpark en thuiswerken. Het beleid blijft hetzelfde, "iedereen werkt thuis tenzij". Er zijn werkplekken zat, ook op andere kantoren, dus inschikken door het programma is niet nodig. Het verzoek van [redacted] moet niet worden gericht aan het programma, maar aan [redacted]. De afspraak is namelijk: als je wilt afwijken van het thuiswerkbeleid, dan bespreek je dat met je leidinggevende. Als [redacted] daar vervolgens wat mee wil doen, dan moet hij dat inbrengen bij [redacted], die hiervoor verantwoordelijk is, met het regiegroepje huisvesting. **Actie:** [redacted] koppelt dit mondeling terug aan [redacted].
- Meenemen programma in HKZ-audit oktober. De auditors zijn er zelf niet happig op. Je gaat tegen die tijd al richting ontmanteling van het programma en we leggen over kwaliteit al verantwoording af aan IGJ. We hoeven dit niet te doen. Conclusie: gaan we niet doen.

4. **Verrichten: projecten**

- BCO:
    - Landelijke schil. Voorstel is aangehouden. We houden een vinger aan de pols hoe het voorstel gewijzigd gaat worden.
    - Scholenteam: terechte vraag om JGZ te verzoeken eerste aanspreekpunt voor scholen te zijn, ook bij vragen over infectiepreventie. *Inmiddels heb ik begrepen dat dit vandaag al nader is besproken. Ik stip dit morgen nog aan in het overleg met het sectormanagement.*
- Vaccinatie: signaal [redacted] n.a.v. issue Cuijk. **Actie:** [redacted] gaan gesprek aan met [redacted].

10.4
Archived: donderdag 12 mei 2022 09:38:48
From: [redacted]
Sent: maandag 8 februari 2021 19:51:46
To: [redacted]
Cc: [redacted]
Subject: Financiering verbeterplan gegevensbescherming
Importance: Normal
Sensitivity: None
Attachments:
20210205 Verbeterplan gegevensbescherming vs2.pptx; 20210208 Actielijst verbeterplan gegevensbescherming en datadiefstal.xlsx;

Dag [redacted],

Vanmiddag hebben [redacted] en ik de voorgestelde aanpak gepresenteerd voor de verbetering van de gegevensbescherming en gevolgbestrijding datadiefstal. Jammer genoeg was je er niet bij. Bijgevoegd de presentatie en ook de achterliggende actielijst met per spoor en actielijn de concrete actiepunten die momenteel al zijn uitgezet. Op de laatste slide van de presentatie kun je zien dat we extra personele inzet is die wij hebben ingeschat. Volgende week moet dit besluitvormend terugkomen in het MT. [redacted] heeft mij daarom nadien gevraagd om bij jou na te gaan wat de financierbaarheid is van deze inzet. Wat denk jij: welke sporen/actielijnen en personele inzet zouden in aanmerking komen voor de Compensatieregeling?

Met vriendelijke groeten,

[redacted]

[redacted]

GGD Hart voor Brabant

Pettelaarpark 10

's-Hertogenbosch

www.ggdhvb.nl

[redacted]

[redacted]@ggdhvb.nl

10.9
Archived: donderdag 12 mei 2022 09:36:44
From: [redacted]
Sent: dinsdag 26 januari 2021 16:08:07
To: [redacted]
Cc: [redacted]
Subject: RE: IV communicatie GGD GHOR - datalek
Importance: Normal
Sensitivity: None

Hoi [redacted] en de anderen,

Eens met jouw aandachtspunt. Ter aanvulling: ik snap niet waarom nog steeds WhatsApp gebruikt wordt voor dit soort cruciale informatie. Er is immers toch wel bekend dat dit niet zon veilig platform is. Misschien ook een aandachtspunt.

P.S. Misschien is het handig alle punten wat betreft governance van de applicaties CoronIT en HP Zone te verzamelen en die in een keer aan [redacted] mee te geven.

Met vriendelijke groet,

[redacted]

[redacted]

GGD Hart voor Brabant
Pettelaarpark 10, 5216 PD 's-Hertogenbosch
www.ggdhvb.nl
[redacted]
[redacted]@ggdhvb.nl
Aanwezig op: ma-di-do-vrij
Gezond doet leven!

Van: [redacted]
Verzonden: dinsdag 26 januari 2021 15:29
Aan: [redacted]
CC: [redacted]
Onderwerp: RE: IV communicatie GGD GHOR - datalek

Dag [redacted] en [redacted],

Helemaal eens. Hoe vanuit GGD GHOR NL de communicatielijnen lopen [redacted] (evenals de governance in brede zin). Ik zal het signaal langs deze weg nog extra onder de aandacht brengen bij [redacted] b.v. haar overleggen met de DPG'en. Als jullie vanuit BI, applicatiebeheer en FG's (in HvB of samen met NOG, BZO, WB) nog nadere wensen/ideeën hebben over hoe dit landelijk beter kan worden georganiseerd, geef het maar zo concreet mogelijk aan.

Met vriendelijke groeten,

[redacted]

[redacted]

10.9
Pettelaarpark 10
's-Hertogenbosch
www.ggdhvb.nl
[redacted]
[redacted]@ggdhvb.nl

Van: [redacted]@ggdhvb.nl>
Verzonden: dinsdag 26 januari 2021 14:34
Aan: [redacted]@ggdhvb.nl>; [redacted]@ggdhvb.nl>; [redacted]@ggdhvb.nl>; [redacted]@ggdhvb.nl>
CC: [redacted]@ggdhvb.nl>
Onderwerp: RE: IV communicatie GGD GHOR - datalek

Hoi [redacted],

Terecht punt. Vanmorgen in het standup-overleg over de datadiefstal is ook geconstateerd dat de onduidelijke/ontbrekende governance en beheerstructuren rondom de landelijke systemen [redacted]. [redacted] zal dat ook meenemen op DPG niveau.

Daarbij gaat het niet alleen over de communicatie, maar vooral ook over besluitvorming en prioritering van maatregelen en wijzigingen. [redacted]

Groeten,

[redacted]

[redacted]

Ringbaan West 227 Tilburg
Postbus 3024, 5003 DA Tilburg
www.ggdhvb.nl
[redacted]@ggdhvb.nl
Aanwezig op: di-wo-do-vr

Gezond doet leven!

Van: [redacted]@ggdhvb.nl>
Verzonden: dinsdag 26 januari 2021 12:21
Aan: [redacted]@ggdhvb.nl>; [redacted]@ggdhvb.nl>; [redacted]@ggdhvb.nl>
CC: [redacted]@ggdhvb.nl>; [redacted]@ggdhvb.nl>
Onderwerp: IV communicatie GGD GHOR - datalek
Urgentie: Hoog

Hoi,

Vanuit NOG vernam ik net dat er vanuit GGD GHOR een appgroep genaamd Siilo bestaat om communicatie omtrent IV werkprocessen af te stemmen en te delen. Vanuit deze app communiceert [redacted] (zie voorbeeld printscreen bijlage) met o.a. NOG projectleiders administratie, telefonie, BCO, Testen. Ik weet niet wie verder nog in deze appgroep zitten vanuit de andere GGD'en (waaronder wij?) en hoe lang deze appgroep al bestaat. Nu blijkt dat er een datalek heeft plaatsgevonden wordt er dus op deze manier richting de GGD'en gecommuniceerd over de volgende gewijzigde IV zaken:

1. In HP zone (lite) is het niet meer mogelijk bestanden te exporteren – queries draaien in het scherm kan nog wel

2. In CoronIT is het niet meer mogelijk het afsprakenoverzicht af te drukken

3. De ‘oude’ tableau export van CoronIT is niet meer beschikbaar.

In hoeverre zijn jullie hiervan op de hoogte? Zitten wij ook in deze appgroep of worden wij op een andere manier geïnformeerd? Is dit de enige manier waarop de GGD GHOR communiceert omtrent IV wijzigingen e.d.? Ik zou namelijk verwachten dat er een GHOR IV groep aanwezig is/wordt opgezet om dit soort belangrijke IV zaken te communiceren. Zeker gezien de datalek dat nu speelt.

Als [redacted] wil ik graag in de eerste linie zitten om dit soort informatie te verkrijgen zodat ik hierop kan voorsorteren en bekijken welke consequenties bepaalde maatregelen gaan hebben op onze werkprocessen. Nu kom ik dus via deze weg aan de informatie.

In hoeverre kunnen we hier invloed op uitoefenen en betrokken worden in de communicatie? Kunnen we samen met de andere GGD’en optrekken (applicatiebeheerder, FG’s)?

Ik hoor het graag.

Groet,

[redacted]

Met vriendelijke groet,

[redacted]

[redacted]

GGD Hart voor Brabant

Pettelaarpark 10,

5216 PD ‘s Hertogenbosch

www.ggdhvb.nl

[redacted]@ggdhvb.nl

Aanwezig op: ma-di-wo-do

[redacted]

Van: [redacted]@ggdnog.nl>
Verzonden: dinsdag 26 januari 2021 11:29
Aan: [redacted]@ggdhvb.nl>; [redacted]@ggdwestbrabant.nl>; [redacted]@ggdbzo.nl>; [redacted]@hetservicecentrum.nl>
Onderwerp: Screenshot [redacted]

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

12.0 Tekst Wob-verzoek en register documenten

Tekst verzoek (xii)

lnformatie over de overname van het beheer van HPZone (Lite) door GGD GHOR

Register

Een screenshot van de verkennerpagina van map 11:

12.1 DPIA GGD Contact v1.1.3

12.10 DPIA GGD C...um 01 Zelf BCO 1.0

12.11 DPIA GGD C...03_Zwartgemaakt

12.2 Check maatre...GGD Contact HvB

12.3 FW_ Overeen...tact (15)_Redacted

12.4 FW_ Overeen...Contact_Redacted

12.5 FW_ Voorbeel...T-syste_Redacted

12.6 Getekende ov...Contact_Redacted

12.7 GGD Contact...regelen _Redacted

12.8 RE_ Overeen...tact_Zwartgemaakt

12.9 DPIA GGD Co...ct _Zwartgemaakt

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]	[redacted]	- Inzage & advies tussenversie DPIA
0.2			- FG advies opvragen
0.3			- Aanpassingen naar aanleiding FG advies & review
0.4			- Delen concept versie DPIA ter review VWS
0.5			- Review DPIA (op hoofdlijnen)
0.6			- Tekstvoorstel betrokken partijen en rolverdeling
0.7			- Tekstvoorstel Telecommunicatiewet

	[redacted]	
1.0	[redacted]	- 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]	Samenvoeging referentie DPIA 1.0 met Addenda: Zelf-BCO, BCO Vragenlijst + Osiris Vragenlijst, Evaluatie GGD Contact
1.1.2	[redacted]	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

12.1

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.

Bewaartermijn applicatie GGD Contact

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.

Bewaartermijn datasluis

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.

Bewaartermijn BCO webportaal

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. <u>Onjuiste koppeling van gegevens aan dossier</u>

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. Onjuiste aanlevering van gegevens door Index

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. <u>Verwerken persoonsgegevens indexen die buiten RIVM Protocol vallen</u>

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. Gebruik van GGD Contact door landelijke partners

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. Strijd met het transparantiebeginsel, art 5.1 AVG

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. Verwerking van klachten door GGD blijkt niet-noodzakelijk

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

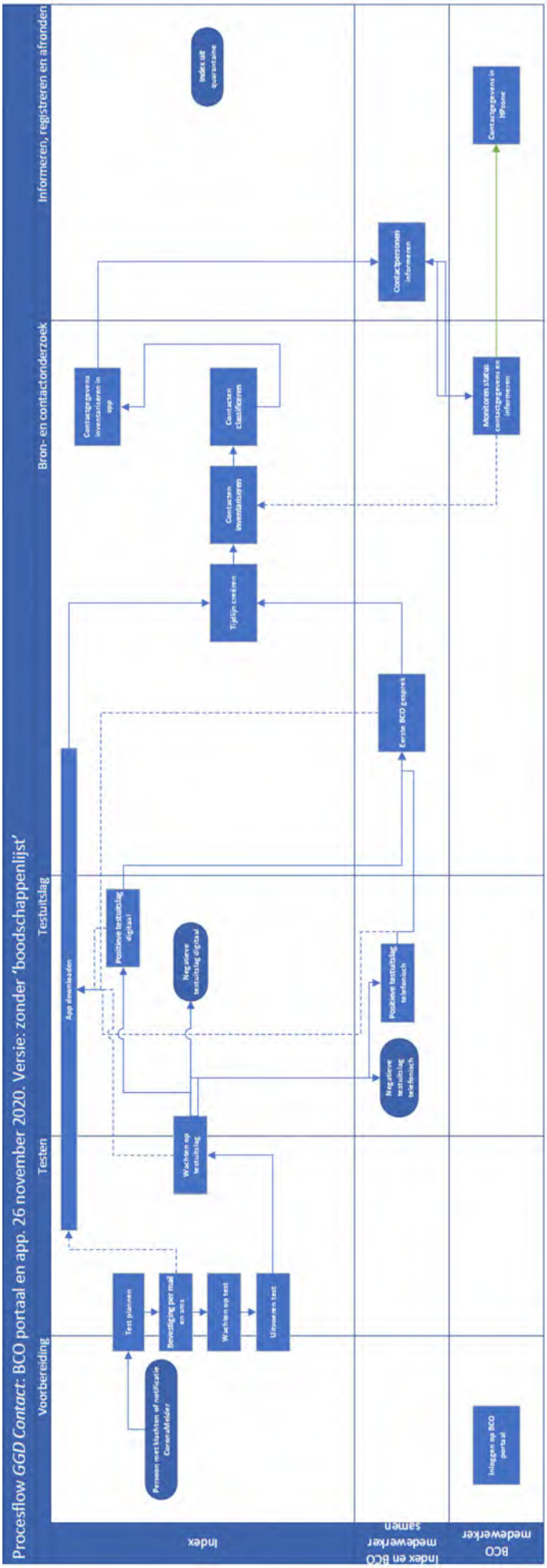
Indien de gegevens zijn aangeleverd door de index kan de BCO-medewerker een inventarisatie maken welke contacten geïnformeerd dienen te worden. Deze contactpersonen zullen worden geïnformeerd dat zij in contact zijn geweest met iemand die positief getest is op COVID-19 en nadere informatie krijgen in 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

12.1

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.

GGD moet zelf nog een inschatting maken in hoeverre de maatregelen getroffen zijn / haalbaarheid
GGD GHOR doet hier nog een check op

Kolom1	Maatregelen	Helpt bij risico	Geimplementeerd	Landelijke maatregel	GGD maatregel	Acties	Eigenaar	HSC/HvB ready	Nb
1	Geheimhoudingsverklaringen BCO-medewerkers	13		X, voor medewerkers landelijke schil	X		GGD	Ja	voor GGD-mdw zeker
2	Autorisatiematrix	13			X	* Opnemen rollen in GGD-eigen autorisatiematrix	GGD	Ja	Nog te toetsen
3	Overeenkomsten en/of convenanten	5, 11	Nee		X	* Convenant GGD'en/VWS/GGD GHOR --> Wordt opgesteld * LET OP: moeten GGD'en sluiten met Intermax (VWS) verwerkersovereenkomst Intermax-VWS-GGD'en --> Op Teams-pagina GGD Contact * SLA met PO en interne SLA GGD GHOR --> Wordt opgesteld	VWS/GGD GHOR /GGD	?	
4	Logging	13, 15		X	X	*Landelijk: Monitoring in I-Hub+applicatie *GGD: AD logiging zelf voorzien	VWS/GGD GHOR	Ja	AD logging
5	Gebruik identificatie	10	Ja	X			VWS/GGD GHOR		
6	Security testen	1, 1.2, 2, 4, 14	Ja	X		* Testen worden doorlopend uitgevoerd	VWS		
7	SSL Pinning	1, 1.2, 13, 14	Ja	X			VWS		
8	Duidelijke informatievoorziening richting BCO-medewerker dan wel richting betrokkenen	1, 1.1, 3, 4, 6 t/m 8, 10, 12, 1324	Ja	X		* E-learning op landelijk niveau m.b.t. de bco-medewerkers * campagne VWS voor betrokkenen	VWS/GGD GHOR	Business (GGD)	
9	Gebruik sterke en beperkte code	1, 1.1, 1.2	Ja	X			VWS		
10	Leveranciers kiezen die aantoonbaar informatiebeveiliging op orde hebben	2, 5, 11	Ja	X			VWS		
11	Controle en evaluatie op (beheer)procedures	14, 15, 21	Ja (?)	X	X (?)		GGD GHOR/VWS		
12	Training BCO-medewerker	3, 10, 12, 18, 24		X	X	* Training gemaakt op landelijk niveau, GGD'en dienen zelf de BCO-medewerkers te trainen.	GGD	Business (GGD)	
13	Duidelijke informatieverstrekking op websites GGD'en en in de privacyverklaring	8, 9		X	X	* Landelijk: Privacyverklaring App + BCO-portaal * GGD:Privacyverklaring website --> Staat op Teams-pagina is landelijk opgesteld	GGD/VWS	Business (GGD)	
14	Bewaartermijnen technisch inregelen	7	Ja	X			VWS		
15	Gebruik van oudere versies op mobiele telefoon staken bij afwezigheid beveiligingspatches	4	Ja	X			VWS		
16	Dataminimalisatie toepassen	3	Ja	X		* De wijze van uitvoering wordt nader toegelicht in documentatie privacy by design	VWS		
17	Unieke code	1.1	Ja	X			VWS		
18	Vermijden verwisselbare karakters	1.2	Ja				VWS		
19	Informatieverstrekking vanuit Rijksoverheid/VWS	6	Ja	X			VWS		
20	Procedures rechten van betrokkenen	9			X	* Verwijzing naar aangereikte richtlijnen vanuit GGD GHOR hoe om te gaan met inzage en verwijderingsverzoeken. Uitvoering ligt bij de GGD.	GGD/ GGD GHOR	Business (GGD)	Procedures
21	Doorgifte vereisten (sub)verwerkers	9		X	X	*GGD'en dienen te zorgen voor tekenen van de verwerksovereenkomst met partijen in de keten. Verwerkingsovereenkomsten zijn opgenomen op de teams-pagina hoeven niet zelf te worden opgesteld.	GGD	Under construction	Nb. Op volledigheid en actueel zijn check uitvoeren.
22	Borgen technische aspecten	18	Ja				VWS		
23	Inrichten van de Governance structuur	11, 14, 17, 26	Ja	X			VWS/GGD GHOR		
24	Vastlegging contractuele afspraken	2, 5, 17, 19, 21, 25, 26	Nee. Zie 3	X	X		VWS/GGD GHOR /GGD		
25	Periodieke verantwoording door leveranciers	11, 14, 26	Ja (contractueel borgen)	X			VWS		
26	NEN7510/ISO27001of soortgelijke certificering bij leveranciers/partijen in de keten	2, 11, 14	Ja	X			VWS		
27	Authentiseren/verifiëren van de index	12	n.v.t. 1e release		X	Momenteel maakt dit onderdeel uit van algemene procesbeschrijving (LCI-richtlijn Osiris). 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	12	n.v.t 1e release	X	X	* Plausibiliteitschecks invoeren in de werkinstructie (bekende Nederlander, etc.). Bij twijfel dient door de BCO-coördinator meegekeken te worden (werkinstructie).			
29	Informatiebeveiligingsbeleid GGD GHOR Nederland	13, 25	Ja	X			GGD GHOR		
30	Dossiertoegang loggen	13, 25	Ja	X		*Beoordeling van de monitoring van de logging ligt bij GGD GHOR voor deze release	VWS/GGD GHOR		
31	Inzicht in technische kwetsbaarheden (Applicatie)	14, 15	Ja	X			VWS		
32	Opzetten en implementeren van ICT beheersprocessen	15, 19	Ja	X			VWS		
33	Eisen ICT beheerprocessen	15, 19		X		Betreffen de landelijke partners en afspraken met de nieuwe securty maatregelen (nen7510)	GGD GHOR		
34	Afspraken over (gedeelde) verantwoordelijkheden	17, 27	Nee, zie 3	X			VWS/GGD		
35	Redundante uitvoering	18	Deels	X		VWS: productieomgeving en acceptatieomgeving redundant uitgevoerd GGD GHOR: Identity Hub (?)	VWS/GGD GHOR		
36	Afstemming met RIVM protocol	20	Nee	X			VWS		
37	DPIA opstellen/vaststellen	22		X	X	* Landelijk is de referentie DPIA opgesteld. Opgesteld: Ja (excl advies FG) * GGD: toevoeging van FG-advies + acceptatie DPIA door organisatie	GGD		
38	Vastlegging toestemming	23	Ja	X			VWS		
39	Actief volgen van gelijksoortige Apps	6	Ja	X			VWS		
40	Monitoring van verdacht gedrag	1.2	Ja	X			VWS/GGD GHOR		
41	Uitvoeren juridische checks	5	Ja	X		* Onderzoek Mendix is afgerond	GGD GHOR		
42	Toelichting omtrent gebruik/toepassing vrije velden	3	Ja(?)	X		onderdeel v.d. acceptatietest	VWS		
43	Vrije velden verwijderen	3	Ja	X		Niet noodzakelijke vrije velden zijn verwijderd, vrije velden voor zover nog opgenomen zijn door product owners als relevant bevonden	VWS		
44	Monitoring van verdacht gedrag	1.1, 1.2	Ja	X			VWS/ GGD GHOR		
45	Contracteren met partijen binnen EER	5	Ja	X			VWS		
46	Technische maatregelen databehoud binnen EER	5	Ja	X			VWS		
47	Bewaartermijn by design inrichten	7	Ja	X			VWS		
48	Periodieke kwaliteitscontrole op (afwijkingen) van het dossier	10	n.v.t. 1e release		X		GGD	Business (GGD)	
49	Instellen pincode voorafgaande toegang GGD Contact	24	Ja	X		Technisch ingeregeld dat de App signaleert dat er geen pincode op het toetsel in gebruik is.	VWS		
50	Rolverdeling VWS	28	Nee, zie 3	X			VWS/GGD		
51	Versleuteling van data op het device	8	Ja	X			VWS		
52	Attack surface minimization	14	Ja	X			VWS		
53	Toepassing TLS	14, 16, 19	Ja	X			VWS		
54	Certificaten vastleggen in applicatie	2	Ja	X			VWS		
55	2FA Identity Hub	25	Ja?	X			GGD GHOR?		
56	Ghost responses	1b	Ja	X			VWS		
57	Encryptie (at rest)	8, 14, 16, 19	Ja	X			VWS		
58	Toepassing RPA technologie	29	n.v.t.						
59	GGD security maatregelen (NEN7510)				X		GGD	Ja	HSC NEN7510 gecertificeerd
	Maatregelen [redacted]								
	Tijdelijke unieke sleutels per sessie via TLS. Deze sleutelparen worden door de applicatie slechts voor de sessie gebruikt en worden nergens opgeslagen. Na het verdwijnen van de sleutels uit het geheugen van de server en client is er ook na afloop niks meer te doen met de versleutelde data ook al zou deze opgeslagen zijn						VWS		
60	**Veilige diffie hellman sleuteloverdracht tussen apps en backend.** Hiermee worden sleutels op een correcte manier uitgewisseld waarbij en geen kennis over de uiteindelijke versleuteling wordt over de verbinding wordt gestuurd						VWS		
61	**Tijdelijke unieke sleutels per app-sessie.** Er wordt voor elke koppeling tussen de app en de backend een nieuw uniek sleutelpaar aangemaakt aan beide kanten.						VWS		
62	**Eenrichtingsverkeer tussen de app en portaal (via de sluis).** Hiermee is het zeker dat er alleen vanuit de portaal acties uitgevoerd kunnen worden						VWS		

63	**Een aantal queue based koppelingen (redis)** Hiermee kan een cliënt nooit een service kan overloaded en tevens je nooit meer kan doen dan data in/uit een queue halen. De verwerking aan de binnenkant vindt dus onafhankelijk van het process wat zich aan de buiten afspeelt plaats.						VWS		
64	Tussen de ontvangende en de verwerkende server is er a**lleen de mogelijkheid om door de verwerkende server acties te initiëren**. Hiermee bepaalt de verwerkende server de snelheid en de acties. Vanuit het internet is hier dus geen actieve mogelijkheid toe. à check met ontwikkelaar.						VWS		
65	Login via identity hub met bestaande ggd account providers					verwerkt in de tekst niet expliciet als maatregel.	GGD GHOR		
66	**Portaal ontsloten via diginet** Hiermee is de portaal alleen bereikbaar vanaf diginet aangesloten GGD'en en is de zekerheid van veiligheid van de oorsprong voor deze acties zeker gesteld.					besproken dat TLS een alternatief is.	VWS		
67	**Containerized hosting voor compartimentering en minimalizatie van attack surface** Hierbij worden alle delen van de applicatie apart opgestart met slechts de minimale benodigheden die nodig zijn voor het functioneren.						VWS		
68	Containers opgedeeld in meerdere netwerken **waarbij precies is ingeregeld welk component bij welk ander component mag.** Hiermee is firewalling tussen de componenten aanwezig. En kan een component niet meer dan van te voren toegestaan.						VWS		
69	**sftp koppeling met rivm via ssh keys beveiligd** Dataoverdracht op basis van public/private sleutels, waardoor geen wachtwoorden meer nodig zijn en deze dus ook niet gekraakt, gegokt of afgeluisterd kunnen worden. à niet opgenomen omdat gegevens met rivm in deze DPIA nog niet is opgenomen.		n.v.t. 1e release				VWS		
70	**JWT authorisatie tussen sluis en portal** Dit zijn cryptografisch ondertekende toegangssleutels voor automatische toegang, waarbij de toegang ook weer in te trekken is indien dit nodig is.						VWS		
71	**Alles open source** hiermee is het voor elke belanghebbende mogelijk om zelf de correcte werking van de software te (laten) controleren.						VWS		
72	**Het gebruik van standaard opensource software voor encryptie en decryptie.** De software voor de zelf gebruikte encryptie (libsodium) staat het gebruik van foute parameters of onveilige (oude) encryptie methoden niet toe omdat deze niet worden ondersteund.						VWS		
73	**hsm voor backing alle secret keys en random input voor key generatie** De bovengenoemde sleutels aan de kant van de portaal worden beheerd onder controle een HSM installatie. Deze levert de waarborgen dat sleutelbeheer op een veilige manier plaatsvindt en de encryptiesleutels voorzien zijn van gewaarborgde randomness.						VWS		
74	**injected secrets aan de server kant (geen secrets in code)** De sleutels voor automatische communicatie, decryptie van de databasevelden en andere zaken staan niet bij de applicatie opgeslagen, maar in een apart proces wat deze bij het opstarten aanlevert aan het serverproces.						VWS		
75	**alle payloads even groot zodat er uit passief meegeluisterd verkeer** niet af te leiden is of en wat voor type data er uitgewisseld wordt.						VWS		
76	**Versleutelde backup**s. Backups worden versleuteld opgeslagen. Dit op een manier zodat de backups alleen terug te halen zijn door geautoriseerde personen en alleen op expliciete opdracht.						VWS		
77									

12.3
Archived: donderdag 12 mei 2022 09:40:09
From: [redacted]
Sent: woensdag 8 september 2021 16:49:37
To: [redacted]
Cc: [redacted]
Subject: FW: Overeenkomsten GGD Contact
Importance: High
Sensitivity: None
Attachments:
2.3 Dossier Afspraken en Procedures GGD Contact v1.1.pdf; 2.4 Verwerkingsovereenkomst GGD GHOR Nederland v1.1.pdf; 2.5 Checklist Onboarding applicaties v1.02.pdf; 1.0 DVO GGD Contact - GGD Hart voor Brabant.pdf; 1.1 Verwerkersovereenkomst - GGD Hart voor Brabant.pdf; 2.0 DVO GGD GHOR Nederland v.1.1.pdf; 2.1 Dienstbeschrijving GGD GHOR Nederland v1.1.pdf; 2.2 Service Level Agreement GGD Contact v1.1.pdf;

Goedemiddag [redacted], [redacted],

Graag wil ik de dienstverleningsovereenkomsten GGD Contact ook bij het management van programma corona ter review wegleggen. Ik zal de overeenkomsten zelf ook doornemen. Het gaat om de document 1.0 DVO GGD Contact – GGD HvB en document 2.0 DVO GGD GHOR NL. Deze documenten zijn door GGD GHOR opgesteld en al meerdere keren gereviewd en afgestemd met afgevaardigden van een aantal GGD Regio's. Zouden jullie mee willen lezen en beoordelen?

[redacted] zal de beoordeling van de verwerkersovereenkomsten op zich nemen. De overige documenten hoeven niet expliciet getekend te worden.

Idealiter kunnen we de overeenkomsten vóór maandag 13 september tekenen, zodat de documenten ondertekend zijn bij de livegang. Mocht dit niet lukken, willen we de livegang toch door laten gaan. Zijn jullie daarmee akkoord? Er zijn al meerdere GGD'en gestart met het gebruik van GGD Contact, dus ik verwacht geen onoverkomelijke zaken in de overeenkomsten.

Ik hoor graag van jullie.

Met vriendelijke groet,

[redacted]

[redacted]

Programma Corona

GGD Hart voor Brabant

Pettelaarpark 10,

5216 PD 's-Hertogenbosch

www.ggdhvb.nl

[redacted]@ggdhvb.nl

Gezond doet leven!

Van: [redacted]@minvws.nl>
Verzonden: donderdag 2 september 2021 08:33

Aan: [redacted]@ggdhvb.nl>
CC: [redacted]@ggdhvb.nl>; 'vervangingHPZone' <vervangingHPZone@ggdghor.nl>
Onderwerp: Overeenkomsten GGD Contact

Geachte [redacted]

Hierbij stuur ik u de overeenkomsten t.b.v. GGD Contact toe.

Het gaat om:

- 1.0 Dienstverleningsovereenkomst VWS voor GGD Contact release 1.1, incl. bijlage:
  - 1.1 Verwerkersovereenkomst ARVODI VWS voor GGD Contact
- 2.0 Dienstverleningsovereenkomst GGD GHOR Nederland, incl. bijlagen:
  - 2.1 Dienstbeschrijving
  - 2.2 Service Level Agreement
  - 2.3 Dossier Afspraken en Procedures
  - 2.4 Verwerkersovereenkomst
  - 2.5 Checklist onboarding applicaties

Deze overeenkomsten zijn opgesteld met inbreng vanuit vele inhoudelijke experts.

De concept versies van deze documenten zijn op 15 juni 2021 aangeboden aan de stuurgroep fase 1 vervanging HP Zone (Lite) ter review en de commentaren die hierop zijn ontvangen zijn verwerkt in de definitieve versies zoals vastgesteld op de stuurgroep van 25 juni 2021.

Documenten 1.0, 1.1, 2.0 en 2.4 dienen door u ondertekend te worden.

Graag ontvang ik de door u getekende stukken retour, zodat ik deze kan laten ondertekenen door de overige partijen.

Vergeet niet om een datum in te vullen als hierom gevraagd wordt in het document.

U ontvangt na ondertekening door alle partijen het complete pakket van mij retour.

Met vriendelijke groet,

[redacted] GGD Contact
.....
Ministerie van Volksgezondheid, Welzijn en Sport
Directie Informatiebeleid/CIO
Programma Realisatie Digitale Ondersteuning

Parnassusplein 5 | 2511 VX | Den Haag
Postbus 20350 | 2500 EJ | Den Haag
.....
T [redacted]
E [redacted]@minvws.nl

12.4
Archived: donderdag 12 mei 2022 09:40:24
From: [redacted]
Sent: donderdag 9 september 2021 15:04:15
To: [redacted]
Subject: FW: Overeenkomsten GGD Contact
Importance: High
Sensitivity: None
Attachments:
2.3 Dossier Afspraken en Procedures GGD Contact v1.1.pdf; 2.4 Verwerkingsovereenkomst GGD GHOR Nederland v1.1.pdf; 2.5 Checklist Onboarding applicaties v1.02.pdf; 1.0 DVO GGD Contact - GGD Hart voor Brabant.pdf; 1.1 Verwerkersovereenkomst - GGD Hart voor Brabant.pdf; 2.0 DVO GGD GHOR Nederland v.1.1.pdf; 2.1 Dienstbeschrijving GGD GHOR Nederland v1.1.pdf; 2.2 Service Level Agreement GGD Contact v1.1.pdf;

Hallo allen,

Mijn opmerkingen mbt deze overeenkomsten:

- Ik heb de verwerkersovereenkomsten en de te tekenen DVO snel gelezen en kom een aantal kleine punten tegen waarvan ik vind dat dit beter en concreter beschreven kan worden in deze overeenkomsten. Vanuit privacy oogpunt wat mij betreft nu geen reden om niet te tekenen, ook gezien het feit dat GGD Contact nog niet uitontwikkeld is en dat VWS in de toekomst het beheer/ontwikkeling van GGD Contact zal overdragen aan een andere partij.
- GGD Twente ([redacted] gisteren nog gebeld. Zij geeft aan dat er tijdens mijn vakantie in het landelijke overleg van de Functionaris Gegevensbescherming deze overeenkomsten zijn besproken en er nog opmerkingen waren. Toen is aangegeven dat er de opmerkingen verzameld gaan worden voor een toekomstige aanpassing, maar dat de GGD'en wel tekenen.
- Vandaag nog GGD Rotterdam gebeld ([redacted] en ook hij gaf aan dat er getekend wordt en dat de opmerkingen in een later addendum verwerkt gaan worden. Een aantal GGD'en (Rotterdam, Twente, West Brabant, Rotterdam-Rijnmond, Friesland) hebben reeds opmerkingen naar [redacted] en [redacted] (GGD Ghor gemaild).

Met vriendelijke groeten,

[redacted]

GGD Hart voor Brabant
Pettelaarpark 10 Den Bosch
Postbus 3024, 5003 DA Tilburg
www.ggdhvb.nl
[redacted]@ggdhvb.nl
Aanwezig op: ma-di-wo-do
Gezond doet leven!

Van: [redacted]@ggdhvb.nl>
Verzonden: donderdag 9 september 2021 08:02
Aan: [redacted]@ggdhvb.nl>
Onderwerp: FW: Overeenkomsten GGD Contact

Urgentie: Hoog

Hoi [redacted]
Klopt toch dat jij [redacted] laat weten wanneer contract getekend kan worden? Graag met cc naar directiesecretariaat.

Met vriendelijke groeten,

[redacted]

Hart voor Brabant
Gezond doet leven!

Pettelaarpark 10
's-Hertogenbosch
Postbus 3024, 5003 DA Tilburg
www.ggdhvb.nl

[redacted]@ggdhvb.nl
Aanwezig op: ma-di-do-vrij

Van: [redacted]@ggdhvb.nl>
Verzonden: donderdag 2 september 2021 09:48
Aan: [redacted]@ggdhvb.nl>; [redacted]@ggdhvb.nl>; [redacted]@ggdhvb.nl>
CC: [redacted]@ggdhvb.nl>; [redacted]@ggdhvb.nl>; [redacted]@ggdhvb.nl>; [redacted]@ggdhvb.nl>
Onderwerp: Overeenkomsten GGD Contact

Goedemorgen allemaal,

De afgelopen maanden zijn we bezig geweest met de voorbereidingen voor de implementatie van GGD Contact. We zijn ondertussen goed voorbereid en starten deze week met het opleiden van de eerste medewerkers. 13 september willen we met de eerste groep medewerkers over gaan naar het nieuwe systeem voor de uitvoering van het Bron- en contactonderzoek.

Idealiter zijn vóór de livegang (13 september) de benodigde documenten getekend. Vandaag is voor ons allemaal de eerste keer dat we de documenten toegestuurd krijgen en zijn jullie ([redacted] en [redacted] nog op vakantie. Vandaar mijn vraag: Denken jullie dat het haalbaar is de overeenkomsten vóór 13 september te beoordelen en bij akkoord te tekenen? Als dit niet in de planning past zou ik graag met jullie afstemmen wat dat betekent voor de livegang van GGD Contact.

Mochten jullie interesse hebben, dan kan ik jullie wat meer vertellen over wat de eerste oplevering van GGD Contact gaat doen en hoe het ontwikkel-/ implementatieproces is verlopen. Ik hoor graag of hier animo voor is.

Alvast bedankt voor jullie reactie.

Met vriendelijke groet,

[redacted]
Programma Corona
Aanwezig: Ma, di, wo, do

Hart voor Brabant
Gezond doet leven!

Pettelaarpark 10,
5216 PD 's-Hertogenbosch
www.ggdhvb.nl

[redacted]@ggdhvb.nl

Van: [redacted]@minvws.nl>

Verzonden: donderdag 2 september 2021 08:33
Aan: [redacted]@ggdhvb.nl>
CC: [redacted]@ggdhvb.nl>; 'vervangingHPZone' <vervangingHPZone@ggdghor.nl>
Onderwerp: Overeenkomsten GGD Contact

Geachte mevrouw [redacted],

Hierbij stuur ik u de overeenkomsten t.b.v. GGD Contact toe.

Het gaat om:

- 1.0 Dienstverleningsovereenkomst VWS voor GGD Contact release 1.1, incl. bijlage:
  - 1.1 Verwerkersovereenkomst ARVODI VWS voor GGD Contact
- 2.0 Dienstverleningsovereenkomst GGD GHOR Nederland, incl. bijlagen:
  - 2.1 Dienstbeschrijving
  - 2.2 Service Level Agreement
  - 2.3 Dossier Afspraken en Procedures
  - 2.4 Verwerkersovereenkomst
  - 2.5 Checklist onboarding applicaties

Deze overeenkomsten zijn opgesteld met inbreng vanuit vele inhoudelijke experts.
De concept versies van deze documenten zijn op 15 juni 2021 aangeboden aan de stuurgroep fase 1 vervanging HP Zone (Lite) ter review en de commentaren die hierop zijn ontvangen zijn verwerkt in de definitieve versies zoals vastgesteld op de stuurgroep van 25 juni 2021.

Documenten 1.0, 1.1, 2.0 en 2.4 dienen door u ondertekend te worden.

Graag ontvang ik de door u getekende stukken retour, zodat ik deze kan laten ondertekenen door de overige partijen.
Vergeet niet om een datum in te vullen als hierom gevraagd wordt in het document.

U ontvangt na ondertekening door alle partijen het complete pakket van mij retour.

Met vriendelijke groet,

[redacted] GGD Contact
.....
Ministerie van Volksgezondheid, Welzijn en Sport
Directie Informatiebeleid/CIO
Programma Realisatie Digitale Ondersteuning

Parnassusplein 5 | 2511 VX | Den Haag
Postbus 20350 | 2500 EJ | Den Haag
.....
T [redacted]
E [redacted]@minvws.nl

12.5
Archived: donderdag 12 mei 2022 09:40:40
From: [redacted]t
Sent: maandag 15 februari 2021 13:30:10
To: [redacted]
Cc: [redacted]
Subject: FW: Voorbeeldbrief informeren besturen Vervangen van ICT-systeem HP-Zone
Importance: Normal
Sensitivity: None

Hi [redacted],

Zie onderstaande mailwisseling. De vervanging van HPZone krijgt hiermee ook impact op onze begroting. Wellicht toevoegen aan de alinea over het datalek die we al schreven in de paragraaf 'gebeurtenissen na balansdatum'?

Hartelijke groet,

[redacted]

[redacted]

GGD Hart voor Brabant

Pettelaarpark 10
5216 PD, 's-Hertogenbosch
Postbus 3024, 5003 DA Tilburg
www.ggdhvb.nl

[redacted]@ggdhvb.nl
Aanwezig op: ma t/m vr
[redacted]
[redacted]

Gezond doet leven!

Van: [redacted]@ggdhvb.nl>
Verzonden: maandag 15 februari 2021 12:03
Aan: [redacted]@ggdhvb.nl>; [redacted]@ggdhvb.nl>
CC: [redacted]@ggdhvb.nl>; [redacted]@ggdhvb.nl>; [redacted]@ggdhvb.nl>
Onderwerp: RE: Voorbeeldbrief informeren besturen Vervangen van ICT-systeem HP-Zone

Beste [redacted],

Wat mij opvalt in de brief is de volgende zin:

De Minister van VWS treedt op als opdrachtgever voor het vervangingstraject, op zijn verzoek coördineert GGD GHOR landelijk de vervanging.

Een aantal alinea's later wordt aangegeven

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 gemeentelijk bijdrage.

12.5

Dit is goede input voor het nog af te spreken IT Governance traject, want mijns inziens zit hier een discrepantie.

Overigens zal het aanspreekpunt voor de implementatie van GGD Contact / BCO Portaal [redacted] zijn. Hij is nu op de hoogte van het besluit van de vervanging van HP Zone door GGD Contact.

Met vriendelijke groet,

[redacted]

[redacted]

Hart voor Brabant

Pettelaarpark 10, 5216 PD 's-Hertogenbosch

www.ggdhvb.nl

[redacted]

[redacted]@ggdhvb.nl

Aanwezig op: ma-di-do-vrij

Gezond doet leven!

Van: [redacted]
Verzonden: maandag 15 februari 2021 10:49
Aan: [redacted]
CC: [redacted]
Onderwerp: RE: Voorbeeldbrief informeren besturen Vervangen van ICT-systeem HP-Zone

Dag [redacted] en [redacted] de DPG'en hebben dus definitief het besluit genomen om HPZone op korte termijn te vervangen door de GGD Contact app. Hebben we via onze landelijke contactpersonen al nadere duiding gekregen over het tijdpad en de implementatiestappen? Pakken jullie dit op met [redacted]?

Ik zou bij voorkeur de brief pas naar het AB willen sturen als we ook kunnen aangeven welk tijdpad wij in onze regio hanteren.

Van: [redacted]@ggdhvb.nl>
Verzonden: zondag 14 februari 2021 20:48
Aan: [redacted]@ggdhvb.nl>; [redacted]@ggdhvb.nl>; [redacted]@ggdhvb.nl>
Onderwerp: FW: Voorbeeldbrief informeren besturen Vervangen van ICT-systeem HP-Zone

Een voorbeeldbrief voor de informatie aan ons bestuur over HP Zone.

Hartelijke groet,

[redacted]

Van: [redacted]@ggdghor.nl>
Verzonden: zondag 14 februari 2021 17:22
Aan: Directie GGD GHOR Nederland <directie@ggdghor.nl>
Onderwerp: Voorbeeldbrief informeren besturen Vervangen van ICT-systeem HP-Zone

Beste DPG'en,

Bijgaand met dank aan collega's van de GGD IJsselland bijgaand een voorbeeldbrief die kan worden gebruikt om jullie bestuur te informeren over de vervanging van HPZone.

Voor de volledigheid ook nog de link naar de Kamerbrief van 12 februari "Stand van zakenbrief digitale ondersteuning pandemiebestrijding": https://www.tweedekamer.nl/kamerstukken/brieven_regering/detail?id=2021Z03135&did=2021D06898.

Met vriendelijke groet,

[redacted]

Drs. [redacted]
[redacted]

GGD GHOR Nederland
Zwarte Woud 2
3524 SJ Utrecht

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

Dit bericht is uitsluitend bestemd voor de geadresseerde. Het bericht kan vertrouwelijke informatie bevatten. Als u dit bericht per abuis hebt ontvangen, wordt u verzocht het te vernietigen en de afzender te informeren. GGD GHOR Nederland is niet aansprakelijk voor onjuiste en onvolledige overbrenging van de inhoud van een verzonden e-mail bericht, of een te late ontvangst daarvan.

12.6
Archived: donderdag 12 mei 2022 09:40:47
From: Directiesecretariaat GGD Hart voor Brabant
Sent: Thu, 9 Sep 2021 16:36:09
To: [redacted]
Cc: [redacted]
Subject: Getekende overeenkomsten GGD Contact
Importance: Normal
Sensitivity: None
Attachments:
2.3 Dossier Afspraken en Procedures GGD Contact v1.1.pdf; 2.5 Checklist Onboarding applicaties v1.02.pdf; 2.1 Dienstbeschrijving GGD GHOR Nederland v1.1.pdf; 2.2 Service Level Agreement GGD Contact v1.1.pdf; 1.0 DVO GGD Contact - GGD Hart voor Brabant.pdf ondertekend.pdf; 1.1 Verwerkersovereenkomst - GGD Hart voor Brabant.pdf ondertekend.pdf; 2.0 DVO GGD GHOR Nederland v.1.1.pdf ondertekend.pdf; 2.4 Verwerkingsovereenkomst GGD GHOR Nederland v1.1.pdf ondertekend.pdf;

Dag [redacted],

Hierbij ondertekend retour de bijlagen 1.0 – 1.1 – 2.0 en 2.4

Met vriendelijke groeten,

[redacted]

[redacted]

GGD Hart voor Brabant

Pettelaarpark 10
's-Hertogenbosch
Postbus 3024, 5003 DA Tilburg
www.ggdhvb.nl

[redacted]
[redacted]@ggdhvb.nl
Aanwezig op: ma-di-do-vrij

Gezond doet leven!

Van: [redacted]@ggdhvb.nl>
Verzonden: donderdag 2 september 2021 09:48
Aan: [redacted]@ggdhvb.nl>; [redacted]@ggdhvb.nl>; [redacted]@ggdhvb.nl>
CC: [redacted]@ggdhvb.nl>; [redacted]@ggdhvb.nl>; [redacted]@ggdhvb.nl>; [redacted]@ggdhvb.nl>
Onderwerp: Overeenkomsten GGD Contact

Goedemorgen allemaal,

De afgelopen maanden zijn we bezig geweest met de voorbereidingen voor de implementatie van GGD Contact. We zijn ondertussen goed voorbereid en starten deze week met het opleiden van de eerste medewerkers. 13 september willen we met de eerste groep medewerkers over gaan naar het nieuwe systeem voor de uitvoering van het Bron- en contactonderzoek.

Idealiter zijn vóór de livegang (13 september) de benodigde documenten getekend. Vandaag is voor ons allemaal de eerste keer dat we de documenten toegestuurd krijgen en zijn jullie ([redacted] en [redacted]) nog op vakantie. Vandaar mijn vraag: Denken jullie dat het haalbaar is de overeenkomsten vóór 13 september te beoordelen en bij akkoord te tekenen? Als dit niet in de planning past zou ik graag met jullie afstemmen wat dat betekent voor de livegang van GGD Contact.

Mochten jullie interesse hebben, dan kan ik jullie wat meer vertellen over wat de eerste oplevering van GGD Contact gaat doen en hoe het ontwikkel-/ implementatieproces is verlopen. Ik hoor graag of hier animo voor is.

Alvast bedankt voor jullie reactie.

Met vriendelijke groet,

[redacted]

[redacted]

[redacted]

Aanwezig: Ma, di, wo, do

Hart voor Brabant

Pettelaarpark 10,

5216 PD 's-Hertogenbosch

www.ggdhvb.nl

[redacted]@ggdhvb.nl

Gezond doet leven!

Van: [redacted]@minvws.nl>
Verzonden: donderdag 2 september 2021 08:33
Aan: [redacted]@ggdhvb.nl>
CC: [redacted]@ggdhvb.nl>; 'vervangingHPZone' <vervangingHPZone@ggdghor.nl>
Onderwerp: Overeenkomsten GGD Contact

Geachte mevrouw [redacted],

Hierbij stuur ik u de overeenkomsten t.b.v. GGD Contact toe.

Het gaat om:

- 1.0 Dienstverleningsovereenkomst VWS voor GGD Contact release 1.1, incl. bijlage:
  - 1.1 Verwerkersovereenkomst ARVODI VWS voor GGD Contact
- 2.0 Dienstverleningsovereenkomst GGD GHOR Nederland, incl. bijlagen:
  - 2.1 Dienstbeschrijving
  - 2.2 Service Level Agreement
  - 2.3 Dossier Afspraken en Procedures
  - 2.4 Verwerkersovereenkomst
  - 2.5 Checklist onboarding applicaties

Deze overeenkomsten zijn opgesteld met inbreng vanuit vele inhoudelijke experts.

De concept versies van deze documenten zijn op 15 juni 2021 aangeboden aan de stuurgroep fase 1 vervanging HP Zone (Lite) ter review en de commentaren die hierop zijn ontvangen zijn verwerkt in de definitieve versies zoals vastgesteld op de stuurgroep

van 25 juni 2021.

Documenten 1.0, 1.1, 2.0 en 2.4 dienen door u ondertekend te worden.

Graag ontvang ik de door u getekende stukken retour, zodat ik deze kan laten ondertekenen door de overige partijen.

Vergeet niet om een datum in te vullen als hierom gevraagd wordt in het document.

U ontvangt na ondertekening door alle partijen het complete pakket van mij retour.

Met vriendelijke groet,

[redacted]

.....
Ministerie van Volksgezondheid, Welzijn en Sport
Directie Informatiebeleid/CIO
Programma Realisatie Digitale Ondersteuning

Parnassusplein 5 | 2511 VX | Den Haag
Postbus 20350 | 2500 EJ | Den Haag
.....
T [redacted]
E [redacted]@minvws.nl

12.7
Archived: donderdag 12 mei 2022 09:39:14
From: [redacted]
Sent: woensdag 24 februari 2021 10:20:02
To: [redacted]
Cc: [redacted]
Subject: GGD Contact beveiligingsmaatregelen
Importance: Normal
Sensitivity: None
Attachments:
Factsheet Privacy GGD Contact 1.0.pdf; Beveiligingsmaatregelen GGD voor gebruik van webapplicatie met medische informatie v3.1.pdf; Bijlage IV - 08_12_2020 Def. DPIA GGD Contact v1.0.docx;

Hallo collega's,

Zoals afgesproken heb ik op onze teamsite 'Implementatie GGD Contact' de veilig werken documenten vanuit de GGD GHOR geplaatst. Bijgaand een tweetal documenten die specifiek ingaan op de beveiliging en de DPIA.

Belangrijk hierbij is dat de opgenomen beveiligingsmaatregelen vereisten bevat waar GGD GHOR NL en de GGD aan moet voldoen voor ingebruikname BCO Portaal (een uitgebreidere checklist/self-assesmenent voor de NEN7510 zal binnenkort verschijnen en met jullie gedeeld worden).

Aan jullie drieën het verzoek om deze maatregelen intern te toetsen en jullie bevindingen in de DPIA op te nemen bij de opgesomde risico's vanaf pagina 41.

Met vriendelijke groeten,

[redacted]

[redacted]

[redacted]

GGD Hart voor Brabant

Pettelaarpark 10 Den Bosch

Postbus 3024, 5003 DA Tilburg

www.ggdhvb.nl

[redacted]

[redacted]@ggdhvb.nl

Aanwezig op: ma-di-wo-do

Gezond doet leven!

12.8
Gearchiveerd: maandag 2 mei 2022 20:22:53
Van: [redacted]
Verzonden: donderdag 9 september 2021 17:42:23
Aan: [redacted] Directiesecretariaat GGD Hart voor Brabant
Onderwerp: RE: Overeenkomsten GGD Contact
Urgentie: Normal
Precisie: None

Eens. Kan getekend worden.

Van: [redacted]ggdhvb.nl>
Verzonden: donderdag 9 september 2021 15:38
Aan: [redacted]
Hart voor Brabant <[redacted]ggdhvb.nl>
Onderwerp: RE: Overeenkomsten GGD Contact

Beste allemaal,

Wat mij betreft na deze check van [redacted] geen belemmeringen om te tekenen.

Met vriendelijke groeten,

[redacted]

GGD Hart voor Brabant
Pettelaarpark 10, 5216 PD 's-Hertogenbosch
Postbus 3024, 5003 DA Tilburg
www.ggdhvb.nl
[redacted]
Gezond doet leven!

Van: [redacted]
Verzonden: donderdag 9 september 2021 15:03
Aan: [redacted]
Onderwerp: FW: Overeenkomsten GGD Contact
Urgentie: Hoog

Hallo allen,

Mijn opmerkingen mbt deze overeenkomsten:

- Ik heb de verwerkersovereenkomsten en de te tekenen DVO snel gelezen en kom een aantal kleine punten tegen waarvan ik vind [redacted] Vanuit privacy oogpunt wat mij betreft nu geen reden om niet te tekenen, ook gezien het feit dat GGD Contact nog niet uitontwikkeld is en dat VWS in de toekomst het beheer/ontwikkeling van GGD Contact zal overdragen aan een andere partij.
- GGD Twente (Functionaris Gegevensbescherming) gisteren nog gebeld. Zij geeft aan dat er tijdens mijn vakantie in het

landelijke overleg van de Functionaris Gegevensbescherming deze overeenkomsten zijn besproken en er nog opmerkingen waren. Toen is aangegeven dat er de opmerkingen verzameld gaan worden voor een toekomstige aanpassing, maar dat de GGD'en wel tekenen.

- Vandaag nog GGD Rotterdam gebeld (FG/jurist) en ook hij gaf aan dat er getekend wordt en dat de opmerkingen in een later addendum verwerkt gaan worden. Een aantal GGD'en (Rotterdam, Twente, West Brabant, Rotterdam-Rijnmond, Friesland) hebben reeds opmerkingen naar [redacted]s en [redacted] (GGD Ghor gemaild).

Met vriendelijke groeten,

[redacted]
Functionaris gegevensbescherming

Hart voor Brabant
Pettelaarpark 10 Den Bosch
Postbus 3024, 5003 DA Tilburg
www.ggdhvb.nl
[redacted]
Gezond? doet leven!

Van: Directiesecretariaat GGD Hart voor Brabant <[redacted]ggdhvb.nl>
Verzonden: donderdag 9 september 2021 08:02
Aan: [redacted]
Onderwerp: FW: Overeenkomsten GGD Contact
Urgentie: Hoog

Hoi [redacted]
Klopt toch dat jij [redacted] laat weten wanneer contract getekend kan worden? Graag met cc naar directiesecretariaat.

Met vriendelijke groeten,
[redacted]

Hart voor Brabant
Pettelaarpark 10
's-Hertogenbosch
Postbus 3024, 5003 DA Tilburg
www.ggdhvb.nl
[redacted]
Gezond? doet leven!

Van: [redacted]
Verzonden: donderdag 2 september 2021 09:48
Aan: Directiesecretariaat GGD Hart voor Brabant <[redacted]ggdhvb.nl>; [redacted]
Onderwerp: Overeenkomsten GGD Contact

Goedemorgen allemaal,

De afgelopen maanden zijn we bezig geweest met de voorbereidingen voor de implementatie van GGD Contact. We zijn ondertussen goed voorbereid en starten deze week met het opleiden van de eerste medewerkers. 13 september willen we

met de eerste groep medewerkers over gaan naar het nieuwe systeem voor de uitvoering van het Bron- en contactonderzoek.

Idealiter zijn vóór de livegang (13 september) de benodigde documenten getekend. Vandaag is voor ons allemaal de eerste keer dat we de documenten toegestuurd krijgen en zijn jullie ([redacted] en [redacted] nog op vakantie. Vandaar mijn vraag: Denken jullie dat het haalbaar is de overeenkomsten vóór 13 september te beoordelen en bij akkoord te tekenen? Als dit niet in de planning past zou ik graag met jullie afstemmen wat dat betekent voor de livegang van GGD Contact.

Mochten jullie interesse hebben, dan kan ik jullie wat meer vertellen over wat de eerste oplevering van GGD Contact gaat doen en hoe het ontwikkel-/ implementatieproces is verlopen. Ik hoor graag of hier animo voor is.

Alvast bedankt voor jullie reactie.

Met vriendelijke groet,

[redacted]
Programma Corona
Aanwezig: Ma, di, wo, do

GGD Hart voor Brabant
Gezond doet leven!

Pettelaarpark 10,
5216 PD 's-Hertogenbosch
www.ggdhvb.nl

[redacted]

Van: [redacted]minvws.nl>
Verzonden: donderdag 2 september 2021 08:33
Aan: [redacted] <[redacted]ggdghor.nl>
Onderwerp: Overeenkomsten GGD Contact

Geachte mevrouw [redacted]

Hierbij stuur ik u de overeenkomsten t.b.v. GGD Contact toe.

Het gaat om:

- 1.0 Dienstverleningsovereenkomst VWS voor GGD Contact release 1.1, incl. bijlage:
  - 1.1 Verwerkersovereenkomst ARVODI VWS voor GGD Contact
- 2.0 Dienstverleningsovereenkomst GGD GHOR Nederland, incl. bijlagen:
  - 2.1 Dienstbeschrijving
  - 2.2 Service Level Agreement
  - 2.3 Dossier Afspraken en Procedures
  - 2.4 Verwerkersovereenkomst
  - 2.5 Checklist onboarding applicaties

Deze overeenkomsten zijn opgesteld met inbreng vanuit vele inhoudelijke experts.
De concept versies van deze documenten zijn op 15 juni 2021 aangeboden aan de stuurgroep fase 1 vervanging HP Zone (Lite) ter review en de commentaren die hierop zijn ontvangen zijn verwerkt in de definitieve versies zoals vastgesteld op de stuurgroep van 25 juni 2021.

Documenten 1.0, 1.1, 2.0 en 2.4 dienen door u ondertekend te worden.

Graag ontvang ik de door u getekende stukken retour, zodat ik deze kan laten ondertekenen door de overige partijen.

Vergeet niet om een datum in te vullen als hierom gevraagd wordt in het document.

U ontvangt na ondertekening door alle partijen het complete pakket van mij retour.

[redacted]

PMO GGD Contact
.....
Ministerie van Volksgezondheid, Welzijn en Sport
Directie Informatiebeleid/CIO
Programma Realisatie Digitale Ondersteuning

Parnassusplein 5 | 2511 VX | Den Haag
Postbus 20350 | 2500 EJ | Den Haag
.....
[redacted]

12.9
Gearchiveerd: dinsdag 3 mei 2022 11:20:38
Van: [redacted]
Verzonden: zondag 14 november 2021 18:11:54
Aan: [redacted]
Onderwerp: DPIA GGD Contact
Urgentie: Normal
Precisie: None
Bijlagen:
DPIA GGD Contact v1.1.3 def. versie opnemen FG advies .docx;

Hallo collega's,
Bijgaand de afgeronde DPIA GGD Contact voorzien van mijn advies. Deze DPIA is landelijk opgesteld en voorzien van FG advies voordat de definitieve versie is ontvangen. In bijgevoegd advies heb ik mij beperkt tot de maatregelen die wij als lokale GGD moeten oppakken cq monitoren.

Zijn er vragen, dan hoor ik het graag.

Met vriendelijke groeten,

[redacted]

Hart voor Brabant
Gezond doet leven!
Pettelaarpark 10 Den Bosch
Postbus 3024, 5003 DA Tilburg
www.ggdhvb.nl
[redacted]
Aanwezig op: ma-di-wo-do

DPIA GGD CONTACT

Addendum 01 Zelf BCO

Auteurs:
Veronique Kwaaitaal (VWS)

DATUM	**29-1-2021**
STATUS	Definitief
VERSIE	1.0
BOUWT VOORT OP DPIA VERSIE	DPIA GGD CONTACT V1.0 8 DECEMBER 2020

MANAGEMENTSAMENVATTING

Dit DPIA GGD Contact Addendum nr. 2 Zelf BCO bevat een risicoanalyse van wijzigingen in de functionaliteit van de applicatie GGD Contact en de toepassing daarvan. Deze DPIA bouwt voort op vorige versies en addenda op de eerste definitieve versie van de DPIA GGD Contact.

OMSCHRIJVING VAN NIEUWE FUNCTIONALITEIT

De index selecteert in de app welke corona-gerelateerde klachten hij had/heeft en op welke dag deze klachten zijn begonnen. Aan de hand van de ingegeven datum wordt de besmettelijke periode vastgesteld (2 dagen voordat de klachten zijn begonnen). Indien er geen klachten zijn, wordt gevraagd naar de testdatum, die dan wordt aangehouden als start van de besmettelijke periode.

DPIA ANALYSE

Deze wijziging heeft impact op de DPIA-onderwerpen Dataminimalisatie, Opslag en Transparantie.

RISICO'S EN MAATREGELEN

De nieuwe functionaliteit brengt de volgende risico's en maatregelen met zich mee. Deze nieuwe risico's en maatregelen zijn opgenomen in de GGD Contact Risicomatrix.

Nr.	Risico	Belang / impact	Maatregel
x	Strijd met het transparantiebeginsel van art. 5.1 AVG.	laag	De privacyverklaring moet worden aangevuld.
y	De verwerking van klachten door de GGD kan niet noodzakelijk blijken.	hoog	Noodzaak onderbouwen (in DPIA van het reguliere BCO). Als blijkt dat de noodzaak niet

Nr.	Risico	Belang / impact	Maatregel
			kan worden onderbouwd, moet Functionaliteit zelf BCO worden gewijzigd.

1 INLEIDING OP HET ADDENDUM

1.1 GGD Contact

Ten behoeve van infectieziektebestrijding hebben GGD'en op basis van Wet publieke gezondheid (**Wpg**) de taak gekregen om bron- en contactopsporing (**BCO**) uit te voeren. Om het proces te versnellen maken de GGD'en in Nederland gebruik van een BCO-ondersteunende app met een bijbehorend webportal (**GGD Contact**).

1.2 Nieuw functionaliteit

In dit document wordt een analyse gedaan op de toevoeging van functionaliteit waarbij klachten en datums worden uitgevraagd ter vaststelling van de besmettelijke periode, Functionaliteit zelf BCO op GGD Contact.

1.3 Doel van dit document

Dit document bevat een Data Protection Impact Assessments op Functionaliteit zelf BCO. De DPIA Functionaliteit zelf BCO is bedoeld om de risico's en te nemen maatregelen ten aanzien van de wijzigingen die Functionaliteit zelf BCO met zich meebrengen overzichtelijk weer te geven voor de GGD'en.

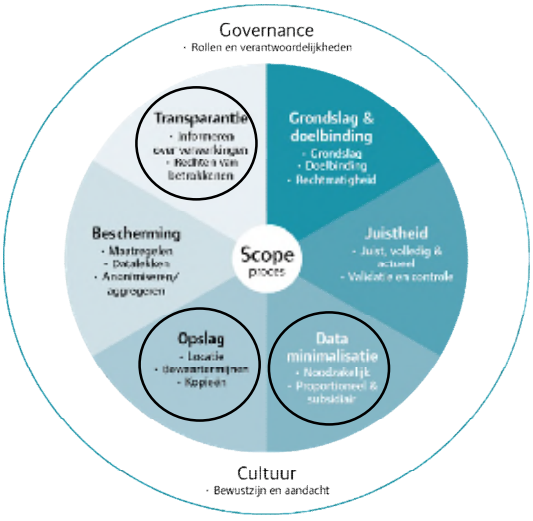
1.4 Onderzoeksopzet

Het vertrekpunt voor de addenda op de Landelijke Referentie Data Protection Impact Assessment voor GGD'en GGD Contact ter ondersteuning BCO (**DPIA GGD Contact**) is de eerder vastgestelde DPIA GGD Contact en de daarin reeds benoemde risico's en maatregelen. Voor iedere nieuwe functionaliteit wordt in een apart addendum een DPIA-risicoanalyse gemaakt die alleen ziet op de wijzigingen die de nieuwe functionaliteit met zich meebrengt.

Ieder addendum bevat:

- Flowchart van de situatie as-is.
- Flowchart van de technische wijzigingen die de nieuwe functionaliteit met zich meebrengt.
- DPIA-analyse van de wijzigingen door op de onderwerpen:
    - governance & cultuur
    - grondslag en doelbinding
    - juistheid
    - dataminimalisatie
    - opslag
    - bescherming
    - transparantie

Wanneer er een wijziging is ten opzichte van de GGD Contact DPIA wordt dat hiernaast visueel weergegeven in het DPIA-wiel.



Afbeelding 1. Template VKA DPIA wiel + focuspunten addenda

1.5 Document historie

Tabel 1. Document historie

Datum	Versie	Wie	Toelichting wijziging
22-1-2021	0.1	Veronique Kwaaitaal	Aanmaak document
29-01-2021	1.0	Veronique Kwaaitaal	Wijzigingen n.a.v. FG reviewsessie

Tabel 2. Overzicht addenda

Datum	Functionaliteit	Toelichting wijziging
29-1-2021	1	Vaststellen besmettelijke periode ahv klachten en datum eerste klachten of testdatum

1.6 Afstemming GGD'en

GGD	FG	Datum
Praktijktestregio's per 28/01/2021		28/01/2021

Tabel 3. Afstemming ter goedkeuring

2 RISICOANALYSE

2.1 Nieuwe functionaliteit

2.1.1 Omschrijving nieuwe functionaliteit

Met Functionaliteit zelf BCO selecteert de index zelf in de app zijn klachten uit een lijstje met COVID-19-gerelateerde klachten en voert de datum in dat de klachten begonnen. Aan de hand van de ingegeven datum wordt in de app de eerste dag van de besmettelijke periode vastgesteld: 2 dagen voordat de klachten zijn begonnen. Het maakt daarbij niet uit welke klacht(en) wordt/worden geselecteerd. Indien er geen klachten zijn, voert de index de testdatum in, die dan wordt aangehouden als begindatum van de besmettelijke periode.

De gegevens (klachten, begindatum of testdatum) worden verzonden naar het BCO-portaal en daar opgeslagen, zodat de BCO-medewerker ze in een telefonische follow-up kan verifiëren en eventueel aanpassen.

In de as-is situatie worden klachten en begindatum/testdatum telefonisch doorgegeven door de index aan de BCO-medewerker, die de besmettelijke periode vaststelt en dit opneemt in het BCO-portaal. In de soll-situatie wordt deze besmettelijke periode vastgesteld door de index in de GGD Contact-app en via de app verstuurd naar het BCO-portaal. Een tweede verschil is dat in de as-is situatie de BCO-medewerker de aanvang van de besmettelijke periode bepaalt, terwijl in de soll-situatie de app dat berekent aan de hand van een door de index ingegeven datum.

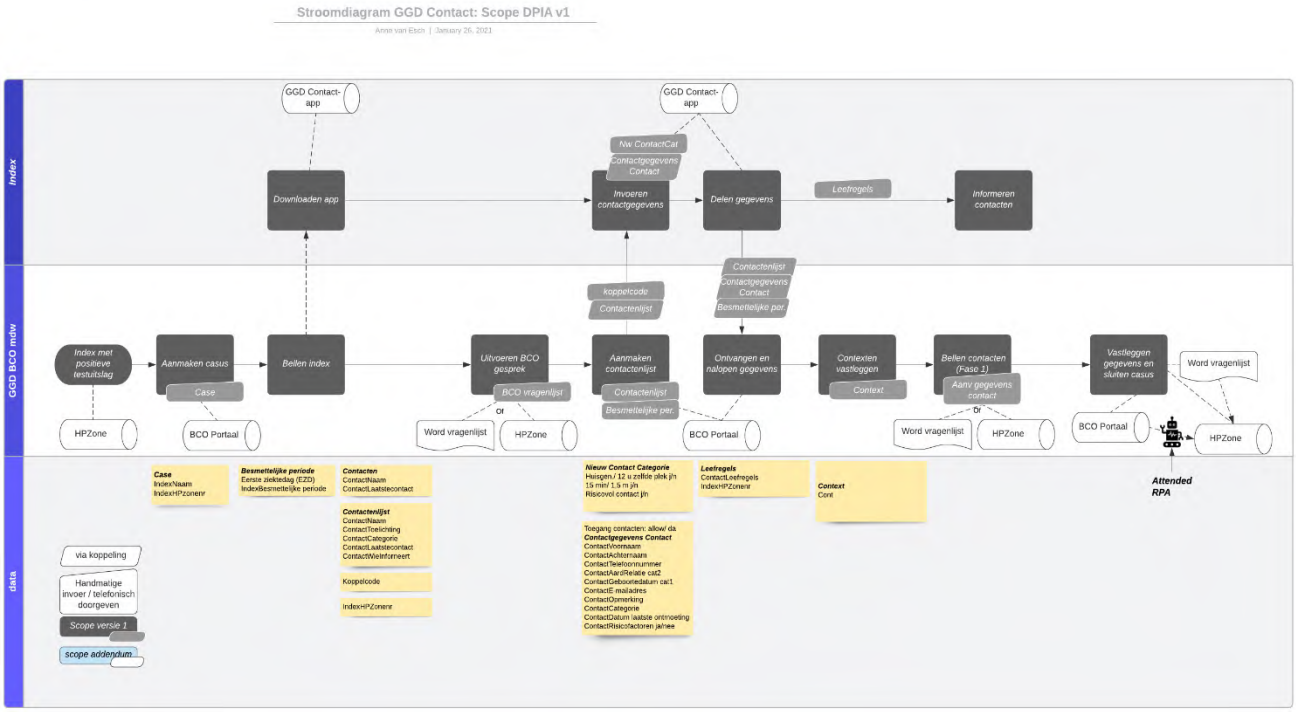
De gegevens (klachten, begindatum, testdatum) in deze functionaliteit worden alleen gebruikt voor het vaststellen van de begindatum van de besmettelijke periode. De gegevens bakenen daarmee de omvang van het BCO af. Deze gegevens worden niet gebruikt voor diagnose, monitoring en/of behandelen van COVID-19 en GGD Contact met Functionaliteit zelf BCO kwalificeert daarom niet als medisch hulpmiddel. De kwalificatie van de mogelijke toepassing van de verordening rondom het zijn van een medisch hulpmiddel is uitgevoerd door Pels Rijcken, d.d 22 januari 2021.[1]

Functionaliteit zelf BCO wordt alleen gebruikt als in het BCO-portaal nog geen besmettelijke periode is vastgelegd.

[1] Zie advies inzake Kwalificatie GGD-Contact van Pels Rijcken, zaaknummer 11015043 d.d. 22 januari 2021.

2.1.2 Proces flow chart huidige situatie (as is)

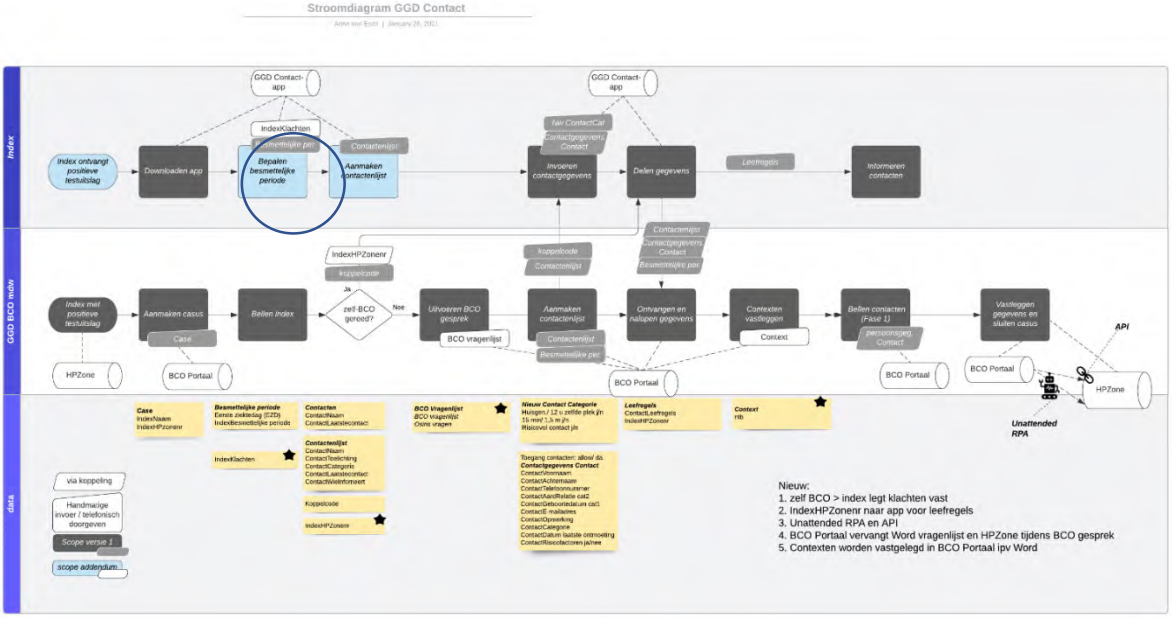
In afbeelding 2 is het proces van de huidige situatie visueel weergegeven.



Afbeelding 2: Proces flow chart (as is)

2.1.3 Flow chart toekomstige situatie nieuwe functionaliteit (soll)

In afbeelding 3 is het toekomstige proces na toevoeging van de nieuwe functionaliteit visueel weergegeven.



Afbeelding 3: Proces flow chart (soll)

2.2 DPIA – herijking

De nieuwe functionaliteit kan ten opzichte van de GGD Contact DPIA en eventuele voorafgaande addenda een wijziging teweegbrengen in de risicoanalyse ten aanzien van de gegevensbescherming. In de volgende onderdelen wordt een analyse gemaakt van op de thema's: governance & cultuur, grondslag en doelbinding, juistheid, dataminimalisatie, opslag, bescherming en transparantie.

2.2.1 Governance & cultuur

ANALYSE

De nieuwe functionaliteit brengt geen wijzigingen met zich mee ten aanzien van het thema governance en cultuur.

2.2.2 Grondslag en doelbinding

ANALYSE

De nieuwe functionaliteit brengt geen wijzigingen met zich mee ten aanzien van het thema grondslag en doelbinding.

2.2.3 Juistheid

ANALYSE

De nieuwe functionaliteit brengt geen wijzigingen met zich mee ten aanzien van het thema juistheid.

2.2.4 Dataminimalisatie

ANALYSE

Open/gesloten velden

In de GGD Contact-app wordt gebruik gemaakt van gesloten vraag met betrekking tot de eerste ziektedag. Dit betreft een datumveld met een beperkte range aan data waaruit gekozen kan worden.

De klachten die geselecteerd kunnen worden door de index, betreffen checkboxen waar de index kan toevoegen welke klachten van toepassing zijn. 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.

Verkorte duur BCO-gesprek

Met Functionaliteit zelf BCO worden meer gegevens verwerkt in de GGD Contact-app dan in de as-is situatie (namelijk: klachten, datum eerste klacht, testdatum). Deze invoer in de GGD Contact-app door de index is nodig om het aantal uur dat de GGD per index besteedt aan bron- en contactopsporing te verminderen (primaire doel van GGD Contact). Doordat de index de klachten in de app invoert, krijgt het opvolgende BCO-telefoongesprek een meer controlerend karakter. Het telefoongesprek kan hierdoor worden verkort.

Bewuste klachtenselectie door index

De index kiest actief tussen de klacht-keuzemogelijkheden. Hij moet per klacht aanvinken of hij die heeft. Hierdoor is hij bewuster met de lijst bezig dan wanneer sec een lijst met bij COVID-19 passende klachten wordt gepresenteerd en hij die alleen kan lezen. Onderzoek (en ervaring van BCO-medewerkers) laat zien dat indexen vaak (lichte) klachten niet aan COVID-19 linken, en dat ze daarmee vaak in eerste instantie een te conservatieve inschatting maken van hun besmettelijke periode. Het echt actief processen van deze lijst is daarom noodzakelijk. Het is ook noodzakelijk deze klachten apart weer te geven in een selectielijst in plaats van de klachten in groepen te clusteren. Hierdoor wordt de index bij elke klacht actief aan het denken gezet. Het clusteren van klachten zou dit actief denken belemmeren waardoor de besmettelijke periode niet goed wordt vastgesteld en er mogelijk te veel of te weinig contacten worden verzameld. In het BCO-gesprek dat volgt op invullen van zelf BCO zal de GGD-medewerker nogmaals met de index door de aangevinkte klachten heenlopen. Eerst met clusters van klachten werken en daarna alsnog de individuele klachten uitvragen en vastleggen is dubbel werk.

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. Deze DPIA is ten tijde van het schrijven van dit Addendum nog niet gereed. Het risico bestaat dat de noodzakelijkheid van de verwerking van klachten door de GGD niet kan worden onderbouwd, hetgeen Functionaliteit zelf BCO onrechtmatig maakt.

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.

Conclusie

De gegevensverwerking van Functionaliteit zelf BCO is noodzakelijk voor het doel van GGD Contact en deze kan niet verder geminimaliseerd worden.

2.2.5 Opslag

ANALYSE

Er worden in de app meer gegevens verzameld en opgeslagen, namelijk klachten, datum eerste klachten en testdatum. Deze gegevens worden doorgestuurd naar het portaal. De bewaartermijnen in app en portaal veranderen niet. Kortom, de nieuwe functionaliteit brengt geen wijzigingen met zich mee ten aanzien van het thema opslag.

2.2.6 Bescherming

ANALYSE

De gegevens (klachten, datum eerste klachten en testdatum) zijn gezondheidsgegevens en zijn geclassificeerd als bijzondere persoonsgegevens. De gegevens die in de as-is situatie door app en portaal worden verwerkt zijn dat ook. De beveiliging kan daarom hetzelfde blijven.

De nieuwe functionaliteit brengt geen wijzigingen met zich mee ten aanzien van het thema bescherming.

2.2.7 Transparantie

ANALYSE

De gegevens (klachten, begindatum of testdatum) worden verzonden naar het BCO-portaal en daar opgeslagen, zodat de BCO-medewerker ze in een telefonische follow-up kan verifiëren en eventueel aanpassen. De index kan uit de vragenlijst in de app niet opmaken of de klachten ook worden doorgezonden aan de GGD, of alleen de begindatum van de klachten (of de testdatum). Om te voldoen aan het transparantiebeginsel van art. 5.1 AVG moeten betrokkenen hierover worden geïnformeerd. Het toevoegen van de functionaliteit ‘Zelf BCO’ vraagt om een aanpassing van de privacyverklaring.

3 CONCLUSIES

3.1 Risico's, aandachtspunten en maatregelen

De DPIA-analyse uit hoofdstuk 2 op functionaliteit zelf BCO brengt de volgende risico's en maatregelen met zich mee. Deze maatregelen zijn opgenomen in de Risicomatrix GGD Contact.

Nr.	Risico	Belang / impact	Maatregel
x	Art. 13 AVG verplicht niet tot het verstrekken van een beschrijving van de functionaliteit, maar in de privacyverklaring as-is 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.	laag	De privacyverklaring moet worden aangevuld met een toelichting op Functionaliteit zelf BCO. (Landelijk)
y	De verwerking van klachten door de GGD kan niet noodzakelijk blijken.	hoog	Noodzaak onderbouwen (in DPIA van het reguliere BCO). Als blijkt dat de noodzaak niet kan worden onderbouwd, moet Functionaliteit zelf BCO worden gewijzigd. (GGD)

3.2 Restrisico's

De restrisico's zijn laag ingeschaald omdat de eventuele gevolgen van Functionaliteit zelf BCO een acceptabel risico vormen. De kosten en moeite van eventuele aanvullende maatregelen wegen niet op tegen de geringe verdere reductie van het toch al acceptabele restrisico. Gezien de geconstateerde lage restrisico's is voorafgaande raadpleging bij de AP naar de mening van de auteurs niet nodig.

3.3 Evaluatie analyse

Het advies is om deze analyse binnen 2 jaar te herzien, mits er geen wijzigingen aan deze nieuwe functionaliteit plaatsvinden. Bij eerdere wijzigingen aan deze functionaliteit dient voor invoering van de wijziging de functionaliteit te worden herzien door middel van wijziging van dit addendum.

DPIA GGD CONTACT

Addendum Labeling

Auteurs:
Dorus-Jan ten Boom, Leonie Gerding

DATUM	**3-12-2021**
STATUS	Definitief
VERSIE	0.3
BOUWT VOORT OP DPIA VERSIE	20210623 DPIA GGD CONTACT RELEASE 1.1 V 1.1.3

MANAGEMENT SAMENVATTING

Dit Addendum betreft een aanvulling op de referentie DPIA voor GGD Contact en bevat een risicoanalyse op de nieuw toegevoegde functionaliteit 'Labeling'. Hierbij wordt voortgebouwd op de laatste versie van de DPIA en de eerder hieraan toegevoegde Addenda. Dit Addendum kan door GGD'en worden toegevoegd aan de DPIA voor GGD Contact indien een GGD gebruik wil maken van de nieuwe functionaliteit.

Labeling maakt het mogelijk dat een medewerker met de rol 'Werkverdeler' aan een case een kenmerk (label) toevoegt. Dit label geeft aan dat betreffende case door een specifiek team of type medewerker moet worden uitgevoerd of dat een case om een bepaalde reden met urgentie moet worden behandeld. Labeling is hiermee een belangrijk onderdeel van de functionaliteit Werkverdeling.

De toekenning van labels gebeurt vooralsnog alleen handmatig. Indien dit in de toekomst geautomatiseerd wordt, moet een aanvullende beoordeling van de privacyrisico's plaatsvinden.

DPIA ANALYSE

In het kader van dit Addendum is een analyse uitgevoerd op de privacyrisico's die het gebruik van de nieuwe functionaliteit met zich meebrengt, waaronder juridische, operationele en technische risico's. De belangrijkste risico's en bijbehorende maatregelen die uit beide analyses naar voren zijn gekomen zijn opgenomen in onderstaand overzicht.

RISICO'S EN MAATREGELEN

De nieuwe functionaliteit brengt één nieuw geïdentificeerde risico's met zich mee. Dit risico is zonder maatregelen gekwalificeerd als Hoog:

Nr.	Risico	Bruto risico (kans x impact)	Beheersmaatregelen	Netto risico (kans x impact)
1	Ondanks het uitgangspunt dat labels alleen gebruikt mogen worden voor werkverdeling, wordt druk uitgeoefend om de gegevens ook voor andere doeleinden te gebruiken (bijvoorbeeld kwaliteitsonderzoek of analyse van bepaalde groepen), met als gevolg dat de toepassing van labels toch niet beperkt blijft tot routering en prioritering van cases.	Kans: midden Impact: hoog Risico: hoog	Technische maatregel om dit risico te beheersen is labels niet langer op te slaan dan tot drie dagen nadat een dossier de status afgesloten heeft gekregen. Organisatorische maatregel is dat voor de ontwikkeling van een nieuwe toepassing van Labeling een wijzigingsprocedure moet worden doorlopen, waarvan de beoordeling van privacyrisico's een belangrijk onderdeel is en waarbij tevens de FG's van de GGD'en betrokken zijn.	Kans: laag Impact: hoog Risico: midden

Advies FG GGD Hart voor Brabant :

Ik heb alle vertrouwen in dat dit addendum erg zorgvuldig is samengesteld met input van de FG's van de regionale GGD'en tijdens de ontwikkeling van deze functionaliteit (privacy bij design). Functionaliteit is noodzakelijk om in periodes van grote infectiedruk cases goed te kunnen prioriteren en routeren. De labels m.b.t. detentie, AZC en dak/thuisloos liggen bij meerdere GGD'en gevoelig. Besloten is deze niet in de lijst op te nemen. In plaats daarvan kan het label "maatschappelijke instelling worden gebruikt.

<u>Belangrijk is om de volgende maatregelen uit te voeren:</u>
- Werkinstructie worden landelijk opgesteld. Geadviseerd word om conform de landelijke WI te werken. Bij lokale afwijkingen moet nagegaan worden of dit privacy risico's me zich mee brengen;
- Advies is om over 1 jaar de gehele GGD Contact DPIA te reviewen en na te gaan of er wijzigen zijn die privacy risico's met zich meebrengen.
- Labels alleen gebruiken voor werkverdeling en niet voor andere doeleinden (bijvoorbeeld kwaliteitsonderzoek of analyse van bepaalde groepen). Als in de toekomst de wens bestaat om nieuwe labels toe te voegen of om opgeslagen labels ook voor andere doeleinden te gaan gebruiken, dan zal opnieuw privacy en security risico's beoordeeld moeten worden (DPIA bijwerken).

[redacted]

20-1-2022

1 INLEIDING OP HET ADDENDUM

1.1 GGD Contact en nieuwe functionaliteit

Ten behoeve van infectieziektebestrijding hebben de GGD'en op basis van de Wet publieke gezondheid (Wpg) de taak om bron- en contactopsporing (BCO) uit te voeren. Om het proces te versnellen en de informatiebeveiliging te verbeteren is GGD Contact ontwikkeld. GGD Contact bestaat uit de GGD Contact App, waarmee de actieve rol van Indexen bij het BCO-proces wordt vergroot, en het hieraan gekoppelde BCO Portaal, een applicatie die het werkproces van de BCO-medewerker ondersteunt.

De functionaliteit Labeling heeft primair betrekking op het onderdeel BCO Portaal. Het gebruik van de GGD Contact App door een persoon die als Index is aangemerkt verandert hierdoor niet.

1.2 Doel van dit document

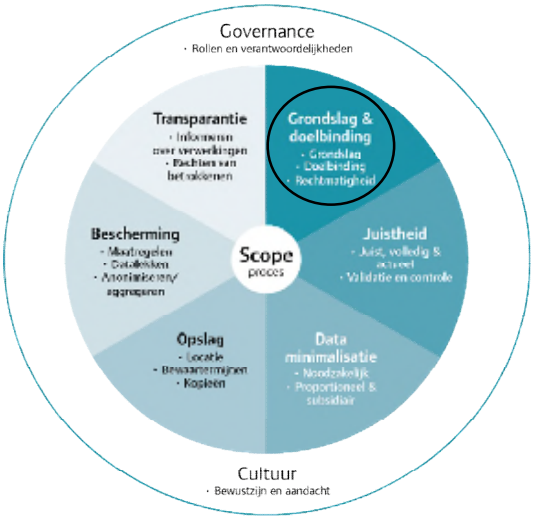
Dit document beschrijft hoe de nieuwe functionaliteit er op hoofdlijnen uitziet, analyseert welke privacyrisico's de nieuwe functionaliteit met zich meebrengt en welke maatregelen genomen kunnen worden om de risico's te beheersen.

Dit Addendum is opgezet als aanvulling op de referentie DPIA voor GGD Contact. Dit betekent dat dit Addendum, evenals de DPIA, door de GGD'en zelf 'op maat' moet worden gemaakt voor de eigen organisatie. Dit kan bijvoorbeeld betekenen dat in dit Addendum gesignaleerde risico's niet voor alle GGD'en gelden, of niet voor alle GGD'en even zwaar wegen. Het is nadrukkelijk aan de GGD'en zelf om hierin de eigen keuzes te maken, en deze in de eigen DPIA vast te leggen.

1.3 Onderzoeksopzet

Het vertrekpunt voor alle Addenda is de eerder vastgestelde Referentie DPIA voor GGD Contact en de daarin reeds benoemde risico's en maatregelen. Voor iedere nieuwe functionaliteit wordt in een apart Addendum een aanvullende risicoanalyse gemaakt die alleen ziet op de wijzigingen die de nieuwe functionaliteit met zich meebrengt.

De onderwerpen aan de hand waarvan getoetst wordt zijn hiernaast weergegeven in het door VKA ontwikkelde DPIA-wiel. De onderwerpen waarop zich nieuwe risico's voordoen zijn hierin omcirkeld.



Figuur 1: VKA DPIA-wiel met focuspunten

1.4 Document historie

Tabel 1. Document historie

Datum	Versie	Wie	Toelichting wijziging
5-11-2021	0.1	Dorus-Jan ten Boom, Leonie Gerding	Eerste versie voor interne reviewers
9-11-2021	0.2	Dorus-Jan ten Boom, Leonie Gerding	Versie ter review door de GGD'en
3-12-2021	0.3	Dorus-Jan ten Boom, Leonie Gerding	Versie na review door de GGD'en

2 RISICOANALYSE

2.1 Nieuwe functionaliteit

2.1.1 Introductie

De functionaliteit Labeling geeft medewerkers met de rol van Werkverdeler de mogelijkheid om aan elke case één of meerdere vooraf gedefinieerde labels toe te kennen. De toepassing van de functionaliteit Labeling is geen verplichting binnen het BCO Portaal en dient uitsluitend voor het routeren en prioriteren van dossiers, om zo efficiënter en beter uitvoering te kunnen geven aan het BCO. De GGD'en hebben zelf de keuze om binnen hun BCO-proces al dan niet gebruik te maken van Labeling.

De lijst met labels die gebruikt mogen worden is door de Product Owner van GGD Contact afgestemd met de proceseigenaren van de GGD'en en betreft de minimale set om alle GGD'en te kunnen ondersteunen. Uitgangspunt is dat de label-namen zo feitelijk mogelijk zijn en zo min mogelijk stigmatiserend voor betrokkenen. Een overzicht van de te gebruiken labels is opgenomen in paragraaf 2.1.3, met daarbij ook het doel waarvoor de labels gebruikt worden en een korte toelichting hierop.

2.1.2 Beschrijving functionaliteit

De nieuwe functionaliteit ziet er op hoofdlijnen als volgt uit:

- De Werkverdeler voert in GGD Contact cases in waarop BCO moet worden uitgevoerd. Hij doet dit op basis van de op dat moment bij de GGD bekende informatie. Dit betreft informatie die bij het maken van testafspraken is verzameld en gegevens uit de verplichte meldingen van artsen en laboratoria na het vaststellen van een besmetting. Deze informatie is vastgelegd in CoronIT en HP Zone Lite.

  Bij de introductie van de nieuwe functionaliteit is het tijdelijk mogelijk om ook vanuit de rol BCO-medewerker cases in te voeren en labels toe te voegen. Reden hiervoor is dat nog niet alle GGD'en van de rol Werkverdeler gebruik zullen gaan maken. Het is dus van belang dat bij elke GGD duidelijke afspraken worden gemaakt welke personen/rollen labels aan cases mogen gaan toekennen en dat deze personen hiervoor afdoende worden geïnstrueerd.

- Op basis van de bekende gegevens kan de Werkverdeler aan een case één of meerdere labels toevoegen, die aangeven dat het een specifiek type case is. Zaken met een bepaald label kunnen vervolgens aan een gespecialiseerd team of een specifieke behandelaar worden toegewezen of op basis van het label prioriteit toegekend krijgen. Toegekende labels zijn voor de Werkverdeler zichtbaar in de lijst met te verdelen dossiers, en tevens in het dossier voor de behandelaar.
- De medewerker of het team dat een case krijgt toegewezen, ziet deze in de werkvoorraad verschijnen. Ook de aan cases toegekende labels zijn hierin zichtbaar, waardoor bepaalde cases sneller kunnen worden opgepakt of door een specifiek teamlid behandeld kunnen worden.
- Blijkt een toegekend Label achteraf niet juist te zijn, of blijkt dat een case toch beter door een ander team of persoon kan worden behandeld, dan kan de medewerker een case aan de Werkverdeler teruggeven met in de notitie het verzoek het label aan te passen.

- Toegekende labels worden niet vastgelegd in de logging van GGD Contact.
- Een label blijft zichtbaar totdat de Werkverdeler een label handmatig verwijdert of een case de status ‘afgesloten’ krijgt en niet binnen drie dagen wordt heropend.

2.1.3 Labels

De nieuwe functionaliteit is zo opgezet dat alleen gewerkt kan worden met vooraf gedefinieerde labels. Gebruikers kunnen dus zelf geen nieuwe labels toevoegen of bestaande labels aanpassen. Is hieraan toch behoefte, dan moet hiervoor een separaat wijzigingsverzoek worden ingediend (middels de hiervoor geldende wijzigingsprocedure).

De gekozen labels zijn afgestemd met de GGD’en. Hierbij is aansluiting is gezocht bij de bestaande manier van werken bij de verschillende GGD’en, waarbij tevens het aantal labels zo klein mogelijk is gehouden. Onderstaand overzicht geeft weer welke labels aan cases kunnen worden toegevoegd.

	Label	**Doel**	**Toelichting**
1	Zorg (algemeen)	Toedelen aan aparte werkstroom	Wordt gebruikt door GGD’en waarbij alle zorg gerelateerde BCO onder één label valt.
2	Bewoner-zorg	Toedelen aan aparte werkstroom	BCO wordt opgepakt door de instelling zelf, met ondersteuning van de GGD. Omdat dit proces anders is dan het reguliere BCO-proces, is het wenselijk om deze cases bij de werkverdeling aan een aparte werkstroom toe te delen.
3	Medewerker-zorg	Toedelen aan aparte werkstroom	BCO voor zorgverleners wordt gedaan door een reguliere BCO-medewerkers. Het moet echter wel mogelijk zijn om zorgverleners aan specifieke, meer ervaren medewerkers toe te wijzen en deze dus te kunnen onderscheiden van andere indexen.
4	School	Toedelen aan aparte werkstroom	Gaat naar apart team (specifieke kennis/vaardigheden nodig). BCO op scholen wordt opgepakt door scholenteams, die de specifieke schooladviezen kennen en kennis hebben van de lokale scholen.
5	Contactberoep	Nodig om te kunnen prioriteren	Om in een periode van grote drukte de juiste prioriteiten te stellen, is het wenselijk om indexen met een contactberoep te kunnen herkennen, zodat hieraan desgewenst voorrang kan worden gegeven.
6	Maatschappelijke instelling	Toedelen aan aparte werkstroom	Gaat naar apart team (specifieke kennis/vaardigheden nodig).
7	Scheepvaart-opvarende	Toedelen aan aparte werkstroom	Gaat naar apart team (specifieke kennis/vaardigheden nodig).

	Label	Doel	Toelichting
8	Vluchten	Toedelen aan aparte werkstroom	Gaat naar apart team (specifieke kennis/vaardigheden nodig).
9	Buitenland	Toedelen aan aparte werkstroom	Gaat naar apart team (specifieke kennis/vaardigheden nodig).
10	VOI/VOC[1]	Toedelen aan aparte werkstroom	Gaat naar apart team (specifieke kennis/vaardigheden nodig).
11	Herhaaluitslag	Nodig om te kunnen prioriteren.	Dit gaat om indexen die in korte tijd meerdere keren positief zijn getest. Deze cases worden door een apart team en met verhoogde urgentie behandeld
12	Buiten meldportaal/ CoronIT	Toedelen aan aparte werkstroom	Meldingen die niet via het officiële meldportaal of via CoronIT bij de GGD zijn binnengekomen, maar via andere kanalen (bijvoorbeeld telefonisch of via zorgmail).
13	Onvolledige gegevens	Toedelen aan aparte werkstroom	Cases waarin contactgegevens ontbreken komen eerst bij een team dat gespecialiseerd is om deze gegevens nog na te gaan en toe te voegen. Is een case alsnog compleet gemaakt, dan wordt het label door de Werkverdeler weer verwijderd.
14	Index weet uitslag niet	Nodig om te kunnen prioriteren / Toedelen aan aparte werkstroom	Indexen die de testuitslag al kennen krijgen bij drukte een lagere prioriteit dan indexen die nog niet met de uitslag bekend zijn. Is een index nog niet geïnformeerd, dan stelt dit tevens zwaardere eisen aan een medewerker dan de situatie waarin een Index reeds van de besmetting op de hoogte is.
15	Uitbraak	Toedelen aan aparte werkstroom	Testen vindt plaats in aparte teststraat. Cases kunnen daarna toebedeeld aan het team dat met betreffende uitbraak bezig is.

2.1.4 Gevolgen voor Betrokkenen

Het gebruik van de functionaliteit Labeling brengt met zich mee dat cases in GGD Contact in een bepaalde categorie worden geplaatst. Voor degenen die in een dossier voorkomen kan dit voelen alsof zij ‘in een hokje worden gezet’. Belangrijk is dus dat het toekennen van een label geen persoonlijke interpretatie van gegevens plaatsvindt, maar alleen feitelijke informatie wordt gebruikt die al in het dossier zit. Het labelen is dan niet meer dan het naar voren halen van een reeds bestaand dossierkenmerk, zodat de Werkverdeler en de behandelaar snel kunnen zien welk type dossier het betreft.

[1] Variant of Interest / Variant of Concern. Dit label is toegevoegd n.a.v. het opduiken van de Omikron-variant eind november 2021

Deze DPIA ziet alleen op het handmatig toekennen van labels, met als enige toepassing het routeren en prioriteren van cases. Er is dus noch sprake is van een geautomatiseerd proces, noch van evalueren van persoonlijke aspecten. Dit betekent dat geen sprake is van profilering in de zin van de AVG[2].

Als in de toekomst de wens bestaat om nieuwe labels toe te voegen of om opgeslagen labels ook voor andere doeleinden te gaan gebruiken, dan zal hiervoor het vastgestelde wijzigingsproces moeten worden doorlopen. Onderdeel hiervan is het opnieuw beoordelen van privacy en security risico's en het bijwerken van de DPIA, waarbij ook de FG's van de GGD'en betrokken zullen zijn.

> **Risico 1:** ondanks het uitgangspunt dat labels alleen gebruikt mogen worden voor werkverdeling, wordt druk uitgeoefend om de gegevens ook voor andere doeleinden te gebruiken (bijvoorbeeld kwaliteitsonderzoek of analyse van bepaalde groepen), met als gevolg dat de toepassing van labels toch niet beperkt blijft tot routering en prioritering van cases. De kans in de situatie zonder dat maatregelen zijn genomen wordt ingeschat op **Midden**. Omdat dit een inbreuk betekent op het AVG-beginsel van doelbinding is ook de impact ervan **Hoog**. Bij elkaar geeft dit een bruto risicokwalificatie **Hoog**.
>
> Technische maatregel om dit risico te beheersen is labels niet langer op te slaan dan tot drie dagen nadat een dossier de status afgesloten heeft gekregen. Organisatorische maatregel is dat voor de ontwikkeling van een nieuwe toepassing van Labeling een wijzigingsprocedure moet worden doorlopen, waarvan de beoordeling van privacyrisico's een belangrijk onderdeel is en waarbij tevens de FG's van de GGD'en betrokken zijn.
>
> In de situatie met maatregelen wordt de kans dat labels tevens voor andere toepassingen gebruikt worden ingeschat op **Laag**. De impact ervan ingeval het toch gebeurt is hetzelfde, namelijk **Hoog**. Bij elkaar betekent dit dat het netto risico de kwalificatie **Midden** krijgt.

Het labelen van cases komt ook ten goede aan betrokkenen. Het zorgt er immers voor dat Indexen direct door een gespecialiseerde BCO-medewerker worden benaderd en dat indien nodig een hoge urgentie aan hun zaak kan worden toegekend. Dit betekent dat betrokkenen die op deze manier worden benaderd eerder weten waar ze aan toe zijn en dus ook eerder naar het handelingsperspectief kunnen gaan leven.

2.2 DPIA – aanpassing

De nieuwe functionaliteit kan ten opzichte van de vastgestelde DPIA voor GGD Contact en andere, voorafgaande addenda een wijziging teweegbrengen in de risicoanalyse. In deze paragraaf wordt een

[2] Artikel 4 lid 4 AVG definieert profilering als volgt: 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

analyse gemaakt van op de thema's Governance & Cultuur, Grondslag & Doelbinding, Juistheid, Dataminimalisatie, Opslag, Bescherming en Transparantie.

2.2.1 Governance & Cultuur

De nieuwe functionaliteit heeft geen gevolgen op het gebied van Governance & Cultuur.

2.2.2 Grondslag & Doelbinding

GGD Contact heeft tot doel om het BCO-proces efficiënter en sneller te laten verlopen. De toevoeging van labels aan cases ten behoeve van werkverdeling valt geheel binnen deze doelstelling. Gegevens worden hiermee dus niet voor een ander doel gebruikt. Het risico dat gegevens ondanks deze doelbinding toch voor andere doeleinden worden gebruikt, is hiervoor uitgewerkt in paragraaf 2.1.4.

De wettelijke grondslag voor het uitvoeren van BCO ligt in artikel 6 lid 1 sub c AVG (taak van algemeen belang) jo artikel 6 lid 1 sub c Wpg (BCO-taak gemeenten). Deze grondslag is ook de wettelijk basis voor de functionaliteit labeling. Voor de verwerking van bijzondere persoonsgegevens is de uitzondering van artikel 9 lid 2 sub i van toepassing (algemeen belang op het gebied van volksgezondheid).

Ook op het vlak van Grondslag & Doelbinding brengt de nieuwe functionaliteit geen nieuwe risico's met zich mee.

2.2.3 Juistheid

De Werkverdeler voegt labels aan cases toe op basis van de in het dossier beschikbare informatie. Op basis hiervan komt een case in een bepaalde werkstroom terecht. Blijkt een case op een later moment niet in de juiste werkstroom te zitten, dan wordt deze door de behandelende BCO-medewerker teruggezet naar de Werkverdeler, met daarbij de reden waarom dit gebeurd is. De Werkverdeler kan een case dan alsnog van het juiste label voorzien en toewijzen aan de juiste werkstroom.

2.2.4 Dataminimalisatie

Bij het samenstellen van de lijst met labels (zie paragraaf 2.1.3) is door de Product Owner met de GGD'en afgestemd welke labels zij nodig hebben om cases op een goede manier te kunnen toewijzen en te prioriteren. De expliciete vraag hierbij was welke labels hiervoor minimaal noodzakelijk zijn. Dit heeft geleid tot de lijst met labels zoals die nu is.

De teams waarmee GGD'en werken verschilt per regio. Het is dus aan de regio's zelf om te bepalen of zij gebruik willen maken van labels (en zo ja, van welke).

2.2.5 Opslag

Toegekende labels blijven zichtbaar in een dossier totdat deze door de Werkverdeler worden verwijderd of een case de status 'afgesloten' krijgt en niet binnen drie dagen is heropend. Zichtbare labels kunnen alleen worden gebruikt in de context van het toewijzen van cases (door de Werkverdeler) en het oppakken ervan (door BCO-medewerkers).

De nieuwe functionaliteit heeft geen effect op de bewaartermijn van dossiers of op de locaties waarop deze bewaard worden.

2.2.6 Bescherming

Labels kunnen alleen worden aangemaakt of gewijzigd door medewerkers die dossiers kunnen aanmaken. Zoals reeds vermeld in paragraaf 2.1.2, is dit een taak van de Werkverdeler, waarbij het bij de introductie van de functionaliteit tijdelijk mogelijk is dit ook vanuit de rol van BCO-medewerker te doen. Belangrijk is dat het binnen elke GGD'en voor alle medewerkers duidelijk is wie de bevoegdheid heeft om labels aan cases toe te kennen en dat deze persoon tevens hiertoe afdoende is geïnstrueerd.

De nieuwe functionaliteit heeft geen invloed op de beveiliging van de overige gegevens.

2.2.7 Transparantie

De toevoeging van labels aan cases kan betekenen dat informatie die tot dan toe alleen impliciet in een dossier aanwezig was (bijvoorbeeld het adres van een zorginstelling) na toekenning van een label hieraan tevens expliciet wordt toegevoegd (label 'Zorg-bewoner'). Dit betekent dat in het BCO-proces een aantal extra persoonsgegevens verwerkt wordt, namelijk de inhoud van de labels. In het kader van de transparantie kan dit consequenties hebben voor de volgende AVG-documenten[3]:

- De privacyverklaring waarmee de GGD'en aan Betrokkenen informatie geven over het BCO-proces
- Het verwerkingenregister dat de GGD'en, VWS en GGD GHOR hiervoor hebben opgesteld

Verwerking van nieuwe gegevens kan tevens gevolgen hebben voor de specificatie van verwerkte gegevens in verwerkersovereenkomsten. Of aanpassing nodig is hangt af van de mate van detail waarin de categorieën verwerkte gegevens zijn beschreven.

[3] De toevoeging van de functionaliteit Labeling heeft geen invloed op de privacyverklaring in GGD Contact voor BCO-medewerkers en op de privacyverkalring in de GGD Contact App. Aanpassing hiervan is niet nodig.

3 CONCLUSIES

3.1 Risico's, aandachtspunten en maatregelen

Hieronder is een overzicht opgenomen van de gesignaleerde risico's. Van elk risico wordt vervolgens de kans en impact aangegeven in de situatie dat geen beheersmaatregelen zijn genomen (bruto risico). Vervolgens wordt aangeven middels welke beheersmaatregelen het risico kan worden beperkt en wat dan nog het restrisico is (netto risico).

De manier waarop kans en impact gewogen worden bij de classificatie van het risico sluit aan op de systematiek die in de DPIA gehanteerd wordt en is beschreven in paragraaf C15 van de DPIA.

Nr.	Risico	Bruto risico (kans x impact)	Beheersmaatregelen	Netto risico (kans x impact)
1	Ondanks het uitgangspunt dat labels alleen gebruikt mogen worden voor werkverdeling, wordt druk uitgeoefend om de gegevens ook voor andere doeleinden te gebruiken (bijvoorbeeld kwaliteitsonderzoek of analyse van bepaalde groepen), met als gevolg dat de toepassing van labels toch niet beperkt blijft tot routering en prioritering van cases.	Kans: midden Impact: hoog Risico: hoog	Technische maatregel om dit risico te beheersen is labels niet langer op te slaan dan tot drie dagen nadat een dossier de status afgesloten heeft gekregen. Organisatorische maatregel is dat voor de ontwikkeling van een nieuwe toepassing van Labeling een wijzigingsprocedure moet worden doorlopen, waarvan de beoordeling van privacyrisico's een belangrijk onderdeel is en waarbij tevens de FG's van de GGD'en betrokken zijn.	Kans: laag Impact: hoog Risico: midden

3.2 Restrisico's

Bij alle besproken risico's achten de auteurs van dit Addendum het netto risico, oftewel het restrisico na het uitvoeren van genoemde maatregelen, acceptabel. Voorafgaande raadpleging bij de AP wordt derhalve niet nodig geacht.

3.3 Evaluatie analyse

Het advies is om deze analyse na één jaar te herzien, mits er tussentijds geen grote wijzigingen aan de beschreven functionaliteit plaatsvinden. Bij eerdere wijzigingen dient de herziening daaraan voorafgaand plaats te vinden.

Wob-verzoek SOLV/ICAM datalek 2021 coronasysteem

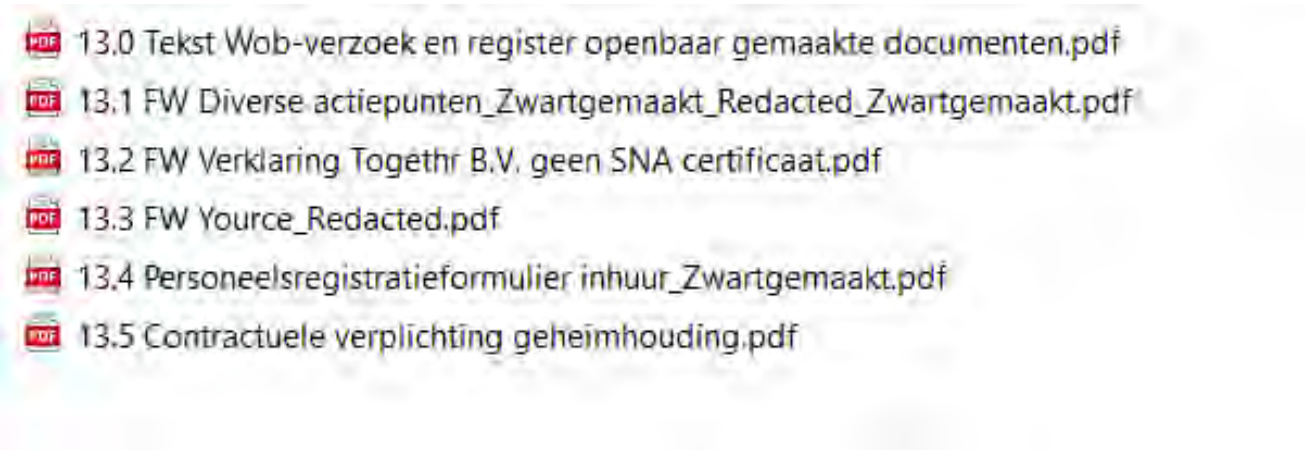
13.0 Tekst Wob-verzoek en register documenten

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:



13.1
Archived: donderdag 12 mei 2022 09:41:10
From: [redacted]
Sent: Wed, 17 Feb 2021 14:30:45
To: [redacted]
Subject: FW: Diverse actiepunten
Importance: Normal
Sensitivity: None
Attachments:
201808 OVK GGDHvB-Yource-Addendum.docx;

Met vriendelijke groet,

[redacted]

Pettelaarpark 10, Den Bosch
Postbus 3024, 5003 DA Tilburg
www.ggdhvb.nl

[redacted]@ggdhvb.nl
Aanwezig op: ma-di-wo-do
[redacted]

Gezond doet leven!

Van: [redacted]
Verzonden: woensdag 19 augustus 2020 13:59
Aan: [redacted]@ggdhvb.nl>
Onderwerp: FW: Diverse actiepunten

Hoi [redacted],

Zie bijgevoegd het voorstel van Yource voor wat betreft de salarisverhoging binnen Yource. Ik heb even bij HR en Yource nagevraagd wat de uursalarissen zijn die nu gebruikt worden. En dat is als volgt:

Yource: BCO medewerker [redacted] euro per uur en meewerkend voorman [redacted] euro per uur
GGD: Binnen het team Bron- en Contactonderzoek is iedere (externe) medewerker ingeschaald tussen schaal [redacted] en schaal [redacted]

Dit betekent voor het uurloon het volgende:

- Schaal [redacted] bruto uurloon [redacted] per uur
- Schaal [redacted] bruto uurloon [redacted] per uur

Yource wilde [redacted] euro per uur verhogen. Hoe gaan we hier mee om?

Met vriendelijke groet,

[redacted]

Pettelaarpark 10, Den Bosch
Postbus 3024, 5003 DA Tilburg
www.ggdhvb.nl

[redacted]@ggdhvb.nl
Aanwezig op: ma-di-wo-do
[redacted]

Van: [redacted] | Yource <[redacted]@yource-group.com>
Verzonden: dinsdag 18 augustus 2020 19:08
Aan: [redacted]@ggdhvb.nl>
Onderwerp: Diverse actiepunten

Hi [redacted],

Er stonden een aantal actiepunten open die ik graag met je wil doornemen. Mijn voorstel is om donderdag naar Den Bosch te komen om onderstaande door te nemen, bij voorkeur in de middag. Ik zal dan gelijk [redacted] meenemen, zodat jij alvast kennis kan maken en we kunnen toetsen of de juiste klik er ook met jou is..

1. Ophoging lonen BCO-ers

In de bijlage tref je een voorstel aan voor een addendum bij het contract voor het ophogen van de salarissen. Hierbij is rekening gehouden met een ophoging met [redacted] euro, waarmee we de lonen gelijk zouden trekken aan die van de medewerkers die hetzelfde werk op jullie eigen lokatie doen. Hierbij zijn wij ervan uitgegaan dat wij deze ophoging [redacted] waarbij we alleen een ophoging doen [redacted]. Een verhoging is noodzakelijk, omdat we zien dat het steeds moeilijker wordt om de juiste mensen te vinden en te behouden, vooral de MV's zijn op dit moment zeer moeilijk vindbaar.

2. Ophoging maximale capaciteit na 9-9

Je hebt me gevraagd of het mogelijk is na 9-9 nog meer mensen in te laten stromen, en daarmee de maximale te verwerken capaciteit verder te verhogen. Ik heb ondanks de ontzettende druk op recruitment de komende weken toch nog met hen overlegd. Zij hebben aangegeven toch ruimte te zien en ik kan zelf een aantal andere projecten vertragen, waardoor ik nog [redacted] zou kunnen werven in september. Hiermee zou ik de capaciteit begin oktober kunnen verhogen naar in totaal [redacted] BCO's per dag uitgaande van [redacted] uur werk per BCO. Graag hoor ik van jou of en hoe je hiermee verder wilt.

3. Focus op kwaliteit

Op dit moment zijn we volop bezig om de focus nog meer te verleggen naar kwaliteit. Inmiddels heb ik een ervaren project/operations manager gevonden, die uitbouw van teams en kwaliteitsverbetering in haar DNA heeft. Haar voornaamste opdrachten zullen zijn:

1. De groei van de afdeling binnen de afgesproken kaders realiseren
2. Een kwaliteitssysteem implementeren dat de kwaliteit waarborgt op basis van de reeds bestaande meetmethodes, aangevuld met nieuwe methodes mbt gesprekstechnieken en gewijzigde inzichten in overleg met jullie artsen. Hier wordt op dit moment al de eerste basis voor gelegd door een van onze teamleiders en de mv's.
3. De communicatie tussen de lokaties Den Bossch en Nijmegen blijven waarborgen

Daarnaast zijn we sinds deze week op zoek naar een derde teamleider. Deze moet uiteraard meehelpen de groei van het team onder controle te houden en de dagelijkse operatie aan te sturen.. Maar daarnaast willen we ook iemand aannemen die ervaring heeft met en passie voor kwaliteitsmanagement, Hiermee kunnen we de competenties en kennis in het team vergroten.

Onze laatste uitdaging ligt met name op het gebied van de MV's. [redacted]. We focussen ons nu ook op de werving van deze personen, maar daarbij zullen de punten bij onderdeel 1 helpen.

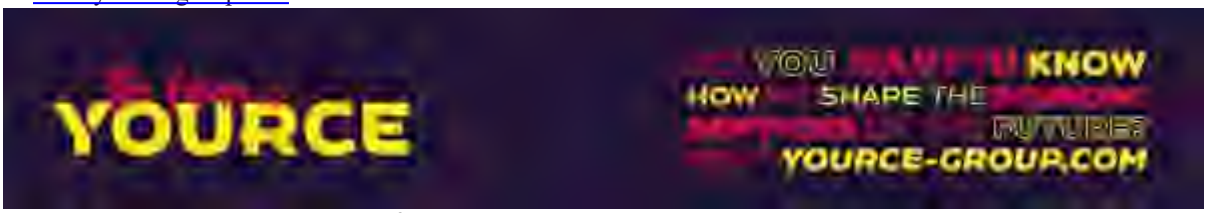
Hierover zal ik morgen ook een mail naar de afdeling sturen, die jij intern kunt gebruken om te delen hoe wij gefocust zijn

op kwaliteit en welke stappen we daarin nemen.

Ik hoor graag van je of je donderdag tijd hebt en hoe laa je zou kunnen.

Truly Yource,

[redacted] | Yource
?? [redacted]@yource-group.com
?? www.yource-group.com



Volg ons op Facebook, Instagram of LinkedIn

13.2
Archived: donderdag 12 mei 2022 09:41:17
From: [redacted]k
Sent: Tue, 16 Nov 2021 08:43:17
To: [redacted]
Subject: FW: Verklaring Togethr B.V. geen SNA certificaat, wel kwalitatief ingericht administratief proces
Importance: Normal
Sensitivity: None
Attachments:
Togethr proces indiensttreding flex v2.pdf; Privacy-verklaring-Togethr-BV-DEF.pdf; Jouw privacy en persoonsgegevens bij Togethr genomen AVG maatregelen .pdf; Gegevens in personeelsdossier - AVG.pdf;

@[redacted]
Hierbij die van TogetHR

Van: [redacted]@ggdwestbrabant.nl>
Verzonden: maandag 15 november 2021 21:11
Aan: [redacted]@hetservicecentrum.nl>
Onderwerp: FW: Verklaring Togethr B.V. geen SNA certificaat, wel kwalitatief ingericht administratief proces

Dag [redacted],

Onderstaande mail ontving ik van Togethr met de vraag deze naar jou als beoordelaar door te zetten (om er zeker van te zijn dat de documenten op de juiste plek komen, ea is ook in Tenderned geupload). Het betreft de onderbouwing hoe Togethr borgt dat het administratief proces kwalitatief is ingericht. Dit als alternatief voor het SNA certificaat.

Groetjes [redacted]

Van: [redacted]@togethr.nl>
Verzonden: maandag 15 november 2021 16:44
Aan: [redacted]@ggdwestbrabant.nl>
Onderwerp: Verklaring Togethr B.V. geen SNA certificaat, wel kwalitatief ingericht administratief proces

Betreft: Verklaring kwalitatief ingericht administratief proces Togethr t.b.v. aanbesteding Externe inhuur GGD West Brabant

Beste mevrouw, mijnheer,

Togethr B.V. is sinds februari 2021 als flexibele partner voor GGD West-Brabant werkzaam in het Covid-19 programma. Wij leveren voornamelijk programma management en specialistische consultancy rollen (denk aan HR en IT consultancy) binnen het programma , veelal in interim constructies. Deze rollen hebben wij voorhanden omdat wij over een groot netwerk met specialisten beschikken. Togethr heeft daarom goed en kritisch gekeken naar de percelen van de aanbesteding en besloten om in te schrijven op perceel 6: Consultants en Projectleiders. Hier ligt de corebusiness van Togethr en verwacht de aanbestedende dienst hierin dan ook te allen tijde adequaat te kunnen faciliteren op korte- en lange termijn.

Wij vinden de match achter de persoon en de GGD essentieel. We matchen uiteraard op hard skills, maar belangrijker nog op

soft/human skills. Daarvoor is meer kennis nodig dan een cv. De mensen die via Togethr aangeboden worden zijn bekend in ons netwerk. We bieden enkel aan, als we weten dat de kandidaat over de juiste kwaliteiten en juiste ervaringen beschikt. Dit zodat we weten dat de juiste mensen aangeboden worden om de klus te doen.

Togethr garandeert dat haar professionals in het bezit zijn van alle benodigde diploma's, aantekeningen, certificaten en verzekeringen om de op door Togethr ingeschreven percelen en daarbij behorende functie in al zijn facetten volgens de wet te kunnen en mogen uitvoeren.

Tevens zullen we gezamenlijk zorgdragen voor onderstaande punten;

1. Kandidaat inzage geven in de geldende procedures, protocollen en beschikbare hulpmiddelen

2. Togethr bouwt een adequaat dossier op met

- een recent cv;
- een geldig VOG (Verklaring Omtrent Goed Gedrag), niet ouder dan twee jaar;
- geldige diploma's en certificaten van opleidingen voor de functieniveaus waarvoor de kandidaat staat ingeschreven en bewijs van adequate nascholing waar vereist;
- een geldig identiteitsbewijs;
- opgebouwd arbeidsverleden en indien van toepassing daarbij behorend opvolgend werkgeverschap.

Specifiek voor ZZP'ers:

- een recent kopie uittreksel van de KvK;
- een ondertekende bemiddelingsovereenkomst met Togethr;
- een door de belastingdienst goedgekeurde passende modelovereenkomst, bij de aard van de werkzaamheden;
- bewijs van een adequate verzekering voor enigerlei schade als uitvloeisel van de werkzaamheden;
- een verklaring waarin de kandidaat verklaart dat er in geval van werkzaamheden GGD, voortvloeiend uit deze overeenkomst van opdracht, nimmer sprake zal zijn van een arbeidsovereenkomst met GGD noch met bemiddelaar en dat kandidaat dit derhalve ook niet beoogd.

3. Togethr verplicht zich om bij elke inzet van medewerker of ZZP'er de GGD een opdrachtbevestiging te sturen per e-mail waarbij de inzet van de opdracht geëffectueerd wordt. Daarbij zal Togethr zorgdragen voor het bijhouden en up to date houden van een adequaat dossier van elke in te zetten medewerker en/ of zelfstandige. Dit dossier is AVG proof.

4. Togethr houdt een urenadministratie voor haar kandidaten bij, die afgetekend worden door GGD.

5. Onze strakke facturatieproces en de goede communicatie met GGD zorgt ervoor dat er afgelopen jaar nog nooit problemen zijn geweest rondom factureren.

Doordat wij aan de achterkant van onze processen en dossiers goed op orde hebben en onze medewerkers en GGD als klant aan de voorkant persoonlijk kennen, kunnen wij er zorg voor dragen dat we snel de juiste kandidaten kunnen aanbieden.

Een SNA keurmerk hebben wij echter niet (dit keurmerk is ook niet gebruikelijk bij bemiddeling van interimmers). Dat wil niet zeggen dat Togethr geen professionele organisatie is. Wij streven naar kwaliteit en AVG proof werken in alles wat wij doen, ook voor onze administratie. Dat doen wij, o.a. door

- Eenduidige processen en werkinstructies (zie voorbeeld instroom proces inleen medewerker);
- Gestandaardiseerde formats (op verzoek aan te leveren;

- Bewaarlocaties van gegevens: afgeschermd met autorisatie in onze systemen (op verzoek verder te specificeren);
- Focus op wettelijke bewaartermijnen en opschoning van (kandidaat) gegevens (bewaartermijnen op verzoek aan te leveren;
- AVG en kwaliteit awareness bij Togethr personeel (presentaties op verzoek te leveren, zie voorbeeldmail aan medewerker i.k.v. avg.);
- AVG audit: Jaarlijks neemt Togethr haar processen onder de loep en verbeteren we evt. constateringen die niet aan AVG richtlijnen voldoen (checklist op te vragen);
- Waarborging van privacy (zie privacy statement);
- Digitaal werken stimuleren onder medewerkers i.p.v. op papier;
- Tijdig aan onze betaalverplichtingen te voldoen (zie document verklaring belastingdienst).

In de bijlagen treft u wat voorbeelden van hoe wij bovenstaande doen. Hiermee verwachten wij te hebben laten zien dat wij onze administratie kwalitatief voeren. Indien nodig kunnen wij onze contactpersoon bij GGD dit laten onderstrepen.

Mochten er vragen zijn, dan beantwoorden wij die graag.

Met vriendelijke groet,

[redacted]

TOGETHR

[redacted]

ADVIES I TRAINING I COACHING

M [redacted]

T [redacted]

Prins Hendrikstraat 97, 4835 PL Breda

www.togethr.nl

13.3
Archived: donderdag 12 mei 2022 09:41:29
From: [redacted]
Sent: Wed, 17 Feb 2021 14:32:46
To: [redacted]
Subject: FW: Yource
Importance: Normal
Sensitivity: None

Met vriendelijke groet,

[redacted]

GGD Hart voor Brabant

Pettelaarpark 10, Den Bosch
Postbus 3024, 5003 DA Tilburg
www.ggdhvb.nl

[redacted]@ggdhvb.nl
Aanwezig op: ma-di-wo-do
[redacted]

Gezond doet leven!

Van: [redacted]@hetservicecentrum.nl>
Verzonden: dinsdag 27 oktober 2020 15:03
Aan: [redacted]@ggdhvb.nl>
CC: [redacted]@ggdhvb.nl>
Onderwerp: RE: Yource

Hoi [redacted],

Toevallig is vandaag het advies van de jurist binnen gekomen. Hierin staat het volgende;
Het uitvoeren van bron- en contactonderzoek is door de GGD aan het begin van de corona uitbraak met een spoedprocedure gegund aan een partij. Er is geen juridische discussie dat dit de juiste procedure was. Het contract loopt tot het einde van het jaar met de mogelijkheid tot verlenging van 3 maanden. Zoals hiervoor is aangegeven moet zo snel mogelijk een versnellingsprocedure of een normale procedure worden gestart. Er kan juridisch discussie worden gevoerd over de looptijd van de reeds gegunde overeenkomst. Deze COVID-19 situatie is echter dusdanig uitzonderlijk dat hier geen jurisprudentie over te vinden is. De overeenkomst kan pas na 31-12-2020 worden beëindigd. Op dit moment is er geen reden de overeenkomst eerder te beëindigen. Nederland zit midden in een tweede golf, het op dit moment met de stijgende drukte inwerken van nieuwe mensen is niet wenselijk. Na het verkoudheidsseizoen zal de GGD hopelijk meer tijd hebben om mensen in te werken en om een aanbestedingsprocedure te starten voor bron- en contactonderzoeken. Het overdragen van de bestaande kennis bij de huidige contractpartij is gezien de drukte niet wenselijk aangezien het de kwaliteit van de uit te voeren bron- en contractonderzoeken niet ten goede komt en vertragend zal werken. Dit zou betekenen dat gezien de huidige vraag de GGD niet meer kan voldoen aan haar verplichtingen, namelijk het op een kwalitatief goede en snelle manier uitvoeren van bron- en contactonderzoeken.
Als de situatie zo blijft en de druk op de GGD'en zo hoog blijft is het zeer waarschijnlijk pas na het verkoudheidsseizoen mogelijk is de dienstverlening over te dragen. Dit vanwege de hiervoor genoemde redenen. Er kan in dat geval beargumenteerd worden dat het is dus te rechtvaardigen is dat GGD Hart voor Brabant het gehele contract, incl. de drie opties tot verlenging met één maand, uitdient. Hierna dient de balans opnieuw opgemaakt te worden en dient er gekeken te worden naar een passende oplossing. Deze afweging zal eind december gemaakt moeten worden.

Ik heb [redacted] gevraagd of hij mij het definitieve standpunt inzake de verlenging kan doorgeven. Ik begreep namelijk dat dit advies nog door het MT moet. Als ze het advies van de jurist volgen kunnen we dus in ieder geval voor 3 maanden verlengen. Ik ga morgen de brief alvast opmaken, dan hoeft er alleen nog maar een handtekening van [redacted] onder. Ik zorg

er voor dat we er gas op blijven houden.
Ik houd je op de hoogte!

Met vriendelijke groet,

[redacted]

[redacted]

T: [redacted]
E: [redacted]@hetservicecentrum.nl

Hét Service Centrum: *het shared service center van GGD Hart voor Brabant, GGD West-Brabant, GGD Noord-en Oost Gelderland en de Regionale Ambulancevoorziening Brabant-Midden-West-Noord.*

Werkzaam op maandag, dinsdag, donderdag en vrijdagochtend.

Van: [redacted]@ggdhvb.nl>
Verzonden: dinsdag 27 oktober 2020 13:51
Aan: [redacted]@hetservicecentrum.nl>
Onderwerp: RE: Yource

Hoi [redacted],

IK ben benieuwd hoe het met de verlenging staat. We hebben wel tijd, maar ik denk dat we geen risico moeten nemen om Yource kwijt te raken, door het heel lang te laten liggen.

Wat is de mening van de jurist?

Met vriendelijke groet,

[redacted]

Pettelaarpark 10, 5216 PD 's-Hertogenbosch
www.ggdhvb.nl

[redacted]@ggdhvb.nl
Aanwezig op: ma-di-do-vrij

Van: [redacted]
Verzonden: maandag 19 oktober 2020 13:05
Aan: [redacted]
Onderwerp: RE: Yource

Hoi [redacted], 13.3

Klopt ik was al op de hoogte inderdaad, maar wilde weten of verder iets hierin voor jullie kon betekenen nog.

Groetjes
[redacted]

Van: [redacted]@ggdhvb.nl>
Verzonden: maandag 19 oktober 2020 12:56
Aan: [redacted]@ggdhvb.nl>; [redacted]@hetservicecentrum.nl>
Onderwerp: Re: Yource

Hoi [redacted],

Mooi,. Ik heb nu geen andere info dan dat we opschalen met aantal en baseline. En daar was je van op de hoogte toch?

Groet

[redacted]

Outlook for Android downloaden

From: [redacted]@hetservicecentrum.nl>
Sent: Monday, October 19, 2020 10:42:45 AM
To: [redacted]@ggdhvb.nl>; [redacted]@ggdhvb.nl>
Subject: Yource

Hallo [redacted] en [redacted],

Ik werd net gebeld door iemand van programma Corona en ik begreep dat [redacted] lekker van zijn herfstvakantie geniet, dus dat mijn mail niet beantwoord wordt.
Ik heb hem gevraagd of wij namens Inkoop nog iets kunnen betekenen inzake de opschaling met Yource. Worden er nieuwe tarieven afgesproken bijvoorbeeld?
Ik hoor het graag als ik daar voor jullie nog een rol in kan spelen.

De definitieve versie van het advies van de jurist is helaas nog niet binnen. Zodra dit akkoord is bevonden door het MT zal ik de verlengingsbrief voor Yource opstellen.
Uiterlijke verlenging is pas 1-12, dus nog tijd genoeg.

Bedankt!

Met vriendelijke groet,

[redacted]

[redacted]

T: [redacted]
E: [redacted]@hetservicecentrum.nl

13.3

Hét Service Centrum: *het shared service center van GGD Hart voor Brabant, GGD West-Brabant, GGD Noord-en Oost Gelderland en de Regionale Ambulancevoorziening Brabant-Midden-West-Noord.*

Werkzaam op maandag, dinsdag, donderdag en vrijdagochtend.

Hart voor Brabant

PERSONEELSREGISTRATIEFORMULIER en

INTEGRITEITS-EN GEHEIMHOUDINGSVERKLARING

EN OVEREENKOMST BESCHIKKING GESTELDE BEDRIJFSAPPARATUUR

INHUUR – GGD HART VOOR BRABANT

WELKOM BIJ GGD HART VOOR BRABANT!

Bij GGD Hart voor Brabant ('GGD') doe je belangrijk werk. Je draagt bij aan de bevordering, bescherming en bewaking van de gezondheid van alle inwoners van ons werkgebied.

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 dat je bewust bent van het feit welke verantwoordelijkheden dit met zich meedraagt.

Daarom vragen we jou om de '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.

Je vult daarnaast het personeelsregistratieformulier in met jouw gegevens en ondertekent dit formulier. Deze gegevens worden ingevoerd in het personeelsregistratiesysteem.

Tot slot lees je de overeenkomst gebruik ter beschikking gestelde bedrijfsapparatuur aandachtig door, ook dit formulier onderteken je.

Zo draag ook jij bij aan een goede bescherming en beveiliging van de gezondheidsgegevens van alle inwoners van Hart voor Brabant!

Veel succes en hartelijke groet,
namens het dagelijks bestuur,

[redacted]
Directeur

Hart voor Brabant

PERSONEELSREGISTRATIEFORMULIER

PERSONALIA

Achternaam (zoals in paspoort/id): Klik of tik om tekst in te voeren.

Achternaam (zoals je wenst te gebruiken): Klik of tik om tekst in te voeren.

Roepnaam: Klik of tik om tekst in te voeren. Voorletters: Klik of tik om tekst in te voeren.

Adres: Klik of tik om tekst in te voeren. Postcode: Klik of tik om tekst in te voeren.

Woonplaats: Klik of tik om tekst in te voeren.

Geboortedatum: Klik of tik om tekst in te voeren. Geslacht: M / V

Geboorteplaats: Klik of tik om tekst in te voeren.

Telefoonnummer (mobiel): Klik of tik om tekst in te voeren.

E-mail: Klik of tik om tekst in te voeren.

Contactpersoon in noodgevallen: Klik of tik om tekst in te voeren.

Telefoonnummer contactpersoon: Klik of tik om tekst in te voeren.

BIG-registratienummer (mits van toepassing): Klik of tik om tekst in te voeren.

Vervaldatum BIG-registratienummer: Klik of tik om tekst in te voeren.

AANSTELLINGSGEGEVENS:

In dienst per: Klik of tik om tekst in te voeren.

Team: Klik of tik om tekst in te voeren.

Functie: Klik of tik om tekst in te voeren.

Aantal uren per week: Klik of tik om tekst in te voeren.

Hierbij verklaar ik het formulier naar waarheid en zonder voorbehoud te hebben ingevuld.

☐ *Ik ga akkoord dat mijn adresgegevens worden verwerkt voor mogelijke persoonlijke attenties.*

Datum	Plaats	Handtekening
Klik of tik om tekst in te voeren.	Klik of tik om tekst in te voeren.	

Hart voor Brabant

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.

Hart voor Brabant

INTEGRITEITS-EN GEHEIMHOUDINGSVERKLARING GGD HART VOOR BRABANT

Achternaam, voornaam en voorletters: Klik of tik om tekst in te voeren.

Geboortedatum: Klik of tik om tekst in te voeren.

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 en/of ik uit dienst ben bij de GGD.
- Ik ben mij ervan bewust dat ik voor de uitoefening van mijn werkzaamheden toegang heb tot vertrouwelijke en zeer gevoelige informatie waaronder medische 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, cliënten, patiënten of derden), interne uitspraken van het management, discussies of verschillen van mening.

Hart voor Brabant

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.
- Ik houd mij aan de geldende regels voor internet en e-mail gebruik en de huisregels van het organisatieonderdeel.
- 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 bewaar vertrouwelijke gegevens niet in mijn persoonlijk bezit.
- Ik verstrek mijn persoonlijke inlogaccount niet aan derden.
- 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.

Hart voor Brabant

4. Verklaring Omtrent het Gedrag

Ik ga ermee akkoord dat ik alleen werkzaamheden zal verrichten bij GGD Hart voor Brabant wanneer ik in het bezit ben van een Verklaring Omtrent het Gedrag. Deze Verklaring Omtrent het Gedrag is niet ouder dan 1 jaar en is gescreend op profiel 45 (Gezondheidszorg en welzijn van mens en dier). Tevens ga ik ermee akkoord dat mijn werkgever een kopie van de Verklaring Omtrent het Gedrag overhandigt aan GGD Hart voor Brabant.

5. 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.

5. OVEREENKOMST GEBRUIK TER BESCHIKKING GESTELDE BEDRIJFSAPPARATUUR

- Zie bijlage 'Overeenkomst gebruik ter beschikking gestelde bedrijfsapparatuur'.

Ik verklaar verder in kennis te zijn gesteld van de inhoud van dit formulier en bijlage 'Overeenkomst gebruik ter beschikking gestelde bedrijfsapparatuur':

- mij te zullen houden aan alle in dit formulier genoemde 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
Klik of tik om tekst in te voeren.	Klik of tik om tekst in te voeren.	
.....	.....	.....

(*maak van dit formulier voor jezelf een kopie)*

Hart voor Brabant

De GGD Hart voor Brabant (verder te noemen "De werkgever") stelt aan haar medewerker bedrijfsapparatuur inclusief toebehoren in bruikleen ter beschikking:

de heer/mevrouw : Klik of tik om tekst in te voeren.
(verder te noemen "De medewerker")
Geboortedatum : Klik of tik om tekst in te voeren.

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 van bedrijfseigendommen
   - "De medewerker" wordt geacht de e-mail (aangeboden door "De werkgever") voor zakelijke doeleinden te gebruiken.
   - Indien "De werkgever" "De medewerker" een computer, laptop, mobiele telefoon of andere apparatuur ter beschikking heeft gesteld, wordt "De medewerker" geacht deze voornamelijk te gebruiken voor zakelijke doeleinden. Afspraken hierover worden vastgelegd in een 'gebruikersovereenkomst'. Incidenteel en beperkt gebruik voor persoonlijke doeleinden van deze elektronische communicatiemiddelen is toegestaan. Hierbij dienen wel de regels van zorgvuldigheid, redelijkheid, integriteit en goede naam in acht te worden genomen.
   - Ter beschikking gestelde apparatuur blijft ten allen tijde eigendom van "De werkgever".
   - "De medewerker" verplicht zich om na afloop van het dienstverband alle ter beschikking gestelde apparatuur in goede staat bij "De werkgever" in te leveren.
   - "De medewerker" wordt geacht als een goed huisvader om te gaan met ter beschikking gestelde apparatuur.
   - Kosten voor vervanging of reparatie van ter beschikking gestelde apparatuur komen voor rekening van de GGD Hart voor Brabant. In het geval kosten voor vervanging of reparatie veroorzaakt door nalatigheid van "De medewerker", worden deze kosten verhaald op "De medewerker".

- Tussentijds te vervangen apparatuur wordt vervangen door eenzelfde of gelijkwaardige apparatuur, ook indien deze kosten voor rekening van "De medewerker" komen.
- Medewerkers van GGD Hart voor Brabant gaan veel om met vertrouwelijke gegevens. Het is niet toegestaan om zonder toestemming van "De werkgever", computerprogrammatuur of andere auteursrechtelijk beschermde werken te kopiëren en/of te vermenigvuldigen.
- Indien afspraken uit de gebruikersovereenkomst niet nagekomen worden, is "De werkgever" bevoegd een geschil betreffende de teruggave van de apparatuur aan het oordeel van de President van de arrondissementsrechtbank te 's-Hertogenbosch of Tilburg (rechtsprekende in kort geding) te onderwerpen.

4. 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".

5. 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.

6. 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".

Hart voor Brabant

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.

7. 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"

8. 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 Servicecentrum.
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 plaatsvinden1;
- 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: __ / __ / ____

Welkom bij de GGD Hart voor Brabant!

Bij de GGD Hart voor Brabant (‘GGD’) doe je belangrijk werk. Je draagt bij aan de bevordering, bescherming en bewaking van de gezondheid van alle inwoners van Hart voor 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 Hart voor Brabant!

Veel succes en hartelijke groet,

MT Hart voor Brabant

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 Hart voor 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. Deze geheimhouding blijft ook van kracht nadat ik uit dienst ben bij de GGD.
- 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. 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.
- Ik houd mij aan de geldende regels voor internet en e-mail gebruik en de huisregels van het organisatieonderdeel.
- 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).

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, 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.

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;
- 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, 272en 273(snelkoppelingen te vinden op internet);
- dat ik de betekenis en het belang van die bepalingen heb begrepen.

Ondertekening medewerker

Datum	**Plaats**	**Handtekening**
.....	.....	.....

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:
geen documenten aanwezig.

Wob-verzoek SOLV/ICAM datalek 2021 coronasysteem

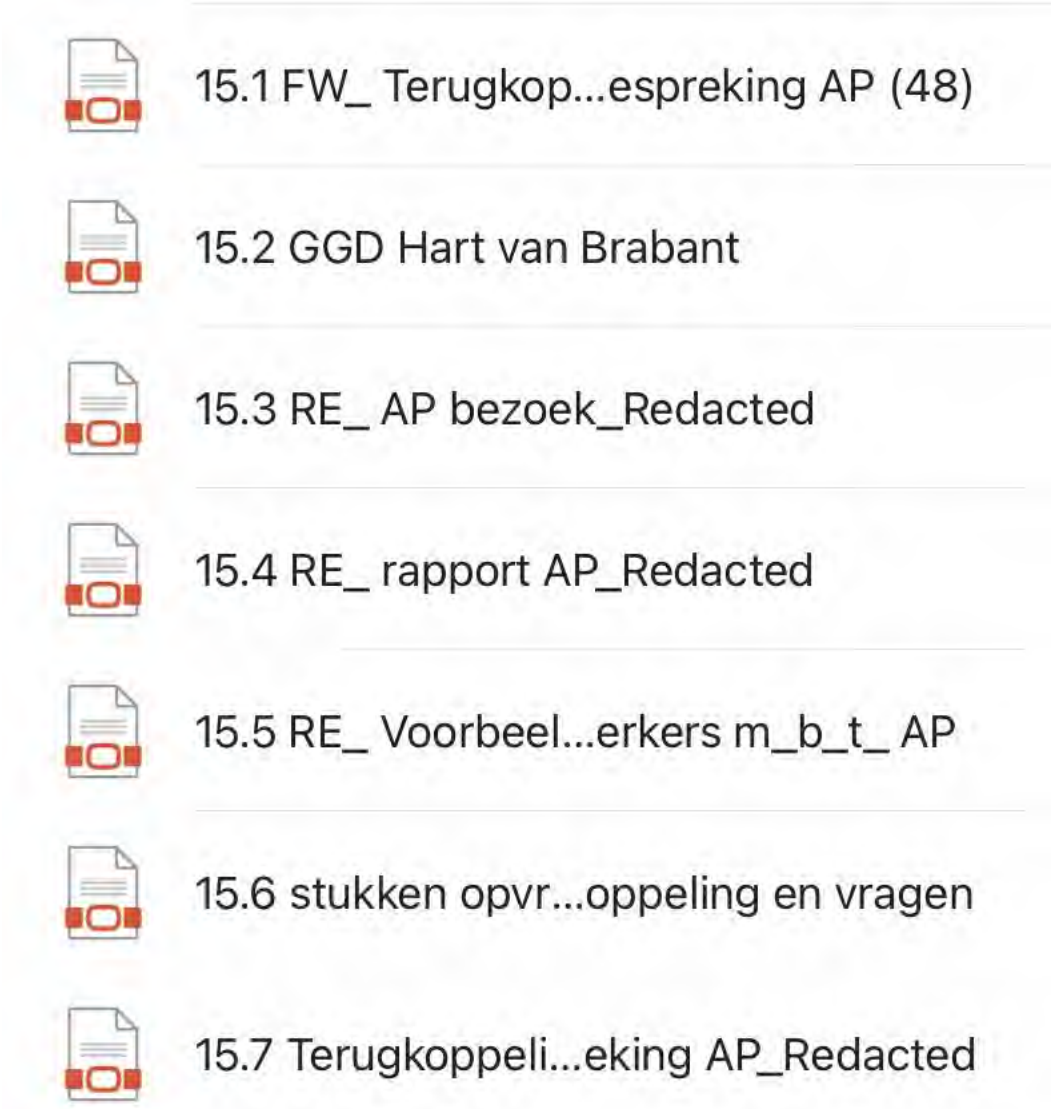
15.0 Tekst Wob-verzoek en register documenten

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:



15.1
Archived: donderdag 12 mei 2022 09:44:26
From: [redacted]
Sent: zondag 7 maart 2021 21:19:59
To: [redacted]
Subject: FW: Terugkoppeling en vragen bespreking AP
Importance: Normal
Sensitivity: None
Attachments:
Overzicht verstrekte stukken AP.xlsx;

Op uitdrukkelijk verzoek van 10 DPG'en hebben we inzicht gekregen in de documenten die de GGD GHOR gedeeld heeft met de AP (zie bijlage).

Hartelijke groet,

[redacted]

Van: [redacted]@ggdghor.nl>
Verzonden: vrijdag 5 maart 2021 12:23
Aan: [redacted]@ggdbzo.nl>
CC: [redacted]@ggdhaaglanden.nl>; [redacted]@vggm.nl>; [redacted]@ggdhn.nl) [redacted]ggdhn.nl>; [redacted]@ggdzl.nl>; [redacted]@ggdzeeland.nl>; [redacted]@ggdgelderlandzuid.nl>; [redacted]@ggdijsselland.nl>; [redacted]@ggdgooi.nl>; [redacted]@ggdwestbrabant.nl>; [redacted]@ggdhvb.nl>; [redacted]@ggdnog.nl>; [redacted]@ggdghor.nl>; [redacted]@ggdghor.nl>
Onderwerp: RE: Terugkoppeling en vragen bespreking AP

Hi [redacted] e.a.,

Dank voor jullie mail.

Ik reageer op jullie verzoek om het delen van documenten die verstrekt zijn aan de AP.

[redacted] werkt aan informatie over contacten/convenanten en besluiten o.a. aangaande HPzone; dat vergt iets meer tijd.

Bijgevoegd vinden jullie de lijst met documenten die we aan de AP verstrekt hebben.

Daarbij dient opgemerkt te worden, dat deze lijst dagelijks groeit want de AP vraagt continu aanvullende documenten bij ons op.

Dat brengt me meteen ook bij een praktisch vraagstuk want al deze documenten overleggen, [redacted]

Daarom is mijn vraag of het met enige regelmaat verstrekken van dit (bijgewerkte) overzicht, toereikend is om in jullie vraag te voorzien?

Mogelijk daarnaast aangevuld met documenten die GGD'en aan de AP overleggen.

Immers zouden we dan bij vragen van de AP kunnen antwoorden dat het document al aan hen verstrekt is.

Zo besparen we elkaar een hoop werk én weet iedereen welke informatie de AP tot haar beschikking heeft.

Aanvullend kunnen we natuurlijk altijd specifieke documenten aan (een deel van) jullie overhandigen, mocht daar behoefte aan zijn.

Ik hoor graag of bovenstaande werkwijze een weg te gaan is, waarbij ik me realiseer dat het verstrekken van dit overzicht slechts een onderdeel is van elkaar inzage geven in het traject AP en dat we ook informatie over de interviews en overige correspondentie met de AP als GGD GHOR beter met jullie dienen uit te wisselen. Daarbij zoek ik nog naar de juiste vorm (wekelijkse nieuwsbrief, mondeling,….). Suggesties van jullie kant hierover zijn zeer welkom.

Hoop jullie hiermee voldoende geïnformeerd te hebben!

Met vriendelijke groet,

[redacted]

Zwarte Woud 2
3524 SJ Utrecht
Telefoon: [redacted]
Mobiel: [redacted]

E-mail : [redacted]@ggdghor.nl
Website : www.ggdghor.nl
Twitter : @ggdnederland en @ghornederland
Afwezig : -

Van: [redacted]@GGDBZO.nl>
Verzonden: donderdag 4 maart 2021 16:42
Aan: [redacted]@ggdghor.nl>; [redacted]@ggdghor.nl>; [redacted]@ggdghor.nl>
CC: [redacted]@ggdhaaglanden.nl>; [redacted]@vggm.nl>; [redacted]@ggdhn.nl) [redacted]@ggdhn.nl>; [redacted]@ggdzl.nl>; [redacted]@ggdzeeland.nl>; [redacted]@ggdgelderlandzuid.nl>; [redacted]@ggdijsselland.nl>; [redacted]@ggdgooi.nl>; [redacted]@ggdwestbrabant.nl>; [redacted]@ggdhvb.nl>; [redacted]@ggdnog.nl>
Onderwerp: Terugkoppeling en vragen bespreking AP

Dag,

Gisteravond hebben we zoals jullie weten een gesprek gehad met elkaar over de ervaringen van [redacted] en onze ervaringen met onze juristen. Om mezelf als voorbeeld te nemen: de jurist die ik heb ingehuurd vraagt om heel veel documenten waar ook om [redacted] heeft gevraagd, namelijk de 60 documenten die GGDGHOR heeft aangeleverd. Wij ontvangen allemaal graag deze documenten . Want in feite zijn ze "van ons". Ook willen we graag een overzicht van wanneer we besluiten hebben genomen over HP zone light, evenals de getekende contracten van het afgelopen jaar. We hebben "velletjes" getekend maar geen complete overeenkomsten terug gekregen van alles wat er getekend is.

Kan dat en wanneer kunnen we dat ontvangen.

Wij horen graag!

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 Hart van Brabant
t.a.v. Directeur Publieke Gezondheid
Postbus 3024
5003 DA Tilburg

Datum
8 november 2021

Ons kenmerk
z2021-16812

Contactpersoon
[redacted]

Onderwerp
Eindbrief AP inzake onderzoek beveiliging persoonsgegevens GGD GHOR en GGD'en

Geachte directeur,

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
8 november 2021

Ons kenmerk
z2021-16512

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]

ir. M.J. Verdier
Vicevoorzitter

Bijlage – Eindbrief onderzoek beveiliging persoonsgegevens GGD GHOR en GGD'en

15.3
Archived: donderdag 12 mei 2022 09:42:45
From: [redacted]
Sent: vrijdag 27 augustus 2021 10:40:04
To: [redacted]
Subject: RE: AP bezoek
Importance: Normal
Sensitivity: None

Zojuist heb ik terugkoppeling gehad in de DPG-raad over de resultaten van het AP-onderzoek: geen handhaving, geen boete, wel een lijstje van dingen die we moeten gaan doen (of al hebben gedaan). Advocaten van GGD GHOR NL en 2 bezochte GGD'en gaan reactie voorbereiden. Dit komt volgende week terug via de DPG-raad.

Van: [redacted]@ggdhvb.nl>
Verzonden: dinsdag 24 augustus 2021 17:14
Aan: [redacted]@ggdhvb.nl>; [redacted]@ggdhvb.nl>; [redacted]@ggdhvb.nl>; [redacted]@ggdhvb.nl>; [redacted]@ggdhvb.nl>; [redacted]@ggdhvb.nl>; [redacted]@ggdhvb.nl>; [redacted]@ggdhvb.nl>; [redacted]@ggdhvb.nl>; [redacted]@ggdhvb.nl>; [redacted]@hetservicecentrum.nl>; [redacted]@ggdhvb.nl>
CC: [redacted]@ggdwestbrabant.nl>; [redacted]@ggdhvb.nl>; [redacted]@ggdhvb.nl>; [redacted]@akd.nl>
Onderwerp: AP bezoek

Beste allen,

Via [redacted] vernam ik dat de AP te kennen heeft gegeven dat zij de onderzoeken naar de datadiefstal heeft afgerond en haar bevindingen met ons wil delen. Dit zal vandaag plaatsvinden waarna wij een terugkoppeling ontvangen van dit gesprek. Het lijkt erop dat we geen ebzoek meer krijgen van de AP.

Wel zullen er naar alle warschijnlijkheid vervolgacties uit naar voren komen. Mijn voorstel is om voor zover van toepassing deze vervolgacties mede op te nemen in het KPMG odnerzoek (security scan en applicatie scan en classificatie)

Groet,

[redacted]

15.4
Archived: donderdag 12 mei 2022 09:43:24
From:
Sent: donderdag 25 november 2021 10:44:19
To: [redacted]
Subject: RE: rapport AP
Importance: Normal
Sensitivity: None

Dag allen,

ik neem jullie teksten mee in de DB-mededelingen, met enige redactie.

Groeten,

[redacted]

GGD Hart voor Brabant
Postbus 3024, 5003 DA Tilburg
www.ggdhvb.nl
[redacted]@ggdhvb.nl
[redacted]
Gezond doet leven!

Van: [redacted]@ggdhvb.nl>
Verzonden: donderdag 25 november 2021 09:19
Aan: [redacted]@ggdhvb.nl>; [redacted]@ggdhvb.nl>
CC: [redacted]@ggdhvb.nl>
Onderwerp: RE: rapport AP

Dag [redacted], een kleine verduidelijkende aanvulling.

Van: [redacted]@ggdhvb.nl>
Verzonden: woensdag 24 november 2021 08:12
Aan: [redacted]@ggdhvb.nl>; [redacted]@ggdhvb.nl>
CC: [redacted]@ggdhvb.nl>
Onderwerp: RE: rapport AP

Goedemorgen [redacted] en [redacted]

Zie onderstaande vraag van [redacted] Ik heb de rood gearceerde tekst toegevoegd. Willen jullie aub aanvullen.

Gr [redacted]

Van: [redacted]@ggdhvb.nl>
Verzonden: donderdag 18 november 2021 08:28
Aan: [redacted]@ggdhvb.nl>
Onderwerp: rapport AP

Dag [redacted];4

In de volgende DB-vergadering doen we een mededeling over het AP-rapport over de datalekken bij de GGD, zie de concept tekst hieronder.

Nu moeten er nog een paar zinnen bij over onze eigen acties of ons commentaar, misschien wel geknipt en geplakt uit eerdere teksten.

Kun jij daarvoor zorgen?

Omschrijving 1. **Rapport onderzoek datalekken**

[redacted] heeft onderzoek naar datadiefstal gedaan bij GGD GHOR Nederland en twee GGD'en (niet de onze). Haar conclusie: er zij verbetermaatregelen waardoor het risico op datalekken is verminderd. Maar de [redacted] ziet nog wezenlijke risico's voor de beveiliging van persoonsgegevens: er zijn geen duidelijke afspraken tussen organisaties over bepaalde beveiligingsaspecten, bijvoorbeeld rond het autorisatiebeheer en de controle van logbestanden. Verder leidt het vervangen van een systeem niet zonder meer tot een betere beveiliging. Uiterlijk

1 maart 2022 moeten GGD GHOR Nederland en de betrokken GGD'en aan de [redacted] een voortgangsrapportage opleveren van de genomen en te nemen maatregelen ter beveiliging van de persoonsgegevens.

De GGD Hart voor Brabant heeft direct na de datadiefstal nogmaals een check uitgevoerd op de VOG verklaringen, de autorisaties nagelopen, autorisatiematrix opgesteld en controles op correct gebruik van systemen uitgevoerd. Tevens is de GGD Hart voor Brabant voornemens aan de NEN norm "informatiebeveiliging in de zorg" (7510/12/13) te gaan voldoen. Hiervoor is inmiddels een traject met KPMG opgestart.

Groeten,

[redacted]

GGD Hart voor Brabant

Postbus 3024, 5003 DA Tilburg

www.ggdhvb.nl

[redacted]@ggdhvb.nl

[redacted]

Gezond? doet leven!

15.5
Archived: donderdag 12 mei 2022 09:43:31
From: [redacted]
Sent: maandag 8 februari 2021 19:13:47
To: [redacted]
Subject: RE: Voorbeeld tekst medewerkers m.b.t. AP
Importance: Normal
Sensitivity: None
Attachments:
20210205 Verbeterplan gegevensbescherming vs2.pptx; 20210208 Actielijst verbeterplan gegevensbescherming en datadiefstal.xlsx;

Dag [redacted] en [redacted], hierbij in vertrouwen het verbeterplan en bijbehorende actielijst. Niet voor verdere verspreiding, want work in progress. Hiermee zijn jullie op vlieghoogte van wat er allemaal wordt ondernomen aan verbeteringen en gevolgbeheersing. Dat kan jullie wellicht helpen om bij de interne communicatie beter te kunnen duiden wat we allemaal aan het doen zijn. Het zijn veel zaken die we oppakken en in de communicatie zou ik ons echt tot de hoofdlijnen willen beperken. Overigens lees ik onder het kopje “wat doen wij?” in het voorbeeld-mailtje van GGD GHOR Nederland alleen procesinformatie over het onderzoek van de AP. Dat is dus veel smaller bedoeld dan alle acties die wij nu oppakken.

Tot slot, in antwoord op de vraag van [redacted]: er is nog geen afspraak met AP gepland en het is ook niet duidelijk of ze meteen alle GGD’en langsgaan of een steekproef en of wij daar dan meteen bij zitten. We hebben überhaupt nog geen formeel schrijven ontvangen. Dat moet eerst, voordat we intern kunnen communiceren.

Fijne avond

Van: [redacted]@ggdhvb.nl>
Verzonden: maandag 8 februari 2021 17:16
Aan: [redacted]@ggdhvb.nl>; [redacted]@ggdhvb.nl>; [redacted]@ggdhvb.nl>; [redacted]@ggdhvb.nl>; [redacted]@ggdhvb.nl>; [redacted]@ggdhvb.nl>; [redacted]@ggdhvb.nl>
Onderwerp: RE: Voorbeeld tekst medewerkers m.b.t. AP

Hallo allen,

Graag ontvangen wij het “verbeterplan gegevensbescherming & gevolgbestrijding datadiefstal” zoals dat vandaag besproken wordt in het MT.

Dan kunnen wij op basis daarvan een bericht schrijven voor medewerkers. Ik stel voor om dit bericht ondertekend door [redacted] per mail te verspreiden onder alle medewerkers.

Groet,

[redacted]

Van: [redacted]@ggdhvb.nl>

Verzonden: maandag 8 februari 2021 09:36
Aan: [redacted]@ggdhvb.nl>; [redacted]@ggdhvb.nl>; [redacted]@ggdhvb.nl>; [redacted]@ggdhvb.nl>; [redacted]@ggdhvb.nl>; [redacted]@ggdhvb.nl>; [redacted]@ggdhvb.nl>
Onderwerp: RE: Voorbeeld tekst medewerkers m.b.t. AP

Dank,

[redacted] en ik stemmen af.

Ik zit nog twee dagen in Utrecht en dan weer fijn 'thuis' bij [redacted] en jullie allen. Vanaf donderdag weer helemaal up to date en vol voor HvB.

Groet,

[redacted]

[redacted]

GGD Hart voor Brabant

Pettelaarpark 10

's-Hertogenbosch

Postbus 3024
5003 DA Tilburg

www.ggdhvb.nl

[redacted]@ggdhvb.nl

Afwezig op woensdag

Gezond doet leven!

Van: [redacted]@ggdhvb.nl>
Verzonden: maandag 8 februari 2021 09:13
Aan: [redacted]@ggdhvb.nl>; [redacted]@ggdhvb.nl>; [redacted]@ggdhvb.nl>; [redacted]@ggdhvb.nl>; [redacted]@ggdhvb.nl>; [redacted]@ggdhvb.nl>; [redacted]@ggdhvb.nl>
Onderwerp: RE: Voorbeeld tekst medewerkers m.b.t. AP

Dag [redacted],

We doen heel veel actief rond de datadiefstal en ook [redacted] is daar nauw bij betrokken, evenals [redacted] Alle acties zijn door [redacted], [redacted] en mij samengebracht in het "verbeterplan gegevensbescherming & gevolgbestrijding datadiefstal" dat vanmiddag wordt besproken in het MT. Na het MT kan dit als input dienen voor communicatie. Overigens geeft de AB-brief van vrijdag ook al input.

Groeten,

[redacted]

Van: [redacted]@ggdhvb.nl>
Verzonden: zondag 7 februari 2021 21:27
Aan: [redacted]@ggdhvb.nl>; [redacted]@ggdhvb.nl>; [redacted]@ggdhvb.nl>; [redacted]@ggdhvb.nl>; [redacted]@ggdhvb.nl>; [redacted]@ggdhvb.nl>

Onderwerp: RE: Voorbeeld tekst medewerkers m.b.t. AP

[redacted],

- Is er al een concrete afspraak voor GGD HvB met AP?
- En wat doen we zelf actief rondom de datadiefstal?
- Wie weet dat (waar kunnen we de info ophalen)?
- Ik zou ook de taak van [redacted] nogmaals onder de aandacht brengen.

Dat zijn belangrijke punten om het bericht persoonlijker te maken en meer gericht op HvB.

Als we dat weten, dan kunnen we daar zo een bericht van maken.

Voorstel: mail aan alle medewerkers namens jou.

Het raakt iedereen.

Groet,

[redacted]

[redacted]

GGD Hart voor Brabant

Pettelaarpark 10

's-Hertogenbosch

Postbus 3024
5003 DA Tilburg

www.ggdhvb.nl

[redacted]@ggdhvb.nl

Afwezig op woensdag

Gezond doet leven!

Van: [redacted]@ggdhvb.nl>
Verzonden: zondag 7 februari 2021 18:31
Aan: [redacted]@ggdhvb.nl>; [redacted]@ggdhvb.nl>; [redacted]@ggdhvb.nl>; [redacted]@ggdhvb.nl>; [redacted]@ggdhvb.nl>; [redacted]@ggdhvb.nl>
Onderwerp: FW: Voorbeeld tekst medewerkers m.b.t. AP

Denken jullie even mee wat het juiste moment is om dit (of ons eigen) bericht intern te delen over het onderzoek van de AP?

Hartelijke groet,

[redacted]

Van: [redacted]@ggdghor.nl>
Verzonden: vrijdag 5 februari 2021 21:32
Aan: Directie GGD GHOR Nederland <directie@ggdghor.nl>
Onderwerp: Voorbeeld tekst medewerkers m.b.t. AP

Beste DPG'en,

Onderstaand ter inspiratie de mail die wij zelf hebben gestuurd aan alle medewerkers bij GGD GHOR Nederland, zoals zojuist afgesproken in het DPG-overleg.

Met vriendelijke groet,

[redacted]

Na alle berichtgeving over de datadiefstal vorige week, heeft de Autoriteit Persoonsgegevens (AP) aangegeven bij ons langs te komen. In de mail lees je hier meer over.

Maar eerst willen we zeggen dat we jullie inzet enorm waarderen. Met hart en ziel hebben jullie je steeds ingezet op tal van terreinen, zowel voor corona als voor alle andere activiteiten. Onze waardering voor al je inspanning staat sowieso als een paal boven water.

Wat is er aan de hand?

Naar aanleiding van de berichtgeving in de Media, maakt de AP zich zorgen over de beveiliging van het grote aantal persoonsgegevens van mensen waarover wij nu beschikken. De AP gaat nu intensiever kijken of GGD GHOR Nederland en/of de GGD'en vanaf 12 maart 2020 tot nu, heeft gewerkt conform de AVG wet- en regelgeving.

Wat merk jij hiervan?

Vrijdag 5 februari is de AP op het kantoor van GGD GHOR Nederland aanwezig zijn. Zij zullen documentatie opvragen en interviews afnemen met van te voren aangewezen en geïnformeerde personen, die informatie kunnen verschaffen over de relevante systemen en de maatregelen die wij hebben genomen en zullen nemen om de gegevens zo veilig mogelijk te verwerken. Na vrijdag verwachten wij dat de AP blijft meekijken naar hoe wij omgaan met de gegevens. Het kan zijn dat de AP hiervoor eerst een afspraak met ons inplant, maar ook kunnen zij onaangekondigd contact met ons opnemen. Belangrijk is ook om te weten dat het de AP te doen is om onze organisatie en niet om personen zoals de mensen die geïnterviewd worden.

Wat doen wij?

Wij werken uiteraard mee met het onderzoek van de AP. Wij vinden het ook belangrijk dat wij steeds veilig met de gegevens omgaan. En wij staan voor de volle 100% achter onze mensen en ondersteunen waar nodig en mogelijk. Wij hebben juristen aangetrokken die de mensen die geïnterviewd worden ondersteunen, door bijvoorbeeld toe te lichten hoe zo'n interview gaat. Ook kunnen zij helpen met het voorbereiden op zo'n interview.

Tot slot

Velen van jullie zullen gebaald hebben van alle negatieve pers over onze organisatie. Wij ook. En misschien worden jullie ook wel hierover bevraagd door familie, vrienden of kennissen. We vinden dit heel erg vervelend voor jullie, na al het harde werk dat jullie verzet hebben. We hebben allemaal ons uiterste best gedaan, met de beste intenties en we gaan dit ook laten zien aan de AP.

Heb je vragen? Bel of mail ons gerust.

Dit bericht is uitsluitend bestemd voor de geadresseerde. Het bericht kan vertrouwelijke informatie bevatten. Als u dit bericht per abuis hebt ontvangen, wordt u verzocht het te vernietigen en de afzender te informeren. GGD GHOR Nederland is niet aansprakelijk voor onjuiste en onvolledige overbrenging van de inhoud van een verzonden e-mail bericht, of een te late ontvangst

daarvan. 15.5

15.6
Archived: donderdag 12 mei 2022 08:34:18
From: [redacted]
Sent: vrijdag 30 april 2021 15:32:18
To: [redacted]
Cc: [redacted]
Subject: stukken opvragen FW: Terugkoppeling en vragen bespreking AP
Importance: Normal
Sensitivity: None
Attachments:
Overzicht verstrekte stukken AP.xlsx;

Hallo [redacted],

Enige tijd geleden heb jij aan onze [redacted], [redacted], onderstaande mail gestuurd met als bijlage een excel bestand ‘overzicht verstrekte stukken AP”. In deze mail geef je aan dat we specifieke documentatie kunnen opvragen.

Op dit moment zijn wij binnen onze GGD Hart voor Brabant druk bezig om alle stukken/documentatie die betrekking hebben op het programma corona bij elkaar te zoeken en te controleren op juistheid, zodat wij goed voorbereid zijn op een mogelijk bezoek van de AP.

Om alles goed in kaart te brengen en juridisch te kunnen beoordelen, hebben wij aanvullende stukken vanuit de GGD GHOR nodig. Bijgaand stuur ik je een overzicht van de documentatie die wij graag zouden willen ontvangen (geel gearceerd) . Uiteraard is dit afgestemd onze [redacted].

Zou je mij kunnen laten weten op welke termijn ik deze stukken zou kunnen ontvangen?

Met vriendelijke groeten,

[redacted]

[redacted]

GGD Hart voor Brabant

Pettelaarpark 10 Den Bosch

Postbus 3024, 5003 DA Tilburg

www.ggdhvb.nl

[redacted]

[redacted]@ggdhvb.nl

Aanwezig op: ma-di-wo-do

Gezond doet leven!

Van: [redacted]@ggdhvb.nl>
Verzonden: maandag 8 maart 2021 09:54
Aan: [redacted]@ggdhvb.nl>
Onderwerp: FW: Terugkoppeling en vragen bespreking AP

Van: [redacted]@ggdhvb.nl>

Verzonden: zondag 7 maart 2021 21:20
Aan: [redacted]@ggdhvb.nl>;
Onderwerp: FW: Terugkoppeling en vragen bespreking AP

Op uitdrukkelijk verzoek van 10 DPG'en hebben we inzicht gekregen in de documenten die de GGD GHOR gedeeld heeft met de AP (zie bijlage).

Hartelijke groet,

[redacted]

Van: [redacted]@ggdghor.nl>
Verzonden: vrijdag 5 maart 2021 12:23
Aan: [redacted]@ggdbzo.nl>
CC: [redacted]@ggdhaaglanden.nl>; [redacted]@vggm.nl>; [redacted]@ggdhn.nl) <[redacted]@ggdhn.nl>; [redacted]@ggdzl.nl>; [redacted]@ggdzeeland.nl>; [redacted]@ggdgelderlandzuid.nl>; [redacted]@ggdijsselland.nl>; [redacted]@ggdgooi.nl>; [redacted]@ggdwestbrabant.nl>; [redacted]@ggdhvb.nl>; [redacted]@ggdnog.nl>; [redacted]@ggdghor.nl>; [redacted]@ggdghor.nl>
Onderwerp: RE: Terugkoppeling en vragen bespreking AP

Hi [redacted] e.a.,

Dank voor jullie mail.

Ik reageer op jullie verzoek om het delen van documenten die verstrekt zijn aan de AP.

[redacted] werkt aan informatie over contacten/convenanten en besluiten o.a. aangaande HPzone; dat vergt iets meer tijd.

Bijgevoegd vinden jullie de lijst met documenten die we aan de AP verstrekt hebben.

Daarbij dient opgemerkt te worden, dat deze lijst dagelijks groeit want de AP vraagt continu aanvullende documenten bij ons op.

Dat brengt me meteen ook bij een praktisch vraagstuk want al deze documenten overleggen, lijkt me niet werkbaar en ook risicovol.

Daarom is mijn vraag of het met enige regelmaat verstrekken van dit (bijgewerkte) overzicht, toereikend is om in jullie vraag te voorzien?

Mogelijk daarnaast aangevuld met documenten die GGD'en aan de AP overleggen.

Immers zouden we dan bij vragen van de AP kunnen antwoorden dat het document al aan hen verstrekt is.

Zo besparen we elkaar een hoop werk én weet iedereen welke informatie de AP tot haar beschikking heeft.

Aanvullend kunnen we natuurlijk altijd specifieke documenten aan (een deel van) jullie overhandigen, mocht daar behoefte aan zijn.

Ik hoor graag of bovenstaande werkwijze een weg te gaan is, waarbij ik me realiseer dat het verstrekken van dit overzicht slechts een onderdeel is van elkaar inzage geven in het traject AP en dat we ook informatie over de interviews en overige

correspondentie met de AP als GGD GHOR beter met jullie dienen uit te wisselen. Daarbij zoek ik nog naar de juiste vorm (wekelijkse nieuwsbrief, mondeling,….). Suggesties van jullie kant hierover zijn zeer welkom.

Hoop jullie hiermee voldoende geïnformeerd te hebben!

Met vriendelijke groet,

[redacted]

Zwarte Woud 2
3524 SJ Utrecht
Telefoon: 030-2525052
Mobiel: [redacted]

E-mail : [redacted]@ggdghor.nl
Website : www.ggdghor.nl
Twitter : @ggdnederland en @ghornederland
Afwezig : -

Van: [redacted]@GGDBZO.nl>
Verzonden: donderdag 4 maart 2021 16:42
Aan: [redacted]@ggdghor.nl>; [redacted]@ggdghor.nl>; [redacted]@ggdghor.nl>
CC: [redacted]@ggdhaaglanden.nl>; [redacted]@vggm.nl>; [redacted]@ggdhn.nl) <[redacted]@ggdhn.nl>; [redacted]@ggdzl.nl>; [redacted]@ggdzeeland.nl>; [redacted]@ggdgelderlandzuid.nl>; [redacted]@ggdijsselland.nl>; [redacted]@ggdgooi.nl>; [redacted]@ggdwestbrabant.nl>; [redacted]@ggdhvb.nl>; [redacted]@ggdnog.nl>
Onderwerp: Terugkoppeling en vragen bespreking AP

Dag,

Gisteravond hebben we zoals jullie weten een gesprek gehad met elkaar over de ervaringen van [redacted] en onze ervaringen met onze juristen. Om mezelf als voorbeeld te nemen: de jurist die ik heb ingehuurd vraagt om heel veel documenten waar ook om [redacted] heeft gevraagd, namelijk de 60 documenten die GGDGHOR heeft aangeleverd. Wij ontvangen allemaal graag deze documenten . Want in feite zijn ze “van ons”. Ook willen we graag een overzicht van wanneer we besluiten hebben genomen over HP zone light, evenals de getekende contracten van het afgelopen jaar. We hebben “velletjes” getekend maar geen complete overeenkomsten terug gekregen van alles wat er getekend is.

Kan dat en wanneer kunnen we dat ontvangen.

Wij horen graag!

[redacted]

15.7
Archived: donderdag 12 mei 2022 09:43:42
From: [redacted]
Sent: maandag 8 maart 2021 09:23:30
To: [redacted]
Cc: [redacted]
Subject: Terugkoppeling en vragen bespreking AP
Importance: Normal
Sensitivity: None
Attachments:
Overzicht verstrekte stukken AP.xlsx;

Hallo [redacted] en [redacted],

Zie onderstaande vragen vanuit de GGD GHOR NL m.b.t. de uitvraag van het AP.

- Moeilijk om continu actueel te zijn, het is een lopend onderzoek
- Dus voorstel om dat met enige regelmaat te doen.
- Hebben wij nog suggesties of toevoegingen voor een periodieke update vanuit de GGD GHOR NL? Nieuwsbrief? Periodiek afstemmingsoverleg met de FG'en?
- Vraag ook aan de regionale GGD'en om aan te geven welke documenten bij hen door de AB worden uitgevraagd te delen met GGD GHOR NL. (prima, goed om centraal overzicht te houden). Wat is het proces? Hoe en bij wie leveren we dat aan?

Graag van jullie reactie.

Groepten [redacted]

Van: [redacted]@ggdhvb.nl>
Verzonden: zondag 7 maart 2021 21:20
Aan: [redacted]@ggdhvb.nl>; [redacted]@ggdhvb.nl>; [redacted]@ggdhvb.nl>; [redacted]@ggdhvb.nl>
Onderwerp: FW: Terugkoppeling en vragen bespreking AP

Op uitdrukkelijk verzoek van 10 DPG'en hebben we inzicht gekregen in de documenten die de GGD GHOR gedeeld heeft met de AP (zie bijlage).

Hartelijke groet,

[redacted]

Van: [redacted]@ggdghor.nl>
Verzonden: vrijdag 5 maart 2021 12:23
Aan: [redacted]@ggdbzo.nl>
CC: [redacted]@ggdhaaglanden.nl>; [redacted]@vggm.nl>; [redacted]

[redacted]@ggdhn.nl) [redacted]@ggdhn.nl>; [redacted]@ggdzl.nl>; [redacted]
[redacted]@ggdzeeland.nl>; [redacted]@ggdgelderlandzuid.nl>; [redacted]
[redacted]@ggdijsselland.nl>; [redacted]@ggdgooi.nl> [redacted]
[redacted]@ggdwestbrabant.nl>; [redacted]@ggdhvb.nl>; [redacted]@ggdnog.nl>; [redacted]
[redacted]@ggdghor.nl>; [redacted]@ggdghor.nl>

Onderwerp: RE: Terugkoppeling en vragen bespreking AP

Hi [redacted] e.a.,

Dank voor jullie mail.

Ik reageer op jullie verzoek om het delen van documenten die verstrekt zijn aan de AP.

[redacted] werkt aan informatie over contacten/convenanten en besluiten o.a. aangaande HPzone; dat vergt iets meer tijd.

Bijgevoegd vinden jullie de lijst met documenten die we aan de AP verstrekt hebben.

Daarbij dient opgemerkt te worden, dat deze lijst dagelijks groeit want de AP vraagt continu aanvullende documenten bij ons op.

Dat brengt me meteen ook bij een praktisch vraagstuk want al deze documenten overleggen, lijkt me niet werkbaar en ook risicovol.

Daarom is mijn vraag of het met enige regelmaat verstrekken van dit (bijgewerkte) overzicht, toereikend is om in jullie vraag te voorzien?

Mogelijk daarnaast aangevuld met documenten die GGD'en aan de AP overleggen.

Immers zouden we dan bij vragen van de AP kunnen antwoorden dat het document al aan hen verstrekt is.

Zo besparen we elkaar een hoop werk én weet iedereen welke informatie de AP tot haar beschikking heeft.

Aanvullend kunnen we natuurlijk altijd specifieke documenten aan (een deel van) jullie overhandigen, mocht daar behoefte aan zijn.

Ik hoor graag of bovenstaande werkwijze een weg te gaan is, waarbij ik me realiseer dat het verstrekken van dit overzicht slechts een onderdeel is van elkaar inzage geven in het traject AP en dat we ook informatie over de interviews en overige correspondentie met de AP als GGD GHOR beter met jullie dienen uit te wisselen. Daarbij zoek ik nog naar de juiste vorm (wekelijkse nieuwsbrief, mondeling,….). Suggesties van jullie kant hierover zijn zeer welkom.

Hoop jullie hiermee voldoende geïnformeerd te hebben!

Met vriendelijke groet,

[redacted]

Zwarte Woud 2
3524 SJ Utrecht

E-mail : [redacted]@ggdghor.nl
Website : www.ggdghor.nl

Telefoon: [redacted]
Mobiel [redacted]
Twitter : @ggdnederland en @ghornederland
Afwezig : -

Van: [redacted]@GGDBZO.nl>
Verzonden: donderdag 4 maart 2021 16:42
Aan: [redacted]@ggdghor.nl>; [redacted]@ggdghor.nl>; [redacted]@ggdghor.nl>
CC: [redacted]@ggdhaaglanden.nl>; [redacted]@vggm.nl>; [redacted]@ggdhn.nl) [redacted]@ggdzl.nl>; [redacted]@ggdzeeland.nl>; [redacted]@ggdgelderlandzuid.nl>; [redacted]@ggdijsselland.nl>; [redacted]@ggdgooi.nl>; [redacted]@ggdwestbrabant.nl>; [redacted]@ggdhvb.nl>; [redacted]@ggdnog.nl>
Onderwerp: Terugkoppeling en vragen bespreking AP

Dag,

Gisteravond hebben we zoals jullie weten een gesprek gehad met elkaar over de ervaringen van [redacted] en onze ervaringen met onze juristen. Om mezelf als voorbeeld te nemen: de jurist die ik heb ingehuurd vraagt om heel veel documenten waar ook om [redacted] heeft gevraagd, namelijk de 60 documenten die GGDGHOR heeft aangeleverd. Wij ontvangen allemaal graag deze documenten . Want in feite zijn ze “van ons”. Ook willen we graag een overzicht van wanneer we besluiten hebben genomen over HP zone light, evenals de getekende contracten van het afgelopen jaar. We hebben “velletjes” getekend maar geen complete overeenkomsten terug gekregen van alles wat er getekend is.

Kan dat en wanneer kunnen we dat ontvangen.

Wij horen graag!

[redacted]

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

Een screenshot van de verkennerpagina van map 16:

16.1 Brief aan ged...datalek_Redacted

16.10 RE_ Gedupe...diefstal_Redacted

16.11 RE_ Gegeve...ant (40)_Redacted

16.12 RE_ informer...diefstal_Redacted

16.13 RE_ rapport AP (3)_Redacted

16.14 RE_ STRIKT...atadiefs_Redacted

16.15 VERTROUW...incident_Redacted

16.2 Datadiefstal _...abant b_Redacted

16.3 FW_ Gedupe...adiefstal_Redacted

16.4 FW_ Gedupe...datalek_Redacted

16.5 FW_ Vervolg...20 afsch_Redacted

16.6 FW_ Vervolg...20 en in_Redacted

16.7 FW_AAN~1_Redacted

16.8 RE_ aantallen...eerden _Redacted

16.9 RE_ E-mail m...sdiefstal_Redacted

16.22 RE_ rapport AP (3)_Redacted

16.23 RE_ STRIKT...atadiefs_Redacted

16.24 Update land...diefstal _Redacted

16.25 VERTROUW...incident_Redacted

16.3 FW_ Gedupe...adiefstal_Redacted

16.4 FW_ Gedupe...datalek_Redacted

16.5 FW_ informer...diefstal_Redacted

16.6 FW_ informer...peerden_Redacted

16.7 FW_ Mail van...e gedup_Redacted

16.8 FW_ reactief t...eerden _Redacted

16.9 FW_ SPOED_...numme_Redacted

16.1
Archived: donderdag 12 mei 2022 09:46:03
From: [redacted]
Sent: vrijdag 19 maart 2021 19:44:07
To: [redacted]@tilburg.nl; [redacted]@cuijk.nl; [redacted]@s-hertogenbosch.nl; [redacted]@boekel.nl; [redacted]@heusden.nl; [redacted]@oss.nl; [redacted]@meierijstad.nl
Cc: [redacted]@cgm.nl; [redacted]@boekel.nl; [redacted]@s-hertogenbosch.nl; [redacted]@s-hertogenbosch.nl; [redacted]@tilburg.nl; [redacted]@meierijstad.nl; [redacted]@oss.nl; [redacted]@tilburg.nl; [redacted]
Subject: Brief aan gedupeerden datalek
Importance: Normal
Sensitivity: None

Geachte leden van ons dagelijks bestuur,

Op 26 en 29 januari en 5 februari, hebben wij u en het algemeen bestuur op de hoogte gebracht van de laatste ontwikkelingen van de datadiefstal uit GGD-systemen. Via dit bericht informeer ik u namens [redacted] over een brief aan circa duizend gedupeerden van deze datadiefstal. Daarvan wonen er 37 in de regio van GGD Hart voor Brabant.

Vandaag is vanuit GGD GHOR Nederland namens GGD Hart voor Brabant een brief aan de gedupeerden in onze regio gestuurd. Daarin worden zij persoonlijk geïnformeerd over de datadiefstal. In de brief staat:

- Wat er is gebeurd;
- Oprechte excuses daarvoor;
- Welke gegevens gestolen zijn;
- Welke maatregelen GGD GHOR Nederland en alle GGD'en genomen hebben;
- Wat de gevolgen kunnen zijn voor de betrokkenen;
- Waar ze eventuele identiteitsfraude kunnen melden.

Met uw voorzitter spraken we af dat we het algemeen bestuur over deze ontwikkeling informeren tijdens zijn vergadering van 24 maart a.s. Ik vertrouw erop u voor nu voldoende geïnformeerd te hebben.

Hartelijke groet,

[redacted]

[redacted]

GGD Hart voor Brabant

Pettelaarpark 10
5216 PD, 's-Hertogenbosch
Postbus 3024, 5003 DA Tilburg
www.ggdhvb.nl

[redacted]@ggdhvb.nl
Aanwezig op: ma t/m vr
[redacted]
[redacted]

Gezond doet leven!

16.2
Archived: donderdag 12 mei 2022 09:46:58
From: [redacted]n
Sent: vrijdag 29 januari 2021 14:04:55
To: [redacted]
Subject: FW: Datadiefstal / Governance systemen / gezamenlijk Brabant breed signaal
Importance: Normal
Sensitivity: None

Ter info, in WB is daar [redacted] mee bezig

Van: [redacted]@ggdwestbrabant.nl>
Verzonden: vrijdag 29 januari 2021 13:36
Aan: [redacted]@ggdbzo.nl>; [redacted]@ggdhvb.nl>
Onderwerp: RE: Datadiefstal / Governance systemen / gezamenlijk Brabant breed signaal

Goedemiddag,

Bij ons is [redacted] er al mee aan de slag gegaan. Hij heeft ook al contact gehad met [redacted] ? vanuit HvB.

Wij vermoeden toch ook wel dat er een WOB verzoek gaat komen.

Groeten,

[redacted]

Van: [redacted]@GGDBZO.nl>
Verzonden: vrijdag 29 januari 2021 13:16
Aan: [redacted]@ggdhvb.nl>
CC: [redacted]@ggdwestbrabant.nl>
Onderwerp: Re: Datadiefstal / Governance systemen / gezamenlijk Brabant breed signaal

Hoi [redacted],

Wat is hier het doel van? Wat willen jullie hiermee bereiken bij GGD GHOR Nederland? Of is dit om ons voor te bereiden op een eventueel WOB-verzoek?

Groet,

[redacted]

Van: [redacted]@ggdhvb.nl>
Verzonden: donderdag 28 januari 2021 21:01
Aan: [redacted]@GGDBZO.nl>; [redacted]@ggdwestbrabant.nl>
Onderwerp: Datadiefstal / Governance systemen / gezamenlijk Brabant breed signaal

Hallo [redacted] en [redacted],

Zouden jullie het onderstaande kunnen uitvragen binnen jullie programma's naar aanleiding van de datalek (landelijk). Zou mooi zijn om gebundeld aan te leveren bij de GGD Ghor NL.

Zou mooi zijn als de personen die hier intern bij jullie mee bezig zijn kunnen koppelen aan die van ons. [redacted] Al is bij ons trekker van dit proces. Hebben jullie een contactpersoon bij NO-Gelderland?

[redacted] (en wij ook) vindt het van groot belang dat wij alle eerdere schriftelijk aan GGD GHOR NL afgegeven signalen over problemen met CoronIT en HP-zone verzamelen en bundelen. Niet alleen ten aanzien van beveiliging, maar in volle breedte: performanceproblemen, prioritering, dashboarding et cetera. Dat geldt voor ons als GGD HvB, maar zouden West, Zuidoost en eigenlijk ook NO-Gelderland ook parallel moeten oppakken. [redacted] wil dit volgende week graag gebundeld aanbieden aan GGD GHOR NL, tegelijk met onze verdere escalatie over governance. Als het kan dus alle signalen namens Brabant.

Groeten [redacted]

Met vriendelijke groet,

[redacted]

[redacted]

GGD Hart voor Brabant

Bezoekadres
Pettelaarsweg 10
's-Hertogenbosch
Postbus 3024
5003 DA Tilburg
www.ggdhvb.nl

[redacted]
[redacted]@ggdhvb.nl
Aanwezig op: di-wo-do

Gezond doet leven!

16.3
Archived: donderdag 12 mei 2022 09:47:15
From: [redacted]
Sent: woensdag 19 mei 2021 12:16:08
To: [redacted]
Cc: [redacted]
Subject: FW: Gedupeerden datadiefstal
Importance: Normal
Sensitivity: None

Hallo [redacted],

Ik heb een tweetal vragen:

1. Voor de AB/DB brief ben ik op zoek naar het aantal gedupeerde burgers nav datadiefstal die zijn aangeschrevenen in 2e ronde:
   In de 1e ronde zijn voor onze GGD 37 gedupeerde burgers aangeschreven. Later heeft de GGD GHOR nog 237 brieven verstuurd. Weet jij of in de tweede ronde nog burgers van onze GGD zijn aangeschreven?

   Dit kan je mogelijk terugzien in de mailbox van [redacted], want GGD GHOR heeft alleen de DGP geïnformeerd (zie mail van [redacted] helemaal onderdaan). [redacted] en [redacted] kunnen deze vraag niet beantwoorden. Het natuurlijk ook zomaar zijn dat er niet meer burgers van onze GGD HvB gedupeerd zijn.

   Kan jij dit voor mij nagaan? Graag uiterlijk morgen als dat lukt….

2. Archiveren ontvangen lijst:
   [redacted] vroeg een hele tijd geleden waar de lijst gearchiveerd kan worden (zie onderstaand mailverkeer). Mocht dit nog gewenst zijn, dan zie ik de lijst wel verschijnen.

Ik hoor het graag,

Met vriendelijke groeten,

[redacted]

GGD Hart voor Brabant
Gezond doet leven!
Pettelaarpark 10 Den Bosch
Postbus 3024, 5003 DA Tilburg
www.ggdhvb.nl
[redacted]@ggdhvb.nl
Aanwezig op: ma-di-wo-do

Van: [redacted]@ggdhvb.nl>
Verzonden: donderdag 15 april 2021 17:33
Aan: [redacted]@ggdhvb.nl>
CC: [redacted]@ggdhvb.nl>; [redacted]@ggdhvb.nl>
Onderwerp: FW: Gedupeerden datadiefstal

Hoi [redacted],16.3

Aanstaande maandag staat het onderwerp archivering op d MT agenda.

Onderstaand reactie vanuit [redacted] op jouw verzoek van enige tijd geleden.
Je kunt de informatie aan [redacted] mailen, zij zal het dan archiveren.

Groet
[redacted]

Van: [redacted]@ggdhvb.nl>
Verzonden: donderdag 15 april 2021 13:14
Aan: [redacted]@ggdhvb.nl>
Onderwerp: FW: Gedupeerden datadiefstal

Hallo [redacted],

Je had aan mij gevraagd om na te gaan waar we de lijst met namen (betrokkene) van de datadiefstal heb beste kunne archiveren.

Zier hieronder het antwoord.

Met vriendelijke groeten,

[redacted]

GGD Hart voor Brabant
Pettelaarpark 10 Den Bosch
Postbus 3024, 5003 DA Tilburg
www.ggdhvb.nl
[redacted]@ggdhvb.nl
Aanwezig op: ma-di-wo-do
Gezond doet leven!

Van: [redacted]@hetservicecentrum.nl>
Verzonden: donderdag 15 april 2021 12:43
Aan: [redacted]@ggdhvb.nl>
Onderwerp: FW: Gedupeerden datadiefstal

Ha [redacted],

Ik heb gister nog even ruggenspraak met [redacted] gehad (Corona archivaris) over jouw vraag.
Jullie insteek om het op te slaan op jullie eigen teamsite is juist, zoals door jou verwoord: “”Mijn voorstel zou zijn om dit als een ‘gewoon’ datalek te bewaren. Ik kan een dossier aanmaken op SharePoint waar alleen [redacted] en ik toegang toe hebben.’

Met daarbij wel opgemerkt dat als er algemene mails met informatie over het datalek Corona is geweest, dit dan wel apart op jullie teamsite op te slaan in een apart dossier Corona datalek zonder privacy gegevens. Als het mettertijd gearchiveerd wordt door jullie, dan kunnen we het als bewaararchief Hotspot Corona aanmerken. Op deze manier is de algemene correspondentie rond om het datalek gewaarborgd en staat het los van de privacy gegevens.

Tenzij de algemene correspondentie over het datalek al is opgeslagen op de teamsite Corona dan hoeven jullie het niet apart

op te slaan. [16.3]

Indien er nog vragen zijn, dan hoor ik het wel.
Fijne dag verder.

Met vriendelijke groeten,

[redacted]

Reitseplein 3 5037 AA Tilburg
Postbus 3024, 5003 DA Tilburg

[redacted]@hetservicecentrum.nl
Aanwezig op: ma-wo-do

Hét Service Centrum: *het shared service center van GGD Hart voor Brabant, GGD West-Brabant, GGD Noord- en Oost-Gelderland en de Regionale Ambulancevoorziening Brabant Midden-West-Noord*

Van: [redacted]@hetservicecentrum.nl>
Verzonden: dinsdag 30 maart 2021 13:27
Aan: [redacted]@ggdhvb.nl>
Onderwerp: Re: Gedupeerden datadiefstal

Hoi [redacted],

Even een korte reactie. Ik ben nl. ziek thuis.
Volgens mij is jullie insteek juist.

Maar ik kom hier zo gauw ik beter ben op terug. Nu niet in de gelegenheid om het uit te kunnen zoeken.

Mvrgr [redacted]

Outlook voor Android downloaden

From: [redacted]@ggdhvb.nl>
Sent: Friday, March 26, 2021 12:32:05 PM
To: [redacted]@hetservicecentrum.nl>
Subject: FW: Gedupeerden datadiefstal

Hallo [redacted],

Ik heb onderstaande vraag gekregen van [redacted]. Samengevat is de vraag:

Onze DPG heeft een PDF-bestand ontvangen, voorzien van een wachtwoord, waarin alle burgers met naam en toenaam genoemd worden die slachtoffer zijn van de datadiefstal bij de GGD GHOR.

Waar en hoe kan een dergelijk bestand het beste gearchiveerd worden?

Ik hoor het graag,

Met vriendelijke groeten,

[redacted]

Pettelaarpark 10 Den Bosch
Postbus 3024, 5003 DA Tilburg
www.ggdhvb.nl

[redacted]@ggdhvb.nl
Aanwezig op: ma-di-wo-do

Gezond doet leven!

Van: [redacted]@ggdhvb.nl>
Verzonden: dinsdag 23 maart 2021 17:09
Aan: [redacted]@ggdhvb.nl>
Onderwerp: RE: Gedupeerden datadiefstal

Goed idee om de archivaris nog even mee te laten denken.

Van: [redacted]@ggdhvb.nl>
Verzonden: dinsdag 23 maart 2021 11:14
Aan: [redacted]@ggdhvb.nl>
Onderwerp: RE: Gedupeerden datadiefstal

Hoi [redacted],

Ja lastige vraag. Ik weet niet of er een aparte plek is om deze gegevens te bewaren.

Mijn voorstel zou zijn om dit als een ‘gewoon’ datalek te bewaren. Ik kan een dossier aanmaken op sharepoint waar alleen Karin van Zandvoort en ik toegang toe hebben.

Of we kunnen onze archivaris nog even laten meedenken.

Met vriendelijke groeten,

[redacted]

Pettelaarpark 10 Den Bosch
Postbus 3024, 5003 DA Tilburg
www.ggdhvb.nl

[redacted]@ggdhvb.nl
Aanwezig op: ma-di-wo-do

Gezond doet leven!

Van: [redacted]@ggdhvb.nl>
Verzonden: maandag 22 maart 2021 21:48
Aan: [redacted]@ggdhvb.nl>
Onderwerp: Fwd: Gedupeerden datadiefstal

16.3

Hoi [redacted],

Is daar een aparte plek voor t filen van deze info?
Groet
[redacted]

Outlook voor Android downloaden

Van: [redacted]@ggdhvb.nl>
Verstuurd: maandag 22 maart 2021 21:33
Aan: [redacted]
Onderwerp: FW: Gedupeerden datadiefstal

Hi [redacted],

Wil jij me laten weten wat de juiste wijze is om deze informatie bij onze GGD te archiveren?

Hartelijke groet,
[redacted]

Van: [redacted]@ggdghor.nl>
Verzonden: maandag 22 maart 2021 17:47
Aan: [redacted]@ggdhvb.nl>
Onderwerp: Gedupeerden datadiefstal

Beste DPG,

Zoals bekend hebben afgelopen vrijdag de circa 1.000 gedupeerden van de datadiefstal, die op dit moment bekend zijn bij ons, een brief ontvangen. Zoals afgesproken ontvang je vandaag de afschriften van de brieven die binnen je regio zijn verstuurd. Dit doen wij - vanuit veiligheidsoverwegingen - door middel van een PDF-bestand voorzien van een wachtwoord. In deze e-mail vind je de instructie om de bestanden te kunnen benaderen.

Werkwijze
Als DPG ontvangt je hierbij een e-mail die alleen aan jou is gericht met in de bijlage één PDF-bestand. Hierin zijn alle brieven van gedupeerden in jouw regio opgenomen. Vanuit veiligheidsoverwegingen is dit bestand voorzien van een wachtwoord en kan er geen tekst uit het bestand gekopieerd worden. Printen van het bestand is eveneens om die reden onmogelijk gemaakt. Hierbij het nadrukkelijke verzoek om dit bestand na ontvangst conform de geldende privacyrichtlijnen op te slaan en te gebruiken.

Inzien van bestanden
Het bestand wordt met een wachtwoord aangeboden. Om het bestand te openen ontvang je als DPG een APP-bericht met daarin een code. Deze code wordt in de loop van de middag of begin van de avond door mij verstrekt en vormt het wachtwoord waarmee het bestand beveiligd is.
Mocht deze mail nog vragen oproepen, dan hoor ik dat graag.

Met vriendelijke groet,
[redacted]

Drs. [redacted] ([redacted]
[redacted]

GGD GHOR Nederland
Zwarte Woud 2
3524 SJ 'a0 Utrecht

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

Dit bericht is uitsluitend bestemd voor de geadresseerde. Het bericht kan vertrouwelijke informatie bevatten. Als u dit bericht per abuis hebt ontvangen, wordt u verzocht het te vernietigen en de afzender te informeren. GGD GHOR Nederland is niet aansprakelijk voor onjuiste en onvolledige overbrenging van de inhoud van een verzonden e-mail bericht, of een te late ontvangst daarvan.

16.4
Archived: donderdag 12 mei 2022 09:47:27
From:
Sent: woensdag 19 mei 2021 23:03:45
To: [redacted]
Subject: FW: Gedupeerden datalek
Importance: Normal
Sensitivity: None
Attachments:
GGD Hart voor BrabantE - 20210331.pdf; GGD Hart voor BrabantE - 20210413.pdf;

Toch nog een andere mail dus met brieven aan gedupeerden. Sorry dat ik die niet eerder gezien heb. Hopelijk heb je deze gegevens nog op tijd.

groetjes,

[redacted]

Van: [redacted] <[redacted]ggdghor.nl>
Verzonden: maandag 26 april 2021 16:13
Aan: [redacted] <[redacted]ggdhvb.nl>
Onderwerp: Gedupeerden datalek

Beste [redacted]

Deze mail is een vervolg op mijn mail van 22 maart j.l. in het kader van de datadiefstal. Er zijn wederom brieven verstuurd naar gedupeerden die deels afkomstig zijn uit de eerdere periode en toen nog niet konden worden meegenomen (zij hebben 29 maart een brief gehad) en deels afkomstig zijn uit de continue monitoring (brieven zijn verstuurd op 31 maart en 13 april). Volgens afspraak ontvang je de afschriften van de brieven die binnen je regio zijn verstuurd. Dit doen wij - vanuit veiligheidsoverwegingen – wederom door middel van een PDF-bestand voorzien van een wachtwoord. In deze e-mail vind je de instructie om de bestanden te kunnen benaderen.

Werkwijze

Als DPG ontvang je hierbij een e-mail die alleen aan jou is gericht met in de bijlage één, twee of drie PDF-bestanden, afhankelijk van het feit of er gedupeerden uit jouw regio in één, twee of drie van de bovengenoemde mailings zaten. In deze bestanden zijn de brieven van gedupeerden in jouw regio opgenomen. Vanuit veiligheidsoverwegingen zijn deze bestanden voorzien van een wachtwoord en kan er geen tekst uit een bestand gekopieerd worden. Printen van een bestand is eveneens om die reden onmogelijk gemaakt. Hierbij het nadrukkelijke verzoek om dit bestand na ontvangst conform de geldende privacyrichtlijnen op te slaan en te gebruiken.

Inzien van bestanden

Het bestand wordt met een wachtwoord aangeboden. Het wachtwoord is voor elk van de bestanden hetzelfde. Om het bestand te openen ontvang je als DPG een APP-bericht met daarin een code. Deze code wordt in de loop van de middag of begin van de avond door mij verstrekt en vormt het wachtwoord waarmee het bestand beveiligd is.

Mocht deze mail nog vragen oproepen, dan hoor ik dat graag.

Met vriendelijke groet,

[redacted]

Drs. [redacted]
[redacted]

GGD GHOR Nederland
Zwarte Woud 2
3524 SJ Utrecht

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

Dit bericht is uitsluitend bestemd voor de geadresseerde. Het bericht kan vertrouwelijke informatie bevatten. Als u dit bericht per abuis hebt ontvangen, wordt u verzocht het te vernietigen en de afzender te informeren. GGD GHOR Nederland is niet aansprakelijk voor onjuiste en onvolledige overbrenging van de inhoud van een verzonden e-mail bericht, of een te late ontvangst daarvan.

16.5
Archived: donderdag 12 mei 2022 09:49:04
From: [redacted]
Sent: Tue, 15 Jun 2021 07:45:44
To: [redacted]
Subject: FW: Vervolg mail van [redacted] m.b.t. datadiefstal 2020 afschriften brieven gedupeerden
Importance: Normal
Sensitivity: None
Attachments:
Brief 1 - GGD Hart voor BrabantE - 343.pdf; Brief 2 - GGD Hart voor BrabantE - 25.pdf; Brief 3 - GGD Hart voor BrabantE - 19.pdf;

Hi [redacted]

De nieuwe sets met brieven. Het gaat om grote aantallen, zoals je ziet.

Hartelijke groet,

[redacted]

Van: [redacted]@ggdghor.nl>
Verzonden: maandag 14 juni 2021 21:06
Aan: [redacted]@ggdhvb.nl>
CC: [redacted]@ggdghor.nl>
Onderwerp: Vervolg mail van [redacted] [redacted] m.b.t. datadiefstal 2020 afschriften brieven gedupeerden

Beste [redacted]

In vervolg op de onderstaande mail van [redacted] van 2 juni j.l., ontvang je hierbij de afschriften van de brieven die binnen je regio zijn verstuurd. Dit doen wij - vanuit veiligheidsoverwegingen – wederom door middel van een PDF-bestand voorzien van een wachtwoord. In deze e-mail vind je de instructie om het bestand te kunnen benaderen.

Werkwijze

Voor deze groep zijn er 6 verschillende brieven uitgegaan:

Deze brieven hebben betrekking op de screenshots van 9 augustus 2020:

- Brief 1 – Dit zijn personen die niet gebeld, maar persoonsgegevens zijn wel ingezien. Totaal zijn dit 343 brieven.

Kenmerk van deze brief is NG-07-PG-001 (tot nummer 343)

- Brief 2 – Dit zijn personen die niet gebeld zijn. Bij deze personen zijn persoonsgegevens plus zorgnetwerk (apotheek/huisarts) ingezien. Totaal zijn van deze brief 25 uitgegaan.

Kenmerk van deze brief is NG-07-ZN-001 (tot nummer 025)

- Brief 3[6.5] deze personen zijn ook niet gebeld, maar naast de persoonsgegevens is er ook een identificatienummer van een rijbewijs, paspoort of identiteitskaart ingezien.

Kenmerk van deze brief is NG-07-IN-001 (tot nummer 019)

De volgende brieven hebben betrekking op 8 september 2020:

- Brief 4 - 50 personen die zijn gebeld ontvangen ook deze brief. Van hen zijn de standaard persoonsgegevens ingezien (net als vermeld in de brief van februari 2021 en de 343 van hierboven);

Kenmerk van deze brief is G-07-PG-001 (tot nummer 050)

- Brief 5 - 1 persoon die is gebeld en ontvangt ook deze brief. Van deze persoon is persoonsgegevens en zorgnetwerk (ZN) ingezien.

Kenmerk van deze brief is G-07-ZNPG-001

- Brief 6 - 8 personen zijn gebeld. Van hen is naast de persoonsgegevens ook de testuitslag van hun covid-test vermeld.

Kenmerk van deze brief is G-07-TUPG-001 (tot en met nummer 008)

De brieven zijn geclusterd per soort brief, waardoor je maximaal zes bestanden ontvangt.

Als DPG ontvang je hierbij een e-mail die alleen aan jou is gericht met één of meer (maximaal zes) bestanden. In deze bestanden zijn de brieven van gedupeerden in jouw regio opgenomen. Vanuit veiligheidsoverwegingen zijn deze bestanden voorzien van een wachtwoord en kan er geen tekst uit een bestand gekopieerd worden. Printen van een bestand is eveneens om die reden onmogelijk gemaakt. Hierbij het nadrukkelijke verzoek om dit bestand na ontvangst conform de geldende privacyrichtlijnen op te slaan en te gebruiken.

Inzien van bestanden

De bestanden worden met een wachtwoord aangeboden. Om het bestand te openen ontvang je als DPG een APP-bericht met daarin een code. Deze code wordt in de loop van de avond door mij verstrekt en vormt het wachtwoord waarmee het bestand beveiligd is.

Mocht deze mail nog vragen oproepen, dan hoor ik dat graag.

Met vriendelijke groet,

[redacted]

Van: [redacted]@ggdghor.nl>
Verzonden: woensdag 2 juni 2021 16:22
Aan: Directie GGD GHOR Nederland <directie@ggdghor.nl>
Onderwerp: Mail van [redacted] m.b.t. datadiefstal 2020 en informeren gedupeerden eind deze week

Beste DPG'en,

GGD GHOR Nederland heeft zeer recent van de politie vernomen dat er in 2020 ook een datadiefstal heeft plaatsgevonden. Het gaat om de gegevens van circa 1250 betrokkenen die op 9 augustus 2020 respectievelijk 8 september 2020 onbevoegd zijn ingezien, gestolen en mogelijk verkocht. Deze gegevens waren opgenomen op schermafdrukken die waren gemaakt van de

systemen van de GGD'en.

De reden dat GGD GHOR Nederland pas recentelijk is geïnformeerd door de politie over bovengenoemde datadiefstallen is dat deze schermafdrukken in het kader van het onderzoek bij de politie zijn achtergebleven. Op basis van de Algemene Verordening Gegevensbescherming (**AVG**) zal het incident zo snel als mogelijk moeten worden gemeld bij de Autoriteit Persoonsgegevens (**AP**), alsook aan de betrokkenen. Deze termijn begint te lopen zodra wij op de hoogte zijn geraakt van de datadiefstallen, dat wil zeggen: nadat de politie ons heeft geïnformeerd en de schermafdrukken heeft overhandigd. Op dit moment hebben wij namelijk kunnen vaststellen op welke betrokkenen deze gegevens betrekking hebben.

De regionale GGD'en hebben GGD GHOR Nederland eerder een volmacht verleend voor de (vervolg)meldingen aan de AP van 22 en 25 januari 2021 en de betrokkenen uit de AVG die gerelateerd zijn aan de eerder in dit jaar voorgevallen datadiefstallen. Gelet op de samenhang van de aard van het onderhavige incident met de (vervolg)meldingen van 22 en 25 januari 2021 - datadiefstallen uit de systemen -, alsook de spoedeisendheid die geboden is om van de datadiefstallen van 9 augustus 2020 en 8 september 2020 zo snel mogelijk melding te maken bij de AP en de relatief kleine groep van betrokkenen (circa 1250), zal GGD GHOR Nederland deze notificatieverplichtingen op zich nemen, en kan GGD GHOR Nederland aan de regionale GGD'en bevestigen dat zij momenteel geen actie dienen te ondernemen. GGD GHOR Nederland houdt de regionale GGD'en uiteraard goed op de hoogte van de ontwikkelingen verband houdende met de meldingen die zij zal doen aan de AP en de betrokkenen.

Mocht dit vragen oproepen dan horen we het graag uiterlijk vrijdagochtend. Het is onze bedoeling om de brieven vrijdagmiddag aan de betrokkenen te verzenden.

Met vriendelijke groet,

[redacted]

dr. [redacted]

[redacted]

Dit bericht is uitsluitend bestemd voor de geadresseerde. Het bericht kan vertrouwelijke informatie bevatten. Als u dit bericht per abuis hebt ontvangen, wordt u verzocht het te vernietigen en de afzender te informeren. GGD GHOR Nederland is niet aansprakelijk voor onjuiste en onvolledige overbrenging van de inhoud van een verzonden e-mail bericht, of een te late ontvangst daarvan.

16.6
Archived: donderdag 12 mei 2022 09:49:15
From: [redacted]
Sent: donderdag 10 juni 2021 12:04:09
To: [redacted]
Subject: FW: Vervolg mail van [redacted] m.b.t. datadiefstal 2020 en informeren gedupeerden eind deze week
Importance: Normal
Sensitivity: None

Van: [redacted]@ggdghor.nl>
Verzonden: vrijdag 4 juni 2021 20:01
Aan: Directie GGD GHOR Nederland <directie@ggdghor.nl>
Onderwerp: Vervolg mail van [redacted] m.b.t. datadiefstal 2020 en informeren gedupeerden eind deze week

Beste DPG'en,

In aanvulling op onderstaande mail het volgende. De brieven aan de gedupeerden zijn niet vanmiddag verstuurd maar dat gebeurt begin volgende week. In het weekeind is het call centrum waar zij met eventuele vragen terecht kunnen namelijk niet bereikbaar. Volgende week kunnen zij, wanneer ze de brief ontvangen, desgewenst direct contact leggen met het call center.

Jullie zullen net als de vorige keren afschriften krijgen van de brieven aan gedupeerden in jullie regio's.

Met vriendelijke groet,

[redacted]

Van: [redacted]
Verzonden: woensdag 2 juni 2021 16:22
Aan: Directie GGD GHOR Nederland <directie@ggdghor.nl>
Onderwerp: Mail van [redacted] m.b.t. datadiefstal 2020 en informeren gedupeerden eind deze week

Beste DPG'en,

GGD GHOR Nederland heeft zeer recent van de politie vernomen dat er in 2020 ook een datadiefstal heeft plaatsgevonden. Het gaat om de gegevens van circa 1250 betrokkenen die op 9 augustus 2020 respectievelijk 8 september 2020 onbevoegd zijn ingezien, gestolen en mogelijk verkocht. Deze gegevens waren opgenomen op schermafdrukken die waren gemaakt van de systemen van de GGD'en.

De reden dat GGD GHOR Nederland pas recentelijk is geïnformeerd door de politie over bovengenoemde datadiefstallen is dat deze schermafdrukken in het kader van het onderzoek bij de politie zijn achtergebleven. Op basis van de Algemene Verordening Gegevensbescherming (**AVG**) zal het incident zo snel als mogelijk moeten worden gemeld bij de Autoriteit Persoonsgegevens (**AP**), alsook aan de betrokkenen. Deze termijn begint te lopen zodra wij op de hoogte zijn geraakt van de datadiefstallen, dat wil zeggen: nadat de politie ons heeft geïnformeerd en de schermafdrukken heeft overhandigd. Op dit moment hebben wij namelijk kunnen vaststellen op welke betrokkenen deze gegevens betrekking hebben.

De regionale GGD'en hebben GGD GHOR Nederland eerder een volmacht verleend voor de (vervolg)meldingen aan de AP van 22 en 25 januari 2021 en de betrokkenen uit de AVG die gerelateerd zijn aan de eerder in dit jaar voorgevallen datadiefstallen.

Gelet op de samenhang van de aard van het onderhavige incident met de (vervolg)meldingen van 22 en 25 januari 2021 - datadiefstallen uit de systemen -, alsook de spoedeisendheid die geboden is om van de datadiefstallen van 9 augustus 2020 en 8 september 2020 zo snel mogelijk melding te maken bij de AP en de relatief kleine groep van betrokkenen (circa 1250), zal GGD GHOR Nederland deze notificatieverplichtingen op zich nemen, en kan GGD GHOR Nederland aan de regionale GGD'en bevestigen dat zij momenteel geen actie dienen te ondernemen. GGD GHOR Nederland houdt de regionale GGD'en uiteraard goed op de hoogte van de ontwikkelingen verband houdende met de meldingen die zij zal doen aan de AP en de betrokkenen.

Mocht dit vragen oproepen dan horen we het graag uiterlijk vrijdagochtend. Het is onze bedoeling om de brieven vrijdagmiddag aan de betrokkenen te verzenden.

Met vriendelijke groet,

[redacted]

dr. [redacted]

[redacted]

Dit bericht is uitsluitend bestemd voor de geadresseerde. Het bericht kan vertrouwelijke informatie bevatten. Als u dit bericht per abuis hebt ontvangen, wordt u verzocht het te vernietigen en de afzender te informeren. GGD GHOR Nederland is niet aansprakelijk voor onjuiste en onvolledige overbrenging van de inhoud van een verzonden e-mail bericht, of een te late ontvangst daarvan.

16.7
Archived: donderdag 12 mei 2022 09:46:25
From: [redacted]
Sent: dinsdag 9 maart 2021 17:02:55
To: [redacted]
Subject: FW: AANGEPASTE VOLMACHTIGING met verzoek ondertekening m.b.t. het informeren van slachtoffers van de datadiefstal, graag uiterlijk woensdag 10 maart 12 uur
Importance: High
Sensitivity: None
Attachments:
[redacted]; 20210225 Aangepaste volmachtiging aan GGD GHOR inzake mededeling datalek aan betrokkenen af te geven door de GGD_en_24 februari 2021 (H+P).docx;

Hi [redacted] en [redacted]

Zie onderstaand. Inmiddels is volgens mij aan alle verzoeken gehoor gegeven door GGD GHOR, behalve dat ik nog niet alle definitieve overeenkomsten ontvangen heb (maar deze toezegging ligt er wel). Gezien mijn beperkte mandaat aan jullie het verzoek om advies: kunnen we deze vraag voorleggen aan ons DB met een positief advies? Ik heb [redacted] al laten weten dat ik hiervoor een akkoord van ons DB nodig heb.

Hartelijke groet,

[redacted]

Van: [redacted]@ggdghor.nl>
Verzonden: dinsdag 9 maart 2021 15:31
Aan: Directie GGD GHOR Nederland <directie@ggdghor.nl>
Onderwerp: AANGEPASTE VOLMACHTIGING met verzoek ondertekening m.b.t. het informeren van slachtoffers van de datadiefstal, graag uiterlijk woensdag 10 maart 12 uur
Urgentie: Hoog

Beste DPG'en,

Op 26 februari hebben jullie van mij een mail ontvangen met het verzoek akkoord te geven op de destijds bijgevoegde volmachtiging. Deze volmachtiging betrof het verzoek om het centraal versturen van brieven aan de gedupeerden van de datadiefstal.

Inmiddels hebben we 12 getekende volmachtigingen retour en van enkelen van jullie ook vragen ontvangen. Wij hebben de

afgelopen dagen deze vragen beantwoord en de feedback die gegeven is op de volmachtiging verwerkt. Dit heeft o.a. geleid in een aanscherping van de reeds verstrekte volmacht (zie bijlage, aangepaste volmachtiging). Deze aanscherping heeft het wezen van de volmacht niet gewijzigd waardoor de reeds retour gekomen volmachten nog steeds rechtmatig en rechtsgeldig zijn.

De doorgevoerde aanpassingen betreft o.a. de toevoeging dat GGD GHOR een afschrift van de brieven stuurt aan de GGD die het betreft. Daarnaast wordt in de aangescherpte volmachtiging gerefereerd aan het convenant ("Convenant Gegevensuitwisseling Gezamenlijk Verantwoordelijken") dat GGD GHOR Nederland in april/mei/juni 2020 met de GGD'en heeft afgesloten.

Wij hopen met de informatie die de afgelopen dagen aanvullend verstrekt is en met de aangescherpte volmachtiging dat alle DPG'en nu hier hun medewerking aan kunnen en willen geven.

En we willen jullie derhalve vragen, indien niet al gedaan, de bijgevoegde volmachtiging te ondertekenen door het ondertekenen van jullie eigen tekenblad en deze **uiterlijk woensdag 10 maart 12.00 uur** aan ons terug te sturen (directie@ggdghor.nl).

Zodra we alle volmachten binnen hebben, geven we aan de politie aan dat het databestand aan GGD GHOR verstrekt kan worden, waarna het proces van het informeren van de gedupeerden direct zal starten.

Ik hoor jullie hiermee voldoende geïnformeerd te hebben en hoor het heel graag als er nog vragen leven.

Met vriendelijke groet,

[redacted]

Van: [redacted]
Verzonden: vrijdag 26 februari 2021 13:54
Aan: Directie GGD GHOR Nederland <directie@ggdghor.nl>
Onderwerp: Verzoek ondertekening volmacht m.b.t. het informeren van slachtoffers van de datadiefstal, graag uiterlijk dinsdag 2 maart

Beste DPG'en,

Op dit moment zijn wij bezig met de afhandeling van de datadiefstal die aan het einde van januari aan het licht kwam. In dat kader zijn wij verplicht ook de eventuele slachtoffers van de datadiefstal te informeren. De gegevens van deze slachtoffers zullen ons binnenkort door de politie worden verstrekt. Dit zijn slachtoffers die op basis van het onderzoek van de politie naar boven zijn gekomen.

Als wij de informatie van de slachtoffers overhandigd krijgen, zijn wij verplicht de slachtoffers zo snel als mogelijk hiervan in kennis te stellen. Wij treffen nu voorbereidingen om dat op een goede, en ook veilige manier te doen. Omdat het mogelijk om slachtoffers van alle regionale GGD'en kan gaan, hebben wij wel een volmacht van alle GGD'en nodig om dit te kunnen doen.

In de bijlage treffen jullie de volmachtiging aan alsmede een tekenblad voor ieder van jullie. Wij willen jullie vragen om het tekenblad voor jullie eigen GGD te ondertekenen en **uiterlijk dinsdag 2 maart** aan ons terug te sturen, naar het mailadres directie@ggdghor.nl .

Met vriendelijke groet,

[redacted]

Drs. [redacted]
[redacted]

16.7

GGD GHOR Nederland
Zwarte Woud 2
3524 SJ Utrecht

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

Dit bericht is uitsluitend bestemd voor de geadresseerde. Het bericht kan vertrouwelijke informatie bevatten. Als u dit bericht per abuis hebt ontvangen, wordt u verzocht het te vernietigen en de afzender te informeren. GGD GHOR Nederland is niet aansprakelijk voor onjuiste en onvolledige overbrenging van de inhoud van een verzonden e-mail bericht, of een te late ontvangst daarvan.

16.8
Archived: donderdag 12 mei 2022 09:49:34
From: [redacted]
Sent: vrijdag 19 maart 2021 16:43:58
To: [redacted]ra
Subject: RE: aantallen gedupeerden
Importance: Normal
Sensitivity: None

Dat zijn er 37

[redacted]

[redacted]

Hart voor Brabant

Pettelaarpark 10

's-Hertogenbosch

Postbus 3024
5003 DA Tilburg

www.ggdhvb.nl

[redacted]@ggdhvb.nl

Afwezig op woensdag

Gezond doet leven!

Van: [redacted]@ggdhvb.nl>
Verzonden: vrijdag 19 maart 2021 16:19
Aan: [redacted]@ggdhvb.nl>; [redacted]@ggdhvb.nl>; [redacted]@ggdhvb.nl>
Onderwerp: aantallen gedupeerden

Hoi [redacted]

Weet jij hoeveel gedupeerden wij als GGD Hvb hebben? Begrijp nu in de meeting dat we al aantallen hebben.

Met vriendelijke groeten,

[redacted]

[redacted]

[redacted]

Hart voor Brabant

Pettelaarpark 10 Den Bosch

Postbus 3024, 5003 DA Tilburg

www.ggdhvb.nl

[redacted]

[redacted]@ggdhvb.nl

Aanwezig op: ma-di-wo-do

Gezond doet leven!

16.9
Archived: donderdag 12 mei 2022 09:49:40
From: [redacted]
Sent: dinsdag 20 juli 2021 13:43:51
To: [redacted]
Cc: [redacted]
Subject: RE: E-mail m.n.t. gegevensdiefstal
Importance: Normal
Sensitivity: None

Hallo collega's,

Ik adviseer de klant te verwijzen naar de GGD GHOR website: https://ggdghor.nl/thema/vragen-antwoorden-datadiefstal/

Daarop wordt de laatste stand van zaken vermeld.

Uitgangspunt is dat inmiddels de gedupeerden schriftelijk zijn geïnformeerd indien zij betrokken zijn bij de datadiefstal. Indien deze burger geen brief heeft gehad, kan hij ervan uitgaan dat zijn gegevens niet zijn aangetroffen.

Het politieonderzoek is nog niet afgerond.

Met vriendelijke groeten,

[redacted]

[redacted]

[redacted]

GGD Hart voor Brabant

Pettelaarpark 10 Den Bosch

Postbus 3024, 5003 DA Tilburg

www.ggdhvb.nl

[redacted]

[redacted]@ggdhvb.nl

Aanwezig op: ma-di-wo-do

Gezond doet leven!

Van: [redacted]@ggdhvb.nl>
Verzonden: dinsdag 20 juli 2021 11:40
Aan: [redacted]d@ggdhvb.nl>
CC: C[redacted]@ggdhvb.nl>; [redacted]@ggdhvb.nl>
Onderwerp: E-mail m.n.t. gegevensdiefstal

Goedemorgen [redacted]

Zou je kunnen bevestigen hoe om te gaan met de onderstaande e-mail m.b.t. de gegevensdiefstal eerder dit jaar?

- Onderwerp **Re: FW: Mijn persoonsgegevens**

- Van"[redacted]@meerkat.eu
- Datum14-7-2021 16:47:06
- Aan"GGD Hart voor Brabant Klantcontactcentrum" contact@ggdhvb.nl

Geachte lezer,

Een half jaar na voorgaande mail ontvang ik graag een update, alvast hartelijk dank.

Met vriendelijke groet,

[redacted]

Van: GGD Hart voor Brabant Klantcontactcentrum contact@ggdhvb.nl
Verzonden: vrijdag 29 januari 2021 10:10
Aan: [redacted]@meerkat.eu
Onderwerp: RE: FW: Mijn persoonsgegevens

Beste meneer [redacted],

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 is het onze plicht u daarover te informeren en dat zullen wij dan ook doen.

Met vriendelijke groet,

[redacted]
Medewerker Klant Contact Centrum

Reitseplein 3, 5037 AA Tilburg
Postbus 3024, 5003 DA Tilburg
www.ggdhvb.nl

contact@ggdhvb.nl
0900 463 64 43

Gezond doet leven!

Van: "GGD Hart voor Brabant" infoHvB@ggdhvb.nl
Aan: "GGD Hart voor Brabant Klantcontactcentrum" contact@ggdhvb.nl
CC:
Verzonden: 29-1-2021 09:03:30
Onderwerp: FW: Mijn persoonsgegevens
Van: [redacted]@meerkat.eu
Verzonden: donderdag 28 januari 2021 22:47
Aan: GGD Hart voor Brabant infoHvB@ggdhvb.nl
Onderwerp: Mijn persoonsgegevens
Geachte lezer,
Na berichtgeving over het datalek bij de GGD verneem ik graag onverwijld of ook mijn persoonsgegevens en die van mijn vrouw en dochter zijn uitgelekt en/of verhandeld.
Dit om mij ervan te verzekeren dat er tengevolge van dit lek geen identiteitsdiefstal met onze gegevens is of gaat worden gepleegd. Daar lopen wij, met meerdere coronatests achter de rug, een gerede kans op.
Spijtig dat het volgen van overheidsadvies deze vervelende consequenties heeft. Dat geeft mijn doorgaans stabiele vertrouwen in diezelfde overheid een flinke knauw.

Ik zie uit naar een spoedig contact, zodat ik weet welk risico wij lopen en maatregelen kan treffen waardoor verdere schade als gevolg van uw gebrek aan zorgvuldigheid vermeden kan worden.
Het uitblijven van een spoedig antwoord zal ik opvatten als een extra uiting van nalatigheid, die in een eventueel juridisch proces zal bijdragen aan het opbouwen van een zaak tegen de GGD.
Ik ben bereikbaar op onderstaand nummer of mailadres.
Vriendelijke groet,

[redacted]

Mobiel [redacted]
Mail [redacted]

Met vriendelijke groet,

[redacted]

[redacted]

GGD Hart voor Brabant

Reitseplein 3, 5037 AA Tilburg

Postbus 3024, 5003 DA Tilburg

www.ggdhvb.nl

[redacted]

[redacted]@ggdhvb.nl

Gezond doet leven!

16.10
Archived: donderdag 12 mei 2022 09:49:47
From: [redacted]
Sent: donderdag 20 mei 2021 09:05:15
To: [redacted]
Subject: RE: Gedupeerden datadiefstal
Importance: Normal
Sensitivity: None

Dankjewel voor je bericht. Ik heb alles ontvangen en er zijn in totaal 40 brieven verstuurd.

Met vriendelijke groeten,

[redacted]

GGD Hart voor Brabant
Gezond doet leven!
Pettelaarpark 10 Den Bosch
Postbus 3024, 5003 DA Tilburg
www.ggdhvb.nl
[redacted]@ggdhvb.nl
Aanwezig op: ma-di-wo-do

Van: [redacted]@ggdhvb.nl>
Verzonden: woensdag 19 mei 2021 21:53
Aan [redacted]@ggdhvb.nl>; [redacted]@ggdhvb.nl>
Onderwerp: RE: Gedupeerden datadiefstal

Hi [redacted]:

Op jouw vragen:

- De 2e ronde zijn er in onze regio nog 4 of 5 brieven verstuurd;
- Als het goed is heb jij via [redacted] inmiddels de beide bestanden ontvangen (incl ww).

Hartelijke groet,
[redacted]

Van: [redacted]@ggdhvb.nl>
Verzonden: woensdag 19 mei 2021 12:16
Aan: [redacted]@ggdhvb.nl>
CC: [redacted]@ggdhvb.nl>
Onderwerp: FW: Gedupeerden datadiefstal

Hallo [redacted],

Ik heb een tweetal vragen:

1. Voor de AB/DB brief ben ik op zoek naar het aantal gedupeerde burgers nav datadiefstal die zijn aangeschrevenen in 2e ronde:
   In de 1e ronde zijn voor onze GGD 37 gedupeerde burgers aangeschreven. Later heeft de GGD GHOR nog 237 brieven verstuurd. Weet jij of in de tweede ronde nog burgers van onze GGD zijn aangeschreven?

   Dit kan je mogelijk terugzien in de mailbox van [redacted] want GGD GHOR heeft alleen de DGP geïnformeerd (zie mail van C[redacted] helemaal onderdaan). [redacted] en [redacted] kunnen deze vraag niet beantwoorden. Het natuurlijk ook zomaar zijn dat er niet meer burgers van onze GGD HvB gedupeerd zijn.

   Kan jij dit voor mij nagaan? Graag uiterlijk morgen als dat lukt….

2. Archiveren ontvangen lijst:
   [redacted] vroeg een hele tijd geleden waar de lijst gearchiveerd kan worden (zie onderstaand mailverkeer). Mocht dit nog gewenst zijn, dan zie ik de lijst wel verschijnen.

Ik hoor het graag,

Met vriendelijke groeten,

[redacted]

Hart voor Brabant
Pettelaarpark 10 Den Bosch
Postbus 3024, 5003 DA Tilburg
www.ggdhvb.nl
[redacted]@ggdhvb.nl
Aanwezig op: ma-di-wo-do
Gezond doet leven!

Van: [redacted]@ggdhvb.nl>
Verzonden: donderdag 15 april 2021 17:33
Aan: [redacted]@ggdhvb.nl>
CC: [redacted]@ggdhvb.nl>; [redacted]@ggdhvb.nl>
Onderwerp: FW: Gedupeerden datadiefstal

Hoi [redacted]

Aanstaande maandag staat het onderwerp archivering op d MT agenda.

Onderstaand reactie vanuit [redacted] op jouw verzoek van enige tijd geleden.
Je kunt de informatie aan [redacted] mailen, zij zal het dan archiveren.

Groet
[redacted]

Van: [redacted]@ggdhvb.nl>
Verzonden: donderdag 15 april 2021 13:14
Aan: [redacted]@ggdhvb.nl>

Onderwerp: FW: Gedupeerden datadiefstal 16.10

Hallo [redacted]

Je had aan mij gevraagd om na te gaan waar we de lijst met namen (betrokkene) van de datadiefstal heb beste kunne archiveren.

Zier hieronder het antwoord.

Met vriendelijke groeten,

[redacted]

GGD Hart voor Brabant
Gezond doet leven!
Pettelaarpark 10 Den Bosch
Postbus 3024, 5003 DA Tilburg
www.ggdhvb.nl
[redacted]@ggdhvb.nl
Aanwezig op: ma-di-wo-do

Van: [redacted]@hetservicecentrum.nl>
Verzonden: donderdag 15 april 2021 12:43
Aan: [redacted]@ggdhvb.nl>
Onderwerp: FW: Gedupeerden datadiefstal

Ha [redacted],

Ik heb gister nog even ruggenspraak met [redacted] gehad (Corona archivaris) over jouw vraag.
Jullie insteek om het op te slaan op jullie eigen teamsite is juist, zoals door jou verwoord: ""Mijn voorstel zou zijn om dit als een 'gewoon' datalek te bewaren. Ik kan een dossier aanmaken op SharePoint waar alleen [redacted] en ik toegang toe hebben.'

Met daarbij wel opgemerkt dat als er algemene mails met informatie over het datalek Corona is geweest, dit dan wel apart op jullie teamsite op te slaan in een apart dossier Corona datalek zonder privacy gegevens. Als het mettertijd gearchiveerd wordt door jullie, dan kunnen we het als bewaararchief Hotspot Corona aanmerken. Op deze manier is de algemene correspondentie rond om het datalek gewaarborgd en staat het los van de privacy gegevens.

Tenzij de algemene correspondentie over het datalek al is opgeslagen op de teamsite Corona dan hoeven jullie het niet apart op te slaan.

Indien er nog vragen zijn, dan hoor ik het wel.
Fijne dag verder.

Met vriendelijke groeten,

[redacted]

Reitseplein 3 5037 AA Tilburg
[redacted]

16.10

Postbus 3024, 5003 DA Tilburg

[redacted]@hetservicecentrum.nl
Aanwezig op: ma-wo-do

Hét Service Centrum: *het shared service center van GGD Hart voor Brabant, GGD West-Brabant, GGD Noord- en Oost-Gelderland en de Regionale Ambulancevoorziening Brabant Midden-West-Noord*

Van: [redacted]@hetservicecentrum.nl>
Verzonden: dinsdag 30 maart 2021 13:27
Aan: [redacted]@ggdhvb.nl>
Onderwerp: Re: Gedupeerden datadiefstal

Hoi [redacted]

Even een korte reactie. Ik ben nl. ziek thuis.
Volgens mij is jullie insteek juist.

Maar ik kom hier zo gauw ik beter ben op terug. Nu niet in de gelegenheid om het uit te kunnen zoeken.

Mvrgr [redacted]

Outlook voor Android downloaden

From: [redacted]@ggdhvb.nl>
Sent: Friday, March 26, 2021 12:32:05 PM
To: [redacted]@hetservicecentrum.nl>
Subject: FW: Gedupeerden datadiefstal

Hallo [redacted]

Ik heb onderstaande vraag gekregen van [redacted] Samengevat is de vraag:

Onze DPG heeft een PDF-bestand ontvangen, voorzien van een wachtwoord, waarin alle burgers met naam en toenaam genoemd worden die slachtoffer zijn van de datadiefstal bij de GGD GHOR.

Waar en hoe kan een dergelijk bestand het beste gearchiveerd worden?

Ik hoor het graag,

Met vriendelijke groeten,

[redacted]

Hart voor Brabant

Pettelaarpark 10 Den Bosch
Postbus 3024, 5003 DA Tilburg
www.ggdhvb.nl

[redacted]@ggdhvb.nl
Aanwezig op: ma-di-wo-do

Gezond doet leven!

Van: [redacted]@ggdhvb.nl>
Verzonden: dinsdag 23 maart 2021 17:09
Aan: [redacted]@ggdhvb.nl>
Onderwerp: RE: Gedupeerden datadiefstal

Goed idee om de archivaris nog even mee te laten denken.

Van: [redacted]@ggdhvb.nl>
Verzonden: dinsdag 23 maart 2021 11:14
Aan: [redacted]@ggdhvb.nl>
Onderwerp: RE: Gedupeerden datadiefstal

Hoi [redacted]

Ja lastige vraag. Ik weet niet of er een aparte plek is om deze gegevens te bewaren.

Mijn voorstel zou zijn om dit als een 'gewoon' datalek te bewaren. Ik kan een dossier aanmaken op sharepoint waar alleen [redacted] en ik toegang toe hebben.

Of we kunnen onze archivaris nog even laten meedenken.

Met vriendelijke groeten,

[redacted]

GGD Hart voor Brabant
Pettelaarpark 10 Den Bosch
Postbus 3024, 5003 DA Tilburg
www.ggdhvb.nl
[redacted]@ggdhvb.nl
Aanwezig op: ma-di-wo-do
Gezond doet leven!

Van: [redacted]@ggdhvb.nl>
Verzonden: maandag 22 maart 2021 21:48
Aan: [redacted]@ggdhvb.nl>
Onderwerp: Fwd: Gedupeerden datadiefstal

Hoi [redacted]

Is daar een aparte plek voor t filen van deze info?
Groet
[redacted]

Outlook voor Android downloaden

Van: [redacted]@ggdhvb.nl>
Verstuurd: maandag 22 maart 2021 21:33
Aan: [redacted]
Onderwerp: FW: Gedupeerden datadiefstal

Hi [redacted]

Wil jij me laten weten wat de juiste wijze is om deze informatie bij onze GGD te archiveren?

Hartelijke groet,
[redacted]

Van: [redacted]@ggdghor.nl>
Verzonden: maandag 22 maart 2021 17:47
Aan: [redacted]@ggdhvb.nl>
Onderwerp: Gedupeerden datadiefstal

Beste DPG,

Zoals bekend hebben afgelopen vrijdag de circa 1.000 gedupeerden van de datadiefstal, die op dit moment bekend zijn bij ons, een brief ontvangen. Zoals afgesproken ontvang je vandaag de afschriften van de brieven die binnen je regio zijn verstuurd. Dit doen wij - vanuit veiligheidsoverwegingen - door middel van een PDF-bestand voorzien van een wachtwoord. In deze e-mail vind je de instructie om de bestanden te kunnen benaderen.

Werkwijze
Als DPG ontvangt je hierbij een e-mail die alleen aan jou is gericht met in de bijlage één PDF-bestand. Hierin zijn alle brieven van gedupeerden in jouw regio opgenomen. Vanuit veiligheidsoverwegingen is dit bestand voorzien van een wachtwoord en kan er geen tekst uit het bestand gekopieerd worden. Printen van het bestand is eveneens om die reden onmogelijk gemaakt. Hierbij het nadrukkelijke verzoek om dit bestand na ontvangst conform de geldende privacyrichtlijnen op te slaan en te gebruiken.

Inzien van bestanden
Het bestand wordt met een wachtwoord aangeboden. Om het bestand te openen ontvang je als DPG een APP-bericht met daarin een code. Deze code wordt in de loop van de middag of begin van de avond door mij verstrekt en vormt het wachtwoord waarmee het bestand beveiligd is.
Mocht deze mail nog vragen oproepen, dan hoor ik dat graag.

Met vriendelijke groet,
[redacted]

Drs. [redacted]
[redacted]

GGD GHOR Nederland
Zwarte Woud 2

3524 SJ 'a0 Utrecht 16-10

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

Dit bericht is uitsluitend bestemd voor de geadresseerde. Het bericht kan vertrouwelijke informatie bevatten. Als u dit bericht per abuis hebt ontvangen, wordt u verzocht het te vernietigen en de afzender te informeren. GGD GHOR Nederland is niet aansprakelijk voor onjuiste en onvolledige overbrenging van de inhoud van een verzonden e-mail bericht, of een te late ontvangst daarvan.

16.11
Archived: donderdag 12 mei 2022 09:49:59
From: [redacted]
Sent: vrijdag 19 maart 2021 09:08:18
To: [redacted]
[redacted] Maassen, Bart
Subject: RE: Gegevens datalek GGD Hart voor Brabant
Importance: Normal
Sensitivity: None
Attachments:
20210315 - brief gedupeerden datadiefst GGD_def in sjabloon - getekend.docx;

Ha [redacted] ik adviseer inderdaad om dit te delen met de bestuurders, omdat het hun eigen inwoners betreft, het mogelijk hernieuwde media-aandacht en raadsvragen oplevert en we eerder hebben toegezegd hen te informeren bij nieuwe ontwikkelingen in dit dossier. Mijn voorstel is om het te doen in de vorm van een korte mail van jou aan het AB. De kern:

- Refereren aan eerdere brief/mails over de datadiefstal, waarin we uiteen hebben gezet wat wij doen aan dat onderwerp
- Melden dat vandaag 37 van onze inwoners (en in de rest van Nederland) een brief krijgen die door GGD GHOR NL namens de GGD is verstuurd
- Dat in de brief mensen worden gewezen op de risico's van identiteitsfraude
- Procesinfo: dat wij de gedupeerden informeren waar ze terecht kunnen met vragen

[redacted] is vandaag vrij. Ik eigenlijk ook. [redacted] ik durf het bijna niet te vragen, maar kun jij dit vandaag oppakken?

Van: [redacted]@ggdhvb.nl>
Verzonden: donderdag 18 maart 2021 22:55
Aan: [redacted]@ggdhvb.nl>; [redacted]@ggdhvb.nl>
Onderwerp: FW: Gegevens datalek GGD Hart voor Brabant

Ter info over de datadiefstal. Ik stuur deze info ook naar [redacted] door. Graag jullie advies of we dit bericht delen met ons bestuur en op welke wijze we dat dan doen…

Hartelijke groet,

[redacted]

Van: [redacted]@ggdghor.nl>
Verzonden: donderdag 18 maart 2021 17:06
Aan: [redacted]n@ggdhvb.nl>
CC: [redacted]@ggdghor.nl>; [redacted]@ggdghor.nl>; [redacted]@ggdghor.nl>
Onderwerp: Gegevens datalek GGD Hart voor Brabant

Beste DPG,

Bij deze geef ik graag een update over het informeren van de gedupeerden van de datadiefstal.

Gistermiddag 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 37 gedupeerden.

Wij 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.

De brieven worden vanmiddag gepost en zullen morgen (vrijdag) bij de gedupeerden worden bezorgd.

Uiterlijk 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.

Mocht je nog vragen hebben, dan kun je contact zoeken met [redacted]@ggdghor.nl) of met ondergetekende.

Met vriendelijke groet,

[redacted]

Drs. [redacted]

GGD GHOR Nederland
Zwarte Woud 2
3524 SJ Utrecht

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

Dit bericht is uitsluitend bestemd voor de geadresseerde. Het bericht kan vertrouwelijke informatie bevatten. Als u dit bericht per abuis hebt ontvangen, wordt u verzocht het te vernietigen en de afzender te informeren. GGD GHOR Nederland is niet aansprakelijk voor onjuiste en onvolledige overbrenging van de inhoud van een verzonden e-mail bericht, of een te late ontvangst daarvan.

16.12
Archived: donderdag 12 mei 2022 09:50:31
From: [redacted]
Sent: woensdag 17 maart 2021 13:05:50
To: [redacted]
Cc: [redacted]
Subject: RE: informeren gedupeerden data diefstal
Importance: Normal
Sensitivity: None

Dag [redacted] heb je feedback van GGD GHOR NL gehad op je commentaren?

Van: [redacted]@ggdhvb.nl>
Verzonden: woensdag 10 maart 2021 19:22
Aan: [redacted]@ggdghor.nl>; [redacted]@ggdghor.nl>; [redacted]@ggdghor.nl
CC: [redacted]@ggdhvb.nl>; [redacted]@ggdhvb.nl>; [redacted]@ggdhvb.nl>
Onderwerp: FW: informeren gedupeerden data diefstal
Urgentie: Hoog

Hallo collega's,

Ik heb bijgaande brief van mijn DPG ontvangen en wil middels deze mail op de inhoud van de brief reageren, ervan uitgaande dat dit nog een concept brief is.

Wat mij opvalt zijn de volgende zaken:

- In het onderwerp en de eerste zin wordt geschreven: de datadiefstal die bij de GGD'en heeft plaatsgevonden. Dit is niet correct, de datadiefstal heeft bij de GGD GHOR plaatsgevonden waarbij data van de GGD'en is gelekt.
- De burger hoeft niet ingelicht te worden over hoeveel betrokkenen het gaat. Het moet een brief zijn die op de individuele burger is geschreven. Mijn advies is om de brief te beginnen met het feit dat er een vervelend incident heeft plaatsgevonden bij de GGD GHOR, tw de datadiefstal, waarbij uw persoonsgegevens helaas onbevoegd zijn ingezien, gestolen en mogelijk doorverkocht.
- Wat is er gebeurd: in deze alinea licht je toe wat er gebeurd is en niet wat de GGD GHOR heeft gedaan. In Jip en Janneke taal leg je uit dat medewerkers print screens hebben gemaakt en deze hebben doorverkocht etc. Nu zeg je eigenlijk niet wat er gebeurd is. Het is een gedeeltelijke herhaling van de 1e alinea. Ook geef je geen antwoord op de vraag die gesteld wordt in alinea 1 'hoe heeft dit kunnen gebeuren'.
- Welke maatregelen hebben wij getroffen? Mijn advies is in deze alinea te noemen dat wij onze verantwoordelijkheid voor het beschermen van de dat zeer serieus nemen. Benoem de maatregelen die GGD GHOR heeft genomen en hou het daar ook bij. Maak er geen politieverhaal van, maar geeft weer welke acties door de GGD GHOR zijn uitgevoerd. En benoem zijdelings dat de politie en het OM nog nader onderzoek doet.

Ik zie graag een reactie tegemoet,

Met vriendelijke groeten,

[redacted]

[redacted]

Hart voor Brabant

Pettelaarpark 10 Den Bosch

Postbus 3024, 5003 DA Tilburg

www.ggdhvb.nl

[redacted]@ggdhvb.nl

Aanwezig op: ma-di-wo-do

Gezond doet leven!

16.13
Archived: donderdag 12 mei 2022 09:45:16
From: [redacted]n
Sent: donderdag 25 november 2021 10:14:35
To: [redacted]
Cc: [redacted]
Subject: RE: rapport AP
Importance: Normal
Sensitivity: None

Prima bericht. In blauw mijn toevoeging.

Groet,

[redacted]

Van: [redacted]@ggdhvb.nl>
Verzonden: donderdag 25 november 2021 09:19
Aan: [redacted]@ggdhvb.nl>; [redacted]@ggdhvb.nl>
CC: [redacted]@ggdhvb.nl>
Onderwerp: RE: rapport AP

Dag [redacted] een kleine verduidelijkende aanvulling.

Van: [redacted]@ggdhvb.nl>
Verzonden: woensdag 24 november 2021 08:12
Aan: [redacted]@ggdhvb.nl>; [redacted]@ggdhvb.nl>
CC: [redacted]@ggdhvb.nl>
Onderwerp: RE: rapport AP

Goedemorgen [redacted] en [redacted]

Zie onderstaande vraag van [redacted] Ik heb de rood gearceerde tekst toegevoegd. Willen jullie aub aanvullen.

Gr [redacted]

Van: [redacted]@ggdhvb.nl>
Verzonden: donderdag 18 november 2021 08:28
Aan: [redacted]@ggdhvb.nl>
Onderwerp: rapport AP

Dag [redacted]

In de volgende DB-vergadering doen we een mededeling over het AP-rapport over de datalekken bij de GGD, zie de concept tekst hieronder.

16.13
Nu moeten er nog een paar zinnen bij over onze eigen acties of ons commentaar, misschien wel geknipt en geplakt uit eerdere teksten.

Kun jij daarvoor zorgen?

Omschrijving 1. **Rapport onderzoek datalekken**

De Autoriteit persoonsgegevens (AP) heeft onderzoek naar datadiefstal gedaan bij GGD GHOR Nederland en twee GGD'en (niet de onze). De bevindingen richten zich op de informatiebeveiliging en AVG waarborgen rondom CoronIT en HPzone(Lite). Haar conclusie: er zijn verbetermaatregelen waardoor het risico op datalekken is verminderd. Maar de AP ziet nog wezenlijke risico's voor de beveiliging van persoonsgegevens: er zijn geen duidelijke afspraken tussen organisaties over bepaalde beveiligingsaspecten, bijvoorbeeld rond het autorisatiebeheer en de controle van logbestanden. Verder leidt het vervangen van een systeem niet zonder meer tot een betere beveiliging. Uiterlijk

1 maart 2022 moeten GGD GHOR Nederland en de betrokken GGD'en aan de Autoriteit Persoonsgegevens (AP) een voortgangsrapportage opleveren van de genomen en te nemen maatregelen ter beveiliging van de persoonsgegevens.

De GGD Hart voor Brabant heeft direct na de datadiefstal nogmaals een check uitgevoerd op de VOG verklaringen, de autorisaties nagelopen, een autorisatiematrix opgesteld en controles op correct gebruik van systemen uitgevoerd. Tevens is de GGD Hart voor Brabant voornemens aan de NEN norm "informatiebeveiliging in de zorg" (7510/12/13) te gaan voldoen. Hiervoor is inmiddels een traject met KPMG opgestart.

Groeten,

[redacted]

GGD Hart voor Brabant
Gezond doet leven!

Postbus 3024, 5003 DA Tilburg
www.ggdhvb.nl

[redacted]@ggdhvb.nl
[redacted]

16.14
Archived: donderdag 12 mei 2022 09:45:23
From: [redacted]
Sent: woensdag 3 februari 2021 16:41:45
To: [redacted]
Subject: RE: STRIKT VERTROUWELIJK: mail van [redacted] i.v.m. datadiefstal
Importance: Normal
Sensitivity: None

Dat snap ik [redacted] maar het is mij uitdrukkelijk gevraagd de info NIET te delen. Alleen met mijn bestuurder.

Van: [redacted]@ggdhvb.nl>
Verzonden: woensdag 3 februari 2021 16:26
Aan: [redacted]@ggdhvb.nl>; [redacted]@ggdhvb.nl>; [redacted]@ggdhvb.nl>; [redacted]@ggdhvb.nl>
Onderwerp: RE: STRIKT VERTROUWELIJK: mail van [redacted] i.v.m. datadiefstal
Urgentie: Hoog

Dag [redacted] dit bericht is ook voor [redacted] en [redacted] van groot belang, aangezien we met ons vieren de communicatie naar DB regisseren.

Ik hoor net van [redacted] dat we het DB bericht nog moeten spiegelen aan een landelijk bericht van GGD GHOR NL dat vanavond komt.

Ik haal dit als actiepunten uit de terugkoppeling:

- [redacted] oordeel en besluit (op ons advies) of de DB-notitie in deze vorm ons aansprakelijkheidsrisico niet vergroot. Maakt bijvoorbeeld de passage over gedeelde signalen ons nu juist sterker of zwakker?
- [redacted] zin over onderzoek AP moet uit DB-brief
- [redacted] willen we het beslispunt over juridisch advies wel of niet aanpassen? Moeten we melding maken van het verzoek om af te stemmen met Van Doorne?
- Allen: moeten we ons laten meeslepen in collectieve juridische ondersteuning en afstemming of onze eigen weg kiezen? We staan wellicht ook deels als GGD tegenover GGD GHOR NL. Zeker gezien onze vraag aan GGD GHOR NL vóór het tekenen van het convenant of er geen Data Protection Impact Assessment (DPIA) moet worden gedaan.
- [redacted] (?): zijn wij verzekerd tegen dit soort aansprakelijkheid?
- Allen: dit wordt m.i. een groot traject. Ik merk dat het nu voor ons allemaal heel veel tijd kost. Ik wil graag samen met jullie en [redacted] en [redacted] overwegen hoe het team eruit moet zien dat alle verbeteracties én AP-onderzoek en juridische vragen gaat oppakken en of we daarbij extra ondersteuning nodig hebben.
- Allen: bewaken van impact op medewerkers, ook juist degenen die in het voortraject hebben geadviseerd over de systemen en databeveiliging. Het kan zijn dat collega's zich ongemakkelijk voelen.

Van: [redacted]@ggdhvb.nl>
Verzonden: woensdag 3 februari 2021 15:41
Aan: [redacted]@ggdhvb.nl>; [redacted]o@ggdhvb.nl>
Onderwerp: FW: STRIKT VERTROUWELIJK: mail van Hugo Backx i.v.m. datadiefstal
Urgentie: Hoog

In vertrouwen. 16.14

DPG-raad gaat over gesprek met de AP van aanstaande vrijdag.

- Juristen zijn aangesloten;
- Bereiden onderzoek van de AP voor n.a.v. datalek;
- Onderzoek richt zich op beveiliging persoonsgegevens en informatieplicht betrokkenen;
- Algemene brief verzonden;
- In overleg met AP is onderzoek verplaatst naar vrijdag;
- Doel is interviews met betrokken medewerkers en vragen stellen tav beveiliging en aanpak;
- Onderzoek van 12 maart tot nu;
- Middels gesprekken, verslag, etc;
- In media al veel gecommuniceerd over datalek, datalek in de kamer, dus van belang is consistent reageren
- Er is meewerkingsplicht;
- We krijgen een instructie van de juristen hoe we moeten handelen als ze naar de ggd'en komen
- Brief is gericht aan de stichting, ggd'en en anderen. De AP's zijn nog zoekende, welke info is er en hoe verhouden wij ons tot elkaar als GGD'en en GGD GHOR;
- Behoefte aan tot welke rechtspersoon dit onderzoek zich richt. Het projectbureau ligt het meest voor de hand, maar komt nu niet goed uit de brief; zij spreken nu alle entiteiten aan. Hij is opgepakt vanuit GGD GHOR, maar eerste opdracht is om in beeld te brengen op welke entiteiten het onderzoek zich richt. Dat kan dus ook op de individuele GGD's, zijn maar in de introductie moet dit helder worden. Nu wordt het verhaal eerst generiek neergezet;
- Wat wordt onze strategie als DPG'en? Doen wij dit vanuit GGD GHOR, of juist decentraal? En hoe gaan we om met individuen die nu al bij ons claims neerleggen? Doen we dat zelf of gezamenlijk? Verzoek om Van Doorne hierin te betrekken door hen te informeren. We zoeken daarin wel dezelfde lijn. Dus ook inhoudelijk afstemmen. Hiervoor willen we graag een contactpersoon bij Van Doorne. Wij zijn wel zelf verwerkingsverantwoordelijk. We moeten voldoen aan wettelijke termijnen. Hierin advies de eigen FG te laten mee-adviseren, de termijnen in acht te nemen en adequaat te reageren. [redacted] er komt een landelijke richtlijn hiervoor. Dit is complex, omdat we te maken hebben met meerdere wetten en regelingen. Vrijdag verwachten we antwoord van de specialistische juridische ondersteuning die hiervoor is ingehuurd;
- Van Doorne is ingeschakeld met opdracht om dit eerst te verhelderen. Vrijdag wordt door Van Doorne gevraagd aan de AP om de onderzoeksvraag preciezer te formuleren. Dus er moet een nieuwe gerichte onderzoeksvraag komen gericht aan de juiste juridische entiteiten. Nu is onduidelijk wie er onderwerp van onderzoek zijn.
- Wat zijn mogelijke uitkomsten en consequenties?
- De vereniging en de stichting zijn opdrachtgever van Van Doorne.
- Kan geen kwaad om contact te leggen met eigen juridische ondersteuning, daar ga je zelf over als DPG. Advies [redacted] is wel juristen te informeren over het collectieve traject en vrijdag af te wachten voordat je ze echt aan de slag zet.
- [redacted] vraagt decharge voor haar portefeuille;
- [redacted] vindt ook dat wij veel te reactief zijn in onze communicatie. Kunnen we ons niet openstellen voor onderzoeken om het vertrouwen te herstellen. Advies Van Doorne om vrijdag af te wachten.
- Is het een voor- of nadeel om met 1 advocatenkantoor te werken vraagt [redacted] En de vraag of wij een voorziening moeten treffen ivm afsluiten boekjaar voor aansprakelijkheden; ook willen we vandaag een lijst met zaken waar we ons op moeten voorbereiden. Van Doorne: op het moment dat er een onderzoek gestart is, moet je dat bespreken met de accountant en opnemen. Van Doorne kan hierbij assisteren.
- [redacted] vraagt of het wel een keuze is op welke entiteit het onderzoek zich richt. (Nee zegt [redacted] dit vloeit voort uit de brief). De AP heeft eerder meegekeken en toen geen reden voor nader onderzoek gedaan. Wil de AP nu zijn straatje schoonvegen? [redacted] de AP is eerder gevraagd te komen kijken en toen hebben ze dat niet gedaan. Dat is onderdeel van onze reactie richting de AP dus dat speelt zeker mee (deze reactie wordt gedeeld na check bij Van Doorne);
- Te vroeg om conclusies te trekken over aansprakelijkheid zegt Van Doorne. De AP heeft afgelopen jaar meegedacht, maar niet echt constructief meegedacht, dat maakt dat de AP nu een onderzoek start en naar buiten wil brengen dat ze

hier scherp op zijn;

- We kunnen wel de bestuurder telefonisch informeren. Nu nog niet schriftelijk ([redacted] staat dit in de DB-brief? want dan moet het er nog even uit.) Dit moment horen we en er komt een landelijke brief.
- Vraag [redacted] zijn wij verzekerd tegen aansprakelijkheid??? Dat moeten we wel scherp houden. We moeten dus wel acteren richting onze verzekeraar. Zij vinden vaak ook nog iets over onze juridische ondersteuning.
- Reactie [redacted] nog niemand kan aantonen dat zijn gegevens door de GGD gelekt zijn en ons daarvoor aansprakelijk zijn. Er kan natuurlijk morgen wel een stichting worden opgericht voor mensen die de belangen behartigt van de (potentiële) gedupeerden;
- Vraag [redacted] wanneer communiceren we naar inwoners?
- [redacted] wat wordt de verwachte doorlooptijd van het onderzoek, wat gaat het opleveren in bevindingen en maatregelen en heeft dit consequenties voor de beslissing voor het vervangen van HP Zone?
- [redacted] iedere GGD richt nu een eigen teampje in en waar is nu de landelijke projectstructuur met aanspreekpunten centraal voor onze mensen? We werken mee aan alles wat nodig is maar we zitten ook nog in een pandemie. Natuurlijk moeten we ons achteraf verantwoorden, maar we zijn van de pandemiebestrijding. Plaats het in dit perspectief aub.
- Voor HP Zone zijn wij als DPG'en al heel snel allemaal aan de beurt zegt [redacted] Dus de verwachting is dat dit 25 onderzoeken moeten gaan worden.
- Oproep denk ook aan de communicatie naar onze medewerkers!
- NB. Niet communiceren (inhoudelijke discussies) via whats app

Hartelijke groet,

[redacted]

Van: [redacted]@ggdghor.nl>
Verzonden: woensdag 3 februari 2021 12:32
Aan: [redacted]@ggdghor.nl>
Onderwerp: STRIKT VERTROUWELIJK: mail van [redacted] i.v.m. datadiefstal
Urgentie: Hoog

Beste mensen,

Gisteren zijn wij door de Autoriteit Persoonsgegevens (AP) geïnformeerd dat zij naar aanleiding van het datalek, dat bij hen op 22 januari 2021 is gemeld, een nader onderzoek zijn gestart naar Stichting Projectenbureau Publieke Gezondheid en Veiligheid Nederland, GGD GHOR Nederland en/of de regionale GGDen, en eventueel andere aan deze organisaties verbonden rechtspersonen (zie bijlage). De AP heeft een sterk vermoeden dat de GGD de AVG heeft overtreden en maakt zich ernstige zorgen over de beveiliging van het grote aantal (bijzondere) persoonsgegevens van burgers waarover de GGD beschikt, zo meldt zij in hun brief aan ons (bijlage). Naar verwachting brengt de AP nog deze week een bezoek aan GGD GHOR Nederland voor nader onderzoek. Wij zullen ons daarbij laten bijstaan door het advocatenkantoor Van Doorne. Wij werken vanzelfsprekend volledig mee met het onderzoek en geven het alle aandacht die nodig is.

Vanmiddag willen we tijdens de extra DPG-vergadering hierover met jullie verder in gesprek.

Met vriendelijke groet,

[redacted]

[redacted]

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.

16.14

Zwarte Woud 2
3524 SJ Utrecht

E-mail : [redacted]@ggdghor.nl
Website : www.ggdghor.nl

Dit bericht is uitsluitend bestemd voor de geadresseerde. Het bericht kan vertrouwelijke informatie bevatten. Als u dit bericht per abuis hebt ontvangen, wordt u verzocht het te vernietigen en de afzender te informeren. GGD GHOR Nederland is niet aansprakelijk voor onjuiste en onvolledige overbrenging van de inhoud van een verzonden e-mail bericht, of een te late ontvangst daarvan.

16.15
Archived: donderdag 12 mei 2022 09:45:45
From: [redacted]
Sent: dinsdag 26 januari 2021 14:23:35
To: [redacted]
Subject: VERTROUWELIJK-NIET VERSPREIDEN Update incident
Importance: Normal
Sensitivity: None

Dag allen,

Gisteren is een nieuwsbericht uitgezonden over het vermeend datadiefstal uit CoronIT en HPZone. Ook RTL nieuws heeft hier uitgebreid over bericht. Dit raakt ons allemaal. In ons werk, maar ook als mens. Graag willen wij jullie informeren over de tot nu toe genomen stappen en de vervolgstappen:

- De politie en wijzelf voeren op dit moment onderzoek uit naar de precieze toedracht. Daarover mogen wij jullie - in het belang van het onderzoek - geen mededelingen doen.
- Natuurlijk hebben wij al de nodige maatregelen genomen en zullen wij nog meer maatregelen nemen om diefstal van data te voorkomen.
- Na het bekend worden van het incident is een voorlopige melding gemaakt bij de Autoriteit Persoonsgegevens (AP), waarin zowel CoronIT als HPZone in worden vermeld.
- De AP heeft hierop contact opgenomen en vragen gesteld over HPZone.

Hoe nu verder:

- Deze vragen gaan we centraal beantwoorden vanuit GGD GHOR Nederland. Die afspraak is gemaakt met jullie DPG'en; reden is dat de GGD'en en GGDGHOR Nederland samen in deze crisis staan. Voor de buitenwacht zijn we 1. Zo worden we ook aangesproken. Wij kunnen ons met elkaar niet permitteren om dit nu niet vanuit 1 punt op te pakken.
- Natuurlijk komen we bij jullie op de lijn, wanneer we jullie hulp nodig hebben bij de beantwoording. En we houden jullie op de hoogte van de antwoorden die wij geven.
- Word je zelf benaderd door de AP, neem dan altijd eerst contact met ons op, voor je vragen beantwoordt zodat we samen bewaken dat we consequent antwoorden.

Zoals gezegd, wij zullen zorgen voor de coördinatie van dit lek, zodat de antwoorden centraal blijven. Indien er updates zijn, zullen jullie DPG'en en jullie op de hoogte worden gesteld. Wij weten dat jullie vragen hebben, maar wij zijn op dit moment aan het werk om alle details boven water te krijgen. Wij willen daarom vragen om jullie begrip en geduld.

Met vriendelijke groeten,

[redacted]

[redacted]

GGD GHOR NEDERLAND

Zwarte Woud 2 E-mail: [redacted]@ggdghor.nl

3524 SJ Utrecht Mobiel: [redacted]

Dit bericht is uitsluitend bestemd voor de geadresseerde. Het bericht kan vertrouwelijke informatie bevatten. Als u dit bericht per abuis hebt ontvangen, wordt u verzocht het te vernietigen en de afzender te informeren. GGD GHOR Nederland is niet aansprakelijk voor onjuiste en onvolledige overbrenging van de inhoud van een verzonden e-mail bericht, of een te late ontvangst daarvan.

Wob-verzoek SOLV/ICAM datalek 2021 coronasysteem

17.0 Tekst Wob-verzoek en register documenten

Tekst verzoek (overig)

Cliente 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 lT-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.

Register

Een screenshot van de verkennerpagina van map Overig:

17.10 20210208 A...ing en ..._Zwartge

17.12 Annotatie Vol...rt _Zwartgemaakt

17.14 Landelijke da...Hart voor Brabant

17.15 Opmerkinge...ten_Zwartgemaakt

17.16 Technische v....v. Kadernota 2022

17.17 Update Coro...bruari 2021 - (DEF

17.2 2.4 Verwerkin...OR Nederland v1.1

17.3 07 Tekenblad...Hart voor Brabant

17.4 07 Tekenblad...ant_Zwartgemaakt

17.5 210129 Inform...tal_Zwartgemaakt

17.6 210204 DB u...ie 3_Zwartgemaakt

17.7 210222 Versla...na_Zwartgemaakt

17.8 210413 Versla...na_Zwartgemaakt

17.9 210909 Versl...ona_Zwartgemaakt

DEZE VERWERKERSOVEREENKOMST IN DE ZIN VAN ARTIKEL 28 AVG (deze "**Verwerkersovereenkomst"**) is getekend op 1 september 2021,

TUSSEN:

(1) De Gemeentelijke Gezondheidsdienst Hart voor Brabant, gevestigd te 's-Hertogenbosch aan het Pettelaarpark 10, ingeschreven in het handelsregister onder KvK nummer 17247544, hierna eveneens te noemen "**GGD**", rechtsgeldig vertegenwoordigd door mevrouw [redacted] (de **"Verwerkingsverantwoordelijke**"); [en]

(2) 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 mevrouw [redacted] (de **"Verwerker**").

De partijen bij deze Verwerkersovereenkomst worden hierna gezamenlijk ook aangeduid als de **Partijen** en ieder als een **Partij**.

OVERWEGENDE DAT:

(A) Verwerkingsverantwoordelijke persoonsgegevens verwerkt in de zin van de 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 (algemene verordening Gegevensbescherming) (de "**AVG**"), waaronder maar niet beperkt tot persoonsgegevens inzake haar GGD Contact waarvan zij het doel van en de middelen voor vaststelt en daarom kwalificeert als verwerkingsverantwoordelijke in de zin van artikel 4 lid 7AVG;

(B) Partijen de Dienstverleningsovereenkomst GGD GHOR – GGD generieke ICT-diensten ten behoeve van GGD Contact met ingangsdatum 7 juli 2021 hebben gesloten (de "Dienstverleningsovereenkomst").;

(C) In het kader van de uitvoering van de Dienstverleningsovereenkomst Verwerkingsverantwoordelijke aan Verwerker direct en/of indirect persoonsgegevens zal verstrekken en/of Verwerker toegang zal verkrijgen tot persoonsgegevens van Verwerkingsverantwoordelijke;

(D) Verwerker in het kader van de uitvoering van de Overeenkomst onder instructie van Verwerkingsverantwoordelijke persoonsgegevens verwerkt, zonder aan diens rechtstreeks gezag te zijn onderworpen en daarbij kwalificeert als verwerker in de zin van artikel 4 lid 8 AVG; en

(E) Partijen, in aanvulling op de Dienstverleningsovereenkomst, hun rechten en plichten vast wensen te leggen in deze Verwerkersovereenkomst overeenkomstig de AVG, de Uitvoeringswet AVG en eventuele overige toepasselijke Europese en nationale wet- en regelgeving op het gebied van privacy ("**Toepasselijke Data Protectie Wetgeving**").

PARTIJEN KOMEN OVEREEN als volgt:

1. DEFINITIES

Partijen hanteren in deze Verwerkersovereenkomst de onderstaande definities:

Autoriteit	De toezichthoudende autoriteit zoals bedoeld in artikel 51 AVG;

Betrokkene	De geïdentificeerde of identificeerbare natuurlijke persoon op wie een Persoonsgegeven betrekking heeft;
Beveiligingsprotocollen	De door Verwerker te hanteren beveiligingsmaatregelen conform artikel 32 AVG;
Datalek	Een inbreuk op de beveiliging van Persoonsgegevens zoals bedoeld in artikel 4 lid 12 AVG;
Persoonsgegeven(s)	Alle informatie over een geïdentificeerde of identificeerbare natuurlijke persoon zoals bedoeld in artikel 4 lid 1 AVG, die Verwerker direct en/of indirect van Verwerkingsverantwoordelijke heeft verkregen en/of waartoe Verwerker toegang tot heeft gekregen van Verwerkingsverantwoordelijke.

2. DOEL VERWERKING PERSOONSGEGEVENS

2.1 Verwerker zal de Persoonsgegevens uitsluitend verwerken ten behoeve van Verwerkingsverantwoordelijke, overeenkomstig de instructies en onder de verantwoordelijkheid van Verwerkingsverantwoordelijke. Verwerker heeft geen zeggenschap over het doel van en de middelen voor de verwerking van de Persoonsgegevens.

2.2 Gelet op het bepaalde in het vorige artikellid, zal de verwerking van Persoonsgegevens door Verwerker uitsluitend plaatsvinden in het kader van:

i. de uitvoering van de Dienstverleningsovereenkomst en deze Verwerkersovereenkomst; en
ii. een wettelijke verplichting die Verwerker tot de verwerking van Persoonsgegevens verplicht, in dat geval stelt Verwerker de Verwerkingsverantwoordelijke voorafgaand aan de verwerking in kennis van dat wettelijk voorschrift.

2.3 De Persoonsgegevens blijven eigendom van Verwerkingsverantwoordelijke dan wel de betreffende Betrokkene.

3. VERPLICHTINGEN VERWERKER

3.1 Verwerker is verplicht op eerste verzoek van Verwerkingsverantwoordelijke die medewerking te verlenen die nodig is om de Persoonsgegevens in te zien, aan Verwerkingsverantwoordelijke over te dragen, te verwijderen en/of te vernietigen.

3.2 Verwerker is verplicht haar verplichtingen onder de Verwerkersovereenkomst schriftelijk op te leggen aan degenen die handelen onder het gezag van Verwerker, waaronder maar niet beperkt tot medewerkers van Verwerker en de door haar ingeschakelde (sub)verwerker(s). Verwerker is jegens Verwerkingsverantwoordelijke volledig aansprakelijk voor (schade voortvloeiend uit) de verwerking van Persoonsgegevens door (sub)verwerkers die zij conform artikel 13 van deze Verwerkersovereenkomst heeft ingeschakeld.

3.3 Verwerker is verplicht om aan Verwerkingsverantwoordelijke redelijke medewerking te verlenen die noodzakelijk is voor het voldoen aan de rechten van de Betrokkene zoals bedoeld in artikel 12 t/m artikel 22 AVG, het uitvoeren van Gegevensbescherming-effectbeoordelingen (ook wel genoemd '*Privacy Impact Assessments*') zoals bedoeld in artikel 35 AVG en het voldoen aan de wettelijke verplichtingen van Verwerkingsverantwoordelijke in dit verband.

3.4 Verwerker is verplicht een administratie te voeren waaruit gedetailleerd blijkt op welke wijze zij voldoet aan haar verplichtingen op basis van deze Verwerkersovereenkomst en de Toepasselijke Data Protectie Wetgeving. Verwerker is verplicht Verwerkingsverantwoordelijke op eerste verzoek

inzage te verlenen in deze administratie en schriftelijk te informeren over de door haar genomen maatregelen met betrekking tot de verplichtingen onder deze Verwerkersovereenkomst en de Toepasselijke Data Protectie Wetgeving.

4. BEVEILIGINGSMAATREGELEN

4.1 Verwerker zal passende technische en organisatorische maatregelen nemen om de Persoonsgegevens te beveiligen tegen verlies en/of enige vorm van onrechtmatige verwerking, ermee rekening houdend dat de Persoonsgegevens tevens bijzondere categorieën van persoonsgegevens in de zin van artikel 9 en artikel 10 AVG, nationaal identificatienummers in de zin van artikel 87 AVG en persoonsgegevens van gevoelige aard bevatten. Verwerker zal zich daartoe in ieder geval, maar niet uitsluitend, houden aan het niveau van beveiliging zoals vastgelegd in de Beveiligingsprotocollen.

4.2 Verwerker is zich bewust van het belang van beveiligingsmaatregelen en zal op verzoek jaarlijks op een door Verwerker aan te wijzen manier kenbaar maken welke passende technische en organisatorische maatregelen Verwerker heeft getroffen ter beveiliging van de Persoonsgegevens.

5. MELDPLICHT DATALEKKEN

5.1 In het geval van een Datalek, zal Verwerker Verwerkingsverantwoordelijke onmiddellijk, maar in ieder geval binnen 48 uur na ontdekking van het Datalek, schriftelijk informeren op het volgende e-mail adres: soc@ggdghor.nl.

5.2 Verwerker zal Verwerkingsverantwoordelijke binnen 48 uur na ontdekking van Datalek, indien op data moment beschikbaar, de informatie verstrekken die benodigd is voor het doen van de melding(en) zoals bedoeld in artikel 33 en 34 AVG en die ten minste betreft:

i. de categorieën en een indicatie van het aantal Persoonsgegevens die zijn getroffen;
ii. de categorieën en een indicatie van het aantal Betrokkene die zijn getroffen;
iii. de aard van het Datalek;
iv. de periode waarin het Datalek heeft plaatsgevonden;
v. de maatregelen die zijn genomen om de negatieve gevolgen van het Datalek te beperken;
vi. een beschrijving van de geconstateerde en de vermoedelijke gevolgen van het Datalek;
vii. de maatregelen die Verwerker en/of de door haar ingeschakelde (sub)verwerker(s) heeft getroffen of voorstelt te treffen om deze gevolgen te verhelpen.

5.3 Verwerkingsverantwoordelijke zal zelf de meldingen als bedoeld in artikel 33 AVG doen aan de Autoriteit en indien noodzakelijk aan de Betrokkene overeenkomstig artikel 34 AVG. Zonder voorafgaande schriftelijke toestemming van Verwerkingsverantwoordelijke, is Verwerker niet gerechtigd om Datalekken te melden aan de Autoriteit en/of Betrokkene.

5.4 Partijen kunnen schriftelijk overeenkomen dat en onder welke voorwaarden Verwerker meldingen in de zin van artikelen 33 en 34 AVG zal doen.

6. DOORGIFTE

6.1 Zonder voorafgaande schriftelijke toestemming van Verwerkingsverantwoordelijke is het Verwerker niet toegestaan om Persoonsgegevens te verstrekken aan derden, behoudens door Verwerker ingeschakelde ZZP'ers en (sub)verwerkers in overeenstemming met artikel 13 van deze Verwerkersovereenkomst.

6.2 Zonder dat een of meerdere waarborgen als bedoeld in artikel 44 t/m artikel 49 AVG zijn getroffen, is het Verwerker niet toegestaan om Persoonsgegevens te verwerken en/of door te geven aan

derde landen of internationale organisaties buiten de Europese Economische Ruimte. Verwerker is verplicht Verwerkingsverantwoordelijke schriftelijk te informeren over de door haar voorgenomen doorgifte van persoonsgegevens aan derde landen of internationale organisaties buiten de Europese Economische Ruimte en de getroffen maatregelen in dit kader.

7. CONTROLE EN AUDIT

7.1 Verwerker zal Verwerkingsverantwoordelijke voorzien van redelijkerwijs benodigde informatie en meewerken aan audits door Verwerkingsverantwoordelijke, of door een door Verwerkingsverantwoordelijke aangewezen derde, die redelijkerwijs verzocht worden en vereist zijn om aan te tonen dat Verwerker voldoet aan diens verplichtingen op grond van deze Verwerkersovereenkomst.

7.2 Het tijdstip waarop een audit zal plaatsvinden wordt in onderling overleg bepaald.

7.3 Verwerkingsverantwoordelijke zal aan Verwerker met inachtneming van een redelijke termijn vooraf een schriftelijke mededeling doen van een audit die Verwerkingsverantwoordelijke verzoekt uit te voeren in overeenstemming met artikel 7.1 met daarbij een toelichting van de gronden van de inspectie. Verwerkingsverantwoordelijke zal de hoeveelheid audits beperken en zorgdragen dat Verwerkingsverantwoordelijke of de door Verwerkingsverantwoordelijke aangewezen derde gebonden is aan geheimhoudingsverplichtingen, de redelijke instructies en aanwijzingen van Verwerker opvolgt, de ter plaatse van de inspectie geldende veiligheids- en andere voorschriften naleeft en geen schade veroorzaakt en ook niet anderszins de bedrijfsvoering verstoort. De Verwerker zal niet gehouden zijn om toegang te geven tot diens bedrijfsruimten voor de doeleinden van een inspectie:

i. aan personen die zich niet kunnen identificeren en geen bewijs van bevoegdheid kunnen overleggen; of
ii. buiten normale werkuren en/of in de weekenden.

7.4 De kosten verbonden aan een audit zullen volledig voor rekening komen van de Verwerkingsverantwoordelijke.

7.5 Verwerkingsverantwoordelijke zal Verwerker zo spoedig mogelijk na het einde van een audit voorzien van een afschrift van het auditrapport en Verwerker een redelijke mogelijkheid bieden om schriftelijk op het auditrapport te reageren.

8. AUTORITEITEN

8.1 Verwerker erkent de bevoegdheid van Autoriteiten om:

i. informatie in te winnen bij Verwerker respectievelijk bij door Verwerker ingeschakelde derden en/of de externe accountant van Verwerker omtrent de verwerking van Persoonsgegevens; en/of
ii. desgewenst onderzoek te doen of te laten doen bij Verwerker respectievelijk bij door Verwerker ingeschakelde derden en/of de externe accountant van Verwerker, bijvoorbeeld onderzoeken naar de bedrijfsvoering en bedrijfsprocessen in het kader van de verwerking van Persoonsgegevens. En verplicht zich om aan dergelijke verzoeken redelijke medewerking te verlenen.

9. RECHTEN VAN BETROKKENE

9.1 Verwerker is verplicht Verwerkingsverantwoordelijke binnen een kalenderweek, te informeren als een Betrokkene een verzoek heeft gedaan ter uitoefening van zijn of haar rechten als bedoeld in artikel 12 t/m artikel 22 AVG.

9.2 Verwerker zal alleen communiceren met een Betrokkene en verzoeken als bedoeld in het vorige artikellid in behandeling nemen na voorafgaande schriftelijke toestemming van Verwerkingsverantwoordelijke.

9.3 Verwerker is verplicht om Verwerkingsverantwoordelijke redelijke medewerking te verlenen die redelijkerwijze noodzakelijk is voor de uitoefening van de rechten van Betrokkene op basis van de AVG.

10. GEHEIMHOUDING

10.1 Verwerker is verplicht tot geheimhouding van de Persoonsgegevens. Verwerker zal deze verplichting tot geheimhouding opleggen aan haar medewerkers en aan door Verwerker ingeschakelde derden.

10.2 Zonder voorafgaande schriftelijke toestemming van Verwerkingsverantwoordelijke, is het Verwerker niet toegestaan om informatie die redelijkerwijze te herleiden is tot deze Verwerkersovereenkomst en/of een Beveiligingsincident en/of een Datalek mede te delen met derden, waaronder maar niet beperkt tot Betrokkene, toezichthoudende autoriteiten en de media.

11. DUUR VAN DEZE VERWERKERSOVEREENKOMST

11.1 Deze Verwerkersovereenkomst treedt in werking na rechtsgeldige ondertekening door Partijen en wordt aangegaan voor de duur van de Overeenkomst. Behoudens hetgeen is bepaald in artikel 12 Verwerkersovereenkomst, eindigt deze Verwerkersovereenkomst van rechtswege op het moment van beëindiging of ontbinding van de Overeenkomst.

11.2 Artikel 10 (Geheimhouding) en artikel 16 (Toepasselijk recht en forumkeuze) zullen ook na de beëindiging of ontbinding van deze Verwerkersovereenkomst voor onbepaalde tijd tussen Partijen voortduren.

12. GEVOLGEN BEEINDIGING VERWERKERSOVEREENKOMST

Voor zover Verwerker na de beëindiging of ontbinding van deze Verwerkersovereenkomst nog beschikt over Persoonsgegevens, zal zij deze zo spoedig mogelijk vernietigen, danwel – naar keuze van Verwerkingsverantwoordelijke – aan Verwerkingsverantwoordelijke retourneren, tenzij Verwerker op grond van geldende wet- of regelgeving gehouden is de Persoonsgegevens te bewaren. In dit laatstgenoemde geval zal Verwerker al haar verplichtingen uit deze Verwerkersovereenkomst nakomen gedurende de gehele periode waarin zij op grond van geldende wet- of regelgeving gehouden is de Persoonsgegevens te bewaren.[1]

13. INSCHAKELEN (SUB)VERWERKERS

13.1 Verwerkingsverantwoordelijke verleent algemene toestemming voor het inschakelen van een (sub)verwerker. Voorafgaand aan het inschakelen van een (sub)verwerker licht Verwerker Verwerkingsverantwoordelijke in over beoogde veranderingen inzake de toevoeging of vervangen van andere (sub)verwerkers, waarbij Verwerkingsverantwoordelijke de mogelijkheid wordt geboden tegen deze veranderingen bezwaar te maken.[2]

13.2 Op eerste verzoek van Verwerkingsverantwoordelijke verstrekt Verwerker aan Verwerkingsverantwoordelijke een overzicht van door haar ingeschakelde (sub)verwerkers.

[1] Artikel 28 lid 3 sub g AVG verplicht Verwerker om Persoonsgegevens terug te geven dan wel te verwijderen na beëindiging van deze Verwerkersovereenkomst, naargelang van Verwerkingsverantwoordelijke.
[2] Artikel 28 lid 2 AVG bepaalt dat Verwerker geen andere verwerker in dienst neemt zonder voorafgaande specifieke of algemene schriftelijke toestemming van Verwerkingsverantwoordelijke. In het geval van algemene schriftelijke toestemming licht Verwerker Verwerkingsverantwoordelijke in over beoogde veranderingen inzake de toevoeging of vervanging van andere verwerkers.

14. KOSTEN

Kosten voortvloeiend uit rechten van Betrokkene zoals bedoeld in artikel 14 t/m artikel 22 AVG, uit Gegevensbescherming-effectbeoordelingen (ook wel genoemd 'Privacy Impact Assessments') zoals bedoeld in artikel 35 AVG en/of uit onderzoeken of audits van de Autoriteit met betrekking tot de Persoonsgegevens zullen worden gedragen door Verwerkingsverantwoordelijke. Kosten die gemaakt worden door Verwerker op verzoek van Verwerkingsverantwoordelijke of Autoriteiten zijn voor rekening van Verwerkingsverantwoordelijke.

15. WIJZIGING IN WET- EN/OF REGELGEVING

Bij de wijziging van bestaande wet- en/of regelgeving en bij de invoering van nieuwe wet- en/of regelgeving, verleent Verwerker op het eerste verzoek van Verwerkingsverantwoordelijke alle medewerking die redelijkerwijze van haar verwacht mag worden, zoals maar niet beperkt tot het wijzigen van deze Verwerkersovereenkomst.

Aldus overeengekomen:

GGD Hart voor Brabant	GGD GHOR Nederland
_____	_____
[redacted]	[redacted]
Directeur Publieke Gezondheid	Waarnemend Algemeen Directeur

Bijlage 1
Beschrijving verwerking Persoonsgegevens
Verwerker zal de Persoonsgegevens uitsluitend verwerken overeenkomstig de onderstaande instructies van Verwerkingsverantwoordelijke.

Onderwerp, aard en geschatte termijn van de verwerking
Het onderwerp, de aard en de geschatte termijn van de verwerking staan nader opgenomen in de Dienstverleningsovereenkomst (inclusief Bijlagen).

Doelen en wettelijke grondslagen van de verwerking
De doeleinden voor de verwerkingen inzake GGD Contact zijn opgenomen in de referentie DPIA inzake GGD Contact, waarbij de dienstverlening van GGD GHOR in dit kader nader is uitgewerkt in de Dienstverleningsovereenkomst (inclusief Bijlagen). De wettelijke grondslag voor de GGD is het uitvoeren van een taak van algemeen belang, zoals tevens nader uitgewerkt in de DPIA inzake GGD Contact.

Categorieën Persoonsgegevens
De categorieën Persoonsgegevens zijn de Persoonsgegevens die worden verwerkt in GGD Contact. Deze persoonsgegevens zijn opgenomen in de referentie DPIA inzake GGD Contact.

Categorieën Betrokkene
De categorieën Betrokkenen zijn de Betrokkenen waarvan Persoonsgegevens worden verwerkt in GGD Contact. Deze Betrokkenen zijn als volgt:
- Index
- Contact Index
- BCO-medewerker

VOLMACHT AAN GGD GHOR INZAKE MEDEDELING DATALEK AAN BETROKKENEN

25-02-2021

7. De Gemeentelijke Gezondheidsdienst Hart voor Brabant, gevestigd te ‘s-Hertogenbosch aan de Vogelstraat 2, ingeschreven in het handelsregister onder KvK nummer 17247544, hierna eveneens te noemen “**GGD**”, rechtsgeldig vertegenwoordigd door mevrouw T. Claassen;

.....

VOLMACHT AAN GGD GHOR INZAKE MEDEDELING DATALEK AAN BETROKKENEN

25-02-2021

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

.....

17.5

Hart voor Brabant

Aan: het algemeen bestuur van GGD Hart voor Brabant

Datum: 29 januari 2021

Behandeld door: [redacted]

E-mail: [redacted]

Onderwerp: Datadiefstal

Geachte leden van ons algemeen bestuur,

Begin deze week kwam aan het licht dat sprake is geweest van onzorgvuldig omgaan met bijzondere persoonsgegevens en het stelen van data uit GGD-systemen door GGD-medewerkers. Systemen die door de Nederlandse GGD'en gebruikt worden ter ondersteuning van de bestrijding van het Coronavirus. Naar aanleiding van en in reactie op de speculaties en berichtgeving over die diefstal, zal GGD GHOR Nederland vandaag bijgevoegde uitleg publiceren. Graag deel ik via deze weg dat bericht met u.

Graag benadruk ik nogmaals dat het hier geen medewerkers van GGD Hart voor Brabant betreft. Het is nog niet duidelijk of de gestolen data ook daadwerkelijk is verhandeld. Ook is nog niet duidelijk over welke data het precies gaat, en of tussen de gedupeerden ook inwoners uit ons werkgebied zitten. Dit is allemaal nog onderdeel van het grootschalige en grondige onderzoek van politie en justitie.

Als er nieuwe relevante ontwikkelingen zijn op dit dossier, dan stel ik u daar zo snel mogelijk van op de hoogte. Voor nu vertrouw ik erop u met dit schrijven voldoende geïnformeerd te hebben. Tijdens uw vergadering van 24 maart praten we u verder bij. Tot die tijd zal ik eventuele belangrijke en/of spoedeisende zaken steeds via een brief met u delen.

Met vriendelijke groet,

[redacted]

Wnd. Directeur Publieke Gezondheid

GGD Hart voor Brabant
Postbus 3024
5003 DA Tilburg
0900 463 64 43

www.ggdhvb.nl
info@ggdhvb.nl

Hart voor Brabant

Gezond² doet leven!

Vergadering dagelijks bestuur

Datum	**4 februari 2021**	DB 20210204-1.0-0
Onderwerp	**Update datadiefstal**	
Agendapunt		
Afzender	[redacted]	
Portefeuille	[redacted]	

Omschrijving

Aanleiding

Op maandag 25 januari zijn de 25 GGD'en ingelicht dat een vermoedelijke datadiefstal uit de GGD-systemen is gesignaleerd. Hierover is vanaf die dag uitgebreid in de media bericht. Op vrijdag 29 januari is een informatiebrief gestuurd aan het Algemeen Bestuur met daarbij de reactie van GGD GHOR Nederland ("GGD en haar data – Hoe zit het echt?"). Op verzoek van de voorzitter is een extra DB ingelast om bijgepraat te worden over de datadiefstal en de regionale gevolgen daarvan.

In voorliggende notitie worden de achtergronden en actualiteiten geschetst, alsmede de wijze waarop de GGD Hart voor Brabant in het verleden is omgegaan met gegevensbescherming en de maatregelen die zijn en worden getroffen.

Wat is er precies gebeurd?

Op vrijdag 22 januari heeft een journalist van RTL de koepel GGD GHOR Nederland getipt dat op internet tegen betaling persoonsgegevens uit twee GGD-systemen wordt aangeboden. In systeem CoronIT worden persoonsgegevens bijgehouden van iedereen die een test laat uitvoeren.[1] Voor zover nu bekend zijn uit CoronIT gericht persoonsgegevens van individuen (o.a. BN'ers) ingezien en gedeeld, maar geen grote datasets met gegevens van duizenden mensen. In het systeem HPZone worden persoonsgegevens bijgehouden uit het bron- en contactonderzoek, alleen van mensen die positief zijn getest. Uit HPZone zijn wél grote datasets gedownload. Om hoeveel gegevens het gaat en van wie wordt nog landelijk onderzocht. GGD GHOR Nederland heeft meteen contact opgenomen met de politie, aangifte gedaan en een melding gedaan bij de Autoriteit Persoonsgegevens. Vervolgens heeft GGD GHOR Nederland controles uitgevoerd in de systemen én volledige toegang gegeven aan de politie om de opsporing zo goed mogelijk plaats te kunnen laten

[1] CoronIT wordt ook gebruikt voor de vaccinaties, maar in een gescheiden databestand. De call center-medewerkers hebben alleen toegang tot testen of tot vaccineren. De datadiefstal is ontstaan in het deel 'testen'.

vinden. De politie heeft aanwijzingen gevonden dat twee medewerkers van het landelijk call center persoonsgegevens van burgers hebben gestolen uit CoronIT. Het lijkt erop dat zij die gegevens te koop hebben aangeboden of gedeeld met onbevoegden, maar op dit moment is niet bekend of deze ook daadwerkelijk zijn verkocht of verhandeld. Sindsdien zijn drie medewerkers van het landelijke coronatest afsprakennummer aangehouden op verdenking van datadiefstal. Het onderzoek van politie en justitie loopt nog.

Heeft er datadiefstal plaatsgevonden binnen de GGD Hart voor Brabant?
Geen van de gearresteerde personen was werkzaam bij onze GGD. Wij hebben tot op heden geen aanwijzingen van politie en justitie dat (vaste of ingehuurde) medewerkers van onze GGD worden verdacht. De GGD die dit wel betreft (Twente) is daarvan actief op de hoogte gesteld. We hebben ook zelf op dit moment geen aanwijzingen dat door onze medewerkers data zouden zijn gestolen. Wij hebben een nadere check uitgevoerd van onze 'logging-bestanden' en geen onregelmatigheden aangetroffen. Het is evenwel nog niet duidelijk of door de gearresteerde medewerkers van het landelijk call center of andere GGD'en ook gegevens zijn gestolen en/of ten onrechte ingezien van inwoners uit ons werkgebied. Dit is wel mogelijk. Dit is allemaal nog onderdeel van het grootschalige en grondige onderzoek van politie en justitie.

Wat is de achtergrond van beide systemen?
CoronIT is het administratiesysteem voor het test- en vaccinatieproces. Als men een afspraak maakt voor een coronatest via het callcenter, de coronatest website of een arts, komen de persoonsgegevens in CoronIT. Dit geldt ook als iemand een afspraak maakt voor een vaccinatie. CoronIT is een relatief nieuw systeem. Hier zijn de GGD'en in mei 2020 mee gaan werken toen het ministerie van VWS de opdracht gaf om mensen grootschalig te gaan testen op het coronavirus. Dit was tot dat moment geen rol van de GGD. CoronIT is in zeer korte tijd en onder zeer hoge druk landelijk ontwikkeld door GGD GHOR Nederland in samenwerking met het RIVM en VWS.

HPZone is een elektronisch dossier dat 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. HPZone stamt uit 2003 en is dus al jarenlang in gebruik bij 23 GGD'en voor de infectieziektebestrijding. Vóór de pandemie werd dit systeem gebruikt door een kleine groep artsen en verpleegkundigen bij lokale uitbraken van een infectieziekte. Door dit kleinschalige gebruik door een beperkt aantal professionals waren er geen problemen met het systeem. Toen corona uitbrak is onder hoge druk en in korte tijd de keuze gemaakt om HPZone als basis te blijven gebruiken voor het uitvoeren van bron- en contactonderzoek maar dan voor een veelvoud aan gevallen. Hiervoor is een versie 'HPZone Lite' ontwikkeld.

Welke data zijn opgenomen in deze systemen?
Het is nog niet duidelijk welke data precies zijn gestolen of onrechtmatig ingezien. In CoronIT zijn persoonsgegevens vastgelegd zoals naam, adres, woonplaats, telefoonnummer/e-mailadres, BSN, geslacht, geboortedatum. Daarnaast afhankelijk van

het contact ook test- en/of vaccineerafspraken en testresultaten. In HPZone wordt 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. Deze informatie is beperkt.

Wat doen medewerkers in de systemen?
Medewerkers van het callcenter (inbound – die gebeld worden) kunnen via CoronIT testafspraken en vaccinatieafspraken maken. Verder kunnen de (outbound – die mensen bellen) callagents de testuitslagen zien, aangezien zij mensen, zonder DigiD, bellen met hun testuitslag. Bron- en contactonderzoekers leggen alle gegevens rondom een besmetting vast in HPZone. Binnen de GGD worden de data uit de systemen geanonimiseerd gebruikt voor de corona-dashboards en voor onderzoek ten behoeve van de gemeenten.

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 call-centrum voor testafspraken zijn bijvoorbeeld de gezondheidsverklaringen die voor vaccinaties worden ingevuld niet zichtbaar. Registratie van bijwerkingen is alleen toegankelijk voor mensen met medische autorisatie.

Wat zijn de mogelijke gevolgen voor burgers?
Het is nog onduidelijk of er daadwerkelijk gegevens zijn verhandeld, welke gegevens dan en op welke schaal. Dit wordt onderzocht door politie en justitie. Als er daadwerkelijk persoonsgegevens door criminelen worden gebruikt, dan zijn de risico's volgens de politie oplichting (phishing) en identiteitsfraude.

Waren de risico's vooraf bekend en zijn hierover signalen afgegeven?
Vanaf het begin is landelijk duidelijk geweest dat HPZone (Lite) niet heel goed geschikt is om zo grootschalig en zo intensief te worden gebruikt als nu nodig is bij het bestrijden van de coronapandemie. Het is onvermijdelijk dat HPZone een relatief open systeem is, omdat bij bron- en contactonderzoek informatie moet worden uitgewisseld tussen regio's. Daar is door GGD GHOR Nederland 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.

Naar aanleiding van het GGD-crisisteam van 30 april 2020 heeft de GGD Hart voor Brabant aan GGD GHOR Nederland het signaal afgegeven dat de GGD'en beter betrokken moeten worden bij de inrichting van CoronIT. Ook is GGD GHOR Nederland gevraagd om juridisch advies over de omgang met data in HPZone. Begin mei 2020 is een landelijk convenant getekend tussen GGD GHOR Nederland en de 25 GGD'en over de gegevensuitwisseling in CoronIT. De GGD Hart voor Brabant heeft bij de beoordeling van dit convenant vooraf gevraagd of er landelijk niet een Data Protection Impact Assessment (DPIA) zou moeten worden opgesteld. Dit is niet gedaan. Naar aanleiding van het GGD-

crisisteam van 18 mei 2020 is wederom bij GGD GHOR Nederland aandacht gevraagd voor het juridische eigenaarschap van het systeem CoronIT en de data daarin. Naar aanleiding van intern overleg op 1 juni 2020 heeft de GGD Hart voor Brabant bij GGD GHOR Nederland aandacht gevraagd voor de invulling van data in CoronIT door het landelijk call center, de benodigde toestemming van patiënten voor gegevensuitwisseling en de mogelijkheid voor medewerkers om databestanden te downloaden. Op 29 juni 2020 is in intern afstemmingsoverleg van de GGD Hart voor Brabant besproken en vervolgens naar GGD GHOR Nederland gesignaleerd dat het ontbrak aan een landelijke stuurgroep en gebruikersgroep voor CoronIT om te regisseren op de ervaren problematieken. Deze zijn in augustus uiteindelijk ingericht.

Op 2 juli 2020 is door GGD-professionals een brief gestuurd aan de landelijk portefeuillehouder testen van GGD GHOR Nederland over CoronIT. Hierin is erop gewezen dat de GGD'en onaangenaam verrast waren dat personen met een niet-medische rol toegang hebben tot medische informatie in CoronIT. Gevraagd is wie er allemaal toegang hebben tot de data in CoronIT. Er is op gewezen dat de data in CoronIT per regio eigendom zijn van de lokale GGD en/of van de aanvragend arts. Deze data kunnen slechts onder strikte voorwaarden anoniem met bepaalde personen of partijen worden gedeeld. Dit kan uitsluitend nadat er vooraf schriftelijke afspraken zijn gemaakt tussen betrokken GGD'en en de andere partij. Ook is in die brief erop gewezen dat de gebruikers die toegang hebben tot uitslagen, deze niet alleen voor de eigen GGD maar voor heel Nederland op naam kunnen opzoeken. Ook hiervoor is gevraagd of er voldoende basis is om data van de ene lokale GGD op deze wijze beschikbaar te laten zijn voor medewerkers van de andere GGD'en (ook al betreft dit medisch-inhoudelijk betrokken artsen en verpleegkundigen en ondersteunend personeel). In de brief is ook erop gewezen dat het gebruik van CoronIT onontkoombaar is, maar dat het daarom extra van belang is dat binnen CoronIT zorgvuldig wordt omgegaan met de juridische kaders, die gelden voor medische registratiesystemen en er niemand toegang heeft tot medische data, die daar niet voor gerechtigd is. Er dienen heldere afspraken ten grondslag te liggen aan wie toegang hebben tot het systeem en met welk doel men over welke gegevens kan beschikken ten behoeve van de landelijke bestrijding. Deze afspraken dienen transparant te zijn, en geaccordeerd door alle 25 GGD'en. Om die redenen is aan GGD GHOR Nederland verzocht per direct c.q. op de kortst mogelijke termijn de toegang tot medische gegevens in CoronIT te beperken tot uitsluitend diegenen die daar uit hoofde van hun functie recht op hebben.

Welke maatregelen zijn vooraf genomen om gegevensmisbruik te voorkomen?
De GGD'en hebben vooraf de volgende maatregelen genomen:

- Controle aan de poort. Mensen moeten een Verklaring Omtrent Gedrag (VOG) aanleveren en een geheimhoudingsverklaring ondertekenen. De GGD Hart voor Brabant heeft in de werkprocessen bij aanname van personeel verzekerd dat altijd en voor iedereen een VOG en geheimhoudingsverklaring voor handen is.
- Autorisatieniveaus. Beide systemen kennen verschillende rollen met bijbehorende autorisatieniveaus. Niet iedereen kan bij alle gegevens en kan alle functionaliteiten (downloads) gebruiken. Binnen de GGD Hart voor Brabant hebben wij een

autorisatiematrix gebaseerd op rol of functie van iedere medewerker. Medewerkers krijgen alleen die autorisatie die nodig is voor zijn of haar functie. De autorisatiematrix wordt bijgehouden bij in-, door- en uitstroom van medewerkers. Er vindt hierop een maandelijkse check plaats.

- Controles op correct gebruik. De GGD'en controleren sinds de start het gebruik van de systemen door de medewerkers, en hebben de controles steeds verder verbeterd en doen dat nog steeds. Vanwege het belang van de virusbestrijding en de gevraagde snelheid zijn de GGD'en – op diverse manieren – met steekproefsgewijze controles van start gegaan. De Autoriteit Persoonsgegevens had vóór het bekend worden van de datadiefstal geen aanvullende vragen gesteld over deze werkwijze. De GGD Hart voor Brabant kan via de logging-functionaliteit van Microsoft 30 dagen terugkijken. De GGD gebruikt dit voor steekproeven en om terug te zoeken bij signalen en incidenten.
- Ontwikkeling nieuw systeem. GGD GHOR Nederland werkt samen met het ministerie van VWS al maanden aan een nieuw systeem 'GGD contact'. Dit systeem moet voldoen 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 – de 'GGD contact app' met een bijbehorend portaal voor bron- en contactonderzoek – in maart operationeel te hebben voor de coronabestrijding. Op dat moment kan bij de bestrijding van de coronapandemie worden overgestapt van HPZone Lite naar het nieuwe systeem. Voor de reguliere infectieziektebestrijding zal door de beperkte groep van vaste GGD-professionals vooralsnog nog wel in HPZone worden gewerkt. De Nederlandse Vereniging voor Infectieziektebestrijding (NVIB) heeft op 29 januari een brandbrief gestuurd waarin de artsen infectieziektebestrijding waarschuwen voor risico's voor de infectieziektebestrijding in Nederland bij een onzorgvuldige en overhaaste vervanging van HP Zone Lite door GGD Contact per 1 maart 2021. De impact op de operatie is enorm en alternatieven zijn onvoldoende verkend. Het deskundig oordeel van de infectieziektebestrijding (GGD / RIVM / GGD GHOR) moet volgens hen doorslaggevend zijn bij de besluitvorming omtrent (het moment van) overstap op een nieuw systeem. Ook het RIVM heeft op 2 februari negatief geadviseerd over de invoering van het nieuwe systeem, ter vervanging van HPZone. Zij vinden het een te groot risico om dit middenin de verwachte 3^{e} golf te doen, met risico op invoerproblemen en verlies van historische data.

Welke maatregelen worden genomen sinds het bekend worden van de datadiefstal?

Landelijk is aangifte gedaan en wordt grootschalig onderzoek gedaan door politie en justitie. De eerder genomen maatregelen zijn gecontroleerd en geïntensiveerd:

- Controle aan de poort. De GGD Hart voor Brabant heeft nogmaals een check uitgevoerd. We hebben vastgesteld dat alle door ons ingezette externe medewerkers een VOG en ondertekende geheimhoudingsverklaring hebben. Bij vaste, interne medewerkers is dit ook het geval voor zover ze bij ons zijn komen werken sinds het beleid omtrent VOG en geheimhoudingsverklaring is geïmplementeerd. Bij enkele oudgedienden die al vele jaren bij ons werken blijken de VOG en geheimhoudingsverklaring te ontbreken. Dit wordt opgelost.

- Autorisatieniveaus. Naar aanleiding van de datadiefstal is doorgelicht wie binnen de GGD Hart voor Brabant geautoriseerd is tot grote downloads (datadump). Dit is een zeer beperkte groep van medewerkers die dit op grond van hun functie daadwerkelijk nodig hebben, bijvoorbeeld om dashboards te maken.
- Controles op correct gebruik. De GGD Hart voor Brabant heeft een nadere check uitgevoerd van onze 'logging-bestanden' en geen onregelmatigheden aangetroffen. We zien geen afwijkingen in de IT-omgeving van onze GGD. Ons beeld is dat er binnen of door de GGD Hart voor Brabant geen gegevens in verkeerde handen zijn gevallen. De GGD Hart voor Brabant wil de periode van logging verlengen van 30 dagen naar 1 jaar, zodat we verder kunnen terugkijken. Verder verwacht GGD GHOR Nederland in maart systemen te implementeren die automatisch en continu zullen controleren op opvallend gebruik van de systemen (zoals grote downloads of onlogische inzage in dossiers).
- Ontwikkeling nieuw systeem. De invoering van de nieuwe GGD contact app met BCO-portaal wordt versneld. Deze is nu voorzien voor begin in plaats van eind maart. Dit is een risico (zie laatste paragraaf).

Verder worden als aanvullende maatregelen genomen:

- Uitzetten van functionaliteiten in de systemen. Om het risico per direct te verminderen zijn in CoronIT en HPzone diverse functionaliteiten uitgezet. Het is niet meer mogelijk om downloads van gegevensbestanden te doen, prints van gegevensbestanden te maken (omdat dit als PDF kon) en om zoekopdrachten te doen (query's) op BSN en postcode. Het risico op verder misbruik is hiermee zoveel mogelijk gereduceerd.
- Verwijdering van gegevens. Mensen hebben het wettelijk recht om een inzage- of verwijderingsverzoek te doen van gegevens in overheidssystemen. De GGD heeft hiervoor al jaren een staand beleid en werkprotocol, conform de Algemene verordening gegevensbescherming (AVG). Landelijk is door GGD GHOR Nederland een speciaal informatienummer ingesteld waar mensen terecht kunnen met vragen over het verwijderen van gegevens. Als mensen daadwerkelijk gegevens willen laten verwijderen dan kunnen zij op de website van hun eigen GGD een formulier vinden voor een verwijderingsverzoek. De GGD Hart voor Brabant heeft sinds vorige week 60 inzage- en verwijderingsverzoeken ontvangen. Of gegevens daadwerkelijk verwijderd of geanonimiseerd kunnen worden, moet op individuele basis worden besloten conform de wettelijke bepalingen in het bestuursrecht, in de Wet publieke gezondheid en omtrent de Geneeskundige Behandelovereenkomst. Indien de GGD in het kader van het bron- en contactonderzoek gerichte medische adviezen heeft gegeven aan een cliënt is er sprake van een andere bewaarplicht dan wanneer mensen negatief zijn getest of alleen algemeen advies is gegeven. Landelijk wordt dit juridisch getoetst.
- Landelijke governance informatievoorziening. De GGD Hart voor Brabant is samen met veel andere GGD'en niet tevreden over de zeer gebrekkige invloed die de GGD'en en de professionals de afgelopen periode hebben kunnen uitoefenen op landelijke IT-keuzes. Op 21 december heeft een gesprek plaatsgevonden met de landelijk portefeuillehouder informatievoorziening van GGD GHOR Nederland, waarop door de koepel een summiere notitie "Contactnetwerk GGD'en Digitalisering en Monitoring" is opgesteld. De GGD Hart voor Brabant heeft het voortouw genomen om samen met

andere GGD'en hierop kritisch te reageren. Wij hebben GGD GHOR Nederland verzocht om de gevoelde vrijblijvendheid weg te nemen, door vast te leggen wie (welk gremium) transparant beslist met welke prioriteit, urgentiebesef en resources regionaal ervaren knelpunten in IT/informatievoorziening wel of niet worden opgepakt. In die governance moeten we als regionale opdrachtgevers van de landelijke ondersteuning een stem krijgen, zowel op directieniveau als op het niveau van de professionals (gebruikers) en ook bestuurders. GGD GHOR Nederland moet nog met nadere voorstellen komen.

- Communicatie. De GGD Hart voor Brabant vindt het van belang om de eigen inwoners gericht te informeren over de situatie, wat wij eraan doen en hoe mensen een verwijderingsverzoek kunnen indienen. We verwijzen ons inwoners in eerste instantie om eerst de landelijke lijst met veelgestelde vragen goed door te nemen. Zit het antwoord op hun vraag er niet bij, dan adviseren wij hen om contact op te nemen met het landelijke nummer voor deze datadiefstal. Dit telefoonnummer (085- 130 82 26) is dagelijks bereikbaar van 09.00 uur tot 21.00 uur. Daarnaast attenderen we inwoners uit onze regio op het inzien of wijzigen van eigen gegevens. Inwoners van de regio Hart voor Brabant kunnen een verzoek indienen om hun gegevens te bekijken. Ook kun men aanvragen of het gebruik, vermelden of bewaren van persoonlijke gegevens kan worden aangepast. Het is belangrijk om te weten dat de GGD een wettelijke bewaarplicht heeft van bepaalde gegevens. Dus per geval zal gekeken moeten worden wat er mogelijk is. Op de website van GGD Hart voor Brabant vindt men via onderdeel corona bij veel gestelde vragen de link naar privacy en corona. Daar is een formulier persoonsgegevens om een aanvraag te kunnen doen.

Wat zijn de risico's voor de GGD Hart voor Brabant?

- Schadeclaims. Burgers die gegevens aan onze GGD hebben gegeven kunnen mogelijk een schadeclaim indienen bij geleden schade door de datadiefstal. De mogelijkheid bestaat dat advocaten een massaclaim indienen. Ook als ons als GGD Hart voor Brabant niet direct iets te verwijten valt, zijn we mogelijk wel aansprakelijk waar het onze data betreft, maar dat is niet zeker. Verder zou de autoriteit persoonsgegevens een sanctie kunnen opleggen als tekortkomingen worden gesignaleerd in onze databeveiliging. Juridisch moet uitgezocht worden wat het eigenaarschap van systemen en databestanden en eventuele verwijtbaarheid van handelen betekent voor aansprakelijkheid van GGD GHOR Nederland, de 25 GGD'en en individuele medewerkers. GGD GHOR Nederland wordt hierin ondersteund door een advocatenkantoor. Ook de GGD Hart voor Brabant wil juridisch advies. De exacte kans en de potentiële financiële impact is moeilijk vooraf in te schatten.
- Belemmering werkprocessen. Door het uitzetten van functionaliteiten in HPZone is het niet meer mogelijk om downloads van gegevensbestanden te doen, prints van gegevensbestanden te maken (omdat dit als PDF kon) en om zoekopdrachten te doen (query's) op BSN en postcode. De GGD'en ervaren hierdoor directe negatieve impact op hun werkprocessen in bron- en contactonderzoek en reguliere infectieziektebestrijding. Het is moeilijker om tussen regio's informatie uit te wisselen voor de BCO's. Ook is het niet langer mogelijk om regionale corona-dashboards te maken en verdiepend onderzoek te doen. De GGD'en zijn hierover in overleg met GGD

GHOR Nederland.

- Imagoschade. De potentiële schade voor het imago van de GGD als betrouwbare overheid is substantieel. De GGD Hart voor Brabant werkt aan een proactieve communicatieaanpak om de schade zoveel mogelijk te beperken.
- Test- en vaccinatiebereidheid. Verder maken wij ons als GGD zorgen over de test- en vaccinatiebereidheid. Het belang van (blijven) testen bij klachten en zoveel mogelijk mensen vaccineren is zeer groot. GGD GHOR Nederland en de GGD'en zijn daarom zo transparant mogelijk over het incident, de onderzoeken en de verbetermaatregelen.
- Moreel medewerkers. Tot slot vinden we een belangrijk risico het afnemen van moreel en motivatie van onze medewerkers. Medewerkers die toegang hebben tot CoronIT en HPZone kunnen het gevoel krijgen dat ze in een kwaad daglicht staan of dat ze verdachte zijn. Alle medewerkers van de GGD hebben last van de negatieve manier waarop de GGD in het nieuws komt. De GGD communiceert intern om medewerkers zoveel als mogelijk gerust te stellen.

Beslispunt(en)

1. Kennisnemen van de analyse en de getroffen maatregelen.
2. Het AB over voorgaande informeren middels een informatiebrief.
3. Binnen het DB de voorzitter als portefeuillehouder voor dit onderwerp benoemen, zodat de directeur snel kan schakelen om bestuurlijke rugdekking te krijgen als er nadere acties nodig zijn.
4. Instemmen met het inwinnen van juridisch advies over aansprakelijkheid.
5. In de BacPG aandacht vragen voor de landelijke governance van informatievoorziening en dan specifiek de betrokkenheid van de GGD'en en GGD-bestuurders bij de besluitvorming over IT.

Eerdere besluiten

Gevolgen

Besluit

De secretaris, [redacted] de voorzitter, [redacted]

Bijlage(n)

1. Brief 2 juli 2020
2.

Verslag gesprek [redacted] en [redacted] over Programma Corona

22-02-2021

Aanwezig: [redacted]

Afwezig: --

Bespreekpunt	
Welkom en opening	Er zijn geen aanvullingen op de agenda.
	De OR geeft aan dat dit gesprek als doel heeft om een beeld te vormen over de gang van zaken binnen Programma Corona. Het maken van afspraken doet de OR met [redacted] en niet in dit overleg. [redacted] geeft aan dat dit doel voor hem helder was en dat de formele rol ligt bij [redacted]
Voortgang vaccineren	Inmiddels heeft de GGD 3 locaties voor vaccineren. Veghel, Tilburg en Den Bosch draaien al. In Oss en Boxmeer zijn locaties gevonden, maar deze draaien nog niet. Voor Uden, Boxtel en Waalwijk wordt nog naar locaties gezocht. Dit worden L of XL locaties, op basis van de nieuwe informatie. De leveranties van vaccins wordt steeds bijgesteld; waar we eerst uitgingen van 7.000 per dag wordt dit nu 12.000. Dit betekent ook iets voor het aantal medewerkers die we nodig hebben. Er zijn berekeningen over hoeveel medewerkers we op korte en langer termijn nodig hebben, in relatie met het aantal vaccins dat je voorradig hebt. De werving hiervoor loopt, waarbij het uitgangspunt is dat dit niet ten koste mag gaan van de reguliere werkzaamheden van de GGD. In de afgelopen week zijn er twee medewerkers uit het reguliere proces ingevlogen, om een acuut tekort op te vangen. De wijzigingen in de vaccins (merken) heeft ook consequenties voor de doelgroepen die gevaccineerd worden. Dit maakt het proces ook lastig voorspelbaar. voor de locatie Veghel is een Arborapport opgesteld. Hierin zitten een aantal operationele verbeterpunten, die

	allemaal worden uitgevoerd. De OR zal dit rapport ontvangen.
Voortgang testen en BCO	Momenteel wordt er weinig getest. Het is rustig op de teststraten. Wel zijn er ontwikkelingen m.b.t. de ademtests. Landelijk zijn apparaten aangeschaft, welke onze GGD 9 zal ontvangen. Deze worden in Den Bosch (Brabanthallen) en Tilburg (een nieuwe locatie, mogelijk de oude GGD-locatie) in gebruik genomen. Doordat het nu rustiger is, worden medewerkers ook tijdelijk minder ingezet. Het doel is wel om mensen aan te houden, zodat ze wel weer inzetbaar zijn als het drukker wordt. Voor BCO geldt dit ook. Momenteel wordt er volledig BCO uitgevoerd. Er is een landelijke schil die weinig te doen heeft en deze medewerkers worden nu door GGD GHOR opgedragen aan de regionale GGD-en. HP-zone is een systeem voor infectieziektebestrijding. Voor Corona is dit aangepast naar HP zone light en wordt nu zelfs vervangen. Het nieuwe systeem heeft dezelfde functies, maar heeft een betere beveiliging. De termijn waarop dit wordt ingevoerd is onduidelijk. Medewerkers moeten hiervoor getraind worden en de gegevens moeten goed opgehaald kunnen worden uit het systeem.
Informatiegegevens / Vertrouwen GGD	Er is afgelopen week een bericht gestuurd naar alle medewerkers over wat er allemaal gaande is op dit gebied. De werkgroep die in eerste instantie bezig was met het datalek wordt overgenomen door een projectgroep gegevensbescherming, die verder aan de slag gaat met gegevens bescherming en de gevolgen van het datalek. Zo worden er nog VOG's opgevraagd van medewerkers die al worden ingezet en mogen nieuwe medewerkers nu pas aan de slag als het VOG binnen is. Voor het projectplan gegevensbescherming is een vacature (36 uur) opengezet, zodat er meer tijd is om alle acties die opgepakt moeten worden ook opgepakt kunnen worden. Hiermee wordt [redacted] ontlast. Met GGD GHOR zal in gesprek worden gegaan over de verhouding met de regionale GGD-en. Moeten de regionale GGD-en door GGD GHOR worden aangestuurd, of opereren zij als opdrachtgever aan GGD GHOR.
Contactbijeenkomsten OR	[redacted] en [redacted] zijn benieuwd naar de voortgang van de contactbijeenkomsten van de OR. Voor a.s. donderdag zijn er 10 aanmeldingen, voor de week erna pas 1. De OR wil hier bespreken wat er goed gaat, wat beter kan en wat hiervoor nodig is. Ook de rol van de OR en het uitspreken van verwachtingen zullen worden besproken.
Beleid thuiswerken	De OR heeft een aantal vragen ontvangen over het thuiswerkbeleid voor medewerkers van het Programma Corona.

	Medewerkers geven aan dat ze min of meer verplicht worden om op locatie te werken, terwijl het landelijk beleid toch is om zoveel mogelijk thuis te werken. [redacted] geeft aan dat een mogelijk kan is dat een reden hiervoor is dat je met deze medewerkers toch in contact wilt blijven, omdat het gaat om complexe situaties. [redacted] geeft aan dat communicatie hierover naar medewerkers belangrijk is.
Rondvraag	--

Verslag gesprek [redacted] en [redacted] over Programma Corona

13-04-2021

Aanwezig: [redacted]

Afwezig: [redacted]

Bespreekpunt	
Welkom en opening	Er zijn geen aanvullingen op de agenda.
	Algemeen: dit gesprek heeft als doel voor de OR om een beeld te vormen over de gang van zaken binnen Programma Corona. Het maken van afspraken doet de OR met [redacted] en niet in dit overleg.
Update Programma	Het proces is in een andere fase gekomen; de blik is erg vooruit gericht. Naar de herstelfase. Het lijkt wat rustiger te worden. Volgende week gaan vaccinatiestraten 6 en 7 open. Daarna volgt alleen nog de straat in Boxtel. Onze GGD heeft gekozen voor straten dicht bij de burger, op maximaal 30 minuten rijden. Vaccinatie: Er vindt landelijk een discussie plaats tussen GGD-en en huisartsen over wie welke doelgroepen vaccineert. De diversiteit aan vaccins en de onduidelijkheden geeft veel onrust bij mensen. Voor spillage is een landelijk beleid op gemaakt. Hiervoor zijn drie doelgroepen gemaakt die hiervoor in aanmerking komen. De groep "mensen tussen de 18-60 jaar met medische indicatie" komt hiervoor vandaag te vervallen. Dan blijven er nog twee doelgroepen over. Het is de bedoeling om de spillage zo klein mogelijk te houden. Er blijven ook weinig vaccins over per dag. Testen: Er wordt in Tilburg een nieuwe locatie geopend voor de blaastesten. De teststraat voor mensen zonder klachten die zich willen laten testen met een sneltest, wordt nu voor gekeken waar deze moet komen. Het is geen publieke taak en hoort dus niet bij de GGD. Toch is er discussie om deze teststraten op dezelfde locatie te organiseren. Het aantal mensen dat zich laat testen loopt op en het aantal positieven is momenteel ook hoger. Er zijn zorgen bij de GGD over de thuis-sneltesten die mensen aanschaffen.

	BCO: we bevinden ons nog steeds in fase 3; mensen bellen zelf hun contacten op. Het aantal clusters is afgenomen. Clusters zie je met name relateert aan de werkplek. Op scholen vlakt het aantal positieven af. KCC en dashboarden: Geen specifieke wijzigingen / zaken. HP-zone light wordt vervangen en is inmiddels getest in pilot-regio's. Onze GGD gaat pas later starten en kan hierdoor profiteren van ervaringen van collega GGD-en. De eerste geluiden over het systeem zijn positief. De instructie in dit nieuwe systeem voor medewerkers moet nog plaatsvinden. VWS is eigenaar van het systeem en dus ook opdrachtgever. Voor de uniformiteit is dit positief. Het kan een voorbode zijn voor de overige systemen van de GGD; dis kan VWS straks geheel in regie nemen. Wanneer er fouten in het systeem zitten, zoals het datalek wat we pas hebben gehad, dan is de regionale GGD aansprakelijk.
Luchtkwaliteit testlocaties	Er zijn metingen van de luchtkwaliteit gedaan op de testlocaties. GGD GHOR heeft hiervoor een toolkit gelanceerd. Dit is een samenwerking met MMK. Er is een eerste scan gedaan bij onze teststraten. Wanneer er een meting wordt uitgevoerd, kan dit ook gevolgen hebben voor het proces. Zodra hier uitkomsten van zijn, komt dit hier terug op de agenda.
Contactbijeenkomsten OR	[redacted] hebben een schriftelijke terugkoppeling gegeven op de punten die uit de OR contactbijeenkomsten met medewerkers. Dit is een heldere weergave van hetgeen er wordt opgepakt. [redacted] geeft aan dat er een aantal nieuwe punten zijn aangegeven bij de OR. Het zou goed zijn als medewerkers dit rechtstreeks aangeven bij hun leidinggevende, zodat ze ook snel kunnen worden opgepakt. De OR heeft dit ook benoemd naar de aanwezige medewerkers. Het verslag is door de OR gedeeld met de aanwezige medewerkers en via Hartslag. [redacted] zal hun reactie hierop en de wijze waarop zij deze oppakken ook via Hartslag communiceren.
Psychosociale opvang medewerkers	De OR stelt de vraag op welke wijze er aandacht is voor de psychosociale opvang van medewerkers. Er is een extern bureau waar medewerkers terecht kunnen bij problemen. Ook onze inhuur medewerkers kunnen hier terecht. Dit is een uitzondering, want zij zouden eigenlijk naar hun eigen uitzendorganisatie moeten hiervoor. Voor agressie en incidenten wordt benadrukt dat medewerkers hiervoor het formulier invullen, zodat deze in beeld

	zijn en opgepakt kunnen worden. De Pshi verzorgt de nazorg van medewerkers. Er is ook de mogelijkheid om een zorgbuddy te krijgen. Dit is speciaal voor zorgmedewerkers en mantelzorgers opgericht. De OR vraagt ook of er aandacht is voor medewerkers die maanden in het Corona Programma hebben gewerkt en weer terug gaan naar hun reguliere taak. Dit zal de OR met [redacted] verder bespreken.

Verslag gesprek [redacted] en [redacted]er Programma Corona
09-09-2021

Aanwezig: [redacted]
Afwezig: --

Bespreekpunt	
Welkom en opening	Er zijn geen aanvullingen op de agenda.
	Algemeen: dit gesprek heeft als doel voor de OR om een beeld te vormen over de gang van zaken binnen Programma Corona. Het maken van afspraken doet de OR met Therese en niet in dit overleg.
Stand van zaken Programma	Landelijk is de daling van de cijfers gestopt; de cijfers blijven stabiel, maar wel te hoog stabiel. Gelukkig blijft onze GGD onder de landelijke cijfers. De uitbraak lijkt zicht te verplaatsen naar de noordelijke provincies. Testen Momenteel loopt vanuit VWS de aanbesteding Laboratorium diagnostiek. VWS heeft aangegeven dat zij de afnamegarantie voor de laboratoria zullen handhaven. Er is door diverse binnen- en buitenlandse partijen bezwaar aangetekend bij de rechter tegen deze gunning. In Den Bosch, wijk de Hambaken is een nieuwe locatie geopend in plaats van de Brabanthallen. Deze is locatie is vergelijkbaar qua capaciteit. Vaccineren Dit onderdeel blijft zwaar in ontwikkeling. We hebben de hoogste vaccinatiegraad van Nederland. We zijn wijken waarin de vaccinatiegraad achterblijft, maar ook binnen bepaalde groepen (jongeren, studenten, arbeidsmigranten, etc.). Met de betreffende gemeenten is contact om te kijken hoe we de vaccinatiegraad hier omhoog kunnen krijgen. In Tilburg blijft een vaccinatielocatie langer open, in de hoop de vaccinatiegraad in bepaalde wijken en onder studenten hier omhoog te krijgen.

Met opmerkingen [BvBI1]: [redacted] klopt dit, want ik kon het niet meer goed terughalen.

	In Den Bosch is locatie De Brabanthallen gesloten op verzoek van de locatie zelf. Zij gaan weer starten met hun hun reguliere programmering. Met Avans Hogeschool zijn gesprekken geweest om ook daar de studenten laagdrempeliger te vaccineren. Er was hiervoor een mogelijke locatie gevonden op de onderwijsboulevard. Hier is toch vanaf gezien, om eventuele dreiging te voorkomen. Met name jongeren 18-, zijn fel aan het protesteren tegen vaccinatie en schuwen hierbij de harde middelen niet (bedreiging, agressie en zelfs nog erger). De locatie op de onderwijs boulevard was moeilijk te beveiligen, daar kon iedereen binnenlopen en er was een MBO-school in de nabije omgeving. Er wordt nu gekeken naar een alternatieve locatie. Ook de vaccinatiegraad bij arbeidsmigranten blijft achter. De vaccinatiebereidheid onder deze groep is laag. De uitzendorganisaties vragen de GGD om ook hier dichterbij te vaccineren, maar dat gaan we niet doen. Speciaal voor deze groep is er voorlichting in diverse talen. Deze wordt op locatie actief worden aangeboden en er zijn tolken aanwezig. De vaccinatie van deze groep blijft op de GGD locaties plaatsvinden. Boosterprik of derde vaccinatie Dit zijn twee verschillende dingen: De derde prik is voor mensen met onderliggend lijden. De verwachting is dat hiervoor volgende week het verzoek komt van VWS om deze groep mensen te vaccineren. Dit zijn ongeveer 200.000 mensen. Boosterprik: de prik voor alle mensen die nu ook in aanmerking komen voor vaccinatie. De gezondheidsraad gaat zich de komende tijd buigen over de vraag of deze in Nederland ingezet moet worden. Zij volgen hierin het voorbeeld van andere landen. De verwachting is dat de politiek het advies van de gezondheidsraad op gaat volgen. Voor de GGD betekent dit enerzijds meer tijd om je hierop voor te bereiden, anderzijds geeft het een langere tijd van onzekerheid. Dit geeft nu al onrust onder de medewerkers van het Programma. Zij weten voorlopig niet of hun contract al dan niet verlengd gaat worden. Doordat er nog geen zicht is op de omvang van het aantal mensen dat een extra prik moeten krijgen en de gunning (aanbesteding) nog loopt, weten zittende partijen niet of zij hun medewerkers straks ook nog bij ons kunnen plaatsen. Er is een beweging ingezet dat medewerkers zelf zoeken naar een andere baan en dus het programma verlaten.

	Op dit moment is het rustig. We hebben 3 vaccinatielocaties open en we hebben een prikbus rondrijden. Wanneer er boosterprikken gezet gaan worden, gaat onze GGD terug naar 8 locaties. De GGD wil zijn inwoners en zijn gemeenten tegemoet komen door dichtbij te vaccineren. De strategie wordt: o De drie huidige vaccinatielocaties blijven ongewijzigd. o Den Bosch en Boxmeer krijgen nieuwe vaccinatielocaties, voor zowel boostervaccinaties als vrije inloop; deze worden gezocht. o Voor de overige drie locaties geldt dat deze weer open gaan als de boosterprikken gezet gaan worden. In alle gemeenten gaan we drie dagen zitten, om iedereen die zich nog wil laten vaccineren de kans hiervoor te geven (vrije inloop). De communicatie hierover moet stevig worden ingezet, zodat onze inwoners hiervan ook op de hoogte zijn. Dit is een tegemoetkoming aan zowel burgers als bestuurders. Het is niet efficiënt, maar wel effectief. BCO Door de opening van de scholen zijn er in de ander provincies al behoorlijke clusters binnen scholen te zien. Zeer waarschijnlijk krijgen wij hier ook mee te maken. Er gaan binnenkort gesprekken plaatsvinden tussen het programma en de reguliere sectoren over hoe verder te gaan na Corona.
Aanbestedingen – stand van zaken	De aanbesteding voor de inhuur van flexibele arbeidskrachten Corona 2022 is nu gepubliceerd. Rond 8 november verwachten ze meer duidelijkheid over wie de gunning gaan krijgen. De OR geeft aan tevreden te zijn over de wijze waarop hij is meegenomen in het proces van aanbesteding en de communicatie met de betrokkenen. Er lopen aanbestedingen voor BCO. De gunning hiervan gaan naar 1 partij. Dat kan de huidige partij zijn, maar dat hoeft niet.

	Er loopt een aanbesteding bij de diensten rondom verkeersregelaars, beveiligers, etc. Dit zijn geen reguliere GGD-taken. Deze aanbesteding kan mogelijk met 1 maand uitgesteld worden, maar dit moet wel voor eind 2021 gegund zijn. Al deze aanbestedingen vragen veel van de afdeling inkoop.
Uitkomsten AP-onderzoek datadiefstal	Er is n.a.v. het datalek een bezoek gebracht aan twee andere GGD-en. Onze GGD is niet bezocht. Er wordt geen boete opgelegd, maar er is een lijst met aanbevelingen opgesteld voor de GGD-en. Van deze punten zijn de meeste door onze GGD al opgepakt / in gang gezet. Er wordt niet verwacht dat dit nu veel extra werk voor ons meebrengt. De GGD-en gaan zich gezamenlijk richten op een NEN-certificering rondom beveiliging persoonsgegevens. Dit vraagt mogelijk wel wat van onze GGD. Dit zijn behoorlijke trajecten.
Medewerkersonderzoek Programma Corona- stand van zaken	De input van de OR is verwerkt in de vragen die zijn afgenomen. De respons was goed, ongeveer 348 medewerkers hebben meegedaan (25% ongeveer). De medewerkers geven de organisatie een gemiddelde 8, tegenover een rapportcijfer van 7,4 voor de feitelijke werkgever. Als verbeterpunt geven zij aan "het luisteren naar medewerkers en het oppakken van feedback". De afschaling door het uitzendbureau gaat snel geven mensen aan. Dat is logisch, omdat de afschaling vaak abrupt gaat. Ook hoeven mensen nu minder vaak te werken en worden ze minder ingeroosterd. Vervolg: o Opstellen van een verbeterplan voor de planning. o Terugkoppeling van de respons aan de uitzendbureaus. o Terugkoppeling van de respons aan de OR. o Bekijken of er een tweede medewerkersonderzoek uit wordt gezet aan het eind van het jaar. De ontvangt het rapport van [redacted] Deze agenderen voor het volgend overleg.
Signaal	Er is een discussie gaande over dat de GGD geen onregelmatigheidstoeslag uitkeert aan medewerkers van schaal 11 en hoger. Dit is vastgelegd in de cao en geldt ook voor medewerkers van het programma. Sommige

	uitzendkrachten kregen dit in het verleden wel, maar dat is teruggedraaid. Op en af laait hier de discussie over op. Doordat deze regeling er is, willen mensen die in salarisschaal 11 of hoger zitten, in de weekenden liever niet werken. Daardoor komen roosters lastig rond.
Rondvraag	--

Actielijst verbeterplan gegevensbescherming & gevolgbestrijding datadiefstal Versie 8-2-2021

Nr.	Actie	Actiehouder GGD HvB	Afwikkelingsniveau landelijk, regionaal of lokaal	Status	Start	Deadline	Uitwerking i.s.m.	Stand van zaken/resultaat
AVG		Trekker: [redacted]						
	Werkprotocollen AVG							
18	Werkinstructies voor testen, BCO, vaccinatie (inclusief AVG)	[redacted]	Lokaal	Loopt	8-2-2021			Werkinstructie teststraten is geanalyseerd en verbeterpunten opgepakt. Werkinstructie BCO is analyse nog niet gereed.
19	Werkinstructies datalek	[redacted]	Lokaal	Loopt	8-2-2021			
	Inzage- en verwijderingsverzoeken							
1	Uitwerken procedure inzage, wijzigen en wissen gegevens	[redacted]	Lokaal	Afgerond	25-1-2021	28-1-2021		
15	Traject inregelen voor afwikkeling van de verzoeken	[redacted] / ….	Lokaal	Loopt		8-2-2021	[redacted] en [redacted]	Werkinstructie vorige week ingeregeld: inzien mailbox. Instructie ligt nu bij artsen over hoe we verzoeken gaan beoordelen. Ontbreekt echter nog aan landelijke kaders. We gaan wel al verzoeken in behandeling nemen voor zover dat nu al wel kan zonder landelijke kaders. Eind van de week nadere communicatie indien we uitstel nodig hebben. Wordt nu gewerkt aan format voor uniform besluit.
ICT		Trekker:						
	0. Governance IT							
20	Uitzetten externe opdracht voor visie op informatievoorziening: start brainstorm sessie governance regionaal-landelijk	[redacted]		Loopt	8-2-2021	8-2-2021	[redacted]	
	1. Visie informatievoorziening							
21	Uitzetten externe opdracht voor visie op informatievoorziening	[redacted]		Loopt	8-2-2021	8-2-2021	[redacted]	
	1a. Applicatielandschap							
22	Opdrachtverzoek uitzetten voor scan van applicatielandschap	[redacted]		Loopt	8-2-2021	8-2-2021		Actie is intern uitgezet. Ter vergelijk (snelheid tegenover kosten) is ook externe partijen om offerte voor dit onderdeel gevraagd
	1b. Security							
2	Logging uitzoeken: wat kon tot op heden wel en wat niet	[redacted]	Lokaal	Afgerond	25-1-2021	28-2-2021		
6	Uitzoeken autorisaties landelijke pool BCO	[redacted]	Lokaal	Afgerond	25-1-2021	1-2-2021		
17	Voorstel loggingtermijn	[redacted]	Lokaal	Loopt		8-2-2021		
23	Brede security scan uitvoeren (systemen, applicaties en infrastructuur)							
24	Vaststellen prioritering en planning voor opstellen van ontbrekende Data Protection Impact Assessments (DPIA)							
40	Nadere analyse van huidige en benodigde logging, ook voor partijen als Yource (landelijk)	[redacted]			8-2-2021			
	2. Implementatie IT-wijzigingen							
7	Aanstellen projectleider "implementatie IT-wijzigingen programma Corona" (landelijke aanpassingen en vernieuwingen systemen en processen)	[redacted]	Lokaal	Loopt	28-1-2021	2-2-2021	[redacted]	Raakvlakken aanleveren aan [redacted] wat ligt er op de stapel en komt er aam? Vervallen functionaliteiten doorgeven (IZB en TO) incl. kijken naar impact (middel)lange termijn
33	Invoeren 2-weg authenticatie en beveiligde VPN	[redacted]	Lokaal	Loopt	8-2-2021			9 februari nut en noodzaak daarvan landelijk bespreken
34	Lessen van pilot contact app ophalen bij West-Brabant							
PERSONEEL		Trekker: [redacted]						
	VOG & geheimhoudingsverklaringen							
3	Aanleveren HR-informatie: check op huidige VOG's en geheimhoudingsverklaringen	[redacted]	Lokaal	Afgerond	25-1-2021	29-1-2021		[redacted] levert tweede versie aan aan [redacted] Alles op orde voor extern personeel en intern personeel na invoering van dit beleid. Vraag hoe om te gaan met vaste medewerkers die al lang in dienst zijn (wel geheimhoudingsplicht op basis van Wrna) VOG: inhaalacties HR
14a	Aanscherpen afspraken met externe bureaus over overaanleveren VOG en controles op uitdenstmeldingen	[redacted]	Lokaal	Afgerond		8-2-2021		
14b	Aanscherpen afspraken met externe bureaus over uit dienst-meldingen			Loopt				
25	Aanscherpen VOG: start in diensttreding pas als VOG er is, niet al als VOG is aangevraagd	[redacted]	Lokaal	Loopt	8-2-2021			Nu al proactief iets mee in het kader van mogelijk personeelstekort. Ook communiceren naar Yource
26	Checken profiel 45 versus specifiek profiel omgaan met persoonsgegevens: doorlooptijd aanvraag?	[redacted]	Lokaal	Loopt	8-2-2021			

	Trainingen & instructies							
27	Checken vakbekwaamheidsbeleid voor 'omgang met personeelsgegevens'	[redacted]	Lokaal	Loopt	8-2-2021			
WERKPROCESSEN								
	Werkprocessen programma Corona							
28	Opstellen PvA invoeren GGD contact app en BCO-portaal							Nog veel onduidelijk of het HPZone light gaat vervangen
29	Planning en projectgroep opzetten voor invoering landelijke e-learning GGD contact app							
	Werkprocessen sectoren							
STAKES		Trekke[redacted]						
	Juridisch							
30	Juridisch advies over grond voor verwijderingsverzoeken (AVG, WGBO, WPG)	[redacted]		Loopt				
31	Juridische afdelingen grote gemeenten verzoeken om advies over [redacted]	[redacted]	Lokaal	Afgerond				
	Onderzoek							
11	Verzamelen documentatie afgelopen maanden over Governance, Performance e.d.	[redacted]	Lokaal	Afgerond	28-1-2021	4-2-2021		
35	Ondersteuning regelen voor FG bij het intern uitzetten van onderzoeksvragen AP	[redacted]		Loopt	8-2-2021			[redacted] en [redacted] nemen dit mee naar MT 8 februari
	Financiën							
32	Financiën: borging van risico in jaarstukken, verantwoording aan DB/AB o.b.v. risicoanalyse							
COMMUNICATIE								
	Externe communicatie							
8	Opstellen proactieve communicatielijn GGD HvB	[redacted] & [redacted]	Lokaal	Afgerond	28-1-2021	1-2-2021	Communicatie & Projectleider bereikbaarheid	Incl. uitwerking instructie uitvoering (KCC) < landelijk telefoonnummer Artikel geplaatst op website en SM! [redacted] ondersteunt landelijk < link Q&A Opdeze termijn geen aanleiding voor extra actie.
10	Q&A uitbreiden	[redacted] & [redacted]	Lokaal	Afgerond	28-1-2021	28-2-2021	Landelijk in de lead	8 februari: landelijk is Q&A aangepast
12	Verwachtingsmanagement richting klanten in communicatie: Jurisdische duiding bij verzoek gegevens wissen uit medische dossier uitwerken & instructie en communicatie (	[redacted] & [redacted]	Lokaal	Loopt	1-2-2021	8-2-2021	[redacted]	Landelijke kaders (richtlijn)is de basis. Individuele beoordeling blijft noodzakelijk
16	Input geven aan communcatie over proces / status	[redacted]	Lokaal	Loopt		8-2-2021	[redacted]	Nieuwsbrief
	Interne communicatie							
	Informeren MT, bestuur, gemeenteraden							
36	Sheets over datadiefstal in webinar 10 februari	[redacted]		Loopt				[redacted] heeft eerste sheet aangeleverd bij [redacted] voor webinar
37	Beantwoording vragen gemeenteraad Dongen	[redacted] [redacted]		Loopt				
41	Beantwoording vraag DB over inzage BN'ers in CoronIT	[redacted]		Loopt	8-2-2021			
OVERIG								
4	Voorstel opzet landelijke governance in DPG-raad	[redacted]	Landelijk	Loopt	28-1-2021	2-2-2021		Input aanleveren 'hoe komen we als GGD in charge' aan [redacted] Brabantbreed: Voorstel / advies over invulling & versterking eigen organisatie binnen / vanuit de regio richting GGD GHOR NL (regionale autonomie en slagkracht).
5	ID Manager in DPG-raad [redacted])	[redacted]	Landelijk	Loopt	28-1-2021	2-2-2021		4 & 5 in overleg 2-2-2021
9	Voorstel organisatie standup-team (o.a.eigenaarschap)	[redacted] & [redacted]	Lokaal	Afgerond	28-1-2021	1-2-2021		Bij plaatsing in staande organsiatie is dit overleg overbodig. [redacted]: op afroep [redacted]/ HR: op afroep
38	Nieuw voorstel projectorganisatie voor verbeterplan	[redacted] [redacted] [redacted]		Loopt	8-2-2021			Behoefte aan structureel overleg, wellicht ook nog voor deelonderwerpen (AVG versus implementatie in programma)
39	Bezien welke extra ondersteuning voor verbeterplan nodig is	[redacted] [redacted] [redacted]		Loopt	8-2-2021			

Annotatie voor [redacted] voor DB 4 maart 2021

Verzoek GGD GHOR NL om volmacht

Op vrijdag 26 maart heeft de GGD GHOR NL bij alle GGD'en het verzoek ingediend om:
Een volmachtiging te ondertekenen en uiterlijk te retourneren op dinsdag 2 maart 2021.

Aanleiding:
De verdere afhandeling van de datadiefstal. In dat kader is de GGD GHOR NL verplicht om eventuele slachtoffers van de datadiefstal te informeren. De gegevens van slachtoffers worden binnenkort door de politie verstrekt. Slachtoffers moeten zo snel als mogelijk over de diefstal van hun persoonsgegevens in kennis worden gesteld.

De GGD GHOR NL treft voorbereidingen om dat op een goede en veilige manier te doen. Omdat het mogelijk om slachtoffers van alle regionale GGD'en kan gaan, heeft de GGD GHOR NL een volmacht van alle GGD'en nodig om dit te doen.

Strekking van de volmacht bij ondertekening

1. GGD HvB GGD geeft volmacht en machtiging aan de GGD GHOR om
   - te voldoen aan de op de GGD'en en GGD GHOR rustende mededelingsplicht aan betrokkenen (art. 34 AVG)
   - gerelateerd aan de (vervolg)meldingen door GGD GHOR van 22 en 25 januari 2021 bij de Autoriteit Persoonsgegevens (art. 33 AVG)
   - en verband houdende (vervolg)onderzoeken van de AP naar ongeautoriseerde toegang tot persoonsgegevens,
   - in de relevante systemen CoronIT en HPZone(Lite).
2. GGD GHOR NL heeft een (concept)brief voor slachtoffers opgesteld, deze zal na vaststelling met de GGD'en worden gedeeld.
3. Deze volmacht is een aanvulling op het "Convenant Gegevensuitwisseling Gezamenlijk Verantwoordelijken" april/mei/juni 2020.

Advies: van onze functionaris gegevensbescherming [redacted]

Voorlopig is mijn advies om hier **geen** akkoord op te geven vanwege de volgende redenen:
- In het convenant wordt gesproken over het feit dat alle partijen zelfstandig verantwoordelijk zijn voor het afhandelen van een incident. Op het moment dat we middels een volmacht deze verantwoordelijkheid uit handen geven aan de GGD GHOR is het belangrijk om precies te weten wat de GGD GHOR gaat doen.
- Het is onduidelijk hoe deze werkzaamheden die ten gevolge van de datadiefstal opgepakt gaan worden door de GGD GHOR organisatorisch worden ingericht worden (hoe verloopt dit proces, wie doet wat, hoeveel personen erbij betrokken etc.).
- Hoe verloopt de communicatie vanuit de GGD GHOR (inhoud brief/ terugkoppeling aan de GGD'en /archivering brieven etc.). Wie is verantwoordelijk voor dat stuk?
- Krijgen wij als regionale GGD inzicht in de aangeschreven burgers van onze gemeenten?
- Wie is verantwoordelijk voor het beantwoorden van vragen van burgers in onze werkgebied? Wie gaat de nieuwsvragen afhandelen?

Beslispunt voor het DB

1. Wij vragen het DB om akkoord te gaan met dit verzoek om volmacht van de GGD GHOR NL, en om de bevoegdheid tot het onderteken van deze volmacht te mandateren aan de voorzitter.

Bijlage 1: Volmachtiging aan GGD GHOR inzake mededeling datalek aan betrokkenen af te geven door de GGD'en.
Bijlage 2: Tekenblad GGD Hart voor Brabant

Landelijke datadiefstal gegevens coronatesten

Aanvullende antwoorden Q&A voor GGD Hart voor Brabant

Wat is er geregeld rondom de aanname van nieuwe mensen en bescherming persoonsgegevens?

- Alle medewerkers die in dienst treden bij GGD HvB leveren een VOG aan en tekenen een geheimhoudingsverklaring.
- Alle medewerkers die worden ingehuurd via een uitzendbureau leveren een VOG aan en tekenen via het uitzendbureau een geheimhoudingsverklaring.

Welke collega's hebben de mogelijkheid om een zogenaamde databasedump uit te voeren?

- N.a.v. het incident is er onderzocht wie geautoriseerd is om dit uit te voeren voor onze regio.
- Een beperkte groep is op dit moment geautoriseerd om deze databasedump uitvoeren.
- N.a.v. eerste check: er zijn geen gegevens in verkeerde handen gevallen
- We zien geen afwijkingen in de IT omgeving van GGD Hart voor Brabant

Hoe heeft GGD HvB de autorisaties geregeld?

- Binnen GGD HvB hebben wij een autorisatiematrix gebaseerd op rol of functie van iedere medewerker.
- Medewerkers krijgen alleen die autorisatie die nodig is voor zijn of haar functie.
- De autorisatiematrix wordt bijgehouden bij in-, door- en uitstroom van medewerkers
- Er vindt hierop een maandelijkse check plaats.

Controles systemen

- Via logging Microsoft kunnen we 30 dagen terugkijken.
- Voorgesteld wordt om deze logging tijd te verlengen.
- N.a.v. eerdere incidenten kunnen we wel nagaan waar mogelijk sprake was van onjuist gebruik van de systemen.

N.a.v. incident zwaardere dijkbewaking nodig. Hoe gaan we dat inregelen?

- Autorisaties binnen het programma corona nog nadrukkelijker controleren.

Opmerkingen privacyconvenant testketen

Overall advies FG/PO:
- nog niet akkoord te gaan met dit opgestelde convenant, gezien alle opmerkingen en vragen die we nog hebben;
- gezien de ervaring met het datalek bij Microvida het zeer belangrijk is dat we onderlinge afspraken goed in het convenant vastleggen;

Artikel 4:

- GGD GHOR wordt als verwerker aangezien. Dit valt inderdaad te beargumenteren maar is wel een verandering in de rolverdeling tussen GGD'en en GGD GHOR. Mogelijk is dit naar aanleiding van de notitie van Hooghiemstra hierover. Wel moet worden gekeken of het convenant tussen de GGD'en en GGD GHOR t.a.v. CoronIT dan nog kloppend is. Daarnaast met de GGD het eens zijn met deze rolverdeling, aangezien hier de eerste stap gemaakt wordt in deze richting.
  Is GGD GHOR verwerker in deze? Hebben de GGD' en voldoende zeggenschap gehad in deze situatie om de rol van verwerkingsverantwoordelijke op zich te nemen? Hier heb ik geen duidelijk beeld van, maar als dit het geval is dan is er geen direct bezwaar tegen deze rolverdeling.
- Er is sprake van een gezamenlijke verwerkingsverantwoordelijkheid tussen de GGD'en en de laboratoria. Deze rolverdeling moet erg zorgvuldig/specifiek worden bepaald. Dit is deels gedaan, maar [redacted] een scherpe rolverdeling over de data die uit de analyse voortvloeit. Uit de analyse vloeit een berekening voort met het aantal virusdeeltjes dat in het afnamemonster voorkomt. Deze berekening is waardevol voor het doen van onderzoek etc. Wanneer het lab verwerkingsverantwoordelijke is voor deze analysefase, dan kunnen zij mogelijk deze data voor eigen doeleinden gebruiken. Het is de vraag of de GGD' en dit wenselijk vinden. Zeker gezien het feit dat een betrokkene mogelijk niet weet dat het lab persoonsgegevens verwerkt. In die zin valt af te vragen in hoeverre er überhaupt sprake is van gezamenlijke verantwoordelijkheid. Het klopt dat het lab de analyse op eigen wijze uitvoert, maar dit kan ook het geval zijn wanneer zij verwerker zijn. Wanneer de GGD van mening is dat zij moeten kunnen bepalen hoe het lab met de gegevens omgaat, ook in de analysefase, [redacted] voor een puur verwerkerschap in plaats van een gezamenlijke verantwoordelijkheid.
- Lid 3: welke doeleinden zijn bepaald? Wat mag het lab doen met de analyse in het kader van onderzoeken bijvoorbeeld? Dit is mogelijk waardevolle data voor het lab en de ziekenhuizen. De doeleinden zoals bepaald in bijlage 1 zijn te summier. Ik zou een duidelijker beeld willen zien van de verwerkingen en de doeleinden van deze verwerkingen. Zo is het ook duidelijk welke verwerkingen plaatsvinden op grond van dit convenant en wanneer er dus een verwerking heeft plaatsgevonden die buiten dit convenant valt. Wanneer dit niet duidelijk wordt omschreven kan dit later zorgen voor discussie wanneer de ene partij stelt dat een verwerking buiten de afspraken in het convenant heeft plaatsgevonden.

Artikel 6:

- Verwerking wordt gebaseerd op WPG. Dit begrijp ik niet omdat er nu juist sprake van is om het 'testen' onder de WGBO te laten vallen.

Artikel 7:

- Er moet duidelijk bepaald worden wat de rolverdeling is bij verwijderverzoeken. Moet de GGD een verwijderverzoek doorsturen naar een lab of moet de betrokkene zelf een verwijderverzoek indienen bij het lab? De betrokkene weet namelijk in de meeste gevallen niet dat er een lab bij betrokken is en als zij dat wel weten, dan is het nog niet duidelijk voor de betrokkene welk lab dit is. Als het lab verantwoordelijke is voor de analyse, dan is het de vraag of de GGD een verwijderverzoek moet doorzetten en of het lab dan ook moet verwijderen (ligt aan de reikwijdte van art. 19 AVG). In principe moet het lab dan zelf een afweging maken over verwijdering wanneer zij als verantwoordelijke worden gezien. Wanneer het lab verwerker is dan is dit niet het geval. Dan moet de GGD het verzoek doorzetten naar het lab en moet het lab ook verwijderen wanneer de GGD dit nodig acht.
- Wanneer er sprake is van gezamenlijke verantwoordelijkheid, moet de GGD de betrokkene goed informeren. Op basis van dit convenant moet de privacyverklaring worden aangepast waardoor betrokkenen beter worden geïnformeerd over de rol van het lab.
- De bewaartermijnen worden bepaald in bijlage 1, maar wat als er eerder een verzoek tot verwijdering wordt gedaan. Wie bepaalt dan of het eerder verwijderd kan worden? Is dit de GGD of het Lab?

Artikel 8

- Is het wenselijk dat de verwerkingsverantwoordelijke een inbreuk in verband met persoonsgegevens in eigen verantwoordelijkheid afhandelt? Dit is wel een gevolg van gezamenlijke verantwoordelijkheid waarbij het lab voor een deel als verwerkingsverantwoordelijke kan worden aangemerkt. Echter, gezien de situatie die zich nu bij Microvida heeft voorgedaan, lijkt dit wellicht niet wenselijk te zijn. Dit hangt echter af van de mate waarin de GGD zich verantwoordelijk acht voor bepaalde zaken. Indien de GGD zich niet verantwoordelijk acht voor hetgeen bij de analyse plaatsvindt en daaruit voortvloeit, dan is deze bepaling voldoende.
- Lid 2: [redacted] het nemen van maatregelen in overleg moet gaan. Zie bijvoorbeeld nu de situatie met Microvida. Daarbij stelt de GGD zich op het standpunt dat de gegevens uit de EPD's verwijderd moeten worden. Als deze bepaling in het vervolg in de weg staat aan het innemen van dergelijke standpunten en het afdwingen daarvan, dan lijkt mij dit niet wenselijk. Wat opvalt is dat er eerst kennelijk stond dat er afstemming moet plaatsvinden en dit is vervangen door informeren. Afstemmen lijkt mij wenselijker gezien de lering die we hebben kunnen trekken uit de situatie met Microvida.
- Lid 3: onverwijld informeren: dit vervangen door een concrete afspraak bijvroobeeld binnen 24 uur.
- Lid 3 en 4 bieden wel waarborgen voor een transparante samenwerking.

Artikel 10:

- Onrechtmatige verwerking in welke zin? Onrechtmatig op grond van de AVG of is het ook onrechtmatig wanneer deze verwerking in strijd is met de doeleinden zoals bepaald in de overeenkomst?

- Lid 4: Wat is de achterliggende gedachte van deze bepaling? Wat is de verhouding tussen deze bepaling en hetgeen bepaald in lid 1? Wanneer we dit vergelijken met de situatie nu bij Microvida, zou deze bepaling dan inhouden dat Microvida niet aansprakelijk kan worden gesteld wanneer blijkt dat er geen grondslag is voor het delen van de gegevens met de ziekenhuizen? Microvida stelt zich op het standpunt dat de gegevensverstrekking in overleg heeft plaatsgevonden, maar kan dit nog niet aantonen. Zou deze bepaling ervoor zorgen dat je in het vervolg labs niet aansprakelijk kan stellen in dergelijke situaties? Is dit een eis van de labs geweest?

<u>Bijlage 1:</u>

- Wat wordt er in het ICT systeem van het lab precies verwerkt. Ik neem aan dat daarin ook een analyse staat in de vorm van een berekening met daarin bijvoorbeeld het aantal virusdeeltjes. Dit zijn gegevens die gebruikt worden voor onderzoek (zie onderzoek GGD HvB en het ETZ bijvoorbeeld). Er is dus meer dan alleen een uitslag negatief/positief.
- In de overeenkomst staat dat partijen de gegevens niet voor andere doeleinden mogen verwerken dan in de overeenkomst bepaalde doelen. Deze doelen zijn echter heel algemeen, namelijk het uitwisselen en testen van monsters en het uitwisselen van de persoonsgegevens en uitslagen door middel van het registratiesysteem CoronIT en het ICT systeem van het lab. Houdt dit in dat het lab de gegevens niet aan derde mag verstrekken? Mag het lab de berekeningen eigenhandig gebruiken voor onderzoek? Als het doel algemeen is dan is er ruimte voor interpretatie vooral wanneer er sprake is van verwerkingsverantwoordelijkheid aan de zijde van het lab.
- T.a.v. de bewaartermijnen: Kan een betrokkene verzoeken eerder de gegevens te verwijderen? Wanneer GGD een verwijderverzoek ontvangt m.b.t. testresultaat, moet die dan worden doorgezet naar het lab? Moet het lab dan zelf beoordelen of deze verwijderd kan worden uit het LIMS (of soortgelijk systeem) of moet het lab deze verwijderen wanneer de GGD dit verzoekt? Dit ook in verband met de klacht die is ingediend waarbij een betrokkene het monster verwijderd wil hebben. Kan dit? Of is dit iets wat onder de verantwoordelijkheid van het lab valt? Dit laatste lijkt mij namelijk niet wenselijk, aangezien de betrokkene zich tot de GGD richt met dergelijke verzoeken. Hierover is geen duidelijke rolverdeling bepaalt. Dit alles hangt ook af van de wijze waarop art. 19 AVG geïnterpreteerd wordt.
- Klopt de bewaartermijn van 5 jaar nog wanneer testen wordt gezien als Wgbo? Ik heb begrepen dat er mogelijk wel een switch wordt gemaakt van Wpg naar Wgbo.

<u>Algemene opmerkingen:</u>

- Er ontbreekt een bepaling dat de gegevens niet aan derde mogen worden verstrekt zonder overleg met de partijen.
- Er ontbreekt wat de rolverdeling is ten aanzien van de achterliggende berekening die voortvloeit uit de analyse. Van wie is deze data en wat mag daarmee gedaan worden?
- Rolverdeling t.a.v. rechten betrokkene is niet duidelijk genoeg. Wie maakt de afweging of gegevens die het lab verwerkt eerder verwijderd kunnen worden?
- Ik zou in ieder geval nog wel een nadere onderbouwing willen van de keuze om voor gezamenlijke verantwoordelijkheid te gaan en niet voor verwerker. In mijn ogen valt namelijk ook goed te beargumenteren dat er sprake is van verwerker ten aanzien van

het lab. Dit zou ervoor zorgen dat de GGD meer zeggenschap heeft over wat er met de data van betrokkene gebeurt. Uit de eerdere opmerkingen blijkt ook dat er eerst stond dat het lab verwerker is. Waarom is dit veranderd?

- Er ligt een dienstverleningsovereenkomst aan dit convenant ten grondslag. Is deze al definitief en wat is daarin bepaald?
- Wat houdt kiemsurvaillance in? Dit staat in het document met opmerkingen. Hierover zou het een en ander bepaald zijn in de overeenkomst dat Dienst Testen met de laboratoria sluit.
- Opmerking 17 van Dienst Gezondheid en Jeugd zhz ben ik het mee eens, dat is ook wat hierboven staat aangegeven. Echter, er is geen tekstaanpassing geweest in dit punt. Gezien de situatie die zich nu heeft voorgedaan met Microvida, lijkt me dit alsnog wenselijk. Wij hebben immers het voorbeeld van hoe het in de praktijk uit kan pakken.

Technische vragen VVD Dongen n.a.v. Kadernota 2022

1. In hoeverre is sprake van toepassing van de AVG -richtlijnen binnen de huidige reguliere bedrijfsvoering? Zijn er Aantoonbare certificaten en/of gehanteerde systemen?

Binnen de reguliere bedrijfsvoering van GGD Hart voor Brabant worden de AVG-richtlijnen gehanteerd. De GGD beschikt over werkprotocollen die in lijn zijn met de AVG. Specifiek voor inzage- en verwijderingsverzoeken heeft hij voor burgers een aanvraagformulier op zijn website gepubliceerd. Vast en tijdelijk personeel dat toegang heeft tot databestanden met persoonsgegevens, wordt bij aanstelling gevraagd om een Verklaring Omtrent Gedrag en getekende geheimhoudingsverklaring.

In de landelijke en regionale werkinstructies t.b.v. testen, bron- en contactonderzoek (BCO) en vaccinatie is rekening gehouden met de rechten en plichten uit de AVG. Hierbij worden medewerkers regelmatig gewezen op het belang van privacy en de wijze waarop zij zorgvuldig met persoonsgegevens om moeten gaan. Dit zal ook in de toekomst regelmatig onder de aandacht worden gebracht bij de medewerkers.

Nadat de datadiefstel werd geconstateerd is de datalekprocedure van GGD Hart voor Brabant opnieuw geoptimaliseerd en onder de aandacht gebracht bij de medewerkers van de GGD. Dit heeft onderdeel uitgemaakt van communicatie richting de medewerkers met betrekking tot bewustwording.

Ook heeft GGD Hart voor Brabant nogmaals een check uitgevoerd. Hij heeft vastgesteld dat alle door hem ingezette externe medewerkers een VOG en ondertekende geheimhoudingsverklaring hebben. Bij vaste, interne medewerkers is dit ook het geval voor zover ze bij de GGD zijn komen werken, sinds het beleid omtrent VOG en geheimhoudingsverklaring is geïmplementeerd. Oudgedienden die al vele jaren bij de GGD werken hebben geen VOG, omdat dit destijds nog niet bestond. Daar staat tegenover dat voor alle ambtenaren (en medewerkers van GGD Hart voor Brabant zijn ambtenaren) sowieso een wettelijke geheimhoudingsplicht geldt. Bij de invoering van de Wet normalisering rechtspositie ambtenaren, hebben alle vaste medewerkers van de GGD digitaal moeten bevestigen dat zij zich houden aan de integriteitsregels, waaronder geheimhouding.

Daarnaast is het goed om te vermelden dat er afgelopen week een Audit NEN 7510 (audit voor informatiebeveiliging) heeft plaatsgehad in Het Servicecentrum (een shared servicecentrum waar GGD Hart voor Brabant met een aantal andere organisaties in deelneemt) door een externe partij, waarbij een “goed beveiligd” keurmerk is afgegeven.

2. “De coronacrisis heeft een impuls gegeven aan onze ambitie om data gedreven te werken, zoals verwoord in onze beleidsvisie.” Vanuit welke data gaat de GGD werken? Komen er koppelingen interregionaal / landelijk en is er additionele input?

Door de Coronacrisis is het bewustzijn over het belang en de meerwaarde van data en datagedreven werekn voor dagelijkse sturing en beleidsvorming vergroot. Binnen de GGD heeft dit er toe geleid dat verschillende disciplines nog hechter zijn gaan samenwerken (zoals onderzoekers, dashboardbouwers en team infectieziektebestrijding). De crisis heeft een snelle ontwikkeling gebracht in de visualisatie van data, zoals via een dashboard veiligheidsregio Brabant-Noord.

Daarnaast heeft de GGD koppelingen gelegd met de informatie van de andere twee Brabantse GGD’en ten behoeve van een Brabantbreed dashboard over de teststraten. Het ligt in de lijn der

verwachting dat deze nieuwe manier van samenwerken ook gebruikt kan worden binnen reguliere GGD vraagstukken, waardoor ook hier meer datagedreven gewerkt kan worden.

De GGD koppelt zijn data met landelijke datasets zoals die van CBS. Ook is hij met zijn gezondheidsmonitors en het gezondheidspanel aangesloten bij de landelijke lijn, waardoor de GGD zijn data kan vergelijken met landelijke cijfers (benchmarking). Veel andere koppelingen zijn er op dit moment niet. Het blijkt in de praktijk ook lastig om dit te kunnen realiseren, zowel omwille van technische redenen als vanuit privacy oogpunt.

3. Is er een risicotoets op actuele processen – gegeven de uiterste onzorgvuldigheid waarmee we te maken hebben gekregen tijdens de coronapandemie ten aanzien van het lekken van persoonlijke gegevens. Dit zorgt voor een enorme deuk in het vertrouwen. Hoe gaat de GGD hiermee om in de toekomst om dit te voorkomen?

Er zijn drie actuele landelijke processen te onderscheiden: testen, bron- en contactonderzoek (BCO) en vaccineren. Voor dat deel van het landelijk ontwikkelde systeem CoronIT dat gebruikt wordt ter ondersteuning van het testproces, is door GGD GHOR Nederland (koepelorganisatie van 25 regionale GGD'en) een Data Protection Impact Assessment (DPIA) in ontwikkeling. Deze wordt op zeer korte termijn definitief landelijk vastgesteld. Hierna zal GGD Hart voor Brabant deze zo snel mogelijk verwerken in een nadere regionale DPIA. Voor dat deel van het landelijk ontwikkelde systeem CoronIT dat gebruikt wordt ter ondersteuning van het vaccinatieproces, is tevens een DPIA in ontwikkeling.

Voor de ondersteuning van de grote landelijke opschaling van het BCO-proces, is in de HPZone lite ontwikkeld voor alle Nederlandse GGD'en. Voor dit systeem is zowel landelijk als regionaal nog geen DPIA opgesteld. Voor HPZone lite wordt inmiddels een landelijk alternatief systeem ontwikkeld, onder de noemer GGD Contact.

Op dit moment zijn er geen aanwijzingen dat een eventueel verlies van vertrouwen als gevolg van de datadiefstal, leidt tot een afname van de test- en vaccinatiebereidheid. Mensen werken ook nog steeds goed mee aan het uitvoeren van bron- en contactonderzoeken. Er is bij GGD Hart voor Brabant een zestigtal verzoeken ingediend voor inzage en/of verwijdering van gegevens.

GGD Hart voor Brabant hecht grote waarde aan zijn betrouwbaarheid, ongeacht of de datadiefstal impact heeft op de test- en vaccinatiebereidheid van zijn inwoners. Hij treft daarom diverse beschermingsmaatregelen, die waar nodig worden verbeterd:

- Controle aan de poort. Mensen moeten een Verklaring Omtrent Gedrag (VOG) aanleveren en een geheimhoudingsverklaring ondertekenen. GGD Hart voor Brabant heeft zich bij de aanname van personeel ervan verzekerd dat altijd en voor iedereen een VOG en geheimhoudingsverklaring voor handen is.
- Autorisatieniveaus. De IT systemen waarmee GGD Hart voor Brabant werkt, kennen verschillende rollen met bijbehorende autorisatieniveaus. Niet iedereen kan bij alle gegevens en kan alle functionaliteiten (zoals het downloaden van data-exports) gebruiken. Binnen GGD Hart voor Brabant is een autorisatiematrix ontwikkeld, gebaseerd op de rol of functie van iedere medewerker. Medewerkers krijgen alleen die autorisatie die nodig is voor zijn of haar functie. De autorisatiematrix wordt bijgehouden bij in-, door- en uitstroom van medewerkers. Er vindt hierop een maandelijkse check plaats. Naar aanleiding van de datadiefstal is ter check nog een keer doorgelicht wie binnen GGD Hart voor Brabant geautoriseerd is tot grote downloads (datadump). Dit is een zeer beperkte groep van

medewerkers die dit op grond van hun functie daadwerkelijk nodig hebben, bijvoorbeeld om dashboards te maken.

- Controles op correct gebruik. De GGD'en controleren het gebruik van systemen door medewerkers, hebben de controles steeds verder verbeterd en doen dat nog steeds. Vanwege het belang van de virusbestrijding en de gevraagde snelheid zijn de GGD'en – op diverse manieren – met steekproefsgewijze controles van start gegaan. In maart van dit jaar verwacht GGD GHOR Nederland bovendien systemen te implementeren die automatisch en continu zullen controleren op opvallend gebruik van de systemen (zoals grote downloads of onlogische inzage in dossiers). De Autoriteit Persoonsgegevens had vóór het bekend worden van de datadiefstal geen aanvullende vragen gesteld over de gehanteerde werkwijze. Specifiek voor GGD Hart voor Brabant geldt dat hij via de logging-functionaliteit van Microsoft 30 dagen kan terugkijken. De GGD gebruikt deze functionaliteit voor steekproefsgewijze controle van systeemgebruik door medewerkers en om terug te zoeken bij signalen en incidenten. GGD Hart voor Brabant gaat de periode van logging verlengen van 30 dagen naar 1 jaar, zodat hij verder terug kan kijken.

Tot slot is het goed om te benadrukken dat geen van de gearresteerde vijf personen werkzaam was bij GGD Hart voor Brabant. Er zijn tot op heden ook geen aanwijzingen ontvangen van politie en justitie dat (vaste of ingehuurde) medewerkers van onze GGD worden verdacht. Ook heeft de GGD zelf intern nadere checks uitgevoerd van zijn 'logging-bestanden' op eventuele onregelmatigheden. Die zijn niet aangetroffen. GGD Hart voor Brabant heeft ook op basis van eigen onderzoek op dit moment geen aanwijzingen dat zijn medewerkers betrokken zouden zijn bij datadiefstal. Het is evenwel nog niet duidelijk of door de gearresteerde medewerkers van het landelijke callcenter of medewerkers van andere GGD'en gegevens zijn gestolen en/of ten onrechte zijn ingezien van inwoners uit de gemeente Dongen. Dit moet duidelijk worden uit het landelijke onderzoek van politie en justitie.

4. De GGD geeft aan in de nota aan dat zij directe en indirecte kosten kunnen terugvorderen bij het ministerie. Is dat ook van toepassing voor vragen (en bijbehorende kosten) n.a.v. de coronacrisis die vragen om begeleiding van de bewoners van Dongen en nu worden doorbelast naar de gemeente? Dat is namelijk een indirect gevolg.

NIET DOOR GGD HART VOOR BRABANT BEANTWOORD.

17.17

CORONA UPDATE

MT

8 februari 2021

Gezond² doet leven!

Hart voor Brabant

Inhoud update programma Corona

Status, ontwikkelingen en knelpunten:

1. Testen
2. BCO
3. IDM&S
4. Datadiefstal
5. Vaccinatie
6. Bereikbaarheid

Testen | *Status*

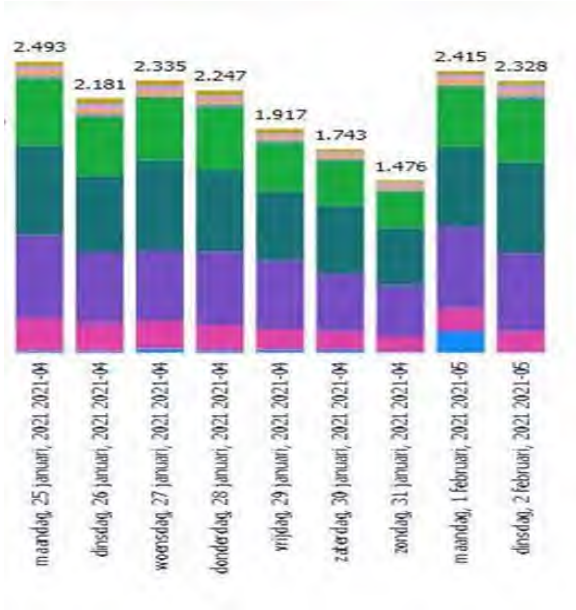
- Gemiddelde wachttijd (week 51) van bellen tot afspraak is 4 uur (Cuijk) en +/- 24 uur (Uden, Den Bosch en Tilburg)
- Het op- en afschalen wordt door de Coördinatoren Testen bepaald afhankelijk van de testvraag. We gaan hierbij uit van een maximale wachttijd van 24 uur
- Het landelijke ServiceLoketTesten wordt ingezet voor het opvullen van gaten in de planning op de teststraten EN bij grote mobiele testvragen (bij meer dan 20 thuisbemonsteringen op 1 locatie)
- Mensen kunnen niet zelf kiezen welke test ze krijgen; worden ter plekke geïnformeerd
- Twee voorrangsgroepen: zorg en onderwijs
- Vanaf 1 december asymptomatischtesten uit BCO en app
- Cuijk max. 7 straten
- Uden max. 8 straten
- Den Bosch max. 12 straten
- Tilburg max. 10 straten

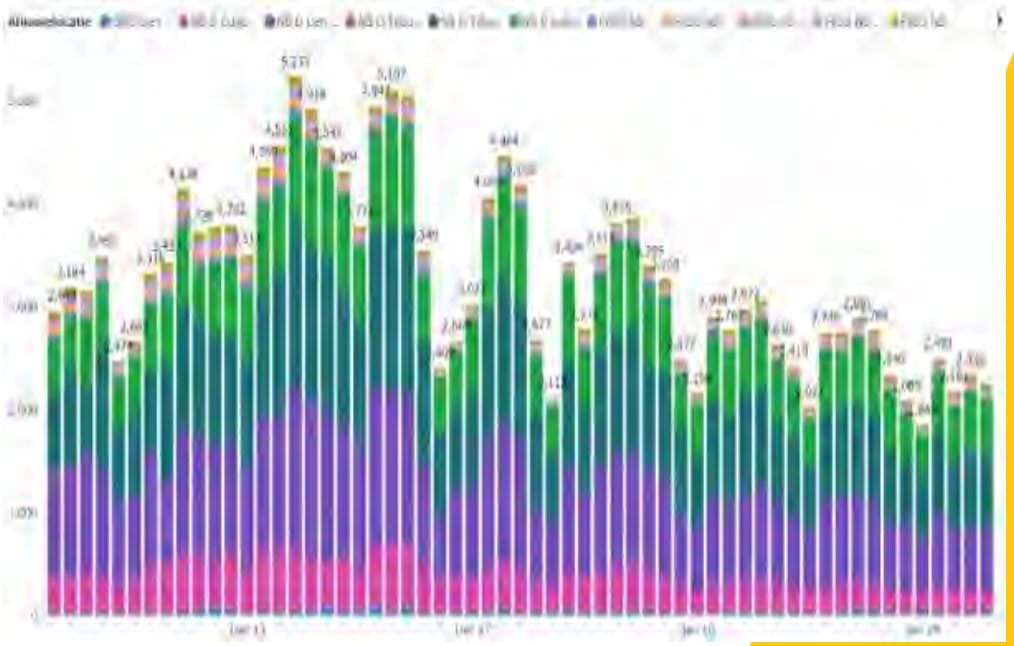
Testen | *Ontwikkelingen*

- Extra personeel geworven om wachttijd te verkorten
- Vanuit GGD GHOR NL volgt een Roadmap 2.0 met nieuwe prognose: ambitie 175.000 testen per dag in maart 2021. We verwachten de nieuwe prognose binnen de huidige testcapaciteit op te kunnen vangen
- Verschillende aanbieders:
  - Commercieel: meldingsplicht, IGJ houdt toezicht
  - 7 tot 10 XL locaties
  - 10 landelijke mobiele units
  - Pilot thuisbemonstering: gestart in Tilburg
- Verschillende testmethoden:
  - PCR testen: reeds in gebruik binnen GGD HvB voor alle testen
  - Speekseltesten: beschikbaar bij testlocatie Tilburg i.s.m. Microvida, in te zetten bij kinderen t/m 5 jaar en kwetsbaren
  - Sneltesten:
    - Tilburg: in samenwerking met Microvida toepassen Antigeentest Abbott vanaf 4 januari
    - Den Bosch: verkenning in samenwerking met MML JBZ toepassen Antigeentest Abbott, datum eind januari
    - Uden: ervaringen Den Bosch afwachten, vervolgens eventueel aansluiten bij MML JBZ
    - Cuijk: verkenning mogelijkheden i.s.m. Dienst Testen
  - Thuistesten: pilot thuistesten in Tilburg. Structurele beschikbaarheid onduidelijk
  - Wordt verwacht, de blaastest.
  - Wordt verwacht, grootschalig testen (scholen, wijken/buurten etc.)

Testen | *Knelpunten*

- Testvraag is onzeker en wordt door verschillende factoren beïnvloed:
  - Andere varianten (VK-variant 2/3 deel van de besmettingen, 1,5 keer meer besmettelijk)
  - Piek griepgolf
  - Veranderingen in beleid, grootschalig testen
  - Testbereidheid





BCO | *Status*

- Voldoende capaciteit om in huidige fase 1 (volledig BCO) de BCO’s uit te voeren en af te ronden

Uitgevoerde BCO’s 25-30 december 2020

BCO, signalering en advies | *Ontwikkelingen*

- *Automatisering Huisartsen informeren (hierdoor is geen telefonisch contact meer nodig)*

Verwachting februari 2021 (uitgesteld). Voorrang is gegeven aan de implementatie van doorgeven vaccinatieberichtgeving

- *GGD Contact* = voorportaal voor zelfregistratie volgt begin Februari 2021

- *Advisering scholen en kinderdagverblijven*

De richtlijnen rond BCO, quarantaine en testen voor kinderen en leerkrachten zijn aangepast en de basisscholen gaan weer open vanaf 8 februari.

De GGD heeft een scholenteam ingericht om de advisering beter te stroomlijnen.

Aan het scholenteam zijn gezondheidsvoorlichters van de GGD (GVO'ers) toegevoegd om beter aan te sluiten op vragen van scholen (communicatie met ouders, psychosociale problematiek e.d.)

- *Signaleringsteam*
  Team komt 2x per week bijeen voor het houden van overzicht op signalen die risico geven op verspreiding en/of onrust. Prioriteert en besluit voor vervolg. Maatregelen zowel proactief als reactief inzetten om risico's te verkleinen. Filteren van informatievoorziening en deskundigheid delen en behouden.

Datalek / *Status*

- HR check op personeel: VOG en Geheimhouding gereed
- Autorisaties: Check autorisatiematrix loopt
- Burgerinformatie: KCC gereed
- Burgervragen verwijderen gegevens: Proces wordt ingericht. FG betrokken. (status ongeveer 30 verzoeken.
- IT systemen
  - Landelijk functies uitgezet (CoronIT en HP Zone)
  - Gevolgen primaire processen in kaart
  - Oók gevolgen reguliere IZB processen

Datalek / *Ontwikkelingen*

- Verbetering/vernieuwing van de systemen n.a.v. Datalek landelijk:
  - Nieuwe applicaties (GGD Contact o.a.)
  - Aanpassing bestaande applicaties (CoronIT) en IT infrastructuur
  - Gevolgen voor primaire processen, autorisaties en infrastructuur

- Sturing op IT ontwikkelingen, Technisch en functioneel beheer
  - Landelijk t.o.v. regionaal
  - Governance
  - Organisatie

- Meer regionale inzet op IT (Brabantbreed en HvB)
  - IT Governance
  - IT landschap, inclusief beveiliging
  - IT projecten overzicht en implementatie kalender. Incl. ondersteuning

IDM&S | *Status*

- **Algemene zaken**:
  - Werkprocessen opnieuw inregelen n.a.v. maatregelen omtrent geconstateerde datalek
  - Samenwerking met andere GGDen verloopt prima; veel wekelijkse afstemming
  - IT Governance escalatie – geen toegang tot juiste HPZone exports en essentiële export velden zijn niet meer beschikbaar
- **Taakgroep IZB dashboard/Surveillance**:
  - Onderzoek in samenwerking met GGD WB en GGD BZO over welke mensen we zien in de teststraten (waarvoor we CBS microdata nodig hebben). Onderzoeker uit GGD WB zal een start maken aan de DPIA; loopt (geen update ivm vakantie)
  - Onderzoek i.s.m. ETZ over de associatie tussen de virale load en besmettelijkheid en verloop van ziekte.
- **Taakgroep BCO**:
  - BCO-dashboard ontwikkeling staat op on-hold; gezien eventueel vervangen HPZone lite door GGD Contact
- **Taakgroep Testen/Vaccinatie**:
  - Focus op verkrijgen toegang CoronIT ruwe database vanuit landelijk ontwikkelde BI omgeving
  - Testen: toevoegen visuals doorlooptijden en type test (PCR, Antigeen, etc.)
  - Regionaal vaccinatiedashboard in ontwikkeling; in afwachting van complete vaccinatiedataset vanuit landelijke GGD GHOR, ontbreken nog veel records
- **Taakgroep Gemeenten/VR**:
  - Veiligheidsregio dashboard beschikt momenteel niet over actuele data door landelijk genomen maatregelen i.v.m. datalek; hierdoor kunnen we niet bij de essentiële HPZone data. Gemeenten zijn geïnformeerd

IDM&S | *Ontwikkelingen*

- Samenwerking met andere GGDen is in ontwikkeling (de positieve ervaring/werkwijze vanuit Programma Corona wordt overgenomen)
- Bestaande projecten: hiervan is gecontroleerd of de wens / behoefte nog bestaat. Afspraken gemaakt om bestaande projecten (op verzoek van actiehouders in het nieuwe jaar) opnieuw op te starten.
- Focus op ontwikkeling regionaal vaccinatiedashboard en optimalisatie teststraten dashboard in samenwerking met andere GGD'en
- Automatisch datakoppeling vanuit GGD GHOR naar DWH betreft testdata en vaccinatiedata. Dit heeft tot gevolg dat er geen handmatige data exports meer gedownload hoeven te worden
- Beschikbaar maken nieuwe CoronIT data omgeving door GGD GHOR waarin de ruwe data te verkrijgen is door de regionale GGD'en

IDM&S | *Knelpunten*

- Zorgen rond verkrijgen – en de kwaliteit van de data vanuit de landelijke applicaties en landelijke communicatielijnen:

  - We zijn nog in afwachting van complete vaccinatie dataset vanuit GGD GHOR; ontbreken records van personen gevaccineerd binnen regio maar woonachtig buiten de regio. Dit is aangegeven bij GGD GHOR maar tot heden geen update. Gegevens die wij tot beschikking hebben komen niet overeen met data getoond in landelijk GGD GHOR dashboard

  - Door bepaalde velden vanuit de landelijke software (CoronIT) niet te verplichten heeft dit gevolgen voor de datakwaliteit (o.a. beroepsgroepen/doelgroepen, geen toestemmingsveld voor vervolgonderzoek).

  - De 'toegezegde' technische datafeed bestaat maar er zitten zorgelijke verschillen (teststraatdata: datum/ tijd/ status afspraak en monsterafname) tussen de handmatige oude data export download en de nieuwe datafeed.

  - Escalatie vanuit DPG's richting GGD GHOR levert (hopelijk) betere communicatie, afstemming en technische oplossingen vanuit GGD GHOR met de GGD'en
    - Volgende escalatie met focus op IT governance en communicatie n.a.v. recente datalek issues en genomen landelijke maatregelen (o.a. intrekken rechten en rollen HPZone)
    - HPZone Lite vervangen door GGD Contact??

Vaccinatie | *Status*

- Locatie Veghel (L/XL)
  - 500 prikken per dag zorgpersoneel (vanaf 6 januari)
  - 140 prikken per dag voor ouderen 90+ en 85+ (26 januari)
  - Capaciteit 1600 prikken per dag, opschaalbaar naar 2400
- Locatie 's-Hertogenbosch (M/L)
  - Gestart op 29 januari
  - Capaciteit 800 prikken per dag, opschaalbaar naar 1600
- Locatie Tilburg (M/L)
  - Operationeel op 9 februari
  - Capaciteit 800 prikken per dag, opschaalbaar naar 1600
- Hierna volgen Uden, Boxmeer, Waalwijk en Oss (S/M) 400 – 800 prikken per dag

- Personeel:
  - Inzet team reizigers wordt ingepland
  - Vrijwillige inzet collega's via ikwilhelpenmetvaccineren@ggdhvb.nl opgehaald en wordt ingepland
  - Voor gat worden externe partijen gecontracteerd, o.a. Rode Kruis
  - Inspectie kinderopvang benaderd voor 'kwaliteitstoezicht' (leren van uitvoeringstoets) en mogelijk als achtervang voor administrateurs in priklijn

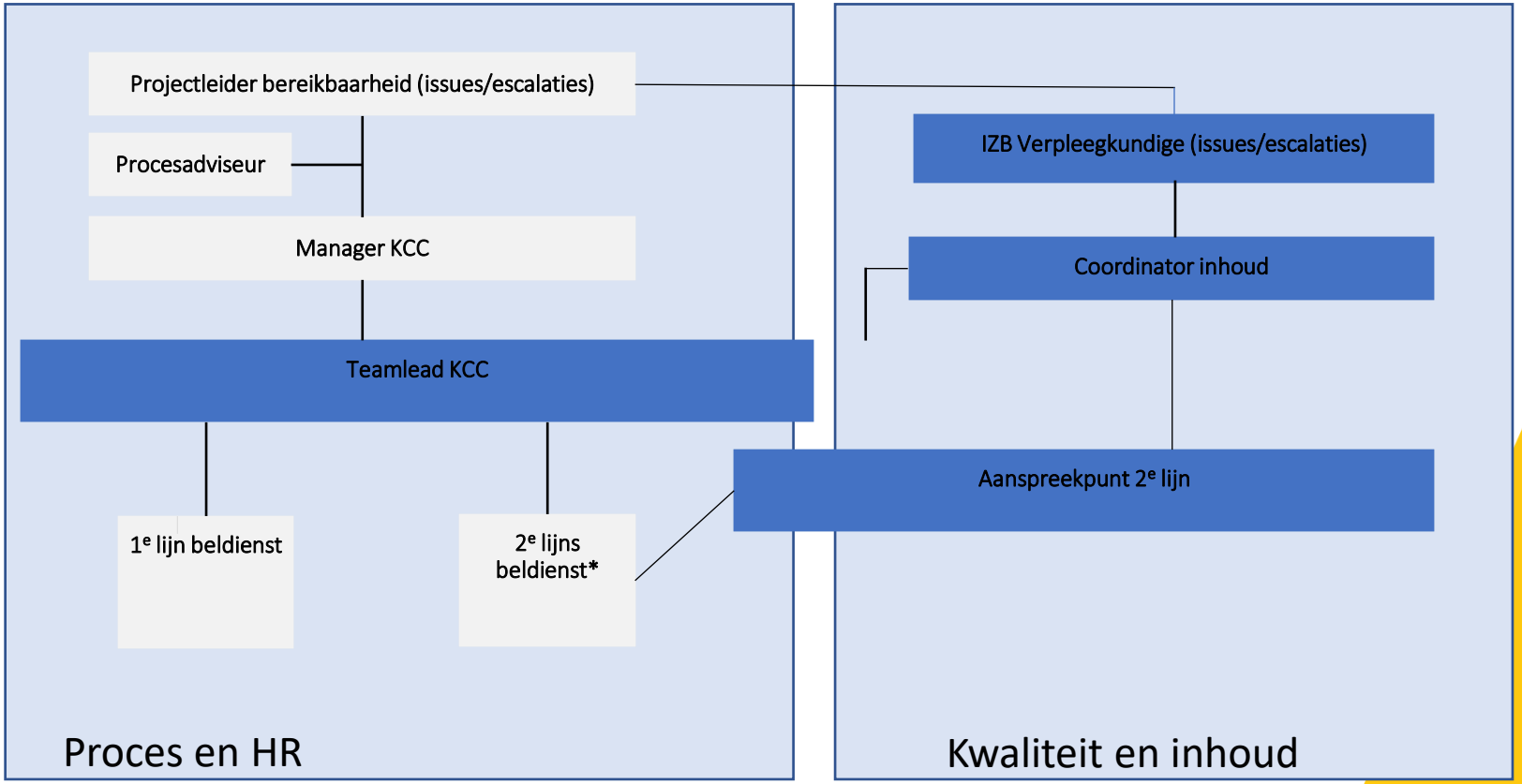
Vaccinatie | *Ontwikkelingen*

- Veel onzekerheden over de levering van vaccins (Astra Zeneca en nu ook mogelijk ook Moderna)
- Gevolg voor de opening van nieuwe locaties (minimaal 300 prikken per dag worden gezet).
- Het RIVM is in week 3 begonnen met de 85-90 jarigen uit te nodigen. De uitnodigen worden verspreid verstuurd.
- Eind week 4 gaan de brieven 80+ de deur uit.
- Na gebruik centrale GGD-locatie(s) voor zorgpersoneel *mogelijke* extra GGD-taken:
  - Mobiele teams ondersteuning kleine instellingen bij intramurale vaccinatie personeel en patiënten
  - Mobiele teams outreachend naar niet-mobiele ouderen (mogelijk rol huisarts)
  - Inzet centrale locaties voor (delen van) ouderen
  - Inzet centrale locaties voor massavaccinatie 18-60 (niet-risicogroepen)

Vaccinatie | *Knelpunten*

- Landelijke onzekerheden maken lange termijn planning moeilijk → *we pleiten landelijk voor scenariodenken*
- Gebreken in landelijke sturing → *we pleiten landelijk voor betere governance*
- Gebreken in landelijke kennis → *we volgen regionaal stabiel onze eigen lijn in de opzet en gebruiken de uitvoeringstoets om te leren*

Bereikbaarheid / *Aansturing*



* Betreft een rol waarop medewerkers ingepland worden. Medewerkers formeel aangestuurd door projectleider BCO, signalering en advies

Bereikbaarheid / *Dagelijkse aansturing Corona KCC (1e en 2e lijn)*

Rol	Taken
Projectleider bereikbaarheid	Aanspreekpunt management voor escalaties vanuit de lijn en implementatie nieuwe ontwikkelingen, afleggen verantwoording over voortgang en bewaken relatie met rest van het programma
Managers KCC	Leidinggevenden 1e lijn *1, verwerken wijzigingen HR, accorderen facturen, aanspreekpunt voor functioneren en verzuim medewerkers. Op- en afschalingsplannen personeel maken en uitvoeren.
Teamlead KCC	Forecasting, inroostering medewerkers, coachen van medewerkers op gebruik statussen en gesprekstechnieken, beoordelen gesprekken (techniek), kwaliteitsmonitoring, beheer kennisbank en dagelijkse aansturing teams samen met aanspreekpunt 2e lijn.
Coordinator inhoud	Kwaliteitsbewaking*2 bestaande uit:1. Actueel houden kennisbank 2. Verwerken nieuwe richtlijnen 3: Scholing en deskundigheidsbevordering team 4. beoordeling gesprekken (inhoud). Daarnaast deelnemen aan signaleringsoverleg en opstellen rapportages voor management en financiën en inrichting samenwerking met 3e lijns experts en scholen- en VVT team
Aanspreekpunt 2e lijn	Inhoudelijk aanspreekpunt voor bellers 2e lijn, afstemming met coördinatoren KCC en gedurende de dag sturen op beschikbaarheid en bereikbaarheid, afstemming hierover met andere teams waar nodig.
1e en 2e lijns medewerkers	Afhandelen vragen Corona (telefonie en mail)

*1 2e lijn valt formeel onder Petra van Wezel. Functionele aansturing vanuit functionarissen bereikbaarheid
*2 Verpleegkundige IZB betrokken

Bereikbaarheid / *Projectgroepleden- en rollen*

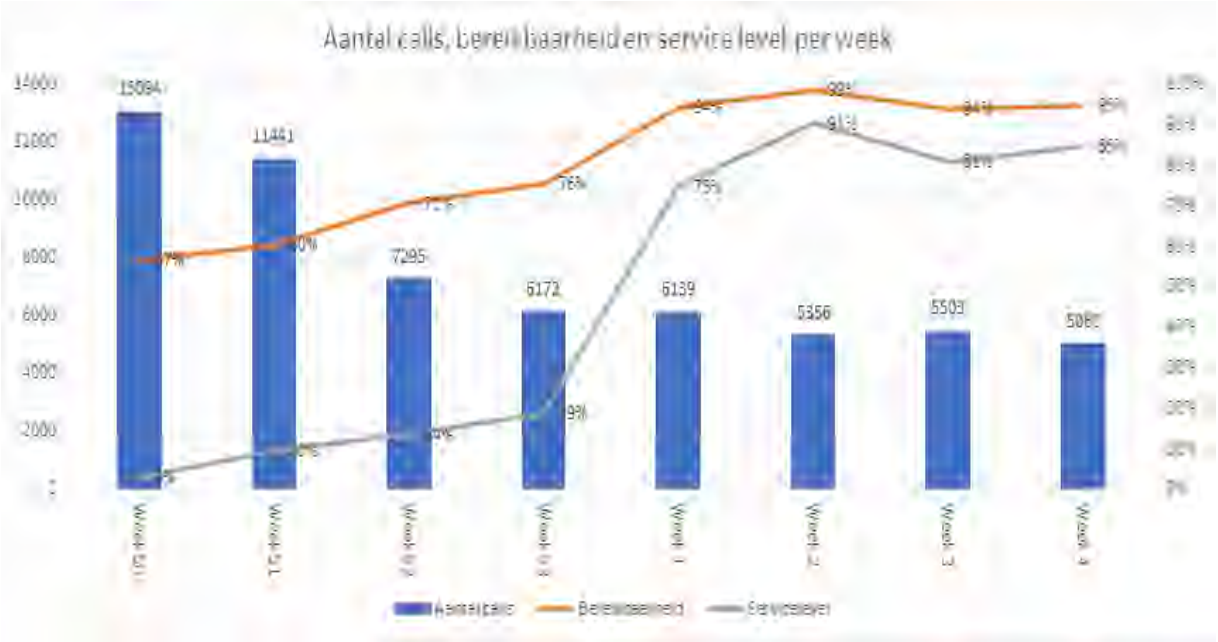
17.17

Rol	Taken
Projectleider	Voorzitten projectgroep, bewaken voortgang en inbrengen breed perspectief vanuit buitenwereld / rest programma
Manager KCC	Expertise en kennis inbrengen op het gebied van ontwikkelen en aansturen KCC. Oppakken vraagstukken op het gebied van personeel
Teamlead KCC	Vertegenwoordigen inbreng vanuit het dagelijkse proces – bereikbaarheid en procesmatige kwaliteit. Oppakken operationele en tactische actiepunten.
Verpleegkundige IZB	Inbrengen perspectief IZB, integraal beoordelen inhoudelijke ontwikkelingen en inrichten kwaliteitsmodel. Oppakken actiepunten op gebied integraal proces.
Coordinator Inhoud	Vertegenwoordigen inbreng vanuit het dagelijkse proces – kwaliteit. Oppakken operationele en tactische actiepunten.
Procesadviseur	Beschrijven en verbeteren van processen rondom bereikbaarheid. Daarnaast implementatie van nieuwe ontwikkelingen aansturen.

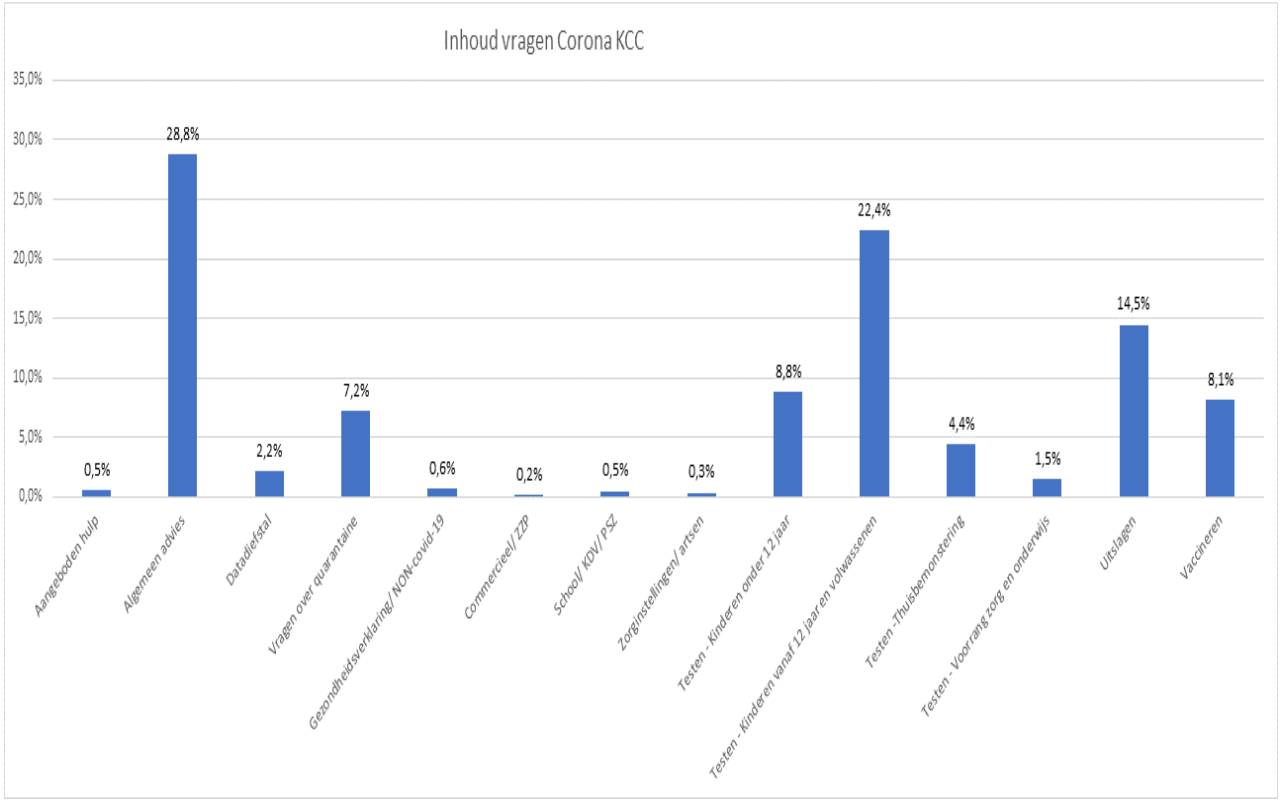
Als projectgroep in het totaal hebben we de verantwoordelijkheid om alle vraagstukken die spelen op het gebied van bereikbaarheid op te pakken en uit te werken.

Bereikbaarheid / C*alls*

- **Corona KCC Calls (1e en 2e lijn)**



Bereikbaarheid / *Vraagverdeling*



17.17

DANK VOOR JE AANDACHT

Gezond² doet leven!

GGD Hart voor Brabant