



West-Brabant

SOLV B.V.

██████████ en ██████████  
Anne Frankstraat 121  
1018 BZ Amsterdam

Kenmerk: ██████████ Datum: 4 juli 2022  
Behandeld door: ██████████ E-mail: ██████████@ggdwestbrabant.nl  
Onderwerp: Nazending deelbesluit Wob-verzoek

Geachte heer ██████████,  
Geachte mevrouw ██████████,

In ons besluit van 1 juni 2022 op uw Wob-verzoek lieten wij weten dat er een nazending zou volgen in een deelbesluit. Middels dit deelbesluit stellen wij u daarom nog enkele documenten beschikbaar. Hieronder vallen de drie documenten waarover wij een zienswijze van derden hebben gevraagd en enkele documenten die wij voor u alsnog hebben achterhaald.

Van de documenten die u verzocht en die wij hierbij openbaar maken, vindt u een overzicht aan het begin van de bijlage: het is één bestand met alle documenten verzameld.

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

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

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

Ik vertrouw erop dat ik u hiermee voldoende heb geïnformeerd.

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



**West-Brabant**

Sebastiaan Baan  
directeur publieke gezondheid

bijlage: Nazending Wob-verzoek ICAM – GGD WB  
per mail verzonden aan: █████@solv.nl en █████@solv.nl  
per brief verzonden aan SOLV B.V.

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

1.0 DVO GGD Contact - GGD West-Brabant_Redacted.pdf .....	2
1.1 Verwerkersovereenkomst - GGD West-Brabant_Redacted.pdf .....	17
2.0 DVO GGD GHOR Nederland v.1.1_Redacted.pdf .....	26
2.4 Verwerkingsovereenkomst GGD GHOR Nederland v1.1_Redacted.pdf .....	33
200614 OV GGDWBijlage02_Redact_Redacted.pdf .....	40
200614 OVK GGDWB_Redacted_Redacted.pdf .....	49
200614 OVK GGDWB-_Redacted_Redacted_Redacted.pdf .....	58
C - Referentie DPIA GGD Contact release 1.1 v 1.1.3_Redacted.pdf .....	107
D - DPIA GGD Contact Addendum BCO Sync extensie 1.0_Redacted.pdf .....	196
FW_ Ter ondertekening_ convenant BCO_Redacted.pdf .....	207
FW_ Vooraankondiging overeenkomsten GGD Contact_Redacted.pdf .....	209
Gedupeerden datalek_Redacted.pdf .....	212
Gegevens datalek GGD West-Brabant_Redacted.pdf .....	214
Overeenkomsten t_b_v_ GGD Contact 2_Redacted.pdf .....	215
Overeenkomsten t_b_v_ GGD Contact_Redacted.pdf .....	216

# Dienstverleningsovereenkomst Ministerie van Volksgezondheid, Welzijn en Sport en GGD West-Brabant

Betreft: Dienstverlening GGD Contact

Datum: 23 08 2021

Status: Definitief

## Colofon

Afzendinggegevens: Ministerie van Volksgezondheid, Welzijn en Sport  
Postbus 20350  
2500 EJ Den Haag

Contactpersoon:



## Inhoudsopgave

Versiebeheer .....	5
1 Algemeen.....	6
1.1 Dienstverlening.....	6
1.2 Looptijd.....	6
1.3 Wijzigingen document.....	6
1.4 Gerelateerde documenten .....	6
1.5 Beëindiging .....	6
2 Dienstverlening.....	7
2.1 Algemene beschrijving dienstverlening .....	7
2.2 Niveau van dienstverlening .....	7
A. Rolverdeling AVG.....	7
B. Bereikbaarheid .....	7
C. Beschikbaarheid .....	7
D. Correctief onderhoud.....	8
E. Incidentmanagement .....	8
F. Change- en releasemanagement .....	9
G. Continuïteitsmanagement.....	9
3 Beveiliging .....	11
3.1 Van toepassing zijnde kaders .....	11
3.2 Logging en monitoring.....	11
3.3 Beveiliging afnemer .....	11
4 Verantwoordelijkheden.....	12
4.1 Verantwoordelijkheden VWS .....	12
4.2 Verantwoordelijkheden GGD .....	12
5 Communicatie .....	13
5.1 Rapporteren .....	13
5.2 Overlegvormen.....	13
6 Tekenblad .....	14

De ondergetekenden

1. de publiekrechtelijke rechtspersoon: **de Staat der Nederlanden (Ministerie van Volksgezondheid, Welzijn en Sport)**, hierna te noemen: VWS,

en

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

De partijen bij deze dienstverleningsovereenkomst ("**DVO**") worden hierna gezamenlijk ook aangeduid als "**de Partijen**" en ieder als een "**Partij**".

## Versiebeheer

<b>Versie</b>	<b>Datum</b>	<b>Auteur</b>	<b>Omschrijving</b>
<b>0.1</b>	26-05-2021	[REDACTED]	Initiële versie
<b>0.2</b>	28-05-2021	[REDACTED]	Eerste review [REDACTED] verwerkt
<b>0.3</b>	04-06-2021	[REDACTED]	Aanvullingen en review verwerkt
<b>0.4</b>	09-06-2021	[REDACTED]	Aanvullingen en review van GGD GHOR verwerkt
<b>0.5</b>	14-06-2021	[REDACTED]	Aanvullingen en review [REDACTED] [REDACTED] verwerkt
<b>0.6</b>	15-06-2021	[REDACTED]	Review
<b>0.9</b>	15-06-2021	[REDACTED]	Review verwerkt
<b>0.99</b>	23-06-2021	[REDACTED]	Review Stuurgroep verwerkt
<b>1.0</b>	23-06-2021	[REDACTED]	Final Review



# 1 Algemeen

In deze Dienstverleningsovereenkomst (DVO) komen VWS en GGD de mate van dienstverlening van GGD Contact overeen.

## 1.1 Dienstverlening

Het doel van de dienstverlening is de GGD te ondersteunen in het Bron- en Contact Onderzoek (BCO) met het leveren, beheren en door ontwikkelen van de applicatie GGD Contact. Dit is de voorziening die het Bron- en Contact Onderzoek voor COVID-19 gerelateerd ondersteunt.

## 1.2 Looptijd

Deze DVO treedt in werking op 23 augustus 2021 en wordt aangegaan voor onbepaalde tijd.

## 1.3 Wijzigingen document

Het actueel houden van dit document is belegd bij de directie RDO van het ministerie VWS. Bij partijen kan de wens ontstaan om dit document te wijzigen. In gezamenlijk overleg wordt de wijziging vervolgens bepaald.

- Overeengekomen wijzigingen worden vastgelegd in een wijzigingsblad;
- Dit wijzigingsblad wordt door beide partijen formeel ondertekend en als addendum toegevoegd;
- De in het addendum opgenomen afspraken worden in de eerstvolgende geactualiseerde versie van de DVO opgenomen.
- De bijlagen in dit document kunnen na en in onderling overleg tussentijds worden geactualiseerd. Het tast de rechtmatigheid van de afspraken in dit document niet aan.

## 1.4 Gerelateerde documenten

De volgende documenten zijn gerelateerd aan deze DVO:

- Procedurebeschrijving beheer GGD Contact (bijlage 1)
- Verwerkersovereenkomst VWS – GGD (bijlage 2)
- Beveiliging GGD Contact release X (bijlage x) wordt vertrouwelijk gedeeld onder TLP:Amber classificatie (need to know basis).
- Landelijke Referentie DPIA GGD Contact
- Lijst Overeenkomsten GGD Contact

Van de gerelateerde documenten kunnen in de loop van de tijd nieuwe versies bestaan. Sommige documenten worden zelfs elke release geüpdatet. Dit heeft geen gevolgen voor de geldigheid van deze DVO.

## 1.5 Beëindiging

Het verzoek van een van de partijen om de DVO te beëindigen vindt schriftelijk plaats met opgave van de reden. Partijen hanteren een opzegtermijn van drie maanden en treden met elkaar in overleg over de wijze van beëindiging.

## 2 Dienstverlening

### 2.1 Algemene beschrijving dienstverlening

De te leveren dienstverlening omvat GGD Contact: het leveren, doorontwikkelen en beheren van de voorziening die de behandeling voor COVID-19 gerelateerd Bron- en Contact Onderzoek (BCO) ondersteunt.

### 2.2 Niveau van dienstverlening

Deze paragraaf beschrijft de specifieke afspraken voor de dienstverlening die door het ministerie wordt geleverd aan de GGD. Voor de dienstverlening levert het ministerie Applicatie- en Technisch beheer.

Aangezien de omvang en inzet van het Bron- en Contact Onderzoek (BCO) varieert op basis van het aantal COVID-19 besmettingen, kan de gewenste dienstverlening ook fluctueren. VWS zal driemaandelijks beoordelen of de dienstverlening nog past bij het gebruik van de applicatie en waar opportuun een voorstel doen voor aanpassing van de dienstverlening om zo kosteneffectief GGD Contact aan te kunnen bieden.

#### A. Rolverdeling AVG

De feitelijke rolverdeling tussen GGD en VWS is bepalend voor de verantwoordelijkheden van GGD en VWS zoals die volgen uit de Algemene Verordening Gegevensbescherming (AVG). De rolverdeling is vastgesteld in de referentie DPIA GGD Contact behorend bij de release. De referentie DPIA is afgestemd met de GGD en VWS.

GGD stemt in met alle (sub)verwerkers die VWS voor haar dienstverlening inschakelt, waarbij VWS zorgdraagt voor de verwerkersovereenkomsten. De lijst met (sub)verwerkers is beschreven in Lijst Overeenkomsten GGD Contact. Deze is opgenomen als bijlage bij deze DVO.

#### B. Bereikbaarheid

De servicedesk GGD GHOR is het centrale loket voor alle verzoeken en meldingen rondom GGD Contact. De GGD sluit een overeenkomst die ingaat op het moment van ingebruikname van GGD Contact.

#### C. Beschikbaarheid

Beschikbaarheid is de tijd dat de dienstverlening onder verantwoordelijkheid van VWS, voor eindgebruikers beschikbaar is. Gepland onderhoud valt buiten de berekening van de gerealiseerde beschikbaarheid. Ook de uitval van een tussenliggende component die niet onder verantwoordelijkheid van VWS valt, zoals generieke ICT-diensten geleverd door GGD (o.a. IdentityHub en een VPN - verbinding), waardoor de systemen voor gebruikers niet beschikbaar zijn, valt hierbuiten.

Per incident (dat leidt tot onbeschikbaarheid) gelden bovendien maximale hersteltijden. Deze zijn opgenomen onder de paragraaf incidentmanagement.

Onderwerp	Toelichting	Norm
<b>Beschikbaarheid</b>	De mate waarin de eindgebruikers GGD Contact functioneel kunnen gebruiken binnen het servicevenster. Onbeschikbaarheid wordt gemeten vanaf het moment van melden door servicedesk aan de Incidentmanager VWS.	Minimaal 99,8% binnen het servicevenster

#### D. Correctief onderhoud

Correctief onderhoud aan GGD Contact (geplande onbeschikbaarheid) wordt enkel uitgevoerd buiten het servicevenster als opgenomen in paragraaf E van deze DVO. Correctief onderhoud wordt bij voorkeur drie weken van tevoren en uiterlijk drie dagen van tevoren gemeld aan de servicedesk. De servicedesk is vervolgens verantwoordelijk voor de communicatie naar de eindgebruikers en afnemers toe. Bij een dreigende verstoring moet er soms direct ingegrepen worden, daarvoor geldt onderstaande norm.

Onderwerp	Toelichting	Norm
<b>Onderhoud</b>	Het benodigde onderhoud om de beschikbaarheid te kunnen garanderen.	90% buiten het Servicevenster

#### E. Incidentmanagement

Het incidentmanagementproces heeft als doel het zo snel mogelijk verhelpen van incidenten. De doelstelling is het terugbrengen van de dienstverlening naar het normale niveau, met zo min mogelijk gevolgen in de vorm van impact, benodigde mensen, middelen (financieel & materieel) en tijd. Het incidentmanagementproces staat uitgebreid beschreven in Bijlage 1 Procedurebeschrijving beheer GGD Contact. Onderstaand een overzicht van de gehanteerde normen.

Onderwerp	Toelichting	Norm <sup>1</sup>
<b>Incidentmelding (storing)</b>	De afhandeling van aangemelde verstoringen tijdens het servicevenster.	P1 Hersteltijd 2 <sup>e</sup> lijn: 4 uur Servicevenster: 7*16u**
	Toewijzing prioriteit vindt plaats op basis van de prioriteitenmatrix (zie hiervoor de procedurebeschrijving).	P2 Hersteltijd 2 <sup>e</sup> lijn: 1 dag Servicevenster: 7*16u**
	NB Responstijd en doorlooptijd 1ste lijn zijn onderdeel van de afspraken GGD GHOR SD met de GGD. De hersteltijd 2 <sup>e</sup> lijn start na ontvangst van het incident van de Servicedesk door de tweede lijn	P3 Hersteltijd 2 <sup>e</sup> lijn: 1 week Servicevenster: 7*16u**
		P4 Hersteltijd 2 <sup>e</sup> lijn: 2 weken Servicevenster: 7*16**

<sup>1</sup> Dit is conform de standaardnormen van de GGD GHOR servicedesk

Afhandeling buiten servicevenster	Alleen bij P1
-----------------------------------	---------------

\*\* Ten tijde van een hoge infectiedruk wordt het servicewindow opgerekt van 5 x 9 (8.00 – 17.00 uur) naar 7 x 16 (7.00 – 23.00 uur).

### Prioriteitenmatrix

Tijdens het aannemen van een incidentmelding door de servicedesk, wordt met de aanmelder een inschatting van de ernst (impact en urgentie) van het incident gemaakt. Op basis daarvan wordt door de servicedeskmedewerker de prioriteit vastgesteld, geregistreerd en afgehandeld.

In de Procedurebeschrijving beheer GGD Contact (bijlage 1) is de prioriteitenmatrix opgenomen.

### **F. Change- en releasemanagement**

Change- en releasemanagement is het proces rondom het gecontroleerd afhandelen van verzoeken tot wijziging van de functionele of technische werking van GGD Contact. Het proces van change- en releasemanagement is uitvoerig beschreven in Bijlage 1 Procedurebeschrijving beheer GGD Contact.

Onderwerp	Toelichting	Norm
<b>Afhandelen wijzigingsverzoeken</b>	De afhandeling van geaccordeerde wijzigingen	Minimaal 95% van de goedgekeurde wijzigingen wordt gerealiseerd conform afspraak
<b>Implementeren releases</b>	Afhandelen van een verzameling van wijzigingen in een release voor GGD Contact	Minimaal 95% van de releases wordt gerealiseerd op de overeengekomen implementatiedatum

### **G. Continuïteitsmanagement**

Continuïteitsmanagement is het proces dat zorgt voor afdoende technische voorzieningen om de continuïteit van de dienstverlening te borgen. De borging van de continuïteit wordt gerealiseerd conform onderstaande normen.

Onderwerp	Toelichting	Norm
<b>Back-up en restore</b>	Het veiligstellen van mail en volledig herstel GGD Contact (inclusief database) op de productieomgeving en het terugzetten hiervan.	<ul style="list-style-type: none"> <li>- 24x per uur, RPO<sup>2</sup> maximaal 1 uur, RTO<sup>3</sup> maximaal 2 uur. Reactietijd: 15 minuten (met best effort voor sneller binnen kantooruren)</li> <li>- 30 x per maand<sup>4</sup>, RPO maximaal 1 dag, RTO maximaal 4 uur.</li> </ul>

<sup>2</sup> Recovery Point Objective of herstelpuntdoelstelling

<sup>3</sup> Recovery Time Objective of hersteltijd-doelstelling

<sup>4</sup> Voor de back-ups die tot 1 maand teruggaan, is de RTO alleen haalbaar op basis van disaster recovery. Dat betekent dat alle databases van een omgeving in één keer terug worden gezet. Bij een lagere RPO en lagere RTO (bijv. bij back-ups die verder dan 1 maand teruggaan) wordt de data in een geïsoleerde omgeving (sandbox) beschikbaar gesteld waar een extract van wordt gemaakt.

		- 12 x per jaar, RPO maximaal 1 maand, RTO maximaal 2 (werk)dagen
<b>Bewaartermijn</b>	Periode dat de veiliggestelde gegevens worden bewaard.	Retentie van 7 jaar
<b>Uitwijk</b>	De mogelijkheid om, na een calamiteit, de dienstverlening te hervatten op een andere wijze of andere locatie.	Het datacentrum van de hostingpartij is dubbel uitgevoerd. Uitwijk bij uitval van het datacenter zal automatisch plaatsvinden. Specifieke uitval wordt opgepakt binnen incidentproces, waarbij back-up en uitrolplan van de specifieke release leidend zijn.

## 3 Beveiliging

In GGD Contact wordt gevoelige informatie verwerkt zoals medische gegevens (bijzondere persoonsgegevens en informatie over de persoonlijke levenssfeer (o.a. persoonlijke contacten)). Informatiebeveiliging is daarmee een belangrijke randvoorwaarde voor een goede en vooral betrouwbare dienstverlening. De ontwikkeling van GGD Contact en het beheer gebeurt conform hoge informatiebeveiligings- en privacybeschermingseisen.

### 3.1 Van toepassing zijnde kaders

Aan de basis van de inrichting, bestendinging en verbetering van beveiliging liggen primair de volgende kader stellende documenten.

- AVG
- NEN 7510-1 en NEN 7510-2 voor zover relevant voor de ontwikkeling van de applicatie.
- NEN 7512 – als subset van beheersmaatregelen uit de NEN 7510-2 voor de vertrouwensbasis voor gegevensuitwisseling.
- NEN 7513 – als ontwerpvoorwaarde voor de applicatielogging.
- DPIA GGD Contact

Deze normen zijn door VWS omgezet in concrete maatregelen die zijn genomen bij de ontwikkeling en het beheer van GGD Contact. In het document Beveiliging GGD Contact is de toelichting en concrete invulling van bovenstaande normen opgenomen. Dit document wordt elke release van GGD Contact geüpdatet en beschikbaar gesteld aan de CISO van de GGD en de kwaliteitsmanager GGD GHOR.

### 3.2 Logging en monitoring

Applicatielogging is ingericht conform NEN7513. RDO geeft inzicht in een selectie van de logging ten behoeve van het herkennen van afwijkende handelingen in de applicatie om misbruik op te sporen. Dit deelt RDO met een partij die door de GGD is aangewezen om de monitoring uit te voeren. Daarnaast is (infrastructuur) logging - en monitoring onderdeel van de dienstverlening van RDO – dit wordt onder eigen beheer uitgevoerd. Afwijkingen worden gemeld aan GGD-GHOR SOC. Waar nodig deelt VWS logbestanden op verzoek van de GGD voor de uitvoering van verzoeken door toezichthouders of wettelijke verplichting in het kader van opsporing.

### 3.3 Beveiliging afnemer

Zowel dienstverlener als afnemer dienen invulling te geven aan de ministeriële regeling voor infectieziektebestrijding<sup>5</sup>. Met het tekenen van deze DVO bevestigen beide partijen hieraan te voldoen.

De wijze waarop de beveiliging van de informatie-uitwisseling met externe bronnen is ingericht moet worden vastgelegd conform de eisen uit de NEN 7512. De uitwisseling wordt pas gestart als deze maatregelen zijn vastgelegd.

---

<sup>5</sup> Regeling van de Minister van Volksgezondheid, Welzijn en Sport van 18 november 2008, nr. PG/ZP-2.892.655, houdende nieuwe eisen inzake de publieke gezondheid (Regeling publieke gezondheid)

## 4 Verantwoordelijkheden

Zowel de GGD als VWS zijn verantwoordelijk voor het niveau van dienstverlening, GGD in de rol van afnemer en VWS in de rol van leverancier. De verantwoordelijkheden zijn hieronder beschreven.

### 4.1 Verantwoordelijkheden VWS

- Het leveren van de diensten conform het dienstenniveau zoals in dit document beschreven.
- Het uitvoeren van de noodzakelijke patches en updates indien dit vanuit beheer en/of beveiliging noodzakelijk blijkt om de bestaande functionaliteit van de diensten in stand te houden.
- Het uitvoeren van applicatie-, en technisch beheer.
- Het contractueel vastleggen van afspraken met externe leveranciers.
- Signaleren en melden van risico's in de keten die invloed hebben op het functioneren van de applicatie, zoals beschreven in Bijlage 1 Procedurebeschrijving beheer GGD Contact.

### 4.2 Verantwoordelijkheden GGD

- Het melden van wijzigingen in de koppeling van eigen systemen, die op enige wijze relevant zijn voor de werking van de afgenomen diensten.
- Het melden van (beveiligings-)technische en functionele onvolkomenheden in de werking van de diensten en de gegevensuitwisseling.
- Het uitvoeren van functioneel beheer.
- Het bewaken van de kwaliteit van de (door de afnemer zelf) vast te leggen gegevens met betrekking tot tijdigheid, juistheid en volledigheid en het gebruik van deze gegevens.
- Het signaleren en melden van beveiligingsrisico's die effect hebben op de veiligheid/beveiliging van GGD Contact.
- Het gestructureerd en geprioriteerd melden van wensen voor doorontwikkeling, conform het wijzigingsproces als gespecificeerd in Bijlage 1 Procedurebeschrijving beheer GGD Contact.
- Afstemming over toevoeging van koppelingen (of wijzigingen hierop).

## 5 Communicatie

### 5.1 Rapporteren

Rapportage over de dienstverlening worden in afstemming met GGD GHOR vastgesteld en zijn onderdeel van het document Procedurebeschrijving beheer GGD Contact.

### 5.2 Overlegvormen

Overleggen ten behoeve van de te leveren dienstverlening zijn omschreven in de Bijlage 1 Procedurebeschrijving beheer GGD Contact.



## 6 Tekenblad

Door de ondertekening stemt ondergetekende in met de overeenkomst voor het gebruik van GGD Contact, als gevolg waarvan een overeenkomst ontstaat tussen VWS en de GGD.

Voor akkoord:

Partij: Staat der Nederlanden (Ministerie VWS)

Datum: ...

Voor deze:  Directeur Informatiebeleid / CIO


## Tekenblad

Door de ondertekening stemt ondergetekende in met de overeenkomst voor het gebruik van GGD Contact, als gevolg waarvan een overeenkomst ontstaat tussen VWS en de GGD.

Voor akkoord:

Partij: Gemeentelijke Gezondheidsdienst GGD West-Brabant

Datum: ...

Voor deze: 

## 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 GGD West-Brabant, gevestigd te Breda aan de Doornboslaan 225-227, ingeschreven in het handelsregister onder KvK nummer 20164916, rechtsgeldig vertegenwoordigd door [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 directeur Informatiebeleid, [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 wenselijk 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 plaats 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 [REDACTED]

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,

<p>Breda, datum:</p> <p>GGD West-Brabant</p> <p>namens deze, de directeur publieke gezondheid</p> 	<p>Den Haag, datum:</p> <p>DE MINISTER/STAATSSECRETARIS Volksgezondheid, Welzijn en Sport</p> <p>namens deze, de directeur Informatiebeleid</p> 
---	--



## Bijlage 1. De Verwerking van Persoonsgegevens

Het onderwerp/aard en doel van de Verwerking	<p>De verwerking door opdrachtnemer betreft het hosten van app, sluis en webportal van 'GGD Contact'.</p> <p>Het doel van GGD Contact is op een goede, veilige en efficiënte manier uitvoeren van bronnen- en contactonderzoek.</p>
Het soort Persoonsgegevens	<ul style="list-style-type: none"><li>• Bijzondere categorieën van gegevens als bedoeld in artikel 9 AVG</li><li>• Wettelijk voorgeschreven identificatienummers</li><li>• Overige persoonsgegevens.</li></ul>
Beschrijving categorieën Persoonsgegevens	<ul style="list-style-type: none"><li>• 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</li><li>• Gegevens van medewerkers die het bronnen- en contactonderzoek uitvoeren, waaronder ook de logging van het gebruik van de applicatie.</li></ul>
Beschrijving categorieën Betrokkenen	<ul style="list-style-type: none"><li>• Met infectieziekte besmette personen ('index')</li><li>• Contacten die mogelijk besmet zijn ('contacten')</li><li>• Medewerkers die bronnen en contactonderzoek uitvoeren</li></ul>
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.

Dienstverleningsovereenkomst  
GGD GHOR Nederland – GGD  
generieke ICT-diensten ten behoeve van GGD Contact

Versie: 1.1  
Datum: 21 juni 2021

## Versiehistorie

Versie	Datum	Auteur	Status document
0.1	31 mei 2021	[REDACTED]	Nieuwe overeenkomst
0.3	3 juni 2021	[REDACTED]	Review commentaar verwerkt
0.98	4 juni 2021	[REDACTED]	Review commentaar/context informatie verwerkt
0.99	7 juni 2021	[REDACTED]	Review commentaar [REDACTED] verwerkt
1.0	8 juni 2021	[REDACTED]	Review [REDACTED]
1.1	21 juni 2021	[REDACTED]	Review commentaren stuurgroep verwerkt.

### De ondergetekenden:

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

### En

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

Hierna gezamenlijk aangeduid als “**de Partijen**” en ieder als een “**Partij**”.

### Overwegende dat:

- De Vereniging GGD GHOR Nederland heeft statutair onder meer ten doel het inhoudelijk functioneren van de GGD organisaties te bevorderen, deskundige en innoverende bijdrages te leveren aan het beleid van de GGD organisaties en de belangen van haar leden te behartigen. In de kern vormt de Vereniging het samenwerkingsverband van de GGD-en;
- De algemene ledenvergadering van GGD GHOR Nederland (“**de DPG-raad**”) bestaat uit de directeuren publieke gezondheid (“**DPG’en**”) van alle GGD’en. De DPG-en zijn belast met de leiding van de GGD-en (art. 14 lid 3 Wet Publieke Gezondheid);
- Contractspartij Stichting Projectenbureau (“**Stichting**”) heeft statutair ten doel de Vereniging GGD GHOR Nederland in haar doelstellingen te ondersteunen en taken te verrichten in opdracht van het bestuur van de Vereniging (“**Presidium**”). De Stichting kan namens en op verzoek van de Vereniging verplichtingen aangaan ten laste van haar leden of rechten bedingen ten behoeve van haar leden;
- In de DPG-raad van 12 februari is door de leden besloten om zo spoedig als juridisch verantwoord mogelijk is, een alternatief voor het systeem (“**HPzone (Lite)**”) dat gebruikt wordt in het bron- en contactonderzoek (“**BCO**”) te ontwikkelen en VWS als stelselverantwoordelijke te verzoeken als opdrachtgever op te treden. In de DPG-raad van 15 april 2021 is besloten om over te gaan tot de installatie van een projectstuurgroep Fase 1 die zich richt op de zo spoedig als mogelijk en verantwoorde uitrol bij de GGD’en van dit alternatieve systeem (“**GGD Contact**”). Deze overeenkomst en de daarin benoemde dienstverlening vloeit voort uit deze besluiten;
- Het ministerie van Volksgezondheid, Welzijn en Sport (“**VWS**”) heeft in haar rol als opdrachtgever, indachtig de besluiten van de DPG-raad, aan GGD GHOR Nederland de opdracht gegeven om de vervanging van HPzone (Lite) door GGD Contact ten behoeve van BCO in het kader van de bestrijding van covid-19 bij de GGD’en te coördineren en een deel van de dienstverlening rondom GGD Contact aan de GGD’en na implementatie op zich te nemen;
- Met de in gebruik name van GGD Contact zal GGD gebruik gaan maken van een aantal generieke ICT-diensten van GGD GHOR Nederland. Hierover wensen partijen middels deze overeenkomst nadere afspraken te maken;
- Deze Dienstverleningsovereenkomst inclusief haar bijlagen is door de projectstuurgroep Fase 1 d.d. op 25 juni 2021 vastgelegd als de standaard overeenkomst voor alle GGD’en die

gebruik gaan maken van GGD Contact en de hiervoor benodigde generieke ICT-diensten van GGD GHOR Nederland;

- In geval van strijdigheid tussen de Dienstverleningsovereenkomst en de bijlagen prevaleert het bepaalde in de Dienstverleningsovereenkomst.

## Partijen verklaren als volgt te zijn overeengekomen

### 1. Doel

- 1.1. Het doel van partijen is zich gezamenlijk in te spannen voor een optimale invoering en gebruik van GGD Contact;
- 1.2. GGD GHOR Nederland zal diensten aan GGD leveren inzake GGD Contact en GGD zal deze diensten van GGD GHOR Nederland afnemen gedurende de looptijd van deze overeenkomst. Deze diensten zijn vermeld in bijlage I welke integraal deel uit maakt van deze overeenkomst;
- 1.3. Deze diensten worden conform de kwaliteitsstandaarden als vermeld in de Service Level Agreement die bijgevoegd is in bijlage II;
- 1.4. De benoemde diensten als genoemd in artikel 1.2. betreffen collectieve diensten die aangeboden worden aan iedere GGD die gebruik maakt van GGD Contact;
- 1.5. Partijen zullen elkaar ten behoeve van de samenwerking telkens tijdig alle relevante gegevens en inlichtingen verschaffen.

### 2. Looptijd en beëindiging

- 2.1. Deze overeenkomst treedt in werking op de datum waarop Partijen deze ondertekenen (“Ondertekendatum”);
- 2.2. De overeenkomst eindigt van rechtswege wanneer de tijdelijke dienstverleningsovereenkomst tussen VWS en GGD GHOR Nederland betreffende GGD Contact stopt. GGD GHOR Nederland informeert GGD hier onverwijld over;
- 2.3. Mocht een wijziging in de bestuurlijke verhoudingen en positionering van GGD GHOR Nederland hier om vragen, dan verplichten partijen zich over en weer mee te werken aan een eventuele overdracht van de rechten en verplichtingen uit hoofde van onderhavige overeenkomst;
- 2.4. In geval van beëindiging van deze overeenkomst zal in gezamenlijk overleg een exit plan worden opgesteld.

### 3. Transitie

- 3.1. De uitrol van GGD Contact zal in iteraties verlopen. In de eerste iteratie wordt GGD Contact naast HPZone (Lite) in gebruik genomen. GGD draagt zorg voor het parallelle gebruik. GGD GHOR Nederland houdt de dienstverlening rondom HPzone (Lite) in stand gedurende de transitieperiode;
- 3.2. De ontwikkeling van de dienst “GGD Contact” wordt uitgevoerd door en onder verantwoordelijkheid van VWS RDO. De projectstuurgroep fase I besluit over de snelheid en wijze van implementatie van GGD Contact. Partijen volgen de besluiten van de projectstuurgroep;
- 3.3. VWS is op het moment van aangaan van deze overeenkomst eigenaar van GGD Contact en verantwoordelijk voor het beheer van deze toepassing;

- 3.4. De afspraken over het gebruik van GGD Contact door GGD en de tijdelijke dienstverlening door VWS in dit kader, zijn onderwerp voor een aparte 'dienstverleningsovereenkomst GGD Contact' tussen GGD en VWS.
- 3.5. GGD GHOR Nederland draagt zorg voor de afstemming met VWS tussen de dienstverlening als benoemd in deze overeenkomst en de dienstverlening als benoemd in 3.4.

#### **4. Kosten**

- 4.1. De kosten voor benoemde diensten worden voorlopig gedekt door VWS. GGD GHOR Nederland zal de kosten voor de dienstverlening aan GGD bij VWS in rekening brengen;
- 4.2. Indien de dekking van de kosten door VWS wegvalt, treedt GGD GHOR Nederland in overleg met de DPG-Raad om tot een alternatieve financiering te komen. Partijen zullen in dat geval meewerken aan het vinden van een passende oplossing.

#### **5. Verplichtingen GGD GHOR Nederland**

- 5.1. GGD GHOR Nederland spant zich in om de dienstverlening als gesteld in bijlage I te leveren conform het vastgestelde kwaliteitsniveau als gesteld in bijlage II;
- 5.2. GGD GHOR Nederland tracht om waar mogelijk personeel met kennis van de organisatie en bedrijfsprocessen van de GGD in de te leveren dienstverlening in te zetten;
- 5.3. GGD GHOR Nederland wijst een vertegenwoordiger aan die als single point of entry, het aanspreekpunt is voor GGD en bevoegd is om beslissingen op het operationele vlak te nemen en maakt deze persoon aan GGD kenbaar;
- 5.4. GGD GHOR Nederland voorziet GGD van rapportages zoals vastgelegd in bijlage III. De rapportages voorzien in een periodieke performance evaluatie van de geleverde services.
- 5.5. GGD GHOR Nederland spant zich in om de door haar geleverde diensten continu te verbeteren. Verbeteringen vinden met vooraanmelding bij GGD plaats.

#### **6. Verplichtingen GGD**

- 6.1. GGD maakt bij het in gebruik nemen van GGD Contact gebruik van de daarbij behorende diensten die aangeboden worden door GGD GHOR Nederland.
- 6.2. GGD maakt gebruik van de opstelde werkinstructies en procedures die verstrekt worden door GGD GHOR Nederland waaronder de checklist onboarding applicaties zoals beschreven in bijlage V.
- 6.3. GGD wijst een vertegenwoordiger aan die als, single point of entry, het aanspreekpunt is voor GGD GHOR Nederland n bevoegd is om beslissingen op het operationele vlak te nemen en maakt deze persoon aan GGD kenbaar.

#### **7. Gegevensbescherming**

- 7.1. De Algemene Verordening Gegevensbescherming (AVG) is van toepassing op de in deze overeenkomst benoemde dienstverlening;
- 7.2. Partijen hebben bepaald dat GGD GHOR Nederland voor bedoelde ICT diensten verwerker is in het kader van de AVG;
- 7.3. Partijen hebben een verwerkersovereenkomst gesloten zoals opgenomen in bijlage IV;
- 7.4. Conform het bepaalde in de verwerkersovereenkomst zal GGD GHOR Nederland op een zorgvuldige wijze, in overeenstemming met de AVG gegevens en documentatie van GGD verwerken.

#### **8. Klachtafhandeling**



- 8.1. De klachtenprocedure van GGD GHOR Nederland is van toepassing op de in deze overeenkomst benoemde dienstverlening;
- 8.2. In geval dat GGD een klacht indient bij GGD GHOR Nederland, zal laatstgenoemde zo spoedig mogelijk in overleg treden met de indiener van de klacht om tot een correcte oplossing te komen.

## **9. Aansprakelijkheid**

- 9.1. Partijen vrijwaren elkaar tegen alle aanspraken van derden die betrekking hebben op hetgeen is overeengekomen in deze overeenkomst en evenals tegen alle aanspraken die betrekking hebben op hun eigen verrichtingen.
- 9.2. Partijen dragen zorg voor een eigen dekkende verzekering voor het vergoeden van eventuele schade.

## **10. Wijzigingen in de overeenkomst**

- 10.1. Partijen zijn gemachtigd om een verzoek tot wijziging van de Dienstverleningsovereenkomst voor te stellen, evenals wijzigingen op de geleverde diensten als benoemd in bijlage I.
- 10.2. Partijen zullen binnen een maand na een verzoek als gesteld in artikel 3.1. met elkaar in overleg treden om de gewenste wijzigingen en de daaruit voortvloeiende consequenties te bespreken conform hetgeen gesteld is in bijlage III;
- 10.3. Partijen nemen bij wijzigingsverzoeken de collectiviteit van de dienstverlening in ogenschouw.

## **11. Geheimhouding**

- 11.1. Partijen zullen over en weer geheimhouding betrachten ten aanzien van alle gegevens, documentatie en know how die hen bekend zijn geworden in het kader van deze Dienstverleningsovereenkomst en alle van de wederpartij ontvangen gegevens waarvan men weet of redelijkerwijs behoort te weten dat deze van vertrouwelijke aard zijn;
- 11.2. Het verbod als benoemd in artikel 11.1. geldt niet indien en voor zover verstrekking van de betreffende gegevens of informatie aan een derde noodzakelijk is ingevolge een rechtelijke uitspraak, een wettelijk voorschrift of op basis van een wettelijk bevel.
- 11.3. De geheimhouding zal Partijen blijvend binden ook na beëindiging of ontbinding van deze Dienstverleningsovereenkomst tot 2 jaar na beëindiging.

Deze Dienstverleningsovereenkomst zal worden uitgelegd in overeenstemming met en worden beheerst door Nederlands recht.

## **Toepasbaarheid**

- Verwijzingen naar wettelijke bepalingen worden zo opgevat als verwijzingen naar wettelijke bepalingen zoals deze luiden bij het aangaan van de Dienstverleningsovereenkomst
- De bijlagen vormen een integraal onderdeel van deze Dienstverleningsovereenkomst
- Hetgeen in de Dienstverleningsovereenkomst overeengekomen is, prevaleert boven de bijlagen in geval van strijdigheid en/of onverenigbaarheid
- In geval van strijdigheid en/of onverenigbaarheid tussen de bijlagen geldt de rangregeling waarbij het hoger gerangschikte document prevaleert boven het lagere gerangschikte:
  - Bijlage I; Dienstbeschrijving
  - Bijlage II; Service Level Agreement
  - Bijlage III; Dossier Afspraken en Procedures

- Bijlage IV; Verwerkersovereenkomst
- Bijlage V; Checklist onboarding applicaties

GGD GHOR Nederland

GGD West-Brabant

Utrecht,

\_\_\_\_\_ (Plaats), \_\_\_\_\_(Datum)

██████████

Waarnemend Algemeen Directeur

██████████

Directeur Publieke Gezondheid

**DEZE VERWERKERSOVEREENKOMST IN DE ZIN VAN ARTIKEL 28 AVG** (deze “Verwerkersovereenkomst”) is getekend op 23 augustus 2021,

**TUSSEN:**

- (1) De Gemeentelijke Gezondheidsdienst GGD West-Brabant, gevestigd te Breda aan de Doornboslaan 225-227, ingeschreven in het handelsregister onder KvK nummer 20164916, hierna eveneens te noemen “GGD”, rechtsgeldig vertegenwoordigd door [REDACTED] (de “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 [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;

<b>Betrokkene</b>	De geïdentificeerde of identificeerbare natuurlijke persoon op wie een Persoonsgegeven betrekking heeft;
<b>Beveiligingsprotocollen</b>	De door Verwerker te hanteren beveiligingsmaatregelen conform artikel 32 AVG;
<b>Datalek</b>	Een inbreuk op de beveiliging van Persoonsgegevens zoals bedoeld in artikel 4 lid 12 AVG;
<b>Persoonsgegeven(s)</b>	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:
- de uitvoering van de Dienstverleningsovereenkomst en deze Verwerkersovereenkomst; en
  - 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. BEVEILIGINGSMATREGELEN**

- 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: [REDACTED]
- 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.<sup>1</sup>

## **13. INSCHAKELLEN (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.<sup>2</sup>
- 13.2 Op eerste verzoek van Verwerkingsverantwoordelijke verstrekt Verwerker aan Verwerkingsverantwoordelijke een overzicht van door haar ingeschakelde (sub)verwerkers.

<sup>1</sup> 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.

<sup>2</sup> 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 West-Brabant

GGD GHOR Nederland

\_\_\_\_\_  
[Redacted Signature]  
Directeur Publieke Gezondheid

\_\_\_\_\_  
[Redacted Signature]  
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

14-juni-2020

**VERWERKERSOVEREENKOMST**

GGD WEST-BRABANT

**YOURCE**

## De ondergetekenden:

1. De besloten vennootschap met beperkte aansprakelijkheid 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>>; 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]

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 (telefonisch) ten aanzien van de door Verwerker te verrichten dienst (hierna: "Overeenkomst" omschreven in Bijlage 1);
- III. Verwerker in het kader van de Overeenkomst persoonsgegevens (hierna: "Persoonsgegevens") in de zin van de Wet bescherming persoonsgegevens (hierna: "AVG") zal verwerken ten behoeve van Verantwoordelijke;
- IV. Partijen - mede ter uitvoering van het bepaalde in artikel 14 lid 2 AVG - in de onderhavige aanvullende overeenkomst (hierna: "Verwerkersovereenkomst") een aantal voorwaarden wensen vast te leggen die van toepassing zijn op hun relatie in verband met de genoemde activiteiten in opdracht van en ten behoeve van Verantwoordelijke.

## Verklaren te zijn overeengekomen als volgt:

### Artikel 1. Onderwerp van de Verwerkersovereenkomst

1. Verantwoordelijke is de verantwoordelijke 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 eventuele overige door de Verantwoordelijke verstrekte instructies.
2. Verwerker verbindt zich om de Persoonsgegevens zorgvuldig te verwerken, alsmede in overeenstemming met de toepasselijke wet- en regelgeving.
3. 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.
4. 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.

### Artikel 2. Technische en organisatorische voorzieningen (beveiliging)

1. Verwerker 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").

Deze maatregelen zullen, rekening houdend met de stand der 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 gegevens met zich meebrengen.

2. 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.
3. 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.

### Artikel 3. Inschakeling derden

Verwerker zal eventuele subverwerkers verplichten de bepalingen van de Verwerkersovereenkomst na te leven. Verwerker blijft te allen tijde verantwoordelijk voor het handelen of nalaten van de subverwerkers.

### Artikel 4. Doorgifte naar derde landen

Het is Verwerker niet toegestaan de Persoonsgegevens door te geven en/of op te (laten) slaan in landen buiten de Europese Unie, tenzij verwerker uitdrukkelijke schriftelijke toestemming van Verantwoordelijke heeft hiervoor en dit op grond van de AVG is toegestaan bijvoorbeeld omdat het betreffende land een passend beschermingsniveau biedt of gebruik wordt gemaakt van een daartoe bestemd ongewijzigd modelcontract, goedgekeurd door de Europese Commissie, met inachtneming van de overige bepalingen van de verwerkersovereenkomst.

### Artikel 5. Verzoeken betrokkenen

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 artikel 35 en 36 van de AVG.

### Artikel 6. Vertrouwelijkheid

1. Verwerker, alsmede alle medewerkers die handelen onder het gezag van Verwerker en 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.
2. Verwerker zal al haar medewerkers die betrokken zijn bij de uitvoering van de Overeenkomst terzake een geheimhoudingsverklaring laten tekenen.

### Artikel 7. Verstrekking & verwijdering

1. 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.
2. Verwerker is verplicht alle Persoonsgegevens op eerste verzoek van Verantwoordelijke volledig en onherroepelijk te verwijderen.

## Artikel 8. Aansprakelijkheid



## 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. Verantwoordelijke is gerechtigd de maatregelen en de naleving van de op Verwerker rustende verplichtingen te controleren.
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 toezichhouders 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. 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

1. 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.
2. Deze overeenkomst heeft een looptijd gelijk aan de Overeenkomst. 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.
3. Wijziging van de Verwerkersovereenkomst is slechts mogelijk door schriftelijke overeenstemming door Partijen.
4. 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.
5. Geschillen tussen Verantwoordelijke en Verwerker worden uitsluitend voorgelegd aan de bevoegde rechter in het arrondissement Rotterdam.

## Ondertekening

Verantwoordelijke GGD:

Naam:

Datum:

Verwerker Yource Outsourcing b.v.:

Naam:

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 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. AVG Art9, lid1 geeft aan dat verwerking gezondheidsgegevens niet is toegestaan.

In Art 9.Lid 2 wordt aangegeven welke voorwaarden verwerking van die gegevens toch mogelijk is.

Hieronder worden de toepasselijke paragrafen gelijst die de grondslag vormen voor de verwerking van de patiëntgegevens van de GGD.

- + Art9.Lid2, Par C) Verwerking ter bescherming van vitale belangen van Betrokkene
- + Art.Lid2, Par G) Zwaarwegend algemeen belang, waarbij de evenredigheid met het nagestreefde doel wordt gewaarborgd, de wezenlijke inhoud van het recht op bescherming van persoonsgegevens wordt geëerbiedigd en passende en specifieke maatregelen worden getroffen ter bescherming van de grondrechten en de fundamentele belangen van de Betrokkene.
- + Art.Lid2, Par H) de verwerking is noodzakelijk voor doeleinden van preventieve of arbeidsgeneeskunde, voor de beoordeling van de arbeidsgeschiktheid van de werknemer, medische diagnoses, het verstrekken van gezondheidszorg of sociale diensten of behandelingen dan wel het beheren van gezondheidszorgstelsels en -diensten of sociale stelsels en diensten, of uit hoofde van een overeenkomst met een gezondheidswerker en behoudens de in lid 3 genoemde voorwaarden en waarborgen;

Verwerking van de Bijzondere Persoonsgegevens door Yource wordt in Art9.Lid3 beschreven als 'Onder de verantwoordelijkheid van een beroepsbeoefenaar die krachtens door bevoegde instanties vastgestelde regels aan het beroepsgeheim is gebonden.'

Yource is daarmee 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.

14-juni-2020

**RAAMOVEREENKOMST**

GGD WEST-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, West- 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 ██████████, 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 7 maanden, 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 redelijkerwijs 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 wegens 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] [REDACTED], zodat Yource de factuur met PO nummer [REDACTED] verstuurt. 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] [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] [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 Artikelliden 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 Breda.

### **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: 

14-juni-2020

**DIENSTOVEREENKOMST**

GGD WEST-BRABANT

**YOURCE**

Regionaal contact- en brononderzoek

Inleiding .....	3
Beschrijving Dienstverlening .....	4
Service Level afspraken .....	6
Forecasting .....	8
Training.....	10
Quality Monitoring (QM).....	12
Rapportage .....	13
Tarieven.....	14
Implementatie; kosten en doorlooptijd .....	16
Facturatie proces.....	19
Calamiteiten .....	21
Change management procedure.....	22
Communicatie & betrokkenheid .....	25
ICT.....	28

## Inleiding

Dit betreft de Dienstenovereenkomst tussen GGD West-Brabant (hierna te noemen Opdrachtgever) en Yource Outsourcing b.v. (hierna te noemen Opdrachtnemer) en behorende 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 geldt voor de looptijd van dit project. Bij het aflopen van de overeenkomst op 31 december 2020, handelt Opdrachtnemer de reeds voor 31 december 2020 in behandeling genomen BCO's af. Ook indien deze afhandeling na de aflooptdatum van deze overeenkomst plaatsvindt. Opdrachtgever en Opdrachtnemer bespreken het afschaalscenario, mocht deze situatie zich voordoen.

Opdrachtgever heeft de mogelijkheid om de overeenkomst met 3 maanden te verlengen tegen dezelfde voorwaarden. Ook dan geldt dat de reeds in behandeling genomen BCO's voor 31 maart 2021 worden afgehandeld na einddatum.

De Hoofdovereenkomst heeft een looptijd tm 31 december 2020 met een stilzwijgende verlenging van 48 maanden. en deze daarbij behorende Dienstenovereenkomst zal minimaal 1 maal per half jaar worden geëvalueerd. In overleg tussen de partijen kunnen ook tussentijds bijstellingen plaats vinden van de Dienstenovereenkomst.

In de kwartaal overleggen worden de wijzigingformulieren (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 worden geformaliseerd.

## 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. Op dagelijkse basis worden er door de landelijke huisartsen en de GGD-en 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

### 1.2 Contact kanalen

Op dagelijkse basis worden er in de middag dossiers met index patiënten op naam van Opdrachtnemer gezet in HP Zone. Deze patiënten moeten uiterlijk binnen 24 uur (na)gebeld worden. Indien een patiënt niet kan worden bereikt, wordt er een nieuwe belpoging in een ander tijdsvenster ingepland.

De Inbound – “burgersvragen” m.b.t. tot RIVM-richtlijnen en/of de overige GGD onderdelen worden door het KlantContactCentrum van de GGD zelf opgevangen en vallen buiten deze Inbound werkzaamheden.

## 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 we gedurende de startfase (train-de-trainer) ook vanaf het kantoor van de GGD Breda werken. 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
- Koninginnedag
- 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 service level 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 terwijl de normen behorende bij de PI's indicatief beschouwd moeten worden. 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 Service level afspraken, zoals opgenomen in hoofdstukken 3.3. en 3.4 worden geëvalueerd, vastgesteld en geformaliseerd. Onder service level afspraken wordt verstaan [REDACTED]

### 2.3 Key Performance Indicators

- [REDACTED]% 1<sup>ste</sup> belpoging [REDACTED] uur na overdracht van de dossier.
- Bezettingsgraad van Opdrachtnemer is minimaal [REDACTED]% t.o.v. werkaanbod
- Van alle afgehandelde BCO's is [REDACTED]% volledig ingevuld, conform instructies van de GGD,
- Van alle afgehandelde BCO's is [REDACTED]% correct ingevuld, o.b.v. de door patiënt verschaft gegevens
- Opdrachtnemer doet [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 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 en 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   % of meer boven het geprognosticeerde volume ligt
- bij systeemstoringen aan de systemen van GGD.
- bij overmacht en calamiteiten.

Opdrachtnemer zal niet later dan   GGD informeren over de invloed van een voorval dat leidt tot een Niet Meetbare dag gedurende deze week.

In elk   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 pool in en kan er op dagbasis worden geschoven. Hierbij wordt gewerkt met een [redacted] planning: [redacted]; 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 [redacted] getrainde parttimers is de Opdrachtnemer in staat om [redacted] af te schalen tot [redacted]% van de bezetting. Indien gedurende het project blijkt, dat het werk aanzienlijk afneemt, stelt de Opdrachtnemer en/of Opdrachtgever voor dat de pool tussentijds wordt 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 [redacted]% van de gebudgetteerde [redacted] uur per BCO wordt besteed in fase A (start dag BCO) en dat [redacted]% na [redacted] dagen en [redacted]% na [redacted] dagen wordt besteed. Zodoende wordt er gestart in week [redacted] met [redacted] uur per dag en in week [redacted] met [redacted] uur per dag (zie de tabel op deze pagina)

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

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

█ worden in rekening gebracht. Dit geldt bij █  
█, █  
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 █ 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 Uur tarief	█	█
E-learning	█	█
Introductie Opdrachtnemer	█	█
Communicatietraining:	█	█
Introductie Opdrachtgever diensten	█	█
Vaardigheidstraining applicaties GGD	█	█
Toets (max. █ minuten)	█	█
Specifieke training Opdrachtgever van nieuwe diensten	█	█
Refreshment toets (max. █ minuten)	█	█

### 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:



### 4.4 Trainingvereisten & Kosten

Van alle medewerkers wordt verwacht dat ze bij aanvang van de werkzaamheden met succes de kennistoets (e-learning) van Opdrachtgever hebben afgelegd. Voorwaarde hierin is dat de agent 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 Yource komen.

In bijlage 2 zijn de `verwachtingsprofielen gedefinieerd waaraan de Opdrachtgever agent en Teamleider moet 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. In afwijking is een aparte regeling overeengekomen, waarbij de Quality Monitoring kosten als additioneel component zijn opgenomen in het agent uur tarief.

### 5.2 Proces Quality monitoring

In bijlage 3 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 gemonitordde 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] [REDACTED]) zal een verbetertraject als beschreven in het detail proces beschrijving 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 monitorings sessie zal de Teamleider in samenwerking met de Auditor een actieve rol gaan spelen in het verbeterplan volgens detail proces beschrijving.

### 5.3 Steekproefgrootte

Opdrachtnemer is verantwoordelijk voor het behalen van 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 facturatie proces
- Basis voor forecasting
- Algemene management informatievoorzieningen

De detailrapportages geven de 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

### 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.

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 de standaard dienstverlening weergegeven. Er wordt gefactureerd op basis van een tarief per ingezet uur: het aantal te bestede uren van [ ] 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	[ ]
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 [ ]% af te schalen naar [ ] uur per dag, op weekbasis wordt er gepland ([ ]).
- Inzetbaarheid van de flexibele schil vanuit [ ] in het geval van "specials".

De uurtarieven zijn exclusief:

- 21% BTW
- Kosten TolkenTelefoon

\* Als Projectmanager gaan we [ ] 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 Opdrachtnemerkantoor 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] 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]	[REDACTED]
Teamleaders (training [REDACTED] x)		[REDACTED]	[REDACTED]
Trainer		[REDACTED]	[REDACTED]
Projectmanager		[REDACTED]	[REDACTED]
Projectcoördinator		[REDACTED]	[REDACTED]
Client Manager		[REDACTED]	[REDACTED]
Specials		[REDACTED]	[REDACTED]
<b>Sommatie</b>			[REDACTED]

### 8.3 Besturingsapparaat

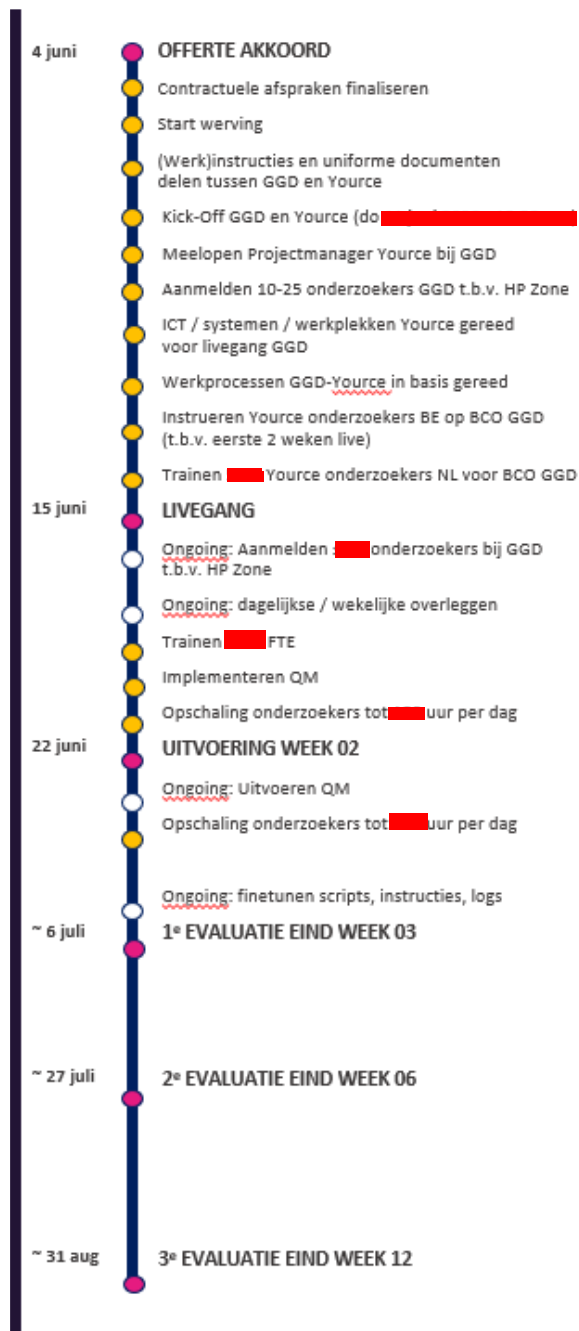
Na implementatie zullen de ingezette uren van de onderzoekers afhangen van het aantal BCO's. Kijkend naar de vaste bezetting, is het voorstel om de trainer voor minder uur wél blijven inzetten om continu in te spelen op de dynamiek in benodigde kennis.

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.

	Tarief	Operatie tot 01 okt 2020		Operatie ná 01 okt 2020	
		Uren week xx	Kosten	Uren week xx	Kosten
Onderzoekers					
Teamleaders					
Trainer					
Projectmanager					
Projectcoördinator					
Client Manager					
Specials					
<b>Sommatie</b>					

## 8.4 Planning (Indicatie)



## 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

- ☞ Formulieren KPI's op kwaliteit

- ☞ Toegang verlenen tot HP Zone

- ☞ Optuigen QM model o.b.v. KPI's GGD

## Facturatie proces

### 9.1 Inleiding

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

### 9.2 Procedure

[REDACTED]

[REDACTED] dagen na afloop van de betreffende maand ingediend te zijn.

De facturen dienen digitaal in PDF-format aangeleverd te worden via [REDACTED] t.a.v. crediteurenadministratie en onder vermelding van de betreffende opdrachtgever.

Factuuradres:

**GGD West-Brabant**  
**Doornboslaan 225-227**  
**4816 CZ Breda**

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 en uiterlijk binnen dertig (30) dagen. 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 service afdeling. 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 RFC-procedure met als uitgangspunt de Forecast garantieregeling van deze Dienstenovereenkomst (op dagbasis).

### 10.3 Niet beschikbaar zijn van Opdrachtnemer applicaties

Indien de Opdrachtnemer in een Calamiteit verkeert, zal Opdrachtnemer Opdrachtgever hierover uiterlijk binnen                      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 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 ■ 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 ■ kalenderdagen. In overleg is een eventuele workaroud, 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 ■ kalenderdagen mag bedragen. Indien deze RFC niet doorgevoerd wordt binnen ■ dagen mag verwacht worden dat dit leidt 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 ■ 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 (■).

#### *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 vervolgtacties te bespreken. Dit laat onverlet dat de partijen al het mogelijke zullen doen om alsnog de gewenste opleverdatum te kunnen realiseren.

#### *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 Gereedmelding*

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

Gereedmelding 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 standaard formulier (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									
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



## 12.4 Communicatiematrix

Naam	Bedrijf	Functie	Telefoonnummer	E-mailadres
	GGD West-Brabant			
	GGD HVB			
	GGD HVB			
	GGD West-Brabant			
	Yource			
	Yource			
	GGD West-Brabant			
	GGD Het Servicecentrum			
	GGD HVB			
	Yource			
	GGD HVB			
	GGD HVB			
	GGD HVB			
	GGD West-Brabant			
	GGD West-Brabant			
	GGD Het Servicecentrum			
	GGD HVB			
	GGD HVB			
	Yource			
	GGD HVB			
	Yource			
	GGD HVB			
	Yource			
	GGD HVB			
	Yource			
	GGD HVB			
	GGD West-Brabant			
	GGD HVB			
	Yource			
	Yource			
	GGD West-Brabant			
	Yource			
	GGD West-Brabant			
	GGD HVB			
	GGD Het Servicecentrum			
	Yource			
	Yource			
	GGD HVB			
	GGD West-Brabant			

## 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.
- ██████████ BCO afwikkeling door Opdrachtnemer per ██████████ 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 [REDACTED].

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.

## Bijlage 1 Loggingtabel

	<b>1</b> "Afgesloten met data" Correct contact/Closed with data	CA/FA had de <u>persoon aan de lijn</u> en het <u>formulier werd volledig ingevuld/doorlopen</u> zoals het script het voor <u>schreef</u> .
	<b>2</b> "Gesloten zonder gegevens" – geen contact onderzoek nodig/Closed without data	CA/FA had de <u>persoon aan de lijn</u> , maar het <u>formulier kon niet (volledig) worden ingevuld/doorlopen om specifieke redenen (zie business rules)</u> .
	<b>3</b> Opnieuw gepland/ Manual Reschedule <sup>(1)</sup>	CA/FA had al dan <u>niet de persoon/gezinslid/vertrouwenspersoon aan de lijn en</u> men vroeg om op een later tijdstip teruggebeld te worden.
	<b>4</b> Bezettoon/Busy	CA/FA had de <u>persoon NIET aan de lijn</u> , maar kwam op de <u>bezettoon terecht</u> . (Het ging niet over naar voicemail en werd niet doorgeschakeld naar een ander nummer.)
	<b>5</b> Geen Antwoord/No Answer <sup>(2)</sup>	CA/FA had de <u>persoon NIET aan de lijn</u> , want de lijn ging niet over naar de voicemail, de lijn werd niet automatisch doorgeschakeld, de lijn werd niet automatisch afgebroken en men kreeg geen bezettoon.
	<b>6</b> Voicemail/Voicemail	CA/FA had de <u>persoon NIET aan de lijn</u> , want de lijn ging over naar de voicemail.
	<b>7</b> Foutief nummer/Wrong number	CA/FA had de <u>persoon NIET aan de lijn, omdat:</u> 1) Het <u>opgegeven nummer niet correct was en niet gecorrigeerd kon worden</u> (bv. +324995444446543) 2) Het <u>nummer niet langer in gebruik was</u>



## Bijlage 2 Verwachtingsprofielen

VERWACHTINGSPROFIEL - BCO		YOURCE®
Onderzoeker		
VERWACHTINGSPROFIEL		
Functietitel	BCO Onderzoeker	
Divisie	Outsourcing	
Subdivisie	Operations	
Functie- & Salarisschaal	Project GGD	
VERWACHTING		
<p>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.</p>		
FUNCTIE-EISEN		
<b>Jij hebt:</b>		
HBO Werk- en denkniveau		
Een service gedreven instelling met daarbij commerciële 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		
<b>Jij bent:</b>		
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 protocollen te werken in de systemen van de GGD		
COMPETENTIES		
	[Redacted]	
	[Redacted]	
	[Redacted]	
	[Redacted]	
	[Redacted]	
	[Redacted]	
	[Redacted]	
	[Redacted]	
	[Redacted]	
	[Redacted]	
	[Redacted]	
	[Redacted]	
	[Redacted]	
	[Redacted]	
	[Redacted]	
	[Redacted]	
	[Redacted]	
	[Redacted]	
	[Redacted]	
	[Redacted]	
	[Redacted]	
	[Redacted]	
	[Redacted]	
	[Redacted]	
	[Redacted]	
	[Redacted]	
	[Redacted]	
	[Redacted]	
	[Redacted]	
	[Redacted]	
	[Redacted]	
	[Redacted]	
	[Redacted]	
	[Redacted]	
	[Redacted]	
	[Redacted]	
	[Redacted]	
	[Redacted]	
	[Redacted]	
	[Redacted]	
	[Redacted]	
	[Redacted]	
	[Redacted]	
	[Redacted]	
FUNCTIETAKEN & VERANTWOORDELIJKHEDEN		
Het verwerken van dossiers van patiënten die besmet zijn met het COVID-19 virus		
Je kunt doormiddel van jouw empathisch 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		
Nauwkeurigheids 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		

<b>VERWACHTINGSPROFIEL - TEAMLEADER</b>		<b>YOURCE<sup>®</sup></b>	
<b>VERWACHTINGSPROFIEL</b>			
Functietitel	BCO Teamleader		
Divisie	Outsourcing		
Subdivisie	Operations		
Functie- & Salarisschaal	GGD Project		
<b>VERWACHTING</b>			
<p>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.</p> <p>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 medewerkttevredenheid het doel is. (Yource cultuur). Een teamleider rapporteert rechtstreeks aan de Projectmanager en Senior Client Manager voor het project GGD</p> <p>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.</p>			
<b>FUNCTIE-EISEN</b>			
<b>Jij hebt:</b>			
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. Uitgebredde 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			
<b>Jij bent:</b>			
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 geanalyseerd, 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 creëren			
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			
<b>COMPETENTIES</b>			
<b>FUNCTIETAKEN &amp; VERANTWOORDELIJKHEDEN</b>			
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 leidinggevend) 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.			
<b>RESULTAATGEBIEDEN</b>			
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 scoringsheet zoals dat bij het BCO in België wordt toegepast. In overleg met GGD kan het scoringsheet worden aangepast.

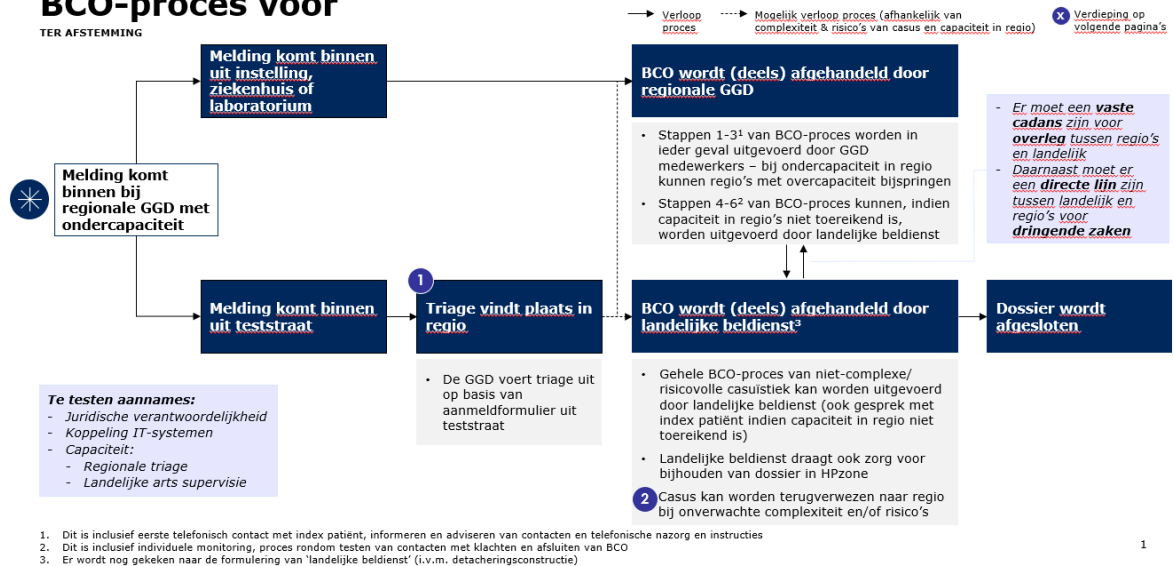
Criteria	Weging	Score 0/1
<b>AANVANG</b>		
Begroeting/intro		
Identificatie van de contactpersoon		
Reden van de oproep		
<b>ANALYSE</b>		
Vragen en doorvragen		
Herformuleren		
Interactie/Dialoog		
Leiding nemen in het gesprek		
<b>ANTWOORD</b>		
Correcte en volledige informatie		
Correct gebruik van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

## Bijlage 4 Kernproces GGD

## De werkgroep stelt de volgende inrichting van het BCO-proces voor



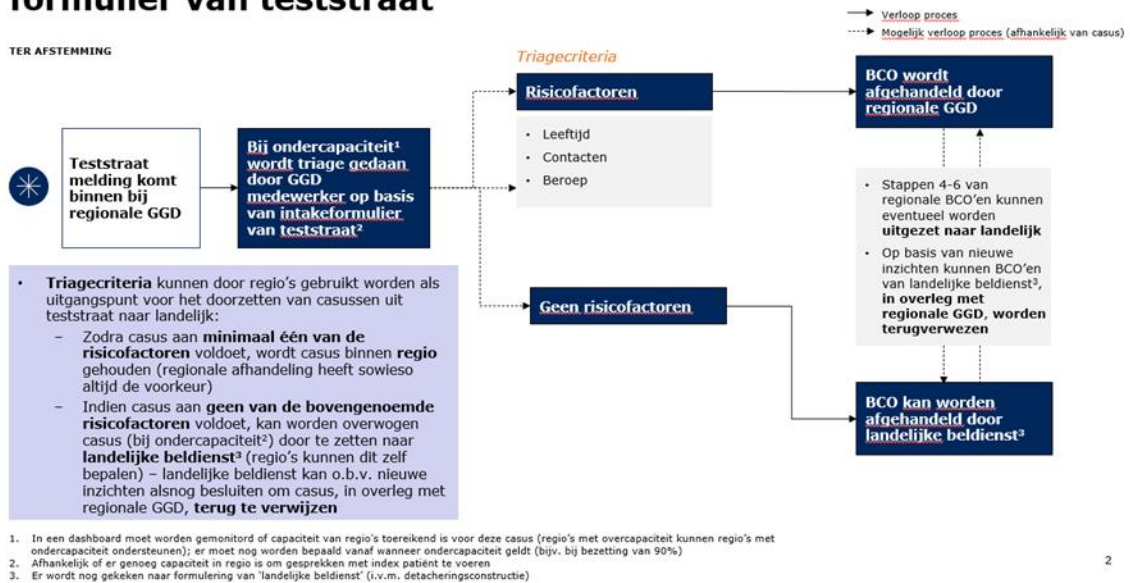
TER AFSTEMMING



## 1 Triage vindt plaats in regio op basis van intakeformulier van teststraat



TER AFSTEMMING



## 2 Landelijke beldienst<sup>1</sup> 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	<ul style="list-style-type: none"> <li>Kwetsbare contacten (70+ en/of onderliggend lijden)</li> <li>Personen die thuiszorg ontvangen</li> </ul>
Risico met beheersing verspreiding	<ul style="list-style-type: none"> <li>Aard en hoeveelheid van contacten<sup>2</sup></li> <li>Meerdere zieke collega's</li> <li>Complexiteit met isoleren index patiënt in woning</li> <li>Specifieke doelgroep (dak/thuis/status-lozen of studenten)</li> <li>Aanwijzingen van weigerende houding index patiënt of contact t.o.v. quarantaine maatregelen</li> </ul>
Overige overwegingen	<ul style="list-style-type: none"> <li>Taalbarrière: Op basis van de specifieke taal moet er gekeken worden of regio of landelijk de beste capaciteiten heeft<sup>3</sup></li> <li>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</li> </ul>

- Tijdens **elke stap** van het BCO-proces kan de landelijke beldienst<sup>1</sup> 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.

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

3

Proces Bron- en contactonderzoek tot en met uitvoeren BCO – 1 juni 2020



## 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		<input type="checkbox"/> Binnen contract <input type="checkbox"/> Buiten contract, zie opm.	
4. Implementatie: A. Kosten (andere kosten dan training) B. Datum	.....  <input type="checkbox"/> in overleg <input type="checkbox"/> anders : <input type="checkbox"/> z.s.m. :	<input type="checkbox"/> Geen implementatiekosten <input type="checkbox"/> Wel implementatiekosten, zie opm.  <input type="checkbox"/> Ja <input type="checkbox"/> Nee, zie opm.	

5. Doorlooptijd change	<input type="checkbox"/> Small Change (implementatie < 2 weken) <input type="checkbox"/> Medium Change (implementatie < 6 weken) <input type="checkbox"/> Large Change (implementatie > 6 weken)	<input type="checkbox"/> Ja <input type="checkbox"/> Nee, zie opm. <input type="checkbox"/> Ja <input type="checkbox"/> Nee, zie opm. <input type="checkbox"/> Ja <input type="checkbox"/> Nee, zie opm.	
6. Volume inschatting	FTE's: ..... Volume: .....minuten Norm: ..... (t.a.v. AHT)	<input type="checkbox"/> Ja <input type="checkbox"/> Nee, zie opm.	
7. Invloed op contactkanaal	<input type="checkbox"/> Schriftelijk/postbus, toelichting zie bijlage <input type="checkbox"/> Telefonie, toelichting zie bijlage <input type="checkbox"/> E-mail, toelichting zie bijlage <input type="checkbox"/> Internet, toelichting zie bijlage <input type="checkbox"/> IVR, toelichting zie bijlage	<input type="checkbox"/> Ja <input type="checkbox"/> Nee, zie opm.	
8. Invloed op andere processen (intern/extern Opdrachtnemer)	<input type="checkbox"/> Frontline: ..... <input type="checkbox"/> Back Office onderdeel: ..... <input type="checkbox"/> Overig: .....	<input type="checkbox"/> Ja <input type="checkbox"/> Nee, zie opm. <input type="checkbox"/> Ja <input type="checkbox"/> Nee, zie opm. <input type="checkbox"/> Ja <input type="checkbox"/> Nee, zie opm.	
9. Wijze van factureren	<input type="checkbox"/> Opnemen in bestaande facturatie <input type="checkbox"/> Aparte factuur (opvragen PO nr. GGD)	<input type="checkbox"/> Ja <input type="checkbox"/> Nee, zie opm. <input type="checkbox"/> Ja <input type="checkbox"/> Nee, zie opm.	
Opmerking 1	.....		
Opmerking 2	.....		
Opmerking 3	.....		
Opmerking 4	.....		
<b>Accordering change</b>			
Akkoord	Namens GGD	Naam: Functie:	Datum:
	Handtekening	.....	

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



Bijlage 6 Offerte West-Brabant: 07 juni 2020



07-juni-2020

**OFFERTE GGD BY  
YOURCE**



1. Uitgangspunten project GGD Yource



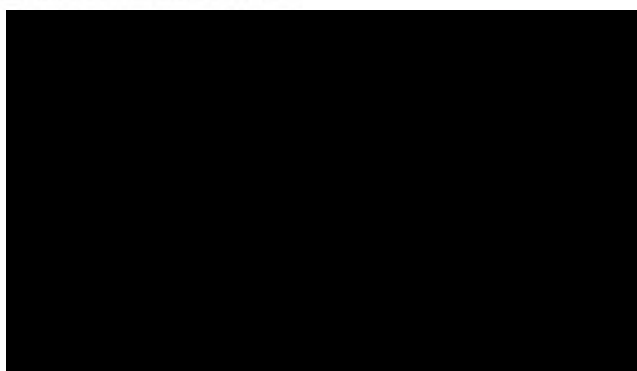
1. Uitgangspunten project GGD Yource (vervolg)



2. Inzet Yource & kwaliteit



Aansturing vanuit Yource



3. Planning



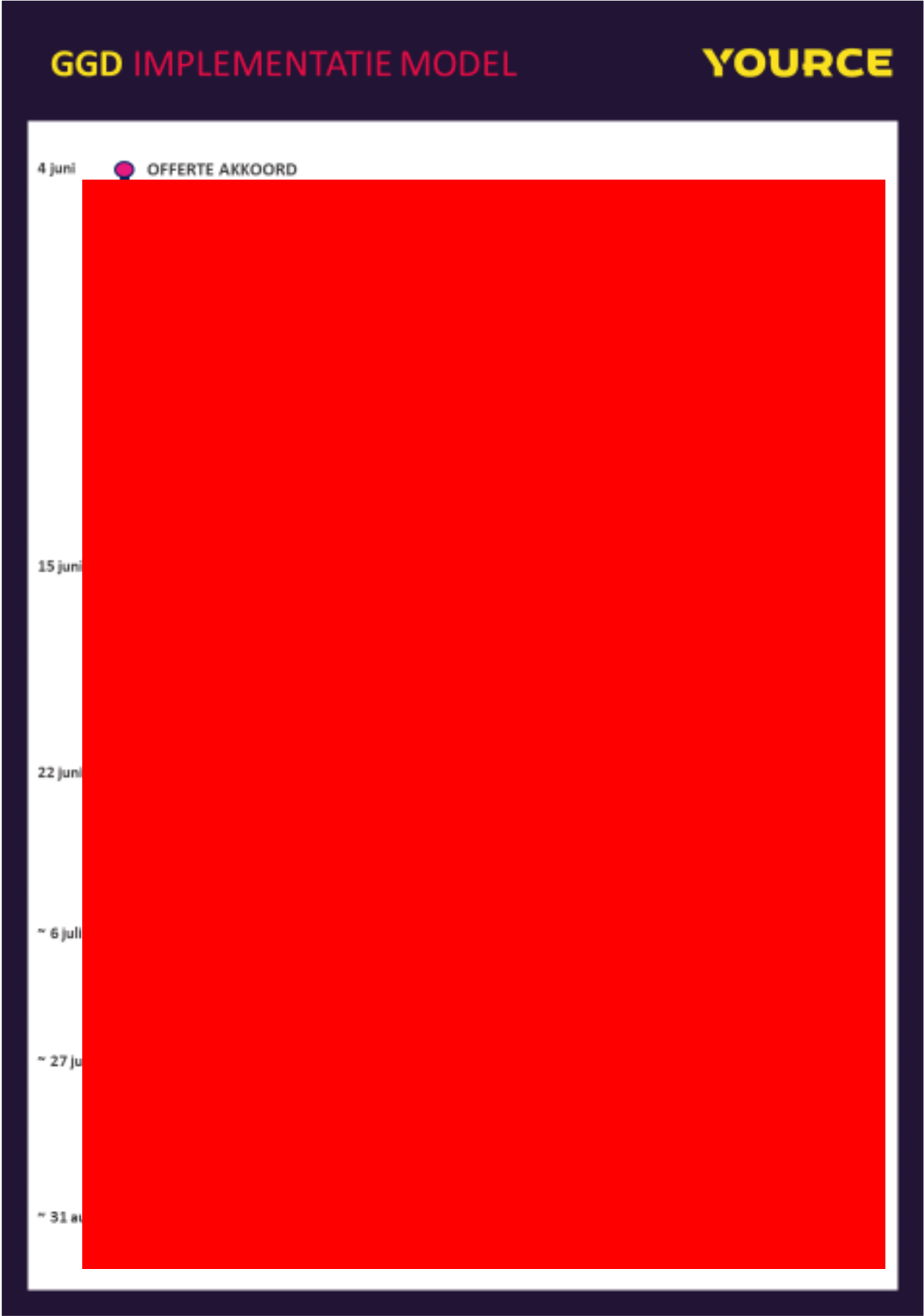
#### 4. Uitgangspunten Offerte Yource



6. Implementatie (kosten)







8. Communicatie & Betrokkenheid (*Involvement Matrix*)



8. Toelichting *Involvement Matrix*





*Truly*  
**YOURCE**

# Referentie DPIA: GGD Contact

23 juni 2021

## Data Protection Impact Assessment (DPIA) GGD Contact ter ondersteuning BCO

- Landelijke referentie DPIA voor GGD'en -

<b>Versiegeschiedenis</b> .....	<b>3</b>
<b>Definities</b> .....	<b>6</b>
<b>Inleiding</b> .....	<b>8</b>
<b>A. Beschrijving kenmerken proces gegevensverwerkingen</b> .....	<b>13</b>
1. Voorstel .....	13
2. Persoonsgegevens .....	13
3. Betrokken partijen en rolverdeling .....	19
4. Gegevensverwerking .....	23
5. Verwerkingsdoeleinden .....	31
6. Belangen bij gegevensverwerking .....	32
7. Verwerkingslocaties.....	34
8. Techniek en methode van gegevensverwerking .....	34
9. Juridisch en beleidsmatig kader .....	36
10. Bewaartermijn .....	37
<b>B. Beoordeling rechtmatigheid gegevensverwerkingen</b> .....	<b>39</b>
11. Rechtsgrond.....	39
12. Doelbinding.....	44
13. Noodzaak en evenredigheid .....	44
14. Rechten van betrokkenen .....	46
<b>C. Beschrijving en beoordeling risico's voor de betrokkenen</b> .....	<b>49</b>
15. Risico's.....	49
<i>Risicocalculatie</i> .....	49
<b>D. Beschrijving voorgenomen maatregelen</b> .....	<b>71</b>
16. Maatregelen .....	71
<b>E. Bijlagen</b> .....	<b>81</b>
Bijlage 1 – Beschrijving Releases.....	82
Bijlage 2 - Procesflow GGD Contact .....	85
Bijlage 3 – Achtergrond risiconiveaus .....	87
Kans.....	87
Impact.....	87
Bijlage 4 – Logging .....	89

## Versiegeschiedenis

Versie	Auteur	Verspreiding bij	Activiteiten
0.1	[REDACTED] [REDACTED] [REDACTED]	<ul style="list-style-type: none"> <li>- [REDACTED] [REDACTED]</li> <li>  [REDACTED] [REDACTED]</li> <li>  [REDACTED] [REDACTED]</li> <li>  [REDACTED] [REDACTED]</li> <li>  [REDACTED] [REDACTED]</li> <li>  [REDACTED] [REDACTED]</li> <li>  [REDACTED] [REDACTED]</li> <li>  [REDACTED] [REDACTED]</li> <li>  [REDACTED] [REDACTED]</li> <li>  [REDACTED] [REDACTED]</li> </ul>	<ul style="list-style-type: none"> <li>- Inzage &amp; advies tussenversie DPIA</li> </ul>
0.2	[REDACTED] [REDACTED]	<ul style="list-style-type: none"> <li>- FG GGD GHOR Nederland</li> </ul>	<ul style="list-style-type: none"> <li>- FG advies opvragen</li> </ul>
0.3	[REDACTED] [REDACTED]	<ul style="list-style-type: none"> <li>- [REDACTED] [REDACTED]</li> </ul>	<ul style="list-style-type: none"> <li>- Aanpassingen naar aanleiding FG advies &amp; review</li> </ul>
0.4	[REDACTED] [REDACTED]	<ul style="list-style-type: none"> <li>- [REDACTED] [REDACTED]</li> <li>  [REDACTED] [REDACTED]</li> <li>  [REDACTED] [REDACTED]</li> <li>  [REDACTED] [REDACTED]</li> <li>  [REDACTED] [REDACTED]</li> <li>  [REDACTED] [REDACTED]</li> <li>  [REDACTED] [REDACTED]</li> </ul>	<ul style="list-style-type: none"> <li>- Delen concept versie DPIA ter review VWS</li> </ul>

Versie	Auteur	Verspreiding bij	Activiteiten
		- ██████████	
0.5	██████████ ██	- ██████████ ██████    ██████████ ██████	- Review DPIA (op hoofdpijnen)
0.6	██████████ ██	- ██████████ ██████    ██████████ ██████	- Tekstvoorstel betrokken partijen en rolverdeling
0.7	██████████ ██	- ██████████ ██████    ██████████ ██████	- Tekstvoorstel Telecommunicatiewet
1.0	██████████ ██	- ██████████ ██████    ██████████ ██████    ██████████ ██████    ██████████ ██████    ██████████ ██████    ██████████ ██████    ██████████ ██████    ██████████ ██████    ██████████ ██████    ██████████ ██████    ██████████ ██████    ██████████ ██████    ██████████ ██████	- Definitieve versie referentie DPIA  - FG advies opvragen praktijkregio's + FG GGD GHOR Nederland



<b>Versie</b>	<b>Auteur</b>	<b>Verspreiding bij</b>	<b>Activiteiten</b>
		<ul style="list-style-type: none"> <li>- ██████████ ██████████</li> <li>█ ████████████████████</li> <li>█ ████████████████████ ██████████</li> </ul>	
<b>1.1</b>	██████████ █		Aanpassingen naar aanleiding van FG Advies, begeleidingscommissie advies en FG advies GGD'en
<b>1.1.1</b>	██████████ █	<ul style="list-style-type: none"> <li>- ████████████████████</li> </ul>	Samenvoeging referentie DPIA 1.0 met Addenda: ZelfBCO, BCO Vragenlijst + Osiris Vragenlijst, Evaluatie GGD Contact
<b>1.1.2</b>	██████████ █ ██████████	<ul style="list-style-type: none"> <li>- ████████████████████ ████████████████████</li> <li>- 25 FG's v.d. 25 GGD'en</li> </ul>	<p>Wijziging naar scope 'Release 1.1'</p> <p>Review ten behoeve van FG-advies</p>
<b>1.1.3</b>	██████████ █ ██████████	<ul style="list-style-type: none"> <li>- Stuurgroep GGD Contact</li> </ul>	Aanpassingen naar aanleiding van feedback FG's GGD'en, GGD GHOR, leden stuurgroep en EY

## 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 werkverdelers (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	Gemeentelijke gezondheidsdienst
GGD Contact	Het deel van het BCO-proces dat gebruik maakt van de functionaliteiten binnen GGD Contact, dit bevat de verwerkingen binnen de GGD Contact 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 ZelfBCO.
GGD GHOR	GGD GHOR Nederland
VWS	Ministerie van Volksgezondheid, Welzijn en Sport

## **Inleiding**

Ten behoeve van infectieziektebestrijding hebben GGD'en op basis van Wet publieke gezondheid (hierna: Wpg) de taak gekregen om BCO uit te voeren.<sup>1</sup> 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 gebruikmaken van een BCO-ondersteunende applicatie 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 referentiedocument 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. De Autoriteit Persoonsgegevens heeft een lijst gepubliceerd van soorten verwerkingen waarvoor een DPIA als bedoeld in artikel 35 van de AVG verplicht is.<sup>2</sup> In deze lijst wordt gesteld dat voor grootschalige verwerkingen van gezondheidsgegevens een DPIA dient te worden uitgevoerd. Hoewel in de GGD Contact App 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 daarmee bijzondere persoonsgegevens.<sup>3</sup> Het doel en noodzaak van GGD Contact impliceert grootschalige gegevensverwerking, nu het potentieel gaat om 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 februari 2020 heeft Nederland te maken met geregistreerde besmettingen 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

---

<sup>1</sup> Artikel 6 lid 1 sub c Wpg.

<sup>2</sup> <https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/stcrt-2019-64418.pdf>

<sup>3</sup> Artikel 9 lid 1 AVG en de daarop van toepassing zijnde overweging 35 AVG.

hiervoor kunnen zijn. Sinds september 2020 is gestart met GGD Contact. 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 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 en is GGD GHOR gevraagd de vervanging landelijk te coördineren.<sup>4</sup> Op 12 februari 2021 heeft de DPG-raad besloten om HPZone Lite te vervangen en daar op korte termijn mee te starten. Het gekozen scenario voor de start van de vervanging op korte termijn en de functionaliteiten die de eerste stap daartoe bevat wordt aangemerkt als release 1.1. De keuze en afweging voor GGD Contact is op 1 april 2021 vastgelegd in de doorlopende besluitenlijst van de DPG'en, onder verwijzing naar oplegnotitie DPG20210401.03.

## Scope

Met GGD Contact kan de GGD sneller en met minder fouten relevante contactgegevens verzamelen die nodig zijn voor BCO. Dit gebeurt doordat de index via de GGD Contact App de contactgegevens van de personen met wie hij in aanraking is gekomen en het type contact dat heeft plaatsgevonden 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 GGD Contact App met daarin ZelfBCO door de index. De index selecteert in de GGD Contact App welke corona-gerelateerde klachten hij had/heeft en op welke dag deze klachten zijn begonnen. Met de GGD Contact App kan de index de contactgegevens verzamelen van de contacten waarmee hij in aanraking is geweest.
- De sluis, betreffende een API<sup>5</sup> tussen GGD Contact en BCO Portaal waarmee de BCO-medewerker gaat werken.<sup>6</sup>
- BCO Portaal 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 of de index zelf met de betreffende contacten. Met behulp van GGD Contact kan beter het juiste advies voor de juiste contacten worden

---

<sup>4</sup> Stand van zakenbrief digitale ondersteuning pandemiebestrijding 12 februari 2021

<sup>5</sup> Application Programming Interface waardoor GGD Contact met het BCO Portaal kan communiceren.

<sup>6</sup> De sluis kan worden gezien als een doorgeefluik waar de gegevens tijdelijk staan opgeslagen totdat deze vanuit GGD Contact aan het BCO Portaal worden doorgegeven.

gegeven. 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.

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 over contacten van de index is niet meer nodig vanwege BCO Portaal dat voor GGD Contact App is ontwikkeld en eraan gekoppeld kan worden.
- In de beoogde toekomstige releases worden ook die functionaliteiten aan BCO Portaal toegevoegd die nodig zijn om BCO Portaal als bronsysteem te laten functioneren en het systeem dat nu gebruikt wordt voor het Covid-19 BCO Proces (HPZone lite) niet langer gebruikt hoeft te worden.
- 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. De vragenlijst in het BCO Portaal kent standaard antwoordopties voor het vastleggen van het BCO-gesprek. Dit verhoogt de snelheid, uniformiteit van data en daarmee datakwaliteit. 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;
- De inzet van de landelijke capaciteit (ook wel 'Landelijke Partners' genoemd) en het gebruik van de landelijke capaciteit van GGD Contact.
- Het proces rondom het informeren van de contacten vanuit GGD contact (mail, sms etc.);
- De verwerking van persoonsgegevens in en naar HPZone Lite van infectieziekten van de GGD, HPZone, HPZone Lite;
- In het BCO Portaal is de volledige BCO-vragenlijst opgenomen en tevens de Osirisvragenlijst. In deze fase van de DPIA is geen privacy-analyse gedaan op de noodzakelijkheid van de vragen in deze lijsten.

### **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 ontwikkeld. 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 VWS-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. Deze release is uitgerold onder de praktijktestregio's. Praktijktestregio's zijn GGD'en die met GGD Contact als pilot zijn gestart.

#### **Release 1.1 Release voorbereidend op vervanging HPZone Lite (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) vragenlijst versie 8.
- Gestandaardiseerde zoekfunctie locaties/contexten (epic-naam: Contexten).
- Beknopte vragenlijst huisgenoten en nauwe contacten (epic-naam: Volledige vragenlijst inclusief contacten).
- GGD Contact App met ZelfBCO 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 GGD Contact omgeving ligt bij het ontwikkelteam van VWS (Programma Realisatie Digitale Ondersteuning Covid-19) en blijft daar voorlopig liggen.
- Hosting GGD Contact omgeving door Intermax onder aansturing van VWS.
- Applicatie en Functioneel beheer GGD Contact ligt tot nader order bij VWS.
- Change Management is een verantwoordelijkheid VWS: wijzigingsverzoeken komen via de product owner en volgt het DevOps proces.

Op termijn zal het volledige beheer van de GGD Contact App worden toegewezen door de GGD'en aan een andere partij.

- GGD GHOR richt de Service Desk in (alleen voor informatie en incidenten).
- Incident Management (met inbegrip van monitoring) is verantwoordelijkheid GGD GHOR.  
VWS



## **A. Beschrijving kenmerken proces gegevensverwerkingen**

### **1. Voorstel**

Het voorstel voor deze DPIA betreft de gegevensverwerkingen die plaatsvinden in:

- De GGD Contact App 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 besmettelijke periode te bepalen en hun contacten aan te leveren aan de GGD. De GGD Contact App is ook te gebruiken door een index wanneer de GGD van zijn regio de App nog niet gebruikt voor doorgeven van informatie vanuit het ZelfBCO.
- Het BCO Portaal van GGD Contact is bedoeld voor de BCO-medewerker. Hierin zet de BCO-medewerker een en ander klaar voor de index zodat deze in GGD Contact eenvoudig zijn contacten kan aanvullen 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 zijn de BCO -vragenlijst en Osiris-vragenlijst in zijn geheel opgenomen. Voor de totstandkoming van die vragenlijsten is een aparte procedure binnen de GGD'en uitgewerkt. Dit is geen onderdeel van deze DPIA
- De sluis tussen GGD Contact en het BCO Portaal. De sluis kan worden gezien als een doorgeefluik waar de gegevens tijdelijk staan opgeslagen totdat deze vanuit GGD Contact aan het BCO Portaal 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 de GGD Contact App, de sluis en het BCO Portaal van de BCO-medewerker worden onderstaande persoonsgegevens verwerkt. De velden die de index in de GGD Contact App kan invullen zijn optioneel.

Er bestaat voor de index 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 GGD Contact App aan de index om nog eens te kijken of voor die contacten er contactgegevens beschikbaar zijn. Uitgangspunt bij de ontwikkeling van de GGD Contact 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 of bijzondere) het gaat. Hoewel in de applicatie geen sprake is van opname van informatie over het ziektebeeld en het welbevinden van de index (anders dan de start van de besmettelijke periode van de index) of diens contacten, zegt de opname van de persoonsgegevens in de GGD Contact App 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.<sup>7</sup>

Hieronder wordt nader ingegaan op de noodzaak van het opvragen van deze persoonsgegevens.

<b>Persoonsgegeven</b>	<b>Gewoon persoonsgegeven</b>	<b>Bijzonder persoonsgegeven</b>	<b>Index en/of contact</b>	<b>Toelichting noodzaak</b>
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

<sup>7</sup> Artikel 9 lid 1 AVG en de daarop van toepassing zijnde overweging 35 AVG.

Risicoclassificatie <sup>8</sup>	Ja	Ja, zie toelichting hierboven.	Contact	B
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
Start besmettelijke periode	Ja	Ja, zie toelichting hierboven.	Index	G
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 **om contact op te kunnen nemen met het contact van de index**, waaronder vragen over voornaam, achternaam, telefoonnummer en e-mailadres.
- B. Instelbare vragen<sup>9</sup> **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

<sup>8</sup> 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 Portaal opgeslagen en niet meer naar GGD Contact gestuurd.

<sup>9</sup> De wijze van het beoordelen van de risicoclassificatie berust op de LCI-richtlijn bron- en contactonderzoek: <https://whimsical.com/8SzFoAMZD5AC14b8g6uLN6>

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. 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 GGD Contact bij het aangeven of de index mogelijk al een contact heeft geïnformeerd. De index kan in de GGD Contact App aangegeven of hij het contact zelf al heeft geïnformeerd.
- D. 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 en op welke datum(s) geadviseerd wordt een coronatest te doen. 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.
- E. 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 eerste besmettelijke dag. 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. Deze informatie is optioneel, de BCO-medewerker is niet verplicht om deze context in te vullen.

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 Portaal 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 Portaal wordt gebruikt. De plek waar de taak ontstaat, dit kan het BCO Portaal 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 BCO Portaal 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 Portaal:

- 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)

### **ZelfBCO door de Index**

Wanneer de index door middel van ZelfBCO in de GGD Contact 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 begin van de besmettelijke periode en kan dat worden ingevuld.

Wanneer de index de eerste ziektedag niet wil invullen kan je de GGD Contact 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 GGD Contact App naar BCO Portaal geldt: de te verwerken gegevens in functionaliteit ZelfBCO 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 een DPIA op 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 Osiris 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 op zichzelf niet direct 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 meldingsplicht van SARS-CoV-2 infecties, verstrekt door de GGD'en aan het RIVM (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 Osiris-vragenlijst moet in de DPIA van het reguliere BCO-proces worden onderbouwd. Voor de 'Referentie DPIA GGD Contact' is deze buiten scope van deze DPIA.

### **Gegevens BCO-medewerkers**

Naast gegevens van de index en contacten, worden in BCO Portaal ook gegevens verwerkt van medewerkers die van het systeem gebruikt maken. Deze verwerking bestaat uit het opslaan van de de user name waarmee de gebruiker is ingelogd en de vastlegging van het gebruik van de applicatie in de logging van de applicatie. Een nadere toelichting op de logging is opgenomen in bijlage 4.

### **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.

#### *GGD'en*

Op grond van artikel 6, eerste lid, onderdeel c, Wpg jo. artikel 14 Wpg heeft de GGD de wettelijke taak om BCO uit te voeren.

Naar aanleiding van de druk op 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 GGD Contact (GGD Contact App en BCO Portaal) te ontwikkelen en kan worden gebruikt ter ondersteuning van de BCO. Daarbij wordt benadrukt dat GGD Contact zich niet beperkt tot BCO in het kader van COVID-19.

De opdracht tot het doen ontwikkelen van GGD Contact past dan ook in de wettelijke taak van de GGD'en.

De verwerking van persoonsgegevens in GGD Contact gebeurt daarom 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 is VWS met name stelselverantwoordelijk voor de inrichting en ontwikkeling van GGD Contact, en het informeren van de gebruikers over de werking van de GGD Contact App. Daarbij is VWS ook verantwoordelijk voor de (tijdelijke) hosting van GGD Contact.

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. De uitwerking daarvan is vastgelegd in een nieuwe governancestructuur.

Voor zover persoonsgegevens worden verwerkt bij de ontwikkeling van de GGD Contact 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). De verwachting is dat na het opleveren van de GGD Contact App de verwerking van persoonsgegevens niet meer noodzakelijk is voor het realiseren van de GGD Contact App en het BCO Portaal.

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 en het BCO Portaal, 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 en de aansluiting van het BCO Portaal daarop.

#### *Conclusie*

Om die reden moeten de GGD'en en de minister van VWS worden aangemerkt als gezamenlijk verwerkingsverantwoordelijk voor zover tijdens de ontwikkeling van GGD Contact 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 en het BCO Portaal, verliest de minister van VWS de zeggenschap over de verwerking die hij had tijdens de ontwikkelingsfase.

De minister van VWS oefent tijdens de praktijkfase dan ook geen zeggenschap uit over het gebruik van het middel, de GGD Contact App en het BCO Portaal, waarmee persoonsgegevens worden verwerkt. De GGD'en behouden daarentegen wel zeggenschap over de werking en inrichting van de GGD Contact App en BCO Portaal 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 BCO Portaal, en het bepalen van het doel van de verwerking van (bijzondere) persoonsgegevens aan de hand van de GGD Contact App en BCO Portaal, 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 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 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.

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.

#### *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 van de GGD Contact. 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 en BCO Portaal.

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 BCO Portaal, de uitvoering van een deel van het beheer (incident management) 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 BCO Portaal, en (het beheren van) HPzone voortduurt, en daarbij door GGD GHOR Nederland (bijzondere) persoonsgegevens worden verwerkt, o.a. ten aanzien van het incident management, 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 Portaal worden gehost bij Intermax. Intermax wordt door VWS ingeschakeld.

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.

#### *NFIR – verwerker*

NFIR is leverancier van het dashboard dat gebruikt wordt voor de monitoring van de logging en heeft hiermee de rol van verwerker. Daarnaast ondersteunt NFIR als subverwerker Intermax bij incidenten en analyses.

#### *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.<sup>10</sup> 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.

---

<sup>10</sup> Artikel 2 AVG.

### *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 Portaal 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.

### *GGD Contact App Gebruiker - geen belanghebbende*

Voor het verwerken van persoonsgegevens in GGD Contact App voordat deze gedeeld worden met de GGD geldt dat de AVG niet van toepassing is nu deze persoonsgegevens worden verwerkt voor huishoudelijk gebruik.

### *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. De AVG verplicht om passende technische en organisatorische maatregelen te nemen ter bescherming van de persoonsgegevens. De persoonsgegevens in de logging 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 via het volgende scherm en via de privacyverklaring BCO Portaal (zie hieronder het bijbehorende scherm).

#### **Dit moet je weten voor je begint:**

- BCO Portaal bevat medische en gevoelige informatie.
- Alles wat je doet in het portaal wordt vastgelegd.
- Jij als gebruiker gaat zorgvuldig om met alle informatie in het portaal.

Wil je meer weten? Lees de [privacyverklaring](#).

Ik heb bovenstaande gelezen en ben klaar om BCO Portaal te gebruiken

Doorgaan

## **4. Gegevensverwerking**

Het gebruik van GGD Contact doorloopt de volgende processen, gebaseerd op de procesflow (**Bijlage 2**):

Stap	Uitwerking
------	------------

<b>1</b>	<b>Verificatie identiteit index</b>
	Het BCO is aan de orde vanaf het moment dat er een melding van infectieziekte is gedaan. <sup>11</sup> Het BCO-proces begint bij de BCO-medewerker die telefonisch contact opneemt met de index. <sup>12</sup>
<b>2</b>	<b>Verzoek om GGD Contact App te downloaden</b>
	<p>Ten tijde van het telefonisch contact met de index vraagt de BCO-medewerker aan de index of hij bereid is om GGD Contact App te downloaden.</p> <p>a) Indien de index ervoor kiest GGD Contact <u>niet</u> 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.</p> <p>b) Indien de index ervoor kiest om GGD Contact <u>wel</u> te downloaden, dan volgt stap 3.</p> <p>De index kan ook op eigen initiatief de GGD Contact App reeds hebben gedownload vóór het telefonisch contact met de BCO-medewerker.</p>
<b>3</b>	<b>Index downloadt GGD Contact App</b>
	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. <sup>13</sup>
<b>4</b>	<b>Privacyverklaring wordt getoond</b>
	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-

<sup>11</sup> Het doen van deze melding na vaststelling van een ziekte als COVID-19 is bij wet verplicht, artikel 22 Wpg.

<sup>12</sup> Hierbij wordt de identiteit van de index geverifieerd. Dit gebeurt door middel van naam, geboortedatum en telefoonnummer.

<sup>13</sup> 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.

	medewerkers is opgenomen te benadrukken dat het gebruik van GGD Contact vrijwillig is.
<b>5</b>	<b>ZelfBCO door de index</b>
	<ul style="list-style-type: none"> <li>• Indien de index op eigen initiatief de App heeft gedownload start het gebruik van de app met het ZelfBCO.</li> <li>• 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.</li> <li>• Indien er geen klachten zijn, voert de index de testdatum in.</li> <li>• 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 <u>niet</u> opnieuw in de GGD Contact App gesteld.</li> <li>• ZelfBCO is ook te doorlopen indien de GGD van de betreffende index 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.</li> </ul>
<b>6</b>	<b>BCO-medewerker vult contactenlijst in het BCO Portaal</b>
	<p>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 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.</p> <p>De BCO-medewerker maakt een nieuwe case aan indien de index niet reeds bekend is en noteert:</p> <ul style="list-style-type: none"> <li>• Naam index</li> <li>• Telefoonnummer index</li> <li>• Casenummer</li> </ul> <p>De BCO-medewerker maakt een eerste aanzet voor de contactenlijst van de index en noteert:</p>

	<ul style="list-style-type: none"> <li>• Laatste contactdatum</li> <li>• Context</li> <li>• Risicocategorie</li> </ul> <p>Op de achtergrond wordt aan deze gegevens de technische velden 'bron' en 'type' gekoppeld. Dit is niet zichtbaar voor de BCO-medewerker.</p> <p>Indien de index door middel van zelfBCO zelf de besmettelijke periode heeft bepaald, kan de BCO-medewerker in het telefoongesprek de informatie verifiëren en eventueel aanpassen.</p>
<b>7</b>	<b>BCO-medewerker registreert BCO-vragenlijst + Osiris Vragenlijst</b>
	<p>Separaat aan het registreren 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 afkomstig zijn uit de Osiris-vragenlijst.</p> <p>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.</p>
<b>8</b>	<b>Activatiecode wordt verstrekt</b>
	<p>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 de GGD Contact App.</p> <p>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 GGD Contact App te downloaden en te activeren.</p>
<b>9</b>	<b>Invoer activatiecode door index</b>
	Tijdens of na het telefoongesprek kan de index de door de BCO-medewerker verstrekte activatiecode in de GGD Contact App invullen.
<b>10</b>	<b>Verificatie van de activatiecode</b>

	Er vindt een verificatie van de activatiecode plaats tussen de GGD Contact App en de backend.
<b>11</b>	<b>Contactenlijst wordt vanuit de backend opgehaald</b>
	De vooraf opgestelde contactenlijst wordt tijdens het telefoongesprek van de BCO-medewerker met de index vanuit de backend naar GGD Contact App opgehaald.
<b>12</b>	<b>Ophalen contactenlijst door de index</b>
	Wanneer de index aangeeft dat hij de privacyverklaring 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 de GGD Contact App geïmporteerd.
<b>13</b>	<b>Toestemming voor toegang tot contacten</b>
	<p>De index krijgt in de GGD Contact App een pop-up scherm waarin 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." waarin 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."</p> <p>a) Wanneer de index toestemming geeft voor het ophalen van de contacten uit het adresboek van zijn telefoon, worden alleen die namen uit de telefoon uitgelezen om een match te maken in de GGD Contact App.</p> <p>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 de GGD Contact App.</p> <p>Bij het ophalen van de contactgegevens uit het adresboek van de telefoon worden alleen de namen van de contactpersonen zichtbaar in de GGD Contact App. De app leest niet de hele contactenlijst van de telefoon van de index uit. 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.</p>
<b>14</b>	<b>Aanvulling contacten door de index</b>
	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

	<p>importeren van de contactenlijst uit het adresboek van de telefoon van de index, stelt de GGD Contact App 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 'Piet K' wordt gekoppeld aan de relatie 'Piet Klaas' uit de telefoon).</p> <p>De index wordt gevraagd om de volgende gegevens in te vullen in de GGD Contact App:</p> <ul style="list-style-type: none"> <li>• Contactgegevens van het contact van de index</li> <li>• 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 (exacte vragen zijn aan verandering onderhevig door de geldende LCI-richtlijn): <ul style="list-style-type: none"> <li>○ langer dan 12 uur op dezelfde plek als het contact geweest (Ja/Nee)</li> <li>○ langer dan 15 minuten in dezelfde ruimte als het contact geweest (Ja/Nee)</li> <li>○ dichterbij dan 1,5 meter bij het contact geweest (Ja/Nee) <i>Hierbij maakt het niet uit of het een kort of langdurig moment is geweest waarbij je dichterbij dan 1,5 meter bij het contact bent geweest.</i> <sup>14</sup></li> </ul> </li> </ul>
<b>15</b>	<b>Aanlevering nieuwe contacten door index</b>
	<p>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 manieren namelijk: ophalen uit het adresboek van de telefoon van de index of handmatig invoeren.</p>
<b>16</b>	<b>Risico-inschatting 'soort contact' door index</b>
	<p>Wanneer de index een nieuw contact invoert in de GGD Contact App, 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/handelingsopties voor deze contactpersoon verschijnt.</p> <p>De risico-inschatting vindt plaats door het stellen van onderstaande vragen aan de index, welke hij in GGD Contact beantwoordt:</p> <ol style="list-style-type: none"> <li>1. Woon je in hetzelfde huis of ben je langer dan 1 uur op dezelfde plek geweest? (Ja/Nee).</li> </ol>

<sup>14</sup> Deze indicatie wordt aangepast aan de hand van de geldende LCI-richtlijn.



	<p>2. Hoe lang waren jullie waarschijnlijk bij elkaar in de buurt? Langer dan 15 minuten/korter dan 15 minuten.</p> <p>a. Bij het antwoord "kortere dan 15 minuten" krijgt de index de vervolgvraag, namelijk: Is een of meerdere van deze dingen tijdens jullie ontmoeten gebeurd?</p> <ul style="list-style-type: none"> <li>- In je gezicht geniesd</li> <li>- Geknuffeld of gezoend</li> <li>- Ander lichamelijk contact</li> </ul> <p>Het antwoord kan zijn: Ja, één of meerdere dingen/Nee, denk het niet.</p> <p>3. Zijn jullie binnen 1,5 meter van elkaar geweest? Het antwoord kan zijn: Ja, denk het wel/Nee, denk het niet.</p> <p>Wanneer was de laatste ontmoeting?</p>
<b>17</b>	<b>Verschijnen van leefregels/handelingperspectief</b>
	<p>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 quarantaine te verblijven. De leefregels/handelingperspectief zijn/is afhankelijk van risicoclassificatie (het soort contact) en de datum van het laatste contact met de index. Zie het protocol van het RIVM<sup>15</sup> voor het handelingsperspectief per risicoclassificatie (huisgenoot/nauw contact/overig contact).</p>
<b>18</b>	<b>Delen van de/het leefregels/handelingperspectief door index</b>
	<p>Wanneer de leefregels in de GGD Contact App 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.</p>
<b>19</b>	<b>Controle vraag voor het informeren van het contact</b>
	<p>Wanneer de index het contact heeft toegevoegd en de leefregels heeft ingezien en vervolgens een nieuw contact wil toevoegen, stelt GGD Contact eerst een controle vraag, namelijk: "Heb jij het contact geïnformeerd en de leefregels gedeeld?". Hierop kan de index antwoorden:</p> <ul style="list-style-type: none"> <li>- Ja;</li> </ul>

<sup>15</sup> <https://lci.rivm.nl/COVID-19-bco>

	<ul style="list-style-type: none"> <li>- Nee, doe ik later;</li> <li>- Nee.</li> </ul> <p>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 (nog) niet heeft gedaan.</p>
<b>20</b>	<b>Opslag gegevens in de sluis</b>
	<p>De sluis is een API tussen de GGD Contact App en het BCO Portaal. Het brengt communicatie tussen de GGD Contact App 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.</p> <p>De sluis zorgt voor de koppeling tussen het device van de index en het BCO Portaal van de BCO-medewerker.</p> <p>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 de GGD Contact App 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.</p>
<b>21</b>	<b>Verzending contactenlijst naar BCO Portaal</b>
	<p>Nadat de index de contactenlijst heeft ingevuld, kan hij op de 'ik ben klaar'-button/'verstuur gegevens naar GGD' drukken. Voor de index is deze stap tekstueel en visueel duidelijk gemaakt. De ingevulde contactenlijst wordt na het aanklikken van de 'verstuur'-knop 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.</p> <p>Bij het niet (volledig) invullen van de velden in de GGD Contact App, 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.</p>
<b>22</b>	<b>Verdeling casenummers onder BCO-medewerkers door werkverdeler</b>
	<p>De werkverdeler van de GGD verdeelt de ontvangen contactenlijsten op basis van een casenummer onder de BCO-medewerkers.</p>
<b>23</b>	<b>BCO-medewerker beoordeelt risicoclassificatie</b>
	<p>Bij handmatige invoer van contacten door de index, checkt de BCO-medewerker of de risicoclassificatie juist is ingevuld.</p>

<b>24</b>	<b>BCO-medewerker kan contact opnemen met contact van index</b>
	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.
<b>25</b>	<b>Nieuwe gegevensaanlevering door index</b>
	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 besmettelijke periode. 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 door de index en het BCO Portaal van de BCO-medewerker.
<b>26</b>	<b>(Handmatige) koppeling gegevens aan HPZone Lite GGD</b>
	De gegevens worden door de BCO-medewerker vanuit het BCO Portaal handmatig gekopieerd naar HPZone (Lite) van de GGD. Voor de toekomstige versies van de GGD Contact App en het BCO Portaal 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 Portaal in HPZone worden gezet. Zoals eerder aangegeven ziet deze DPIA op het gebruik van de GGD Contact App en het BCO Portaal 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. De app GGD Contact (met de bijbehorende sluis en het portaal) 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 Portaal te verzenden.
- BCO Portaal is bedoeld om BCO-medewerkers bij hun werkzaamheden te ondersteunen, onder andere bij het doorlopen van vragenlijsten en het opstellen van contactenlijsten ten behoeve van 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 de GGD Contact App, sluis en BCO Portaal) neemt daarnaast de kwaliteit van BCO toe, doordat het digitaal aanleveren van contactgegevens vanuit de GGD Contact App 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 maatschappelijk belang 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.

### *Ministerie van VWS*

Op basis van diverse internationale regels heeft eenieder het recht op bescherming van de gezondheid.<sup>16</sup> 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 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.<sup>17</sup>

In Nederland heeft deze wettelijke verplichting uitwerking gevonden in de Wet publieke gezondheid (Wpg). 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.<sup>18</sup> 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.

### *Index*

Deelname aan de BCO is voor de index vrijwillig. Het is daarbij van belang dat het doorlopen van het BCO-proces volgens de juiste manier verloopt en in het BCO-gesprek de juiste vragen aan bod komen, wat gefaciliteerd wordt in het BCO Portaal. Door de aanlevering van gegevens via de GGD Contact App kan een contact van de index snel en met de juiste instructies op de hoogte worden gebracht dat het contact in de buurt is geweest van een persoon met een positieve test.

### *Contactpersonen index*

Door de aanlevering van gegevens via de GGD Contact App 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.<sup>19</sup> 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

---

<sup>16</sup> 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.

<sup>17</sup> Artikel 12 lid 1 sub c IVESCR.

<sup>18</sup> Artikel 7 lid 1 Wpg.

<sup>19</sup> Artikel 6 lid 1 sub c Wpg.

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.<sup>20</sup>

#### *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".<sup>21</sup> Met betrekking tot het BCO-proces draagt GGD GHOR Nederland bij aan het mede-coördineren van BCO op landelijke schaal met als hoger gelegen 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 Portaal) 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 Portaal 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 BCO Portaal Gebruiker de autorisatie daartoe heeft verkregen via de GGD waarvoor de BCO Portaal Gebruiker werkzaam is. Het portaal is benaderbaar via een weblink, niet op het publieke internet. De BCO Portaal Gebruiker moet met behulp van de geldende beveiligingsmaatregelen zijn ingelogd. 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:

---

<sup>20</sup> De uitvoering van algemene infectieziektebestrijding is wederom een taak van de GGD, artikel 6 lid 1 Wpg jo artikel 14 Wpg.

<sup>21</sup> Artikel 2 Statuten GGD GHOR Nederland.

- Werkverdelers
- 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.<sup>22</sup> Door middel van een menselijk component, namelijk de BCO-medewerker die de antwoorden afkomstig uit de vragen gebaseerd op de beslisboom in het BCO Portaal 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 plaatsgevonden, 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.

---

<sup>22</sup> Overweging 91 AVG.

## **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 is zodanig ingericht dat aan de voorgaande vereisten is voldaan. Bij het eerste gebruik van de GGD Contact App op de smartphone van de gebruiker wordt de gebruiker geïnformeerd over het plaatsen van de app op de telefoon en het uitlezen van de betreffende gegevens daaruit en moet daarvoor toestemming worden gegeven. Dit zie er als volgt uit:





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. De vrijwilligheid van het gebruik van de GGD Contact App is ook onderdeel van de werkinstructie van de BCO-medewerker. In de e-learning die hiervoor gebruikt wordt, is uitgebreid aandacht voor de vrijwilligheid van het gebruik van de GGD Contact App.

## 10. Bewaartermijn

Ten aanzien van de bewaartermijn van de persoonsgegevens binnen GGD Contact, dient onderscheid te worden gemaakt tussen de gegevens die in de app, de sluis en het BCO Portaal worden opgeslagen.

### Bewaartermijn GGD Contact App

In de GGD Contact App worden de gegevens gewist twee weken na de laatste aanpassing of het delen met de GGD. 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 Portaal voor BCO-onderzoek.
- de index die gebruik maakt van de GGD Contact 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 BCO Portaal 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 Portaal

In BCO Portaal worden de volgende bewaartermijnen gehanteerd:

- Dossier index: 5 jaar na de datum waarop het dossier is aangemaakt.
- Dossier contact: 28 dagen, met aansluitend opslag in gepseudonimiseerde vorm tot 5 jaar na de datum waarop het dossier is aangemaakt.
- Applicatielogging: 5 jaar na de datum waarop de handeling is verricht.

Betreffende gegevens zullen na afloop van deze termijnen automatisch worden verwijderd.

Een contactdossier wordt na de eerste 28 dagen in gepseudonimiseerde vorm bewaard vanwege epidemiologische doeleinden. Gedurende deze periode is het dossier voor medewerkers niet meer direct tot een individu te herleiden. De bewaartermijn van de applicatielogging volgt de termijn van het dossier.

Onderstaand overzicht geeft een overzicht van de bewaartermijnen voor index- en contactdossiers en de rollen die hier toegang toe hebben. De rol van Compliance Officer is naar verwachting beschikbaar vanaf versie 1.1.1.

	<b>Vanaf aanmaken dossier</b>	<b>Na afronden dossier</b>	<b>&gt; Aanmaakdatum +28 dagen</b>	<b>&gt; Aanmaakdatum + 5 jaar</b>
<b>Bewaartermijn dossier</b>				
Index	Volledig	Volledig	Volledig	Verwijderd in dossier, sleutel t.b.v. decryptie wordt verwijderd om herstel uit back-up onmogelijk te maken
Contact	Volledig	Volledig	Gepseudonimiseerd	
<b>Toegang tot dossier</b>				
Rol werkverdeler	Alleen voor regio een geabstraheerd overzicht			
Rol medewerker	Indien toegewezen aan medewerker	Geen toegang	Geen toegang	Geen toegang
Rol compliance officer	Mogelijkheid om PDF te genereren met dossierinhoud of dossiers te verwijderen i.h.k.v. rechten van betrokkenen. Via een zoekactie op "achternaam + geboortedatum", "achternaam + telefoonnummer", "achternaam + e-mail", uniek ID GGD Contact en uniek ID HPzone.			

## 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<sup>23</sup> waarvoor de veiligheidsregio's verantwoordelijk zijn.<sup>24</sup> De uitvoering van BCO is vervolgens een wettelijke taak van de GGD'en.<sup>25</sup> De wettelijke taak om BCO uit te voeren betreft niet de wettelijke plicht om persoonsgegevens te verwerken. Bij wet- regelgeving is immers niet

<sup>23</sup> 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 maatregelen opgelegd kunnen worden om de bevolking te beschermen. 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.

<sup>24</sup> Artikel 6 lid 2 Wpg.

<sup>25</sup> Artikel 6 lid 1 sub c Wpg jo artikel 13 Wpg.

bepaald hoe het BCO-proces dient te worden uitgevoerd en welke gegevensverwerking hiervoor nodig is.

Van de wettelijke mogelijkheid<sup>26</sup> 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<sup>27</sup> 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<sup>28</sup> 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 gezag.<sup>29</sup> 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.

HPZone Lite waarin de verwerkingen in het kader van BCO plaatsvinden betreft geen medisch dossier als bedoeld bij Wgbo.<sup>30</sup> 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"<sup>31</sup> 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 infectieziektebestrijding 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

---

<sup>26</sup> 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.

<sup>27</sup> Artikel 11 Nota van toelichting bij Besluit publieke gezondheid.

<sup>28</sup> <https://lci.rivm.nl/COVID-19-BCO>

<sup>29</sup> Artikel 6 lid 1 sub e AVG.

<sup>30</sup> Artikel 7:454 Burgerlijk Wetboek (Wgbo)

<sup>31</sup> Artikel 7:446 lid 1 Burgerlijk Wetboek (Wgbo)

voor de index om in de GGD Contact App zijn klachten te registreren aan de hand waarvan de eerste besmettelijke dag 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".<sup>32</sup>

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.<sup>33</sup> 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 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 rechtsstructuur 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

---

<sup>32</sup> 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.

<sup>33</sup> Kamerstukken II 2017/18, 34 851, nr. 3, p. 43 (MvT bij UAVG).

van ambt of beroep of wettelijk voorschrift aan geheimhouding zijn verbonden.<sup>34</sup>

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.<sup>35</sup> 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.<sup>36</sup>

Taken van het College van B&W worden uitgevoerd door GGD'en.<sup>37</sup> die onderdeel gaan uitmaken van het door een gemeenschappelijke regeling opgericht openbaar lichaam.<sup>38</sup> De GGD'en zelf kunnen worden aangemerkt als een a-orgaan.<sup>39</sup> 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.<sup>40</sup>

Ambtenaren leggen de eed af of doen de belofte<sup>41</sup> waardoor ambtenaren verplicht zijn tot geheimhouding van hetgeen hen in verband met hun functie ter kennis is gekomen.<sup>42</sup> 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 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.<sup>43</sup> 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.<sup>44</sup> 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.

---

<sup>34</sup> Artikel 2:5 lid 1 Awb.

<sup>35</sup> Artikel 2:5 lid 2 Awb.

<sup>36</sup> Zie Toelichting Besluit Ambtenarenwet 2017

<sup>37</sup> Artikel 14 lid 1 en 2 Wpg.

<sup>38</sup> Zie toelichting bij artikel 2 Uitvoeringsbesluit Ambtenarenwet 2017.

<sup>39</sup> A-orgaan = een orgaan van een rechtspersoon die krachtens publieksrecht is ingesteld (art 1:2 lid 1 sub a Awb)

<sup>40</sup> Artikel 1 Ambtenarenwet 2017.

<sup>41</sup> Artikel 7 Ambtenarenwet 2017.

<sup>42</sup> Artikel 9 Ambtenarenwet 2017

<sup>43</sup> Overweging 41 AVG.

<sup>44</sup> EHRM 26 april 1979, NJ 1980/146 (Sunday Times)

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.

#### Rechtsgrond monitoring en logging

Alle handelingen van medewerkers in BCO Portaal worden gelogd. In bijlage 4 is opgenomen om welke gegevens het gaat. Hierbij worden persoonsgegevens van medewerkers verwerkt. Doel hiervan is:

- het onweerlegbaar aantonen van een activiteit (compliance);
- het controleren op menselijk handelen (onbewust of bewust misbruik);
- incidentbeheer (onderzoek na een incident);
- het vinden van de oorzaak van een foute werking van het systeem (debugging).

De monitoring van de logging vindt plaats onder verantwoordelijkheid van de GGD'en. Wettelijke grondslag voor deze verwerking is artikel 6 lid 1 sub f AVG (gerechtvaardigd belang). Dit belang bestaat uit de verplichting van de verwerkingsverantwoordelijke om passende technische en organisatorische maatregelen te nemen ter bescherming van de verwerkte persoonsgegevens. BCO Portaal bevat gezondheidsgegevens. In lijn met de veldnorm voor het beveiligen hiervan hanteren we de NEN7510 en de onderliggende norm NEN 7513.

Naast de verplichting van de verantwoordelijke om de gegevens adequaat te beveiligen, is tevens het belang relevant dat betrokkenen hebben bij een zorgvuldige gegevensverwerking.

Het bijhouden en monitoren van logfiles is noodzakelijk om de hierboven genoemde redenen. Om de impact van het inzien van persoonsgegevens bij het monitoren van de logging te beperken, worden medewerkersgegevens in het dashboard primair alleen gepseudonimiseerd getoond. Vervolgens is het mogelijk om de logging in meer detail en met herleidbaarheid naar de gebruiker in te zien, mocht dat nodig zijn een vervolgonderzoek. Nadere analyse van een dossier op basis van de unique case identifier uit de logging is alleen mogelijk door een medewerker van de GGD met de applicatierol Compliance Officer.

Medewerkers worden de eerste keer dat zij het systeem gebruiken geïnformeerd over het feit dat het systeem een logging-functie kent. Voorts moet de GGD haar medewerkers ervan op de hoogte stellen aan welke regels voor het gebruik van BCO Contact gelden en welke sancties er zijn als een medewerker zich hier niet aan houdt. Wordt de monitoring van de logging uitgevoerd door GGDGHOR of een andere externe partij, dan is het belangrijk dat betreffende GGD heldere afspraken met deze partij maakt over de wijze waarop de monitoring plaatsvindt, over de criteria die gebruikt worden om te bepalen wanneer vervolgactie nodig is en over het werkproces dat daarbij gevolgd wordt. Met deze maatregelen wordt beoogd de zorgvuldigheid in het proces van

logging en monitoring maximaal te waarborgen en het risico dat hierbij ten onrechte inbreuk wordt gemaakt op de rechten en vrijheden van medewerkers zo veel mogelijk te beperken.

Gezien het belang dat de verwerkingsverantwoordelijke en de betrokkenen hebben bij een veilige verwerking van de gegevens, in combinatie met genoemde maatregelen om de belangen van betrokkenen te beschermen, wordt deze verwerking als acceptabel beoordeeld.

## **12. Doelbinding**

De verwerkingen die binnen GGD Contact, de datasluis en het BCO Portaal plaatsvinden, hebben als doel het BCO-proces ten behoeve van infectieziektebestrijding, efficiënter en sneller te laten verlopen.

De doeleinden van deze verwerkingen zijn verder uitgewerkt in paragraaf 5 van deze DPIA.

## **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 redenen om een alternatieve voorziening voor te bereiden. 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. Daarmee is de stap gezet naar een bronbestand met de juiste passende technische en organisatorische maatregelen en is de eerste stap richting een betere omgeving vanuit gegevensbeschermingsoogpunt.

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 alleen in die gevallen versneld uitgevoerd worden als een 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. Of negatieve gevolgen voor de contacten van de index wanneer zij onterecht in thuisisolatie gaan en zo worden beperkt in hun vrijheden.

De voorgesproken alternatieven dragen niet bij aan een beter BCO waarbij 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 Portaal. Hierbij gaat BCO Portaal op termijn HP Zone Lite vervangen. Het ophalen van het van het adresboek in GGD Contact resulteert daarbij in een verwerking die buiten de grenzen van het reguliere BCO-proces 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 alleen 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 dit minder foutgevoelig is voor overtyp-fouten. In de flow van het BCO-proces worden de ingeladen gegevens van het contact, waarvan de index kiest om ze door te sturen naar de GGD, 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 van deze DPIA.

#### Effect:

Het effect van de verwerking op de betrokkenen met inachtneming van de hierboven genoemde proportionaliteit en subsidiariteit op de bescherming van de persoonlijke levenssfeer is beperkt. Het gebruik van de GGD Contact App en het BCO Portaal op zichzelf is vrijwillig. De wijze waarop de GGD Contact App en het BCO Portaal zijn ingericht is ontworpen met inachtneming van privacy en security by design principes. Het betreft weliswaar een gegevensverwerking die bijzondere persoonsgegevens bevat, maar door het ontwerp, de maatregelen die worden geïmplementeerd en het vrijwillige karakter is het effect beperkt.

#### **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 Portaal. 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 Portaal. 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 opgesteld. 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 Portaal (naar de GGD) zijn verstuurd nadat de window van 48 uur voor aanleveren van de gegevens is verlopen. De Index kan meerder malen uploaden en zo fouten in eerdere aanleveringen herstellen. 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 in het kader van BCO).

*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 besmettelijke periode 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 overeenkomst niet de grondslag is van de verwerking) zal de GGD dit direct 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.

### 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 – gegevens over contacten.
- 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;
- 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. Opslag in onvoldoende beveiligde systemen

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 App 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 of soortgelijke 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. Verwerking van meer gegevens dan noodzakelijk

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 code om te koppelen, 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.
- 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

Restrisico 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 invloedssfeer 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 BCO Portaal vindbaar zijn.
- 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 Portaal inregelen.

- In de GGD Contact App moeten gegevens na verzending aan de GGD automatisch worden gewist na de daarvoor relevante termijn.
- Duidelijke informatieverstrekking naar de index over het verwijderen van gegevens in GGD Contact wanneer niet meer nodig.
- 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.
- Opzetten en implementeren van procedures en afspraken over verantwoordelijkheden (governance en compliance breed inrichten).
- Eén-op-één doorgeven van contractuele vereisten aan (sub)verwerkers, waardoor eenzelfde vereisten gelden voor alle betrokken partijen zoals leveranciers.

Risico voor Betrokkene (voor maatregelen)	Middel
Risico voor Betrokkene (na maatregelen)	Laag

### 9. Onjuiste koppeling van gegevens aan dossier

De door de index geüploade contactgegevens worden door een technische/procedurele oorzaak ten onrechte gekoppeld aan een dossier/BSN van een andere burger. Dit kan zijn door bijvoorbeeld een foutieve koppeling van GGD Contact, waardoor de gegevens onjuist of onveilig worden overgezet.

- De kans dat dit risico zich manifesteert zonder maatregelen is Middel. Een menselijke fout zoals het verkeerd intypen van een naam is mogelijk waardoor informatie in een verkeerd dossier wordt gezet of een verkeerde contactpersoon wordt gebeld.
- De impact van dit risico zonder maatregelen is Middel. Een contact kan onterecht gebeld worden, met als consequentie dat het contact tijdelijk in zijn vrijheden kan worden beperkt en gegevens ten onrechte worden opgenomen in een dossier.

Geadviseerd wordt de volgende maatregelen te nemen:

- Duidelijke instructie voor de BCO-medewerker hoe de gegevens in het BCO Portaal te koppelen (zowel digitaal als handmatig) aan de index (via casenummer).
- 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.
- 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 authentifieren/verifiëren van de index voordat door BCO-medewerker gegevens in dossiers worden ingevoerd door middel van een koppeling van een casnummer 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 (werkstructuur), 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.

Risico voor Betrokkene (voor maatregelen)	Hoog
Risico voor Betrokkene (na maatregelen)	Middel

Restrisico 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 Portaal

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.
- Bij de start van BCO Portaal en in de e-learning wordt de gebruiker geïnformeerd over zijn rechten en plichten.
- Inrichten autorisaties/autorisatiematrix.
- 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.
- BCO-medewerker kan in het BCO Portaal alleen zoeken op aan hem/haar toegewezen dossiers, die regio gebonden zijn, en alleen op actieve BCO dossiers.
- Antecedentenonderzoek nieuwe medewerkers (ook bij samenwerkingspartners)

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 een bewaartermijnbeleid dat na de epidemiologische relevante periode het net werk van contacten van indexen pseudonimiseerd, met behoud van de relaties die epidemiologisch relevant is, en daarmee invulling geeft aan het begrip dataminimalisatie.5) di
- 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 of soortgelijke 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 Portaal.
  - 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



Restrisico 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

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 tijdig 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 de GGD Contact App als in het BCO Portaal 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 Portaal.
  - 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 de GGD Contact App en het BCO Portaal 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 de GGD Contact App en het BCO Portaal.
- 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 Portaal.

- 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 de GGD Contact App en/of het BCO Portaal.
- Opleiding van de BCO-medewerker bij voordoen uitvalscenario's.

Risico voor Betrokkene (voor maatregelen)	Middel
---	--------

Risico voor Betrokkene (na maatregelen)	Laag
---	------

### 18. Onvoldoende veilig ingerichte koppelingen

Koppelingen tussen systemen en applicaties zijn op een onvoldoende veilige manier ingericht.

- De kans dat dit risico zich manifesteert zonder maatregelen is Hoog. Indien voorbij wordt gegaan aan informatiebeveiligingsaspecten m.b.t. het transport van de data tussen systemen of wanneer derden zich toegang tot de koppeling en/of systemen kunnen verschaffen is het aannemelijk dat er onveilige koppeling zijn ingericht.
- De impact van dit risico zonder maatregelen is Hoog. Indien er transport van data plaatsvindt door onvoldoende veilige koppelingen is de koppeling hiermee vatbaar voor inbreuken van buitenaf, waardoor gegevens openbaar kunnen worden gemaakt en/of misbruik van de data plaats kan vinden.

Geadviseerd wordt om de volgende maatregelen te nemen:

- Bij de inrichting van systemen vereisten opstellen (voor leveranciers) waaraan minimaal voldaan dient te worden en testen van deze systemen.
- Opzetten en implementeren van ICT-beheerprocessen. Gebaseerd op een door de directie geaccordeerd informatiebeveiligingsbeleid. Aansluiten bij binnen de markt bekende standaarden zoals ITIL, in combinatie met BIO/NEN 7510/ISO 27001. In ieder geval aandacht voor
  - Security management
  - Access management
  - Availability management
  - Change management
  - Incident management
  - Problem management
  - Patch management
  - Knowledge management
  - Supplier management
- Eisen ten aanzien van ICT-beheerprocessen 1-op-1 vertalen naar de contractuele afspraken met leveranciers ((sub-)verwerkers).
- Goede contractuele afspraken.
- Toepassing TLS: Transport versleuteling (TLS) op alle verbindingen.
- Encryptie (at rest: Encryptie van de (gevoelige) velden voordat deze in de database terecht komen. Tevens at rest encryptie van secrets, data en logging. Hiermee wordt voorkomen dat er toegang tot de data mogelijk is.

Risico voor Betrokkene (voor maatregelen)	Hoog
---	------

Risico voor Betrokkene (na maatregelen)	Laag
---	------

### 19. Verwerken persoonsgegevens indexen die buiten RIVM Protocol vallen

Bij het gebruik van GGD Contact wordt geen onderscheid gemaakt in groepen personen (zoals personen onder de 18 jaar)/functies (zoals contactberoepen). Er wordt in het kader van BCO gevraagd door de GGD'en om gegevens aan te leveren van personen met wie de index in contact is geweest, terwijl in het RIVM-protocol specifieke afspraken zijn opgenomen voor bijvoorbeeld contactberoepen, scholen, kinderopvang en/of kinderen onder de 18. Deze personen behoren niet in dit BCO-onderzoek als contact 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.
- Via werkinstructies wijzen op de het RIVM-protocol.

Risico voor Betrokkene (voor maatregelen)	Hoog
Risico voor Betrokkene (na maatregelen)	Laag

### 20. Ontbreken verwerkersovereenkomsten

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 geven 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 voordoet 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 App vooraf laten gaan door een zelf ingestelde pincode.
- In GGD Contact App het advies opnemen de telefoon te beveiligen met een toegangscode indien dit niet het geval is.

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 Portaal. 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
  - BCO Portaal alleen bereikbaar maken via VPN
  - Sessielengte van de VPN beperken waardoor risico onbeheerde computer/laptop beperkt wordt.
- 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.
- 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 Portaal 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. Ontbreken van afspraken omtrent rolverdeling en verantwoordelijkheden

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 maatregelen 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 indien het niet vastgelegd in het convenant. 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 de GGD contact App, BCO Portaal en sluis.

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 ZelfBCO) 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 ZelfBCO in de GGD Contact App.

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.

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 bijzondere persoonsgegevens 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

- Indiensttreding (integriteitscontrole, geheimhoudingsovereenkomsten)
- 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:

- 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 Portaal. 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 Portaal) over bewegingen in het BCO Portaal 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 Portaal en de systemen die hiermee verbonden zijn uitgevoerd. Denk hierbij aan: pen-test op GGD Contact, de API's, het BCO Portaal 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 Portaal 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 Portaal).

#### 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 Portaal.

#### 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 soortgelijke 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, GGD GHOR en in de privacyverklaring van GGD Contact.

*14. Bewaartermijnen technisch inregelen*

Door het inregelen van een beperkte opslagperiode in het BCO Portaal 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 adoptiegraad 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/RIVM*

Duidelijke informatieverstrekking vanuit Rijksoverheid/VWS. Duidelijke informatieverstrekking vanuit RIVM en e-Learning met betrekking tot jeugdigen.

*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. Authenticeren/verifiëren van de index*

Afdwingen authenticeren/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

- a. Voorkomen: beheerst ontwikkel- en beheerproces en uitvoeren van (technische) penetratietesten op GGD Contact, de sluis en het BCO Portaal.
  - 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 throttling: 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 de GGD Contact App en het BCO Portaal.

*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 mogelijkheden 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 BCO Portaal pas plaatsvindt. Tevens is het hierdoor niet mogelijk dat de aan het internet aangesloten ontvangende server (de sluis) informatie kan ontleen 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 ZelfBCO.

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)

  - COVID-19 symptomen, ziekteverloop.
  - Eerste ziekte dag 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 besmettingslocatie is.
  - Vastleggen settings die meestal geen context zijn (thuisituatie / 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 vlieg reizen 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 werkverdelers 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 werkverdelers 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.

1. Na afloop van het eerste BCO gesprek. De index kan de tijdens het BCO gesprek geïnterviewde 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 BCO Portaal 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

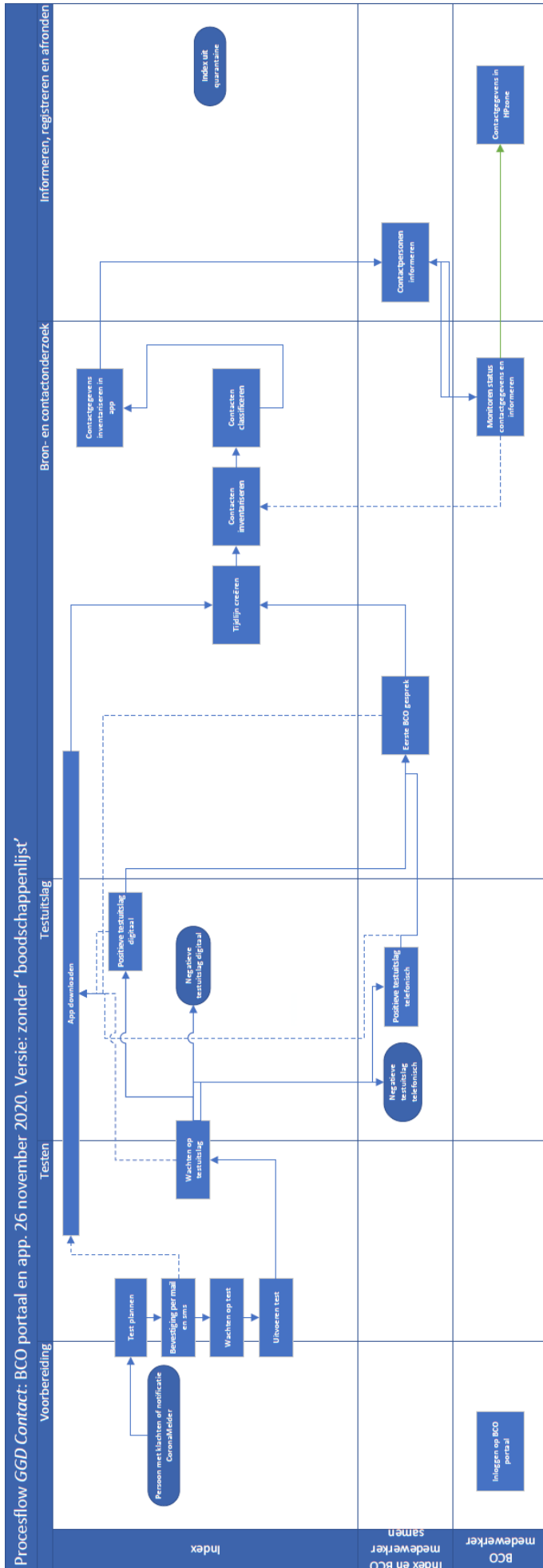
Indien de gegevens zijn aangeleverd door de index kan de BCO-medewerker een inventarisatie maken welke contacten geïnformeerd dienen te worden. Deze contactpersonen zullen worden geïnformeerd dat zij in contact zijn geweest met iemand die positief getest is op COVID-19 en nadere informatie krijgen in 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 BCO Portaal 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

### Bijlage 3 – 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: <ul style="list-style-type: none"><li>• Een kwaadwillende minimale inzet doet hiertoe; of</li><li>• Een medewerker onbewust nalatig handelt of een fout maakt; of</li><li>• Het inherent is aan het risico dat deze zich manifesteert.</li></ul>
Midden	Het risico voor betrokkene zal zich wellicht manifesteren indien: <ul style="list-style-type: none"><li>• Een kwaadwillende voldoende middelen inzet; of</li><li>• Een medewerker bewust nalatig is of opzettelijk handelt; of</li><li>• Het zeer waarschijnlijk is vanwege de aard van het risico</li></ul>
Laag	Het risico voor betrokkene zal zich enkel manifesteren indien: <ul style="list-style-type: none"><li>• Een kwaadwillende buiten proportionele middelen inzet; of</li><li>• Een medewerker bewust zeer nalatig of opzettelijk handelt; of</li></ul>

#### *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	<ol style="list-style-type: none"> <li>1. Kan de reputatie of belang van de betrokkene significant schaden, compromitteren of belemmeren;</li> <li>2. Kan resulteren in sterfte of ernstig letsel;</li> <li>3. Kan een grote inbreuk opleveren in de fundamentele rechten en vrijheid van betrokkene</li> </ol>
Midden	<ol style="list-style-type: none"> <li>1. Kan de reputatie of belang van de betrokkene schaden, compromitteren of belemmeren;</li> <li>2. Kan resulteren in persoonlijk letsel;</li> <li>3. Kan een inbreuk opleveren in de fundamentele rechten en vrijheid van betrokkene</li> </ol>
Laag	<ol style="list-style-type: none"> <li>1. Kan resulteren in beperkte materiële schade;</li> <li>2. Kan de reputatie of belang van de betrokkene schaden</li> <li>3. Kan een kleine inbreuk opleveren in de fundamentele rechten en vrijheid van betrokkene</li> </ol>

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 en NEN 7513.

Uit de verplichte logvelden van de NEN 7510 en NEN 7513 volgt de verwerking van persoonsgegevens.

- Accountgegevens: gebruikersnaam, regio en rol(len)
- Gegevens om de BCO Portaal gebruiker te identificeren;
- Dossieracties van de BCO Portaal gebruiker (aanmaken, toekennen, invoeren, toevoegen, verwijderen, lezen, kopiëren, samenvoegen, splitsen en overdragen, zoeken);
- Data, tijdstippen en details van belangrijke gebeurtenissen, bijvoorbeeld 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.
- Gebruik van speciale bevoegdheden;
- Gebruik van systeemhulpmiddelen en -toepassingen;
- Bestanden die zijn geopend en het type toegang dat is verkregen;
- Netwerkadressen en -protocollen;
- IP-adres BCO Portaal gebruiker

Van de GGD Contact App gebruiker (index) wordt een unieke ID gegenereerd – gekoppeld aan het dossiernummer - bij het uploaden naar het BCO Portaal. Deze unieke ID wordt gelogd. Daarbij wordt dus geen aanvullende identificerende informatie gelogd van een index.

## DPIA GGD CONTACT

### Addendum 01 BCO Sync extensie

---

#### Auteurs:

██████████ (GGD GHOR Nederland)

██████████ (GGD GHOR Nederland)

**DATUM** 22-6-2021  
**STATUS** Definitief  
**VERSIE** 1.0  
**BOUWT VOORT OP** DPIA GGD CONTACT 1.1.4  
**DPIA VERSIE**

---

## MANAGEMENTSAMENVATTING

Dit DPIA GGD Contact Addendum [01] BCO Sync Extensie 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

Ten aanzien van de 1.1.4 versie is in dit addendum een nadere uitwerking gegeven met betrekking tot de BCO Sync extensie die door GGD GHOR Nederland wordt uitgevoerd. Door middel van de BCO Sync extensie kan casedata gesynchroniseerd worden tussen HPZone Lite en het BCO Portaal.

#### DPIA ANALYSE

Deze wijziging in functionaliteit heeft impact op de DPIA onderwerpen: Cultuur, Juistheid en Bescherming.

#### 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. Het bepalen van de risiconiveaus en de risico-calculatie vindt plaats op de wijze die omschreven staat in de DPIA GGD Contact v.1.1.4..

Nr.	Risico	Belang / impact	Maatregel
1	Geen of onvoldoende overzicht op toewijzing en	Laag	Het borgen van een proces voor het verlenen van

---

gebruik van de extensie  
binnen de GGD.

autorisaties voor het  
gebruik van de extensie.

---

---

---

# 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 (de GGD Contact App) met een bijbehorende webportal (het BCO Portaal) (gezamenlijk: **GGD Contact**).

## 1.2 Nieuw functionaliteit

In dit document wordt een analyse gedaan op de toevoeging van BCO Sync extensie waar casedata gesynchroniseerd kan worden tussen HPZone Lite en het BCO Portaal, **Functionaliteit BCO Sync extensie** op GGD Contact.

## 1.3 Doel van dit document

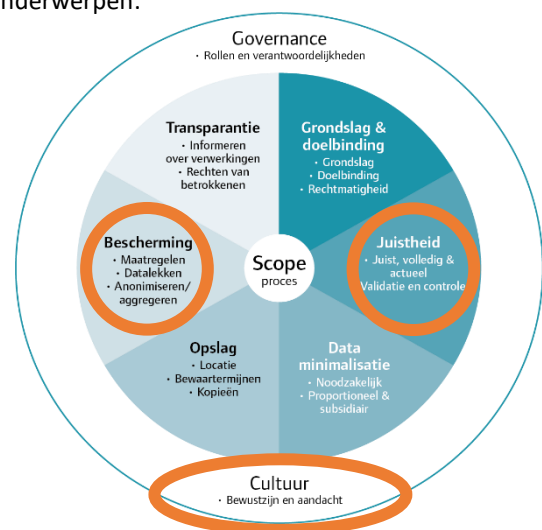
Dit document bevat een Data Protection Impact Assessments (**DPIA**) op de **Functionaliteit BCO Sync extensie**. De DPIA Functionaliteit BCO Sync extensie is bedoeld voor betrokkenen om de risico's en te nemen maatregelen ten aanzien van de wijzigingen die Functionaliteit BCO Sync extensie met zich 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 GGD Contact voor GGD'en 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:
  - o governance & cultuur
  - o grondslag en doelbinding
  - o juistheid
  - o dataminimalisatie
  - o opslag
  - o bescherming
  - o transparantie



Wanneer er een wijziging is ten opzichte van de GGD Contact DPIA wordt dat visueel weergegeven in het DPIA-wiel.



## Afbeelding 1. Template VKA DPIA wiel

### 1.5 Document historie

Tabel 1. Document historie

Datum	Versie	Wie	Toelichting wijziging
	0.1		Opstellen document
	0.9		Aanpassing document na review FG's
	1.0		Definitief (nog niet vastgesteld) naar Stuurgroep

Tabel 2. Overzicht addenda

Datum	Functionaliteit	Toelichting wijziging
	01 BCO Sync extensie	Toevoeging extensie binnen het huidige proces

### 1.6 Afstemming GGD'en

[Nog nader in te vullen door de GGD n.a.v. nog op te stellen afstemmingscyclus bij toevoegen nieuwe functionaliteiten en nieuwe pilot-regio's.

GGD	FG	Datum

Tabel 3. Afstemming ter goedkeuring

## 2 RISICOANALYSE

### 2.1 Nieuwe functionaliteit

#### 2.1.1 Omschrijving nieuwe functionaliteit

Voor GGD Contact ten behoeve van het BCO-proces is een extensie ontwikkeld. Op deze nieuwe extensie is een DPIA uitgevoerd welke is opgenomen in dit addendum.

Bij de uitbraak van COVID-19, waar BCO voor uitgevoerd dient te worden, is het belangrijk om het BCO-proces sneller en efficiënter te laten verlopen, ten behoeve van infectieziektebestrijding. Door het proces te ondersteunen kunnen relevante contacten sneller in beeld worden gebracht voor de GGD, met als resultaat het eerder kunnen delen van het handelingsperspectief met de desbetreffende contacten van de index.

In het BCO-proces ontbreekt een geautomatiseerde koppeling om de gegevens tussen HPZone lite en het BCO Portaal over te zetten. Er is voor gekozen om deze binnen het Programmateam van GGD GHOR Nederland te ontwikkelen tot een kwalitatieve, effectieve en veilige workaround voor de BCO-medewerker.

Voor het proces betekent dit dat bij gebruik van de extensie data gesynchroniseerd kan worden tussen het BCO Portaal en HPZone Lite. Dit proces gaat als volgt

- 1) De BCO-medewerker opent een casedossier in HPZone Lite;
- 2) Maakt a.d.h.v. de extensie een casedossier aan in BCO Portaal;
- 3) De BCO-medewerker voert het BCO uit in het BCO Portaal;
- 4) Bij afronding van het BCO worden de gegevens in het casedossier terug gekopieerd naar HPZone Lite middels de 'kopieerknop'.

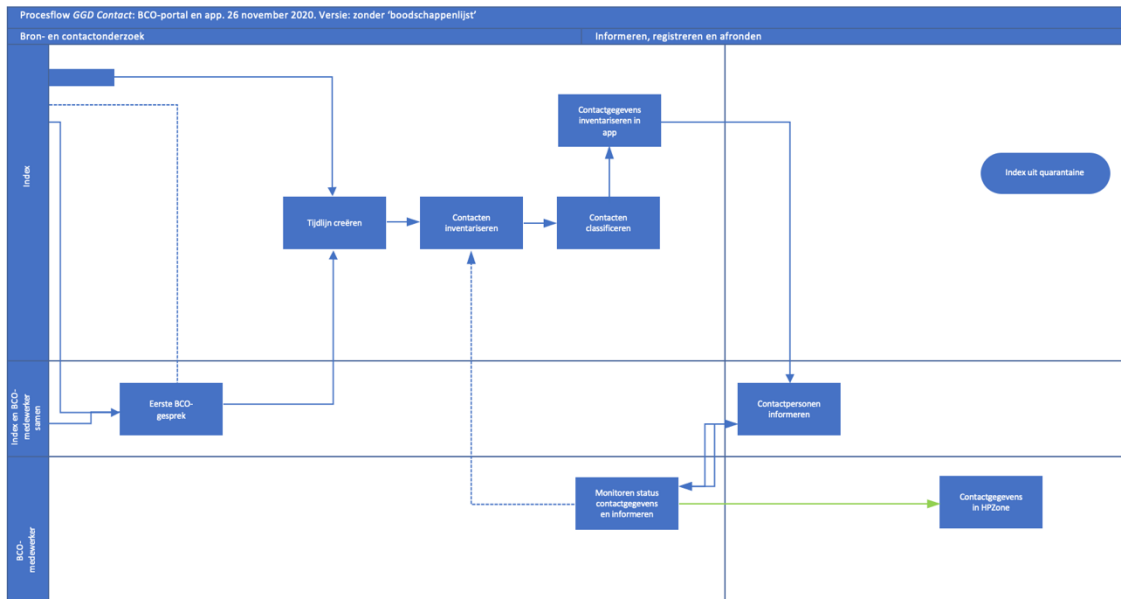
Het doel van de extensie is om de implementatie van BCO Portaal technisch te ondersteunen, door casedata vanuit HP Zone Lite naar BCO Portaal te kopiëren, en vice versa. Het automatiseren van het vele repeterende handwerk en het kopiëren/plakken zorgt ervoor dat het werk van de BCO-medewerker gemakkelijker wordt. Daarnaast neemt de tijdsbestending af, doordat standaard zaken niet handmatig meer ingevuld hoeven te worden. Dit zorgt er tevens voor dat er minder fouten gemaakt worden bij het automatisch overschrijven van de data. Naar verwachting is de juistheid en volledigheid van de gegevens die door de BCO extensie aangeleverd worden beter ten opzichte van de gegevens die handmatig worden doorgevoerd.

Er is geen sprake van een nieuwe technologie, GGD GHOR Nederland maakt gebruik van diverse extensies. Voor het gebruik van de extensie worden er noch andere persoonsgegevens verwerkt dan de persoonsgegevens zoals opgenomen in de DPIA GGD Contact versie 1.1.4. noch persoonsgegevens opgeslagen in de extensie of in het BCO Portaal/HPZone Lite. Voor de techniek en persoonsgegevens betekent dit er geen logging plaatsvindt in de extensie. De logging en monitoring vindt alleen plaats op de acties die de extensie automatiseert door HPZone Lite en het BCO Portaal. Voor de persoonsgegevens geldt verder dat het een vrije keuze aan de kant van de GGD'en is om deze extensie te gebruiken of niet en het aan de functioneel beheerders van de GGD'en is om te bepalen welke

portaal gebruikers toegang krijgen tot de extensie. Hierdoor bestaat de mogelijkheid dat er extra personen toegang krijgen tot de gegevens.

### 2.1.2 Proces flow chart huidige situatie (as is)

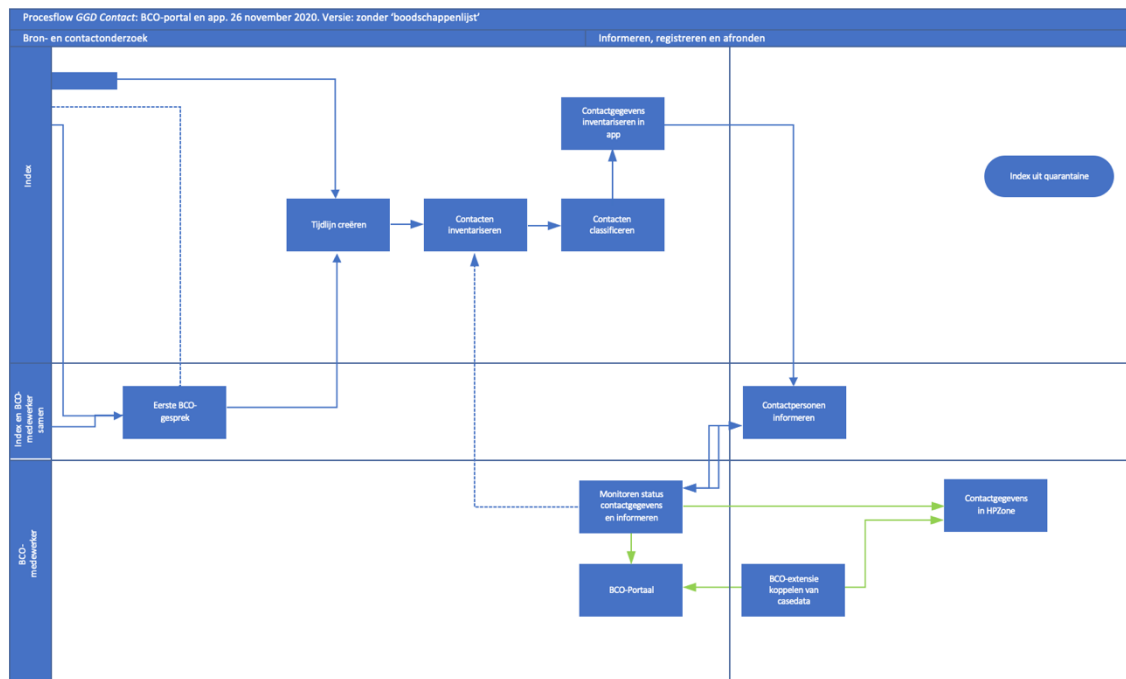
In afbeelding 2 is een gedeelte van het proces van de huidige situatie visueel weergegeven.



Afbeelding 2: Proces flow chart (as is)

### 2.1.3 Flow chart toekomstige situatie nieuwe functionaliteit (soII)

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 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. De betrokken partijen, de rolverdeling en de verantwoordelijkheden zijn zowel tijdens de ontwikkeling van de GGD Contact-app als tijdens de realisatiefase, de praktijkfase en de toevoeging van de nieuwe functionaliteit hetzelfde als omschreven in de DPIA GGD Contact versie 1.1.4. Dit betekent dat de GGD blijft aangemerkt als verwerkingsverantwoordelijke en GGD GHOR Nederland ook in haar rol als beheerder van de extensie optreedt als verwerker. Daarbij verloopt het beheer en support bij incidenten middels GGD GHOR Nederland.

De programma organisatie Vervanging HPZone en HPZoneLite t.b.v. Covid-19 is opdrachtgever van de realisatie van deze extensie. En het Programmateam wil via deze optie een kwalitatieve, effectieve en veilige workaround aan BCO'ers bieden.

De nieuwe functionaliteit brengt wel wijzigingen met zich mee ten aanzien van het thema cultuur. De BCO Sync extensie vergt immers een extra handeling van de BCO-medewerker. Ondanks dat deze extra handeling geen wezenlijke verandering is voor de BCO-medewerker, dient de BCO-medewerker wel middels een handleiding geïnformeerd te worden over deze nieuwe functionaliteit. In de handleiding die

is opgesteld voor de BCO-medewerker is een instructie voor het gebruik van de nieuwe functionaliteit voor de BCO-medewerker opgenomen.

### **2.2.2 Grondslag en doelbinding**

#### **ANALYSE**

De nieuwe functionaliteit brengt geen wijzigingen met zich mee ten aanzien van het thema grondslag en doelbinding. Zoals in de DPIA GGD Contact v.1.1.4 aangegeven zijn de verwerkingen die binnen GGD Contact, de datasluis en het BCO Portaal plaatsvinden, bedoeld om het BCO-proces ten behoeve van infectieziektebestrijding, efficiënter en sneller te laten verlopen. De nieuwe functionaliteit heeft ten doel om het portaal technisch te ondersteunen en het werk te vergemakkelijken, zodat het proces sneller verloopt en er minder fouten worden gemaakt. Hieruit blijkt dat de nieuwe functionaliteit geen wijzigingen met zich mee brengt ten aanzien van het thema doelbinding, zoals eerder is vastgesteld in de DPIA GGD Contact v.1.1.4..

### **2.2.3 Juistheid**

#### **ANALYSE**

De nieuwe functionaliteit brengt wijzigingen met zich mee ten aanzien van het thema juistheid. Het thema juistheid wordt naar verwachting met de extensie geborgd; doordat het kopiëren en plakken niet meer handmatig gebeurt, zullen er minder fouten gemaakt worden. Er zijn checks ingebouwd welke op voorhand valideren of informatie compleet is en/of al reeds eerder zijn gesynchroniseerd. Hiermee wordt het risico dat er foute informatie overgezet wordt door het niet volledig uitvoeren van een kopieeractie wegenomen.

### **2.2.4 Dataminimalisatie**

#### **ANALYSE**

De nieuwe functionaliteit brengt geen wijzigingen met zich mee ten aanzien van het thema dataminimalisatie. In de extensie worden dezelfde persoonsgegevens uit het BCO-proces gekopieerd en geplakt en overgezet naar HPZone Lite of het BCO Portaal. Dit betekent dat de dataset gelijk blijft aan de gegevens die verwerkt worden in het BCO portaal en er geen nieuwe of aanvullende gegevens verwerkt worden. Daarnaast vindt er in de extensie geen logging plaats. Dit betekent dat de persoonsgegevens die zichtbaar zijn de extensie gelijk zijn aan de persoonsgegevens in de DPIA GGD Contact 1.1.4.

### **2.2.5 Opslag**

#### **ANALYSE**

De nieuwe functionaliteit brengt geen wijzigingen met zich mee ten aanzien van het thema opslag. Zoals hierboven wordt aangegeven worden de gegevens gekopieerd en geplakt om de gegevens over te zetten naar HPZone Lite of het BCO Portaal. Het gebruik van de nieuwe functionaliteit leidt tot mutaties in de dossiers van HPZone Lite en het BCO Portaal. De gegevens worden direct van het ene tabblad naar het andere tabblad gestuurd. In de extensie worden geen persoonsgegevens opgeslagen. Om deze reden is het niet vereist om nadere afspraken vast te leggen rondom opslag zoals bewaartermijnen en

vernietiging van de casedata. Hiervoor gelden namelijk de afspraken en bewaartermijnen zoals vastgesteld in DPIA GGD Contact 1.1.4.

## 2.2.6 Bescherming

### ANALYSE

De nieuwe functionaliteit brengt wijzigingen met zich mee ten aanzien van het thema bescherming.

De extensie is geschreven in javascript, bedoeld voor chromium-based browsers (Edge en Chrome). De code wordt geborgd middels 2FA in een github repository, waar eveneens de relevante ontwikkelaars van BCO Portaal toegang toe hebben.

Ten aanzien van de distributie is er sprake van een link achter de identity hub op [ggdtools.nl/extensies](https://ggdtools.nl/extensies), die verwijst naar een verborgen pagina op de Chrome Extension Store en de Edge Extension store.

Fox-IT heeft de browser extensies bekeken, waarbij een 'echte' penetratie test niet mogelijk is geweest, omdat de extensie geen 'echte' applicatie is.

Wel zijn een aantal aanbevelingen door Fox-IT gedaan, namelijk:

Wel zijn een aantal aanbevelingen gedaan:

- Het zou verstandiger zijn om dit soort toepassingen in de applicatie zelf te bouwen → Dit is op de ontwikkellijst van GGD Contact opgenomen.
- Hard coded namen/persoonsgegevens uit de extensie verwijderen → Is inmiddels gedaan.
- Tabs permissie uit het manifest van de extensies halen → Is inmiddels gedaan.
- "Dead code" (zoals `chrome.storage.local.get(["input_bsn"])`) eruit halen → Is inmiddels gedaan.
- De extensie lijst is nu te vinden op [REDACTED] achter authenticatie, deze achter authenticatie plaatsen → Is inmiddels gedaan.
- Er worden wel 'stats' naar de server van GGD GZ gezonden, maar deze zijn geanonimiseerd → De gegevens die GGD GZ ontvangt zijn 'aantallen'. Het aantal keren dat de extensie wordt gebruikt. Dit is niet te herleiden naar herkomst van de data zoals locatie of de persoon.

Ten aanzien van de beveiliging is het noodzakelijk dat vormen van phishing en social engineering de BCO-medewerkers niet moeten kunnen overtuigen om malafide varianten van de extensie te installeren. Om deze reden zijn in de E-learning t.b.v. GGD Contact privacy en security awareness opgenomen.

Daarnaast is ten aanzien van de beveiliging de extensie alleen te distribueren door geautoriseerde functioneel beheerders (middels AD rol). De extensie werkt uitsluitend wanneer geautoriseerde Portaal Gebruikers (ook wel de BCO-medewerker genoemd) zowel HPZone Lite als het BCO-Portaal geopend hebben in twee verschillende tabbladen. De extensie is opgenomen op een afgeschermd GGD tools omgeving. De functioneel beheerders van de GGD bepalen welke Portaal Gebruikers toegang krijgen tot de extensie. Hierdoor wordt een mogelijk risico dat het uitvoeren van semi-geautoriseerde handelingen effect zal hebben op de monitoring van de applicatie weggenomen.

Door de wijze waarop de extensie functioneert wordt HPZone Lite minder belast dan wanneer de BCO-medewerker handmatig eenzelfde handelingen uitvoert. Dit betekent dat de BCO-extensie geen negatieve invloed heeft op de (in)stabiliteit van HPZone Lite.

De extensie maakt gebruik van de browser voor de knip en plak functionaliteit. Bij elke nieuwe knip en plak functie wordt de oude functie verwijderd. Dit is ook gecontroleerd en hierdoor is het gevaar niet groter door het gebruik van de BCO-extensie. Er wordt namelijk maar één record van gegevens naar HPZone Lite of GGD Contact gekopieerd.

Dit betekent dat alle data tijdelijk in het RAM geheugen wordt opgeslagen, ook in de browser, maar dit is onafhankelijk van het wel of niet gebruik van de extensie. Alles wat wordt ingetypt in de applicatie (zowel HPZone Lite als GGD Contact) staat tijdelijk in het RAM geheugen. Een risico voor toegang tot het RAM geheugen betekent dat er toegang is tot de werkplek/laptop waardoor zich los van het RAM-geheugen zich ook de mogelijkheid voordoet om data te kopiëren door een onbevoegde. Het gebruik van de BCO-extensie zorgt hiervoor niet voor een nieuw risico ten opzichte van het niet gebruiken van de extensie. Het hier genoemde reeds bekende risico wordt middels awareness en door juiste contracten met partijen gemitigeerd.

Verder is er met het DevOps team van VWS en de ontwikkelaars van de BCO-extensie reeds een procedure vastgesteld waarbij het DevOps team in geval van wijzigingen in het BCO-portaal deze doorgeeft aan de hoofd-ontwikkelaar. Doordat er per release gekeken wordt naar de mogelijke impact op de extensie, zodat daar geanticipeerd op kan worden, wordt er geborgd dat bij een nieuwe release de functionaliteit in de extensie niet meer werkt en/of niet meer aansluit.

### **2.2.7    Transparantie**

#### **ANALYSE**

De nieuwe functionaliteit brengt geen wijzigingen met zich mee ten aanzien van het thema transparantie. Om deze reden hoeft de gegevensdeling via de BCO Sync extensie niet opgenomen te worden in de privacyverklaring BCO Portaal. De betrokkenen worden afdoende geïnformeerd door de huidige privacyverklaring BCO Portaal en deze behoeft daarom geen aanpassingen. De GGD'en die gebruik maken van de BCO extensie hebben de keuzemogelijkheid om deze toepassing in de privacyverklaring van het BCO Portaal op te nemen.

## CONCLUSIES

### 2.3 Risico's, aandachtspunten en maatregelen

De DPIA-analyse uit hoofdstuk 2.2. op de functionaliteit BCO Sync extensie brengt de volgende risico's en maatregelen met zich mee. Deze maatregelen zijn opgenomen in de Risicomatrix GGD Contact.

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). Op basis van de risiconiveaus staat in de tabel hieronder beschreven welke maatregelen verwacht worden.

Nr.	Risico	Belang / impact	Maatregel
1	Geen of onvoldoende overzicht op toewijzing en gebruik van de extensie binnen de GGD	Laag	Het borgen van een proces voor het verlenen van autorisaties voor het gebruik van de extensie.

### 2.4 Restriscio's

De restriscio's zijn de risico's die na het nemen van de maatregelen zoals hierboven omschreven overblijven. De restriscio's zijn laag ingeschaald omdat de eventuele gevolgen van de Functionaliteit BCO Sync extensie 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 restriscio. Gezien de geconstateerde lage restriscio's is voorafgaande raadpleging bij naar de mening van de auteurs niet nodig.

### 2.5 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.



**Archived:** woensdag 29 juni 2022 22:24:06

**From:** [Directiesecretariaat GGD GHOR Nederland](#)

**Sent:** woensdag 20 januari 2021 10:49:25

**To:** [REDACTED]

**Subject:** FW: Ter ondertekening: convenant BCO

**Importance:** Normal

**Sensitivity:** None

**Attachments:**

[21 01 10-FINAL\\_Convenant landelijke inzet BCO.docx](#); [Bijlage IV.docx](#); [12 Tekenblad \[REDACTED\].docx](#); [18 Tekenblad \[REDACTED\].docx](#); [26 Tekenblad \[REDACTED\].docx](#);

---

Beste DPG'en,

We hebben van jullie drie nog geen reactie mogen ontvangen. In de bijlage vinden jullie jullie tekenbladen, bijlage IV voor eventuele wijzigingen in de contactpersonen en het totale convenant. Zou een reactie vandaag nog lukken? Reactie graag aan [REDACTED] met ons in de cc.

Vast hartelijk dank!

Met vriendelijke groet,

*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.*



Zwarte Woud 2  
3524 SJ Utrecht  
Telefoon: [REDACTED]  
Mobiel: [REDACTED]

E-mail : [directiesecretariaat@ggdghor.nl](mailto:directiesecretariaat@ggdghor.nl)  
Website : [www.ggdghor.nl](http://www.ggdghor.nl)  
Twitter : [@ggdnederland](https://twitter.com/ggdnederland) en [@ghornederland](https://twitter.com/ghornederland)  
Afwezig : vrijdag

---

**Van:** [REDACTED]

**Verzonden:** dinsdag 12 januari 2021 10:11

**Aan:** Directie GGD GHOR Nederland <[directie@ggdghor.nl](mailto:directie@ggdghor.nl)>

**Onderwerp:** Ter ondertekening: convenant BCO

Beste DPG'en,

In bijlage vinden jullie de finale versie van het Convenant BCO ter ondertekening.

**Gevraagde actie**

In bijlage vind je drie verschillende documenten:

- Het Convenant
- Bijlage IV als losse bijlage
- Een apart tekenblad per DPG

Ons verzoek is om:

- De contactgegevens op bijlage IV van het Convenant te controleren (en, indien nodig, te corrigeren en/of aan te vullen)
- Het tekenblad te ondertekenen

Indien bijlage IV akkoord is, graag alleen het getekende tekenblad retour zenden **voor vrijdag 15 januari 17:00 aan ondergetekende** [REDACTED]

Als bijlage IV wel is aangepast, graag ook die bijlage retour zenden met dezelfde deadline. En dan graag de naam wijzigen in Bijlage IV plus de naam van de betreffende GGD.

### **Gevolgd proces**

Een eerste versie (0.1) van het Convenant is in november opgesteld, waarna op 26 november een uitnodiging is gestuurd aan alle FG'en om het convenant te bespreken. Dit overleg heeft op 3 december plaatsgevonden. Daarna is het convenant aangepast en op 9 december een versie 0.2 op Teams gedeeld in de FG omgeving. Op 10 december is in een mail medegedeeld dat die versie online was geplaatst. Daarna zijn geen opmerkingen binnengekomen en is het Convenant op 24 december met de DPG'en gedeeld ter ondertekening. Aangezien daar nog aantal opmerkingen op volgden is op 4 januari een additionele consultatieronde gestart om opmerkingen op te halen. De opmerkingen van deze laatste consultatieronde zijn verwerkt in bijgaande versie.

Bij voorbaat dank, met vriendelijke groet,

[REDACTED]

[REDACTED]  
[REDACTED]  
[REDACTED]



### **GGD GHOR Nederland**

Zwarte Woud 2  
3524 SJ 'a0 Utrecht

E-mail [REDACTED]

Telefoon [REDACTED]

Website [www.ggdghor.nl](http://www.ggdghor.nl)

Twitter @GGDGHORNL

**Archived:** woensdag 29 juni 2022 22:27:34

**From:** [REDACTED]

**Sent:** dinsdag 6 juli 2021 15:05:16

**To:** [REDACTED]

**Subject:** FW: Vooraankondiging overeenkomsten GGD Contact

**Importance:** Normal

**Sensitivity:** None

**Attachments:**

A - DVO GGD GHOR Nederland v.1.1.pdf; A.I - Dienstbeschrijving GGD GHOR Nederland v1.1.pdf; A.II - Service Level Agreement GGD Contact v1.1 (1).pdf; A.III - Dossier Afspraken en Procedures GGD Contact v1.1 (1).pdf; A.IV - Verwerkingsovereenkomst GGD GHOR Nederland v1.1.pdf; A.V - Checklist Onboarding applicaties v1.02.pdf; B - DVO GGD Contact v1.0 Definitief.pdf; B.I - Verwerkerovereenkomst ARVODI.pdf; C - Referentie DPIA GGD Contact release 1.1 v 1.1.3.pdf; D - DPIA GGD Contact Addendum BCO Sync extensie 1.0.pdf;

---

Beste [REDACTED]

We spraken elkaar vanmiddag over het tekenen van bijgevoegde stukken.

Ik heb inmiddels contact gehad met twee andere testregio's [REDACTED], hieruit kwam – kort en goed – naar voren dat er nog 'een waslijst aan aandachtpunten en vragen' zijn en dat men in het ongewisse is over hoe, waar en wanneer deze onder de aandacht kunnen worden gebracht.

Bij dit traject sprake is van een kluwen van relaties tussen vele partijen (VWS, GGD'en, GGD GHOR NL, intermax, etc.) waarbij geldt dat de individuele, deelnemende GGD'en zich door ondertekening verbinden aan allerlei verplichtingen, waarbij niet altijd even helder is wat hiervan de consequenties zijn, of het wel wenselijk is en wie er precies aangesproken kan worden als het misgaat.

Mijn advies is dan ook om meer tijd en gelegenheid te nemen om de zorgen en bezwaren vanuit de deelnemende GGD'en te adresseren en op dit moment niet over te gaan tot ondertekening.

Met vriendelijke groet,

[REDACTED]



M: [REDACTED]

E: [REDACTED]

Wil je weten wat de privacywet (AVG) voor jou betekent? Kijk op [hulpbijprivacy.nl](https://hulpbijprivacy.nl) #hulpbijprivacy

---

**Van:** [REDACTED]

**Verzonden:** maandag 28 juni 2021 19:28

**Aan:** [REDACTED]

**Onderwerp:** FW: Vooraankondiging overeenkomsten GGD Contact

Dag beiden,

Zie hier; is alles in orde zodat ik kan tekenen?

Groet, [REDACTED]

---

**Van:** [REDACTED]

**Verzonden:** maandag 28 juni 2021 17:41

**Aan:** [REDACTED]

**Onderwerp:** Vooraankondiging overeenkomsten GGD Contact

Beste [REDACTED]

De voorgenomen go-live van GGD Contact voor uw GGD komt nu snel in zicht. De beoogde go-live datum is 7 juli as.

Als onderdeel van de go-live dienen de nodige overeenkomsten en documenten op orde te zijn. In dit kader heeft de stuurgroep fase 1. Vervanging HP Zone (Lite) afgelopen vrijdag de standaard dienstverleningsovereenkomsten en documenten vastgesteld behorende bij de in gebruikname van GGD Contact (en de gerelateerde generieke ICT-diensten).

Deze standaard overeenkomsten (met bijlagen) zullen wij op naam zetten voor úw GGD en ter ondertekening aanbieden. Het gaat daarbij om de dienstverleningsovereenkomst voor GGD Contact vanuit VWS en de dienstverleningsovereenkomst voor gerelateerde generieke ICT-diensten vanuit GGD GHOR. Tevens delen we hierbij de door de stuurgroep vastgestelde referentie DPIA voor GGD Contact en de DPIA voor de BCO Sync extensie.

Hieronder een beknopt overzicht van de ingesloten documenten.

A. Dienstverleningsovereenkomst GGD GHOR Nederland

Bijlagen:

- A.I: Dienstbeschrijving
- A.II: Service Level Agreement
- A.III: Dossier Afspraken en Procedures
- A.IV: Verwerkersovereenkomst
- A.V: Checklist onboarding applicaties

B. Dienstverleningsovereenkomst VWS voor GGD Contact release 1.1

Bijlage:

- B.I: Verwerkersovereenkomst ARVODI VWS voor GGD Contact

C. Referentie DPIA GGD Contact release 1.1

D. DPIA GGD Contact Addendum BCO Sync extensie 1.0

Deze overeenkomsten zijn opgesteld met inbreng vanuit vele inhoudelijke experts. De concept versies van deze documenten zijn op 15 juni 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 jl.

Mochten er nog vragen zijn over deze documenten en de gevolgde procedure van vaststelling laat het dan even weten.

Met vriendelijke groet,

[REDACTED]

programmeam Surveillance en Outbreak Management voorziening



Email: [REDACTED]

Mobiel: [REDACTED]

Dit bericht kan informatie bevatten die niet voor u is bestemd. Indien u niet de geadresseerde bent of dit bericht abusievelijk aan u is verzonden, wordt u verzocht dat aan de afzender te melden en het bericht te verwijderen. GGD-GHOR Nederland aanvaardt geen aansprakelijkheid voor schade, van welke aard ook, die verband houdt met risico's verbonden aan het elektronisch verzenden van berichten.

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.

=====  
Op dit e-mailbericht en eventuele bijbehorende attachments is een disclaimer van toepassing, die is opgenomen op onze website: [https://www.ey.com/nl\\_nl/ey-email-disclaimer](https://www.ey.com/nl_nl/ey-email-disclaimer) Indien u niet in staat bent deze disclaimer te raadplegen en/of op te slaan, kunt u een e-mail bericht zenden aan <mailto:contact@nl.ey.com>, waarna wij u de disclaimer zullen toezenden.

=====  
This e-mail and any attachments are subject to a disclaimer which is included on our website: [https://www.ey.com/en\\_nl/ey-email-disclaimer](https://www.ey.com/en_nl/ey-email-disclaimer) If you are unable to retrieve and/or save this disclaimer, please send an e-mail to <mailto:contact@nl.ey.com> and we will send you the disclaimer.

=====

**Archived:** woensdag 29 juni 2022 22:29:19

**From:** [REDACTED]

**Sent:** maandag 26 april 2021 16:12:44

**To:** [REDACTED]

**Subject:** Gedupeerden datalek

**Importance:** Normal

**Sensitivity:** None

**Attachments:**

[GGD West-BrabantE.pdf](#); [GGD West-BrabantE - 20210331.pdf](#); [GGD West-BrabantE - 20210413.pdf](#)

---

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]

[REDACTED]  
[REDACTED]



**GGD GHOR Nederland**

Zwarte Woud 2

3524 SJ 'a0 Utrecht

E-mail [REDACTED]  
Telefoon [REDACTED]  
Website [www.ggdghor.nl](http://www.ggdghor.nl)  
Twitter @GGDGHORN

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.

**Archived:** woensdag 29 juni 2022 22:30:05

**From:** [Directiesecretariaat GGD GHOR Nederland](#)

**Sent:** donderdag 18 maart 2021 17:04:07

**To:** [REDACTED]

**Cc:** [REDACTED]

**Subject:** Gegevens datalek GGD West-Brabant

**Importance:** Normal

**Sensitivity:** None

---

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 [REDACTED] 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] of met ondergetekende.

Met vriendelijke groet,

[REDACTED]

[REDACTED]



**GGD GHOR Nederland**

Zwarte Woud 2  
3524 SJ'a0 Utrecht

E-mail [REDACTED]  
Telefoon [REDACTED]  
Website [www.ggdghor.nl](http://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.



**Archived:** woensdag 29 juni 2022 22:32:47

**From:** [REDACTED]

**Mail received time:** Mon, 23 Aug 2021 15:09:32

**Sent:** maandag 23 augustus 2021 17:09:33

**To:** [REDACTED]

**Subject:** Overeenkomsten t.b.v. GGD Contact

**Importance:** Normal

**Sensitivity:** None

**Attachments:**

[2.2 Service Level Agreement GGD Contact v1.1.pdf](#); [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 West-Brabant.pdf](#); [1.1 Verwerkersovereenkomst - GGD West-Brabant.pdf](#); [2.0 DVO GGD GHOR Nederland v.1.1.pdf](#); [2.1 Dienstbeschrijving GGD GHOR Nederland v1.1.pdf](#);

---

Geachte mevrouw [REDACTED],

Hierbij stuur ik u, op verzoek van [REDACTED], bijgevoegde overeenkomsten t.b.v. GGD Contact toe.

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]  
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]

**Archived:** woensdag 29 juni 2022 22:31:57

**From:** [REDACTED]

**Sent:** maandag 15 maart 2021 19:49:37

**To:** [Directie GGD GHOR Nederland](#)

**Subject:** Overzicht verstrekte stukken aan de AP van GGD GHOR Nederland [REDACTED]

**Importance:** Normal

**Sensitivity:** None

**Attachments:**

[Overzicht verstrekte stukken AP.xlsx](#); [20210126 vervolgmelding fraude januari 2021 \(3\)\[1\].pdf](#); [20212201\\_Melding fraude januari 2021.pdf](#); [REDACTED]

---

Beste DPG'en,

Bijgaand ter informatie het overzicht van de aan de AP verstrekte stukken tot nu toe door GGD GHOR Nederland met de oorspronkelijke melding en de vervolgmelding.

Eveneens ter informatie op verzoek van [REDACTED] het overzicht van documenten die [REDACTED] aan de AP heeft verstrekt.

Met vriendelijke groet,

[REDACTED]

[REDACTED]  
[REDACTED]



**GGD GHOR Nederland**

Zwarte Woud 2

3524 SJ 'a0 Utrecht

E-mail [REDACTED]

Telefoon [REDACTED]

Website [www.ggdghor.nl](http://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.