REFERENTIE DPIA: GGD CONTACT

10 juni 2021

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

- Landelijke referentie DPIA voor GGD'en -

Referentie DPIA: 1

GGD Contact 1

Versiegeschiedenis 4

Definities 6

Inleiding 8

A. Beschrijving kenmerken proces gegevensverwerkingen 13

1. Voorstel 13

2. Persoonsgegevens 13

3. Betrokken partijen en rolverdeling 18

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 35

10. Bewaartermijn 37

B. Beoordeling rechtmatigheid gegevensverwerkingen 38

12. Doelbinding 42

13. Noodzaak en evenredigheid 42

14. Rechten van betrokkenen 44

C. Beschrijving en beoordeling risico's voor de betrokkenen 47

15. Risico's 47

Risicocalculatie 47

D. Beschrijving voorgenomen maatregelen 69

16. Maatregelen 69

E. Bijlagen 79

Volledige BCO vragenlijst index **Epic-naam: volledige vragenlijst inclusief contacten** 80

Gestandaardiseerde zoekfunctie locaties/contexten **Epic-naam: Contexten** 81

Beknopte vragenlijst huisgenoten en nauwe contacten **Epic-naam: volledige vragenlijst inclusief contacten** 81

Cases die niet zijn afgerond aan anderen kunnen toewijzen **Epic-naam: nvt** 81

GGD Contact App met Zelf BCO mogelijkheid **Epic-naam: ZelfBCO App** 81

Bijlage 2 - Procesflow GGD Contact 83

3 – Achtergrond risiconiveaus 86

Kans 86

Impact 86

Bijlage 4 – Logging 89

Versiegeschiedenis

Versie	Auteur	Verspreiding bij	Activiteiten
0.1	x – Pin (Cuccibu)	- x (Regio Twente) - x (GGD West-Brabant) - x (Regio Gooi & Vecht) - x (GGD Zuid – Limburg) - x (VWS) - x (VWS) - x – Schaars (VWS) - x 5.1,2,e) - x (GGD GHOR Nederland) - CISO GGD GHOR	- Inzage & advies tussenversie DPIA
0.2	x – Pin	- FG GGD GHOR Nederland	- FG advies opvragen
0.3	x – Pin	- x (Cuccibu)	- Aanpassingen naar aanleiding FG advies & review
0.4	x – Pin	- x (VWS) - x (VWS) - x – Schaars (VWS) - x (x) - x (GGD GHOR Nederland) - CISO GGD GHOR - x (VWS)	- Delen concept versie DPIA ter review VWS
0.5	x – Pin	- x 5.1,2,e) - x (5.1,2,e)	- Review DPIA (op hoofdlijnen)
0.6	x – Pin	- x 5.1,2,e) - x 5.1,2,e)	- Tekstvoorstel betrokken partijen en rolverdeling
0.7	x – Pin	- x 5.1,2,e) - x 5.1,2,e)	- Tekstvoorstel Telecommunicatiewet

1.0	x – Pin	- x (5.1,2,e) - x 5.1,2,e) - x (Regio Twente) - x (GGD West-Brabant) - x (Regio Gooi & Vecht) - x (GGD Zuid – Limburg) - x (VWS) - x (VWS) - x – Schaars (VWS) - x (Joan Knecht) - x (GGD GHOR Nederland) - CISO GGD GHOR Nederland - FG GGD GHOR Nederland - x (Cuccibu)	- Definitieve versie referentie DPIA - FG advies opvragen praktijkregio's + FG GGD GHOR Nederland
1.1	x – Pin		Aanpassingen naar aanleiding van FG Advies, begeleidingscommissie advies en FG advies GGD'en
1.1.1	x – Pin	- x (VWS)	Samenvoeging referentie DPIA 1.0 met Addenda: ZelfBCO, BCO Vragenlijst + Osiris Vragenlijst, Evaluatie GGD Contact
1.1.2	x & x	- x – Pin (GGD GHOR Nederland) - 25 FG's v.d. 25 GGD'en	Wijziging naar scope 'Release 1.1' **Review ten behoeve van FG-advies**

Definities

Bron – en contactopsporing (BCO)	Een wettelijke taak van de GGD zoals bedoeld in artikel 6 lid 1 sub c Wet publieke gezondheid ten behoeve van infectieziektebestrijding. Het doel van BCO is om contacten te identificeren, hen te informeren over de blootstelling en het risico op besmetting, hen te wijzen op maatregelen die genomen moeten worden om verdere verspreiding te voorkomen en hen hierin te begeleiden. Door middel van BCO wordt tevens mogelijk om locaties of situaties waarin mensen besmet zijn geraakt te monitoren, om eventuele verheffingen of lokale risico's te signaleren en zo mogelijk extra maatregelen te implementeren.
BCO-medewerker	Medewerker die BCO uitvoert. Dit kan een medewerker van de GGD zelf betreffen, maar kan ook een medewerker betreffen die vanuit de landelijke schil wordt ingezet.
BCO Portaal	Het webportaal dat de BCO Portaal Gebruiker gebruikt om BCO uit te voeren
BCO Portaal Gebruiker	Iedere gebruiker van het BCO Portaal, waaronder de BCO-medewerker, de werkverdeler (en in latere releases van het BCO Portaal ook andere functies).
Contactgegevens	Gegevens die de GGD kan gebruiken om een persoon te benaderen, zoals een telefoonnummer of e-mailadres.
GGD	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.[1] GGD'en hebben voor BCO een werkbaar proces voor wat betreft infecties die zich op kleine schaal voordoen. Het reguliere proces van BCO is lastig uitvoerbaar bij een pandemie zoals bij COVID-19 het geval is. Ter ondersteuning van het BCO Proces COVID-19 gaan GGD'en in Nederland 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 referentie-document voor iedere GGD afzonderlijk. In dit document wordt de conform de AVG verplichte gegevensbeschermingseffectbeoordeling (DPIA) op GGD Contact vastgelegd. Iedere GGD kan dit document gebruiken om deze om te zetten en aan te passen op haar eigen interne processen. Het model gegevensbeschermingseffectbeoordeling Rijksdienst (PIA) is gebruikt als uitgangspunt voor het opstellen deze DPIA-rapportage.

Noodzaak tot DPIA

Op de gegevensverwerkingen in GGD Contact is de AVG van toepassing. De Autoriteit Persoonsgegevens heeft een lijst gepubliceerd van soorten verwerkingen waarvoor een DPIA als bedoeld in artikel 35 van de AVG verplicht is.[2] In deze lijst wordt gesteld dat voor grootschalige verwerkingen van gezondheidsgegevens een DPIA dient te worden uitgevoerd. Hoewel in de 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.[3] 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

[1] Artikel 6 lid 1 sub c Wpg.
[2] https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/stcrt-2019-64418.pdf
[3] Artikel 9 lid 1 AVG en de daarop van toepassing zijnde overweging 35 AVG.

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.[4] 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 in de [toevoegen exacte naam en datum beslisnotities] beslisnotities nader uitgewerkt.

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[5] tussen GGD Contact en BCO Portaal waarmee de BCO-medewerker gaat werken.[6]
- 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 gegeven. Indien nodig, kan tijdig quarantaine of thuisisolatie op basis van eigen initiatief van het contact, gestart worden.

[4] Stand van zakenbrief digitale ondersteuning pandemiebestrijding 12 februari 2021
[5] Application Programming Interface waardoor GGD Contact met het BCO Portaal kan communiceren.
[6] De sluis kan worden gezien als een doorgeefluik waar de gegevens tijdelijk staan opgeslagen totdat deze vanuit GGD Contact aan het BCO Portaal worden doorgegeven.

- 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 infectieziektes 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 [datum] (Bijlage 1: Beschrijving Releases)

Release 1.1 is de beoogde landelijke uitrol van de volgende functionaliteiten:

- Volledige BCO-vragenlijst index (epic-naam: Volledige vragenlijst inclusief contacten) 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 GGD Contact, de sluis en het BCO Portaal van de BCO-medewerker worden onderstaande persoonsgegevens verwerkt. De velden die de index in GGD Contact kan invullen zijn optioneel.

Er bestaat geen verplichting om de gegevens aan te leveren. Het is dus ook mogelijk dat de index ervoor kiest geen enkel gegeven in te vullen of wel in te vullen maar niet te verzenden. Bij het delen van de gegevens met de GGD krijgt de index wel een herinnering dat niet alle velden zijn ingevuld. Deze melding kan worden genegeerd door de index. Er is bewust gekozen om de gegevens als optioneel aan te merken in de GGD Contact App zodat de data niet wordt 'tegengehouden' indien aan de kant van de index data niet compleet is. De index uploadt de gegevens namelijk niet een voor een, maar als een batch. Hierdoor kan het voorkomen dat de index contact A wel reeds heeft aangeleverd met een telefoonnummer, maar van contact B alleen nog maar een naam heeft. Door de gegevens als optioneel aan te merken kan het BCO wel reeds

gestart worden met de data die door de index wordt aangeleverd en kunnen in het gesprek worden aangevuld. Daarnaast kan het per situatie verschillen welke gegevens als minimaal noodzakelijk aangemerkt dienen te worden. Zo is het denkbaar dat er gevallen zijn waarbij de IZB-arts aan de hand van alleen de naam en de kennis dat het bijvoorbeeld om een 'broer' gaat, het voldoende informatie is om de betreffende persoon op te zoeken in bestaande data uit HPZone. Indien de index een upload wil uitvoeren waarbij niet minimaal een e-mailadres of telefoonnummer is ingevuld, dan vraagt de 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, bijzondere of wettelijk identificerende) het gaat. Hoewel in de applicatie geen sprake is van opname van informatie over het ziektebeeld en het welbevinden van de index (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.[7]

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

Persoonsgegeven	**Gewoon persoonsgegeven**	**Bijzonder persoonsgegeven**	**Index en/of contact**	**Toelichting noodzaak**
Voor- en achternaam	Ja	Ja, zie toelichting hierboven.	Contact/Index	A
Telefoonnummer	Ja	Ja, zie toelichting hierboven.	Contact/Index	A
E-mailadres	Ja	Ja, zie toelichting hierboven.	Contact	A
Datum laatste contactmoment	Ja	Ja, zie toelichting hierboven.	Contact/Index	E

[7] Artikel 9 lid 1 AVG en de daarop van toepassing zijnde overweging 35 AVG.

Risicoclassificatie[8]	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[9] **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

[8] Risicoclassificatie betreft een drietal vragen om de classificatie te beoordelen. De vragen betreffen of de index in hetzelfde huis woont of langer dan 12 uur op dezelfde plek is geweest. Hoe lang de index en het contact bij elkaar waren en of de index en het contact binnen 1,5m van elkaar zijn geweest. Er zijn 4 mogelijke uitkomsten: 1) Huisgenoten, 2a) Overige nauwe contacten, 2b) Overige nauwe contacten, 3) Overige (niet nauwe) contacten. Indien de BCO-medewerker de risicoclassificatie niet al bij het telefoongesprek met index heeft vastgesteld, moet index deze bepalen a.h.v. een drietal vragen. Indien de BCO-medewerker de risicoclassificatie al heeft vastgesteld, wordt dit in het BCO Portaal opgeslagen en niet meer naar GGD Contact gestuurd.

[9] 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 onderzoeken die RIVM uitvoert t.a.v. COVID-19 pandemie (ook wel 'Osiris-vragenlijst' genoemd)
2. Uitbreiding gebruik voor alle indexen:
    a. Alle gegevens in het portaal zijn bewerkbaar en invulbaar door de BCO-medewerker in een portaal.

De noodzakelijkheid van het verzamelen van de gegevens voor het volledige BCO-gesprek en de 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.

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 de 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 de GGD Contact App zich niet beperkt tot BCO in het kader van COVID-19.

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

De verwerking van persoonsgegevens aan de hand van de GGD Contact App gebeurt daarom ook ten behoeve van de vervulling van de taak van algemeen belang van de GGD'en (als bedoeld in artikel 6, eerste lid, aanhef en onder e, AVG jo. artikel 6, eerste lid, onderdeel c jo. artikel 14 Wpg)

Voor zover bijzondere persoonsgegevens worden verwerkt kunnen de GGD'en gebruik maken van de doorbrekingsgrond uit artikel 9, tweede lid, aanhef en onder i, AVG.

VWS
Naast de wettelijke taak van de GGD'en tot het uitvoeren van de BCO, heeft de minister van VWS op basis van artikel 3, eerste lid, Wpg de taak om de kwaliteit en doelmatigheid van de publieke gezondheidszorg te bevorderen, en zorg te dragen voor de instandhouding en verbetering van de landelijke ondersteuningsstructuur. Daarbij geeft de minister van VWS op basis van artikel 7, eerste lid, Wpg leiding aan de bestrijding van infectieziekten, waaronder COVID-19.

Bij de ontwikkeling van de GGD Contact 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 App en het BCO Portaal 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 de GGD Contact App sprake is van de verwerking van (bijzondere) persoonsgegevens.

Zelfstandige verwerkingsverantwoordelijkheid GGD'en & Verwerkerschap VWS (praktijkfase)
Na het afronden van de realisatiefase, en de ingebruikname van de GGD Contact App 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.[10] Daarnaast stelt de index het doel en de middelen van de verwerking niet vast. De index heeft de keuze uit de aangereikte middelen van de GGD om deel te nemen aan BCO en ten behoeve hiervan verstrekt de gegevens aan de GGD.

Contacten - betrokkene
De contacten waarvan persoonsgegevens worden verwerkt zijn evenals de index aan te merken als een betrokkene van wie de persoonsgegevens in GGD Contact en de bijbehorende datasluis en het BCO 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.

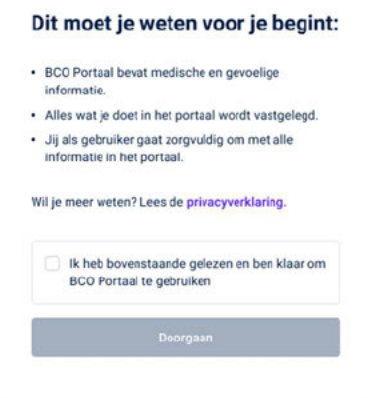
[10] Artikel 2 AVG.

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. Deze logging van deze persoonsgegevens over de BCO-medewerkers worden verwerkt in het kader van de veldnormen voor gegevensverwerking in zorg, die volgen uit de NEN7513. De BCO Portaal Gebruiker wordt over deze logging geïnformeerd bij het eerste gebruik via het volgende scherm en via de privacyverklaring BCO Portaal (zie hieronder het bijbehorende scherm).



4. Gegevensverwerking

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

Stap	Uitwerking
1	**Verificatie identiteit index**
	Het BCO is aan de orde vanaf het moment dat er een melding van infectieziekte is gedaan.[11] Het BCO-proces begint bij de BCO-medewerker die telefonisch contact opneemt met de index.[12]

[11] Het doen van deze melding na vaststelling van een ziekte als COVID-19 is bij wet verplicht, artikel 22 Wpg.
[12] Hierbij wordt de identiteit van de index geverifieerd. Dit gebeurt door middel van naam, geboortedatum en telefoonnummer.

2	**Verzoek om GGD Contact App te downloaden**
	Ten tijde van het telefonisch contact met de index vraagt de BCO-medewerker aan de index of hij bereid is om GGD Contact App te downloaden. a) Indien de index ervoor kiest GGD Contact niet te downloaden, wordt het reguliere BCO-proces gevolgd. Doordat de volledige BCO-vragenlijst is opgenomen in het BCO Portaal kan de BCO-medewerker het BCO Portaal zowel bij gebruiken bij een index die de app wel gebruikt als bij een index die de app niet gebruikt. b) Indien de index ervoor kiest om GGD Contact wel te downloaden, dan volgt stap 3. De index kan ook op eigen initiatief de GGD Contact App reeds hebben gedownload vóór het telefonisch contact met de BCO-medewerker.
3	**Index downloadt GGD Contact App**
	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.[13]
4	**Privacyverklaring wordt getoond**
	De index krijgt voordat hij akkoord gaat met het gebruik van GGD Contact een privacyverklaring te zien. Deze privacyverklaring is tevens te allen tijde binnen GGD Contact gemakkelijk terug te vinden en kan zo worden teruggelezen door de index. Zo is in GGD Contact de tekst opgenomen: 'Help bij het bron- en contactonderzoek. Gegevens blijven op jouw telefoon totdat je ze deelt met de GGD. Lees meer in de privacyverklaring'. Met hierbij een link naar de privacyverklaring. In de tekst op de GGD-website die verwijst naar het bestaan van de app is ook opgenomen dat het gebruik van GGD Contact vrijwillig is. Ook in de werkinstructie en e-learning voor BCO-medewerkers is opgenomen te benadrukken dat het gebruik van GGD Contact vrijwillig is.
5	**ZelfBCO door de index**
	• Indien de index op eigen initiatief de App heeft gedownload start het gebruik van de app met het ZelfBCO.

[13] 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.

	• De index selecteert zijn klachten uit een lijst met COVID-19 gerelateerde klachten en voert de datum in dat de klachten zijn begonnen. Op basis hiervan wordt de besmettelijke periode vastgesteld. • Indien er geen klachten zijn, voert de index de testdatum in. • Wanneer de index de eerste ziektedag niet wil invullen kan je de app niet gebruiken. Hiervoor is gekozen omdat zonder inzicht in de besmettelijke periode het verzamelen van de contacten niet nuttig/mogelijk is. Indien er vooraf contact is geweest met de GGD en de informatie omtrent de eerste ziektedag reeds bekend is, dan wordt deze vraag niet opnieuw in de GGD Contact App gesteld. • 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.
6	**BCO-medewerker vult contactenlijst in het BCO Portaal**
	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. De BCO-medewerker maakt een nieuwe case aan indien de index niet reeds bekend is en noteert: • Naam index • Telefoonnummer index • Casenummer De BCO-medewerker maakt een eerste aanzet voor de contactenlijst van de index en noteert: • Laatste contactdatum • Context • Risicocategorie Op de achtergrond wordt aan deze gegevens de technische velden 'bron' en 'type' gekoppeld. Dit is niet zichtbaar voor de BCO-medewerker.

	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.
7	**BCO-medewerker registreert BCO-vragenlijst + Osiris Vragenlijst**
	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. Indien de index de app wel gebruikt volgt stap 8 en wordt het voorbereide contactlijstje uit stap 7 gedeeld met de index middels een activatiecode.
8	**Activatiecode wordt verstrekt**
	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. 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.
9	**Invoer activatiecode door index**
	Tijdens of na het telefoongesprek kan de index de door de BCO-medewerker verstrekte activatiecode in de GGD Contact App invullen.
10	**Verificatie van de activatiecode**
	Er vindt een verificatie van de activatiecode plaats tussen de GGD Contact App en de backend.
11	**Contactenlijst wordt vanuit de backend opgehaald**
	De vooraf opgestelde contactenlijst wordt tijdens het telefoongesprek van de BCO-medewerker met de index vanuit de backend naar GGD Contact App opgehaald.
12	**Ophalen contactenlijst door de index**

	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.
13	**Toestemming voor toegang tot contacten**
	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." 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. 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. 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.
14	**Aanvulling contacten door de index**
	Voor de index is aan de hand van de reeds opgehaalde contactenlijst inzichtelijk welke contactgegevens hij dient aan te vullen. Indien er toestemming is verleend voor het importeren van de contactenlijst uit het adresboek van de telefoon van de index, stelt 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). De index wordt gevraagd om de volgende gegevens in te vullen in de GGD Contact App: • Contactgegevens van het contact van de index

	• Soort contact. Hier worden vragen gesteld over de ontmoeting met het contact, waardoor het contacttype wordt bepaald. Dit wordt bepaald door de beantwoording van de vragen (exacte vragen zijn aan verandering onderhevig door de geldende LCI-richtlijn): ○ langer dan 12 uur op dezelfde plek als het contact geweest (Ja/Nee) ○ langer dan 15 minuten in dezelfde ruimte als het contact geweest (Ja/Nee) ○ dichter dan 1,5 meter bij het contact geweest (Ja/Nee) *Hierbij maakt het niet uit of het een kort of langdurig moment is geweest waarbij je dichter dan 1,5 meter bij het contact bent geweest.* [14]
15	**Aanlevering nieuwe contacten door index**
	Het is voor de index mogelijk om nieuwe contacten aan te leveren die nog niet door de BCO-medewerker in de contactenlijst zijn opgenomen. Dit is mogelijk op één van de hiervoor beschreven manier namelijk: ophalen uit het adresboek van de telefoon van index of handmatig invoeren.
16	**Risico-inschatting 'soort contact' door index**
	Wanneer de index een nieuw contact invoert in 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/handelingsperspectief voor deze contactpersoon verschijnt. De risico-inschatting vindt plaats door het stellen van onderstaande vragen aan de index, welke hij in GGD Contact beantwoordt: 1. Woon je in hetzelfde huis of ben je langer dan 1 uur op dezelfde plek geweest? (Ja/Nee). 2. Hoe lang waren jullie waarschijnlijk bij elkaar in de buurt? Langer dan 15 minuten/korter dan 15 minuten. a. Bij het antwoord "korter dan 15 minuten" krijgt de index de vervolgvraag, namelijk: Is een of meerdere van deze dingen tijdens jullie ontmoeten gebeurd? - In je gezicht geniesd - Geknuffeld of gezoend - Ander lichamelijk contact Het antwoord kan zijn: Ja, één of meerdere dingen/Nee, denk het niet.

[14] Deze indicatie wordt aangepast aan de hand van de geldende LCI-richtlijn.

	3. Zijn jullie binnen 1,5 meter van elkaar geweest? Het antwoord kan zijn: Ja, denk het wel/Nee, denk het niet. Wanneer was de laatste ontmoeting?
17	**Verschijnen van leefregels/handelingsperspectief**
	Wanneer de index alle informatie omtrent de persoon waarmee hij in contact is geweest, heeft ingevuld, verschijnen de leefregels – ook wel het handelingsperspectief – voor dit specifieke contact. Hierin kan bijvoorbeeld zijn opgenomen dat het betreffende contact wordt geadviseerd om nog 5 dagen in quarantaine te verblijven. De leefregels/handelingsperspectief zijn/is afhankelijk van risicoclassificatie (het soort contact) en de datum van het laatste contact met de index. Zie het protocol van het RIVM[15] voor het handelingsperspectief per risicoclassificatie (huisgenoot/nauw contact/overig contact).
18	**Delen van de/het leefregels/handelingsperspectief door index**
	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.
19	**Controlevraag voor het informeren van het contact**
	Wanneer de index het contact heeft toegevoegd en de leefregels heeft ingezien en vervolgens een nieuw contact wil toevoegen, stelt GGD Contact eerst een controlevraag, namelijk: "Heb jij het contact geïnformeerd en de leefregels gedeeld?". Hierop kan de index antwoorden: - Ja; - Nee, doe ik later; - Nee. De keuze van de index op deze vraagstelling wordt opgeslagen in GGD Contact, zodat indien nodig de BCO-medewerker contact kan opnemen met het contact indien de index dit (nog) niet heeft gedaan.
20	**Opslag gegevens in de sluis**
	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

[15] https://lci.rivm.nl/COVID-19-bco

	vanuit GGD Contact aan het BCO Portaal worden doorgegeven. De sluis zorgt voor de koppeling tussen het device van de index en het BCO Portaal van de BCO-medewerker. 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.
21	**Verzending contactenlijst naar BCO Portaal**
	Nadat de index de contactenlijst heeft ingevuld, kan hij op de 'ik ben klaar'-button/'verstuur gegevens naar GGD' drukken. 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. 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.
22	**Verdeling casenummers onder BCO-medewerkers door werkverdeler**
	De werkverdeler van de GGD verdeelt de ontvangen contactenlijsten op basis van een casenummer onder de BCO-medewerkers.
23	**BCO-medewerker beoordeelt risicoclassificatie**
	Bij handmatige invoer van contacten door de index, checkt de BCO-medewerker of de risicoclassificatie juist is ingevuld.
24	**BCO-medewerker kan contact opnemen met contact van index**
	Wanneer de BCO-medewerker het nodig acht om bijvoorbeeld nog gegevens aan te vullen van een contact in het BCO Portaal, kan de BCO-medewerker contact opnemen met het betreffende contact. Tevens kan de BCO-medewerker een handelingsperspectief delen met het contact als hier aanleiding voor is.
25	**Nieuwe gegevensaanlevering door index**
	Het kan voorkomen dat de index zich op een later moment bedenkt dat hij tevens met nog een nieuw contact in contact is geweest gedurende de 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.
26	**(Handmatige) koppeling gegevens aan HPZone Lite GGD**
	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. 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.
- Daar waar GGD Contact (de applicatie zelf) voor de index is bedoeld, is het BCO Portaal voor de BCO-medewerkers bedoeld om contactenlijsten klaar te zetten voor de index. Hierdoor neemt de tijdsbesteding aan het BCO af, waardoor in tijden van grootschalige infectieziektebestrijding een BCO-medewerker meer werk aankan.

Door het geheel van de verwerkingen (in 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.[16] 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.[17]

[16] 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.

[17] Artikel 12 lid 1 sub c IVESCR.

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.[18] 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.[19] Het belang van de GGD bij het inzetten van GGD Contact het op een snelle wijze verkrijgen van de gegevens voor BCO waardoor efficiënter kan worden gewerkt. Dit bespaart de BCO-medewerkers tijd en vermindert de kans op fouten nu voor BCO relevante gegevens niet telefonisch hoeven te worden doorgegeven en vervolgens genoteerd. Het snel kunnen starten van BCO (door middel van GGD Contact) draagt bij aan infectieziektebestrijding wat weer een taak is van de GGD.[20]

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

[18] Artikel 7 lid 1 Wpg.
[19] Artikel 6 lid 1 sub c Wpg.
[20] De uitvoering van algemene infectieziektebestrijding is wederom een taak van de GGD, artikel 6 lid 1 Wpg jo artikel 14 Wpg.

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". [21] 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:
- Werkverdeler
- BCO-medewerker

Geen hoog-risico verwerkingen

Ten aanzien van de verwerkingen binnen GGD Contact wordt van geen van de onderstaande technieken gebruik gemaakt:

- Analyse van databestanden op persoonsniveau
- (Semi-)geautomatiseerde besluitvorming

[21] Artikel 2 Statuten GGD GHOR Nederland.

- 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.[22] 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.

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)

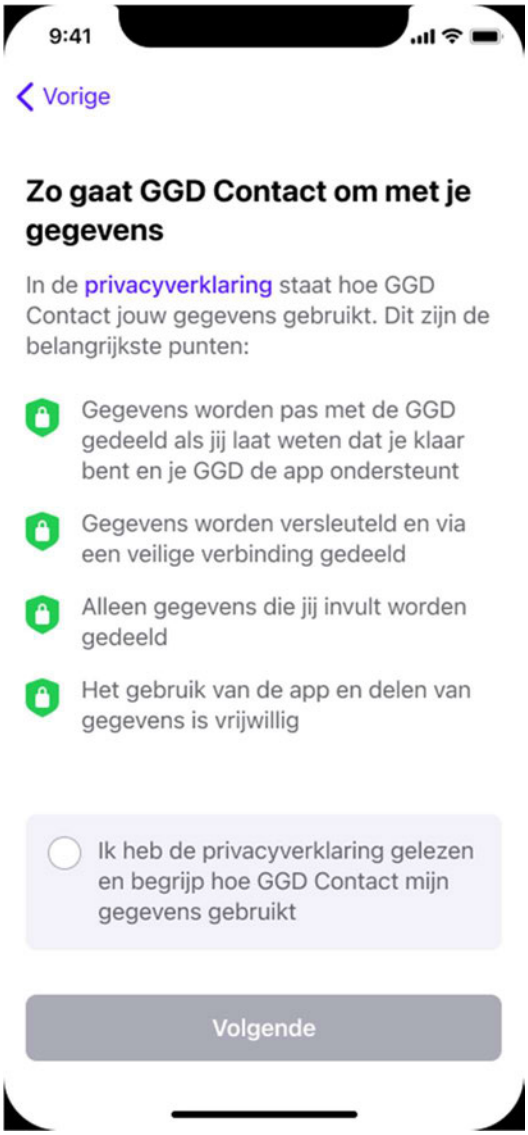
Op grond van artikel 11.7a van de Telecommunicatiewet (hierna: Tw) is het via een elektronisch communicatienetwerk (zoals internet) plaatsen of uitlezen van informatie op een randapparaat,

[22] Overweging 91 AVG.

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 een termijn tot 5 jaar na de datum waarop het dossier is aangemaakt waarin het uitsluitend in gepseudonimiseerde vorm bewaard wordt
- Applicatie-logging: 5 jaar na de datum waarop de logging is aangemaakt

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

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[23] waarvoor de veiligheidsregio's verantwoordelijk zijn.[24] De uitvoering van BCO is vervolgens een wettelijke taak van de GGD'en.[25] De wettelijke taak om BCO uit te voeren betreft niet de wettelijke plicht om persoonsgegevens te verwerken. Bij wet- regelgeving is immers niet bepaald hoe het BCO-proces dient te worden uitgevoerd en welke gegevensverwerking hiervoor nodig is.

Van de wettelijke mogelijkheid[26] 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[27] 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[28] 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

[23] Artikel 1 Regeling 2019-nCoV. Meldingsplichtige ziekten zijn verdeeld over de groepen A, B1, B2 en C. Deze indeling is gebaseerd op de mate waarin dwingende matregelen opgelegd kun worden om de bevolking te bescherming. Bij groep A zijn mogelijke wettelijke maatregelen: gedwongen opname tot isolatie of thuisisolatie, gedwongen onderzoek, gedwongen quarantaine (inclusief medisch toezicht), verbod van beroepsuitoefening. Zie: https://www.rivm.nl/meldingsplicht-infectieziekten/welke-infectieziekten-zijn-meldingsplichtig voor een recent overzicht van ziekten die onder groep A vallen.
[24] Artikel 6 lid 2 Wpg.
[25] Artikel 6 lid 1 sub c Wpg jo artikel 13 Wpg.
[26] 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.
[27] Artikel 11 Nota van toelichting bij Besluit publieke gezondheid.
[28] https://lci.rivm.nl/COVID-19-BCO

van een taak van algemeen belang of een taak in het kader van de uitoefening van het openbaar gezag.[29] 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.[30] 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"[31] 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 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".[32]

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.[33] 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

[29] Artikel 6 lid 1 sub e AVG.
[30] Artikel 7:454 Burgerlijk Wetboek (Wgbo)
[31] Artikel 7:446 lid 1 Burgerlijk Wetboek (Wgbo)
[32] 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.
[33] Kamerstukken II 2017/18, 34 851, nr. 3, p. 43 (MvT bij UAVG).

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 van ambt of beroep of wettelijk voorschrift aan geheimhouding zijn verbonden.[34]
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.[35] 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. [36]

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

Ambtenaren leggen de eed af of doen de belofte[41] waardoor ambtenaren verplicht zijn tot geheimhouding van hetgeen hen in verband met hun functie ter kennis is gekomen.[42] Medewerkers van de GGD zijn ambtenaren die werkzaam zijn op basis van een arbeidsovereenkomst en omdat

[34] Artikel 2:5 lid 1 Awb.
[35] Artikel 2:5 lid 2 Awb.
[36] Zie Toelichting Besluit Ambtenarenwet 2017
[37] Artikel 14 lid 1 en 2 Wpg.
[38] Zie toelichting bij artikel 2 Uitvoeringsbesluit Ambtenarenwet 2017.
[39] A-orgaan = een orgaan van een rechtspersoon die krachtens publieksrecht is ingesteld (art 1:2 lid 1 sub a Awb)
[40] Artikel 1 Ambtenarenwet 2017.
[41] Artikel 7 Ambtenarenwet 2017.
[42] Artikel 9 Ambtenarenwet 2017

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.[43] 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.[44] Een maatregel die hieraan voldoet betreft het eerder genoemde BCO-protocol. Dit protocol vloeit voort uit lidstatelijk recht, is duidelijk en nauwkeurig opgesteld en wordt door de GGD'en gevolgd. In dit BCO-protocol zijn voldoende passende en specifieke maatregelen opgenomen ter bescherming van de rechten en vrijheden van betrokkenen. Bijvoorbeeld de expliciete aandacht voor verwerking van gegevens van kinderen en/of met een kinderopvang welke is opgenomen in het protocol.

Concluderend met betrekking tot de grondslag kan worden geoordeeld dat de GGD (bijzondere) persoonsgegevens mag verwerken voor BCO op basis van artikel 6 lid 1 sub e jo. 9 lid 2 sub i AVG.

<u>Rechtsgrond monitoring en logging</u>
Alle handelingen van BCO-medewerkers in BCO Contact worden gelogd. 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, SIEM, wettelijk voorgeschreven audit, vreemde apparaten);
- Het vinden van de oorzaak van een foute werking van het systeem (debugging).
- Capaciteitsbeheer (statusinformatie en monitoring van SLA-afspraken).

De monitoring van de logging vindt plaats onder verantwoordelijkheid van de GGD'en. Als wettelijke grondslag voor deze verwerking is gekozen voor artikel 6 lid 1 sub f AVG (gerechtvaardigd belang). Dit belang bestaat uit het de verplichting van de verwerkingsverantwoordelijke om passende technische en organisatorische maatregelen te nemen ter bescherming van de verwerkte persoonsgegevens. Omdat in het BCO portaal verwerking van gezondheidsgegevens plaats vindt, is de veldnorm die hiervoor geldt NEN7510, die m.b.t. logging nader is uitgewerkt in NEN 7513. BCO Portaal voldoet aan deze eisen. Naast de verplichting van de verantwoordelijke om de gegevens adequaat te beveiligen, is tevens het belang relevant dat betrokkenen hebben bij een zorgvuldige gegevensverwerking.

[43] Overweging 41 AVG.
[44] EHRM 26 april 1979, *NJ* 1980/146 (Sunday Times)

Het bijhouden en monitoren van logfiles is noodzakelijk om de hierboven genoemde redenen. Om de impact van het inzien van de logging door medewerkers die met de monitoring zijn belast te beperken, worden medewerkersgegevens in het dashboard primair alleen gepseudonimiseerd getoond. Nadere analyse van een achterliggend dossier is alleen mogelijk door een medewerker die de rol van compliance officer heeft. De impact die de verwerking van medewerkersgegevens heeft op de betrokkenen wordt daarmee zo veel mogelijk beperkt.

Gezien het belang dat de verwerkingsverantwoordelijke en de betrokkenen hebben bij een veilige verwerking van de gegevens, en de relatief kleine inbreuk van de impact op de belangen van betrokkene, wordt deze verwerking als acceptabel beoordeeld.

12. Doelbinding

De verwerkingen die binnen GGD Contact, de datasluis en het BCO Portaal plaatsvinden, zijn bedoeld om het BCO-proces ten behoeve van infectieziektebestrijding, efficiënter en sneller te laten verlopen. De doelbinding is als dusdanig beschreven in de privacyverklaring GGD Contact (App en BCO Portaal voor GGD'en).

13. Noodzaak en evenredigheid

Bij het ontwikkelen van de GGD Contact is rekening gehouden met de beginselen proportionaliteit ('Staat het doel in verhouding tot de inbreuk?') en subsidiariteit ('Is dit de beste/minst ingrijpende manier om het doel te bereiken?').

Proportionaliteit: GGD Contact is opgebouwd om het BCO-proces te ondersteunen, te versnellen en het registreren van de gegevens van de contacten zorgvuldiger te laten verlopen. Daarnaast voldoet het huidige systeem dat gebruikt wordt voor de registratie van deze gegevens niet aan de vereiste gegevensbeschermende waarborgen. Dit is een van de reden om een alternatieve voorziening voor te bereid. Release 1.1. biedt op korte termijn de door de product owners gewenste functionaliteit en is daarnaast de voorbereidende release op de vervanging van HPZone Lite. 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. <u>Opslag in onvoldoende beveiligde systemen</u>

Opslag van (bijzondere) persoonsgegevens vindt plaats op onvoldoende beveiligde systemen (systemen die niet voldoen aan de IB-standaarden zoals NEN7510/BIO) binnen de procesketen met mogelijke inbreuken tot gevolg.

- De kans dat dit risico zich manifesteert zonder maatregelen is Middel. Betrouwbare en bekende partijen worden ingeschakeld om de opslag van de GGD Contact 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 invloedsfeer van de GGD'en, dit betreft acties van kwaadwillenden, welke mogelijkheid blijft bestaan.

6. *Te lange bewaartermijnen*

Persoonsgegevens worden onnodig lang bewaard door het niet naleven van bewaartermijnen.

- De kans dat dit risico zich manifesteert zonder maatregelen is Middel. Door de drukte bij GGD'en is het denkbaar dat gegevens langer dan nodig in het web 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 authentiseren/verifiëren van de index voordat door BCO-medewerker gegevens in dossiers worden ingevoerd door middel van een koppeling van een casenummer op de achtergrond.
    - Invoer van gegevens op aangeven van de index is pas mogelijk na een positieve test. Bij deze test is de index reeds geverifieerd aan de hand van geldig ID-bewijs bij het doen van een coronatest.
- Plausibiliteitschecks invoeren (bekende Nederlanders etc.). Bij twijfelt dient door de BCO-coördinator meegekeken te worden (werkinstructie), eventueel wordt de index nogmaals benaderd. Hiervoor dient een werkbare definitie te worden opgesteld, indien nog niet aanwezig ter voorkoming van dubbel werk voor de coördinator.

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-learing 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. <u>Data index en contact niet beschikbaar</u>

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. <u>Onvoldoende veilig ingerichte koppelingen</u>

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

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

Geadviseerd wordt om de volgende maatregelen te nemen:

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

Risico voor Betrokkene (voor maatregelen)	Hoog

Risico voor Betrokkene (na maatregelen)	Laag

19. <u>Verwerken persoonsgegevens indexen die buiten RIVM Protocol vallen</u>

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

Met alle betrokken partijen die aangemerkt kunnen worden als verwerker dient een verwerkersovereenkomst te worden gesloten tussen GGD'en (mogelijk met GGD GHOR Nederland als facilitator) en de verwerkers. Dit betreft de hostingpartij Intermax.

- De kans dat dit risico zich manifesteert zonder maatregelen is Hoog. Momenteel is met nog niet alle partijen, zoals de hostingpartij, een verwerkersovereenkomst gesloten.

- De impact van dit risico zonder maatregelen is Hoog. Het ontbreken van verwerkersovereenkomsten zorgt voor een ongecontroleerde deling van gegevens met derden waardoor misbruik van gegevens mogelijk is. Tevens is het ontbreken van verwerkersovereenkomsten in strijd met de AVG

Geadviseerd wordt om de volgende maatregelen te nemen:

- Opstellen van contractuele afspraken met name verwerkersovereenkomsten indien er sprake is van een verwerkingsverantwoordelijke – verwerker rolverdeling.
- Inrichten van Governancestructuur (leveranciersmanagement):
    - Inrichten stuurgroep tijdens ontwikkelfase
    - Controle en evaluatie op de nakoming van contractuele afspraken in ontwikkel- en beheerfase

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

21. Ontbreken vastlegging toestemming

De toestemmingsvraag in GGD Contact die aan de index wordt gesteld omtrent het ophalen van de adreslijst, wordt niet expliciet vastgelegd.

- De kans dat dit risico zich manifesteert zonder maatregelen is Hoog. Door de huidige instellingen in het ontwerp van GGD Contact wordt de keuze van het wel/niet gegeven van toestemming niet vastgelegd.
- De impact van dit risico zonder maatregelen is Hoog. Er wordt niet voldaan aan de verantwoordingsplicht in het kader van de AVG.

Geadviseerd wordt om de volgende maatregelen te nemen:

- Vastleggen en documenteren van wel/niet gegeven toestemming in GGD Contact op basis van een opt-in.

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

22. Toegang door derden in de GGD Contact

GGD Contact is niet met een wachtwoord beveiligd of anderszins beveiligd bij de toegang van de applicatie.

- De kans dat dit risico zich manifesteert zonder maatregelen is laag. Dit is een kans die zich 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. <u>Onduidelijkheid omtrent beheerstaken GGD GHOR Nederland</u>

Op het moment van schrijven van de DPIA is niet duidelijk welke beheertaken GGD GHOR Nederland op zich gaat nemen en hoe GGD GHOR Nederland deze taken gaat uitvoeren.

- De kans dat dit risico zich manifesteert zonder maatregelen is Hoog. Momenteel is niet duidelijk hoe de beheertaken door GGD GHOR Nederland uitgevoerd gaan worden.
- De impact van dit risico zonder maatregelen is Hoog. Doordat verantwoordelijkheden niet helder zijn kunnen o.a. privacy en informatiebeveiligingsvraagstukken omtrent het beheer blijven liggen of liggen deze elders waardoor er geen grip op is voor GGD GHOR Nederland en de GGD'en.

Geadviseerd wordt om de volgende maatregelen te nemen:

- Op de korte termijn verduidelijken en vastleggen van de beheertaken van GGD GHOR Nederland.
- Navolging van vastgestelde beheerstaken.

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

26. <u>Ontbreken van afspraken omtrent rolverdeling en verantwoordelijkheden</u>

Ten tijde van schrijven van deze DPIA zijn er nog geen afspraken gemaakt tussen de partijen over de verdeling van hun verantwoordelijkheden ten aanzien van de uitoefening van de rechten van betrokkenen en 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. <u>Strijd met het transparantiebeginsel, art 5.1 AVG</u>

Art. 13 AVG verplicht niet tot het verstrekken van een beschrijving van de functionaliteit, maar in de privacyverklaring as-is (zonder toevoeging functionaliteit 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. <u>Verwerking van klachten door GGD blijkt niet-noodzakelijk</u>

Door het niet onderbouwen van de noodzaak van de gegevens die vanuit het reguliere BCO worden uitgevraagd kan de noodzakelijkheid van het verwerken van de persoonsgegevens niet worden gewaarborgd.

- De kans dat dit risico zich manifesteert is Hoog. Naar aanleiding van navraag bij de GGD'en blijkt er géén DPIA te zijn van het reguliere BCO-proces.
- De impact van dit risico zonder maatregelen is Hoog. Er dient een adequate risicoanalyse uitgevoerd te worden op het regulier BCO-proces om de noodzaak van de uitgevraagde persoonsgegevens in beeld te krijgen om een onrechtmatige verwerking van gegevens te voorkomen.

Geadviseerd wordt om de volgende maatregelen te nemen:

- Uitvoeren DPIA regulier BCO/onderbouwing noodzaak van gegevens regulier BCO.

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 mogendheden en entiteiten bij de data kunnen.

47. Bewaartermijn by design inrichten

By design mogelijkheden onderzoeken om gegevens voor een bepaalde termijn houdbaar te maken in GGD Contact.

48. Periodieke kwaliteitscontrole op (afwijkingen) van het dossier
Zoals bijvoorbeeld rapportering door BCO-medewerker bij opvallen foutieve koppeling

49. Instellen pincode voorafgaande toegang GGD Contact

Toegang tot GGD Contact vooraf laten gaan door een zelf ingestelde pincode van de index.

50. Rolverdeling VWS
Vanuit gezamenlijke verantwoordelijkheid een convenant opstellen met de rol en verantwoordelijkheden van VWS daarin opgenomen.

51. Versleuteling van data op het device

Op het device van de index (telefoon/tablet) zal de data die de index heeft ingevoerd versleuteld worden opgeslagen waarbij gebruik gemaakt wordt van de beste versleutelingsmogelijkheden die het apparaat biedt. Dit betekent dat andere apps op het apparaat niet bij de gegevens kunnen komen en kunnen uitlezen wat er opgeslagen of verzonden is. Er is sprake van End-To-End versleuteling van de data in de GGD Contact App waarbij de decryptie in BCO Portaal pas plaatsvindt. Tevens is het hierdoor niet mogelijk dat de aan het internet aangesloten ontvangende server (de sluis) informatie kan ontlenen aan de verzonden informatie.

52. *Attack surface minimization*

Een minimaal aantal API's aan de buitenkant van de sluis aanbieden die vanaf het internet beschikbaar zijn. Hierdoor is er geen mogelijkheid om vanaf het internet de "achterkant" van het systeem te benaderen.

53. Toepassing TLS

Transport versleuteling (TLS) op alle verbindingen. Waarbij wordt versleuteld conform de meest veilige standaard/stand van techniek. Tevens een TLS pinning in de apps.

54. Certificaten vastleggen in applicatie

De gebruikte certificaten en/of de uitgever van het certificaat worden vastgelegd in de applicatie.

55. 2FA Identity Hub

Door middel van 2 factor authenticatie op de identity hub login is het zeker dat een medewerker niet alleen een username en password weet, maar tevens een geactiveerd device in het bezit heeft.

56. Ghost responses

Door gebruik te maken van ghost responses is het voor een hacker niet inzichtelijk of hij met een achterhaalde key succes heeft. Door gebruik te maken van niet van echt te onderscheiden antwoorden kan bij een niet-echte gebruiker (hacker) die een verzoek doet voor informatie wel een antwoord worden teruggegeven. Hierdoor is op het passief netwerk niveau niet te ontdekken of dit correcte data is.

57. Encryptie (at rest)

Encryptie van de (gevoelige) velden voordat deze in de database terecht komen. In de applicatie worden (privacygevoelige) velden versleuteld opgeslagen (zie hiervoor ook versleuteling van data op het device). Tevens at rest encryptie van secrets, data en logging. Hiermee wordt voorkomen dat er toegang tot de data mogelijk is.

58. Aanvulling van de privacyverklaring n.a.v. nieuwe functionaliteiten

De privacyverklaring moet worden aangevuld met een toelichting op de functionaliteit 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 ziektedag en test, aanleiding testen, herbesmetting.
  - Vaccinatie.
  - Gegevens evt ziekenhuisopname.
  - Onderliggend lijden, zwangerschap, post-partum.
  - Medicijnen en/of immuunrisico.
  - Vastleggen gegevens huisarts.
- **Woon & werkgegevens**
  - Alternatief verblijfadres
  - Index woont in instelling / AZC of andere risicolocatie
  - Mogelijkheid tot thuisisolatie
  - Werkgegevens (bedrijfsnaam, sector, vervolgvragen als index in besmettelijke periode gewerkt heeft)
  - School, kinderdagverblijf, gastouder incl hint om aan te maken als context
- **Brononderzoek**
  - Vastleggen van positief geteste bronpersonen (incl hpzone nummer), bronpersonen met coronagerelateerde klachten en aangeven welke een waarschijnlijke bron is.
  - Vastleggen broncontexten + bezoekdata, relatie tot context en of context waarschijnlijke besmettlingslocatie is.
  - Vastleggen settings die meestal geen context zijn (thuissituatie / bezoek, etc).
  - Buitenlandreizen (datums, landen, vervoermiddelen)
- **Contactonderzoek**
  - Link naar CoronaMelder portaal
  - Vastleggen contacten binnen besmettelijke periode
  - Schatting aantal categorie 3 contacten
  - Vastleggen contexten binnen besmettelijke periode.
  - Link naar meldportaal GGD Kennemerland voor vliegreizen in besmettelijke periode.

- **Afronden & status**

- Overzicht van alle verzamelde contacten en contexten.
- HPZone: Voor-ingevulde tabellen voor diagnostic notes en events index.
- HPZone: Voor-ingevulde tabellen voor contexten en contacten.
- De voor-ingevulde tabellen kunnen door de BCO-er naar het dossier van de index in HPZone worden gekopieerd.

Gestandaardiseerde zoekfunctie locaties/contexten

Epic-naam: Contexten

- Voor het vastleggen van contexten in bron- en besmettelijke periode maken we gebruik van een door VWS ontwikkelde schil om Google Maps en BAG voor het toevoegen van nieuwe ad-hoc contexten. Die zijn daarmee altijd voorzien van een uniforme naamgeving en actuele adresgegevens.
- Contexten in het BCO portaal zijn gestructureerd tot op afdelingsniveau. Bezoek datums en tijden worden gestructureerd vastgelegd.

Beknopte vragenlijst huisgenoten en nauwe contacten

Epic-naam: volledige vragenlijst inclusief contacten

- Vastleggen persoonsgegevens, aanvullen contactgegevens
- Vastleggen wie een contact informeert (GGD/Index)
- Verslag contactgesprek (klachten, vaccinatie, coronatest gedaan ja/nee)
- Vastleggen of een contact geïnformeerd is.

Cases die niet zijn afgerond aan anderen kunnen toewijzen

Epic-naam: nvt

- Gebruikers met de rol werkverdeler hebben een overzicht van cases waarvan het bco nog niet is afgerond en die op dit moment niet aan een specifieke medewerker zijn toegewezen. Deze cases kunnen worden toegewezen aan een medewerker.
- Gebruikers met de rol werkverdeler kunnen zien welke medewerkers met welke cases bezig zijn. Mochten ze daarin een medewerker tegenkomen die vandaag niet werkt, dan kunnen ze de case toewijzen aan een andere medewerker.

GGD Contact App met Zelf BCO mogelijkheid

Epic-naam: ZelfBCO App

Voor indexen is de GGD Contact App beschikbaar. Die kan op twee manieren gebruikt worden.

1. Voorafgaand aan het BCO gesprek. De index download de app direct na het vernemen van de positieve testuitslag. In de app wordt met behulp van een aantal vragen de besmettelijke periode vastgesteld (EZD of testdatum bij geen symptomen) en met behulp van een aantal geheugensteuntjes een reconstructie gemaakt van ontmoetingen in de besmettelijke periode. De gevonden contacten worden met behulp van een beslisboom gecategoriseerd in de juiste categorie (1,2a/2b/3a/3b) en per contact is obv de laatste contactdatum meteen het juiste advies zichtbaar. De index kan dit contact telefonisch doorgeven aan het contact, of via een zelfgekozen digitaal kanaal (copy/paste -- we mogen dit niet vanuit de app faciliteren).

   De EZD, symptomen en verzamelde contacten zijn tijdens het BCO gesprek met een GGD-er die het portaal gebruikt eenvoudig en veilig over te zetten naar het BCO portaal, en kunnen daar meteen verder verwerkt worden.

1. Na afloop van het eerste BCO gesprek. De index kan de tijdens het BCO gesprek geïnventariseerde contacten bekijken, contactgegevens aanvullen en deze gebruiken om het contact a) zelf te informeren of b) de gegevens met de GGD te delen. Deze functionaliteit is bruikbaar in alle fases van het BCO waarin GGD samen met index de contactinventarisatie doet. In fase 1/2a zijn de door de index aangeleverde gegevens bovendien te gebruiken om contact op te nemen met huisgenoten/nauwe contacten.

Bijlage 2 - Procesflow GGD Contact

Het proces voor deze DPIA start op het moment dat de index de GGD Contact App gaat downloaden voor de volledigheid is ook het proces van de index voorafgaand aan het downloaden van de GGD Contact App weergegeven. De voorgaande stappen hebben betrekking op de index die wacht op zijn of haar testresultaat naar aanleiding van een coronatest. Met betrekking tot onderstaande procesflow wordt per aangegeven stap het volgende toegelicht:

- App downloaden

De index wordt door de BCO-medewerker gevraagd om GGD Contact te downloaden. Dit kan na het verkrijgen van een positief testresultaat en/of tijdens het eerste BCO-gesprek.

- Eerste BCO-gesprek/ Tijdlijn creëren / Contacten inventariseren

In het eerste telefoongesprek met de BCO-medewerker wordt een eerste inventarisatie gemaakt van de personen met wie de index in contact is geweest. De tijdlijn wordt gecreëerd wanneer de klachten van de index zijn begonnen en met wie hij in deze periode in contact is geweest.

- Contacten classificeren

Door de BCO-medewerker vindt een eerste risicoclassificatie plaats ten aanzien van de contacten van de index. Aan de hand van hoelang en wat voor een soort contact de index met het contact heeft gehad wordt bepaald of het contact een huisgenoot, nauw contact of overig contact is. Dit bepaalt op een later moment welk handelingsperspectief er met het contact gedeeld dient te worden.

- Contactgegevens inventariseren in de app

Vervolgens vraagt de BCO-medewerker aan de index of hij de reeds opgestelde contactenlijst verder kan aanvullen in de app. Door middel van de activatiecode die de index door de BCO-medewerker verkrijgt is de contactenlijst zichtbaar in de GGD Contact App bij de index.

- Monitoren status contactgegevens en informeren

De BCO-medewerker kan vanaf het moment dat de contactenlijst naar de index is gestuurd tot aan het moment de index de gegevens heeft aangeleverd in 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

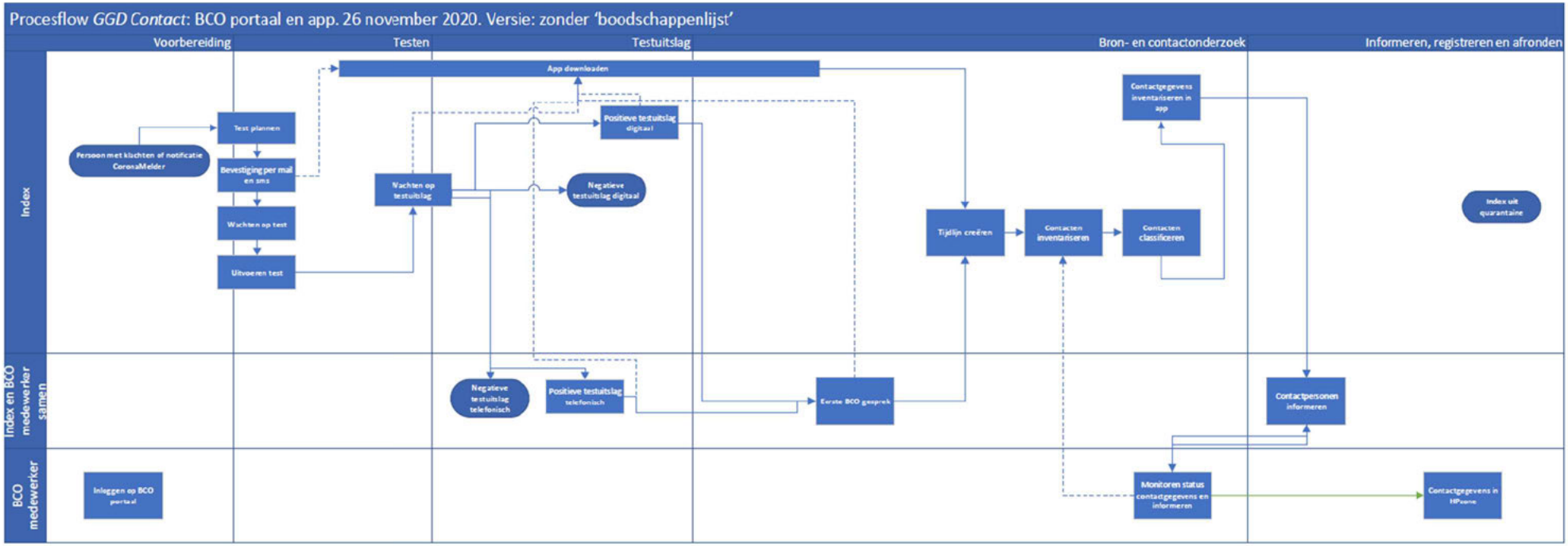
Indien de gegevens zijn aangeleverd door de index kan de BCO-medewerker een inventarisatie maken welke contacten geïnformeerd dienen te worden. Deze contactpersonen zullen worden geïnformeerd dat zij in contact zijn geweest met iemand die positief getest is op COVID-19 en nadere informatie krijgen in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

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: • Een kwaadwillende minimale inzet doet hiertoe; of • Een medewerker onbewust nalatig handelt of een fout maakt; of • Het inherent is aan het risico dat deze zich manifesteert.
Midden	Het risico voor betrokkene zal zich wellicht manifesteren indien: • Een kwaadwillende voldoende middelen inzet; of • Een medewerker bewust nalatig is of opzettelijk handelt; of • Het zeer waarschijnlijk is vanwege de aard van het risico
Laag	Het risico voor betrokkene zal zich enkel manifesteren indien: • Een kwaadwillende buiten proportionele middelen inzet; of • Een medewerker bewust zeer nalatig of opzettelijk handelt; of

Impact

De impact van een geëffectueerd risico wordt beschreven in termen van de mogelijke schadelijke gevolgen die de betrokkene kan ondervinden.

Impact niveau	Impact Beschrijving

Hoog	1. Kan de reputatie of belang van de betrokkene significant schaden, compromitteren of belemmeren; 2. Kan resulteren in sterfte of ernstig letsel; 3. Kan een grote inbreuk opleveren in de fundamentele rechten en vrijheid van betrokkene
Midden	1. Kan de reputatie of belang van de betrokkene schaden, compromitteren of belemmeren; 2. Kan resulteren in persoonlijk letsel; 3. Kan een inbreuk opleveren in de fundamentele rechten en vrijheid van betrokkene
Laag	1. Kan resulteren in beperkte materiële schade; 2. Kan de reputatie of belang van de betrokkene schaden 3. Kan een kleine inbreuk opleveren in de fundamentele rechten en vrijheid van betrokkene

Vervolgens vindt er een risico-calculatie plaats, waarna op basis van de risiconiveaus wordt bekeken welke soort maatregelen verwacht worden per niveau. Dit is reeds eerder beschreven in de DPIA.

Bijlage 4 – Logging

Logging van BCO Portaal zal plaatsvinden conform de vereisten en doeleinden van de NEN 7510 e.v.

Meer specifiek bevat dit de volgende persoonsgegevens:

- Accountgegevens
- Gegevens om de BCO Portaal Gebruiker te identificeren;
- Systeemactiviteiten van de BCO Portaal Gebruiker;
- Data, tijdstippen en details van belangrijke gebeurtenissen, bijv. in- en uitloggen;
- Identiteit of indien mogelijk de locatie van de apparatuur en de systeemidentificatie;
- Registratie van geslaagde en geweigerde pogingen om toegang te verkrijgen tot het systeem;
- Registratie van goedgekeurde en geweigerde gegevens en overige pogingen om toegang te verkrijgen tot bronnen van informatie.
- Systeemconfiguratieveranderingen;
- Gebruik van speciale bevoegdheden;
- Gebruik van systeemhulpmiddelen en -toepassingen;
- Bestanden die zijn geopend en het type toegang dat is verkregen;
- Netwerkadressen en -protocollen;
- Alarmen die worden afgegeven door het toegangsbeveiligingssysteem;
- Activering en de-activering van beschermingssystemen, zoals antivirussystemen en inbraakdetectiesystemen;
- Verslaglegging van transacties die door gebruikers in toepassingen zijn uitgevoerd.
- Case regio
- Regio BCO Portaal Gebruiker
- Rol BCO Portaal Gebruiker
- IP-adres BCO Portaal gebruiker

Van de GGD Contact App-gebruiker wordt een unieke ID gegenereerd bij het uploaden naar het BCO Portaal en deze unieke ID wordt gelogd.