DPIA:
NATIONALE CAPACITEIT Bron- & Contactonderzoek

November 2020

Data Protection Impact Assessment (DPIA) Nationale Capaciteit Bron- en Contactonderzoek (BCO)

- Landelijke referentie DPIA voor GGD'en -

Inleiding ... **3**

A. Beschrijving kenmerken gegevensverwerkingen ... **5**

1. Voorstel ... 5

2. Persoonsgegevens ... 6

3. Betrokken partijen en gegevensverwerking ... 9

4. Verwerkingsdoeleinden ... 18

5. Belangen bij gegevensverwerking ... 19

6. Verwerkingslocaties ... 19

7. Techniek en methode van gegevensverwerking ... 20

8. Juridisch en beleidsmatig kader ... 20

9. Bewaartermijn ... 20

B. Beoordeling rechtmatigheid gegevensverwerkingen ... **21**

10. Rechtsgrond ... 21

11. Bijzondere persoonsgegevens ... 21

12. Doelbinding ... 22

13. Noodzaak en evenredigheid ... 22

14. Rechten van betrokkenen ... 24

C. Beschrijving en beoordeling risico's voor de betrokkenen ... **25**

15. Risico's ... 25

D. Beschrijving voorgenomen maatregelen ... **36**

16. Maatregelen ... 36

E. Bijlagen ... **39**

Bijlage 1: Advies Functionaris Gegevensbescherming ... 39

Bijlage 2: Toelichting risico niveaus ... 40

Inleiding

Bron- en contactonderzoek (BCO) is een essentieel onderdeel van de bestrijding van de huidige COVID-19-pandemie. Effectief bron- en contactonderzoek verkort namelijk de duur tussen het ontstaan van klachten en het starten van isolatiemaatregelen en reduceert daarmee transmissie.[1] De uitvoering is een verantwoordelijkheid van het College van Burgemeesters & Wethouders (Art. 6, lid 1, sub c, Wet publieke gezondheid (Wpg)). De feitelijke uitvoering van bron- en contactonderzoek wordt echter gerealiseerd door de gemeentelijke gezondheidsdiensten (hierna GGD'en), zoals weergeven in de onderstaande afbeelding.



Bron: Kamerstuk 32620 nr. 132, Beleidsdoelstellingen op het gebied van Volksgezondheid, Welzijn en Sport.

Bron- en contactonderzoek kan pas geïnitieerd worden als er een melding is gedaan. In de Wpg is vastgelegd dat Groep-A-infectieziekten, zoals COVID-19, onverwijld na vaststellingen gemeld moeten worden door de behandelend arts en het laboratorium (Art. 22-25). Het doel van bron- en contactonderzoek is om zo snel mogelijk de bron van besmetting te achterhalen, contacten te identificeren, hen te informeren over de blootstelling en risico op besmetting, hen te wijzen op maatregelen die genomen moeten worden om verdere verspreiding te voorkomen en hen hierin te begeleiden.

De uitvoering van bron- en contactonderzoek is, in beginsel, de verantwoordelijkheid van de 25 regionale GGD'en. Sinds begin juni zijn de GGD'en drukdoende met het opschalen van hun capaciteit om te zorgen dat zij tijdig en adequaat BCO kunnen blijven uitvoeren ten tijde van stijgende besmettingspercentages. Om de verspreiding van het coronavirus binnen Nederland onder controle te krijgen en vervolgens te houden en het gewone maatschappelijke leven weer op gang te brengen, is het van belang dat in kaart wordt gebracht welke burgers positief testen, waar zij het virus hebben

[1] Bi Q, Wu Y, Mei S, Ye C, Zou X, Zhang Z, et al. Epidemiology and transmission of COVID-19 in 391 cases and 1286 of their close contacts in Shenzhen, China: a retrospective cohort study. Lancet Infect Dis. (27 April, 2020).

opgelopen, en met wie zij in contact zijn geweest. Het opschalingsplan van de GGD'en is gebaseerd op berekeningen van het RIVM over het verwachte aantal testaanvragen en het verwachte besmettingspercentage.

De aard en de omvang van de huidige COVID-19-pandemie vereisen een flexibele aanpak waarbij men adequaat kan inspelen op regionale uitbraken. Het Ministerie van Volksgezondheid, Welzijn en Sport (VWS) heeft juist daarom gekozen om, behalve de regionale opschaling, ook landelijke BCO-capaciteit in te schakelen zodat er ook op piekmomenten snel bron- en contactonderzoek uitgevoerd kan blijven worden. Wanneer een GGD capaciteitskrapte opmerkt, kan deze GGD een beroep doen op landelijke BCO-medewerkers die worden opgeleid en aangeleverd door externe callcenters. In het kader van nationale opschaling, zorgt GGD GHOR Nederland (hierna GGD GHOR) in opdracht van het Ministerie van VWS voor het realiseren van voldoende capaciteit door contractering van externe partners, waaronder Nederlandse alarmcentrales SOS International, Eurocross, VHD, ANWB en het Rode Kruis.

De inzet van externe partners betekent dat medewerkers van deze partners persoonsgegevens zullen verwerken voor de GGD'en. Deze landelijke partners verwerken de persoonsgegevens volgens een door GGD GHOR Nederland, in samenspraak met de praktijk en naar voorbeeld van de RIVM richtlijn, opgestelde landelijke richtlijn.

Disclaimer: het verloop van de COVID-19-pandemie is onvoorspelbaar, waardoor RIVM-protocollen en daarop gebaseerde BCO-processen onderhevig zijn aan continue ontwikkeling. Deze DPIA is gebaseerd op de informatie die beschikbaar was voor en tijdens de uitvoering van deze risicoanalyse (September, 2020). Raadpleeg de website van het RIVM voor de laatste versie van het BCO-protocol: https://lci.rivm.nl/COVID-19-bco

Deze DPIA is gericht op de nationale opschaling van het bron- en contactonderzoek. Het gaat hier dus om een risicoanalyse van de BCO-processen zoals uitgevoerd door de landelijke partners volgens de landelijke werkinstructie BCO. BCO-medewerkers van de regionale schil kunnen onderhevig zijn aan afwijkende instructies gezien de 25 GGD'en (nog) niet werken volgens een uniforme landelijke werkinstructie. Deze DPIA kan door GGD'en worden overgenomen en aangepast aan de eigen richtlijnen, waarbij op de aanpassingen een eigen risicoanalyse moet worden uitgevoerd.

Expliciet out of scope van deze DPIA is de verwerking van persoonsgegevens van BCO-medewerkers en overige werknemers van GGD GHOR, de GGD'en en andere externe partijen in het kader van de inhuur.

A. Beschrijving kenmerken gegevensverwerkingen

DPIA: landelijke format voor GGD'en

Het model gegevensbeschermingseffectbeoordeling Rijksdienst (PIA) is gebruikt als uitgangspunt voor het opstellen deze DPIA. GGD'en kunnen de inhoud van deze DPIA gebruiken en, indien nodig, DPIA aanpassen en/of aanvullen op basis van de situatie binnen de lokale GGD.

1. Voorstel

Aanleiding

De traditionele wijze van bron- en contactonderzoek is erg intensief. Tijdens deze COVID-19 pandemie kan, met het grote aantal bekende besmettingen, daarom extra capaciteit nodig zijn om het bron- en contactonderzoek snel uit te blijven voeren. GGD'en kiezen er daarom voor om landelijke BCO-capaciteit in te schakelen zodat op piekmomenten kan worden bijgeschakeld. Het college van Burgemeester en Wethouders blijft hierbij zorg dragen voor de uitvoering van infectieziektebestrijding, waaronder bron- en contactonderzoek (zie artikel 6 lid 1 sub c Wpg).

De Bestuurlijke Adviescommissie Publieke Gezondheid kan besluiten landelijke BCO-capaciteit te organiseren ter ondersteuning van GGD'en. Regionale GGD'en kunnen een hulpvraag neerleggen bij de landelijke projectorganisatie in het geval van capaciteitskrapte. Waar mogelijk worden BCO-medewerkers van de landelijke schil toegewezen aan een regionale GGD om zo capaciteitsdruk te verlichten. Deze medewerkers uit de landelijke schil van BCO-capaciteit komen te werken onder de verantwoordelijkheid van de regionale GGD'en door middel van een detacheringsconstructie.

Voorstel

Het Ministerie van VWS heeft aan GGD GHOR de opdracht gegeven uitvoering te geven aan de nationale opschaling van bron- en contactonderzoek. Meer specifiek houdt dit in: het realiseren van ondersteuning in mankracht (fte) voor het telefonisch bron- en contactonderzoek, het opleiden van de personen die deze ondersteuning gaan verrichten en het coördineren van deze ondersteuning bij het uitvoeren van het bron- en contactonderzoek ten behoeve van de bestrijding van COVID-19. De opdracht wordt door de Minister aan GGD GHOR verleend op grond van dwingende spoed in de zin van artikel 2.32 lid 1 sub c Aanbestedingswet 2012. De coördinatie en ondersteuning in fte voor het telefonisch bron- en contactonderzoek moet met de grootst mogelijke spoed worden verricht, waardoor het in acht nemen van algemene, maar ook verkorte termijnen, onmogelijk is.[2]

Dit bron- en contactonderzoek dient te worden uitgevoerd conform het Protocol bron- en contactonderzoek COVID-19 van het RIVM.[3] Dit protocol wordt gestart als een betrokkene positief wordt getest op COVID-19 en wordt door de GGD'en uitgevoerd. Hierbij initieert de GGD het bron-

[2] §1.4 Dienstverleningsovereenkomst ARVODI-2018, Contractnummer: 1707384-207088-PG, Verplichtingen-/referentienummer: 4067-23826.
[3] Raadpleeg deze website voor de laatste versie: https://lci.rivm.nl/COVID-19-bco

en contactonderzoek zo spoedig mogelijk nadat een melding van een patiënt met (laboratorium) bevestigde COVID-19 is ontvangen.

2. Persoonsgegevens

Door de BCO-medewerkers worden verschillende persoonsgegevens verwerkt onder verantwoordelijkheid van de GGD'en. Voor het bron- en contactonderzoek wordt een positief getest persoon aangeduid als 'index'. Het bron- en contactonderzoek start met het verzamelen van gegevens over de index en zijn/haar ziektebeloop (Tabel 1).

Vervolgens wordt, door ondervraging van de index, gepoogd om de bron van de besmetting te achterhalen (Tabel 2). Tot slot, wordt er contactonderzoek uitgevoerd waarbij er een onderscheid wordt gemaakt tussen huisgenoten (Tabel 3), nauwe contacten (Tabel 4) en overige contacten (Tabel 5). De persoonsgegevens die worden verzameld zijn allen noodzakelijk voor de accurate en volledige uitvoering van het bron- en contactonderzoek.

In de onderstaande tabel is per persoonsgegeven weergegeven om wat voor type persoonsgegevens (gewone, bijzondere of wettelijke identificerende) het gaat.

Informatie over index

Persoonsgegeven	**Gewoon persoonsgegeven**	**Bijzonder persoonsgegeven**	**Wettelijk identificerend persoonsgegeven**
Voornaam en achternaam	Ja		
Geboortedatum	Ja		
BSN			Ja
Telefoonnummer	Ja		
E-mailadres	Ja		
Naam huisarts	Ja		
Naam praktijk	Ja		
Locatie huisartsenpraktijk	Ja		
Datum testen	Ja		
Datum eerste ziektedag (EZD) of asymptomatisch		Ja	
Soort klachten vanaf EZD		Ja	
Aanwezigheid klachten		Ja	
Verloop van klachten		Ja	
Datum start besmettelijke periode		Ja	
Behoren tot medische risicogroep		Ja	

Sprake van gestoorde afweer		Ja	
Ziekenhuisopname (IC ja/nee + datum)		Ja	
Details ziekenhuisopname: naam ziekenhuis, adres ziekenhuis, naam behandelaar, contactgegevens behandelaar	Ja		
Indien overlijden: Datum overlijden en onderliggend lijden		Ja	
Huidige verblijfplaats (e.g. zorginstelling, asielzoekerscentrum, serviceflat, studentenhuis)	Ja	Ja, in sommige omstandigheden wel	
Beroep	Ja		
Betrokkenheid thuiszorg of mantelzorger en diens contactgegevens		Ja, in de meeste gevallen	
Settingen waar index is geweest (bv. werk, school, restaurant)	Ja		
Toestemming index om naam te noemen aan contacten	Ja		
Bijzonderheden BCO (bv. weigert samenwerking, onrust, taalbarrière)	Ja	Ja, in sommige gevallen	

Tabel 1: Informatie over Index

Contactpersoon: Indien het contact via de index namens een contactpersoon is gedaan, wordt de naam van de contactpersoon, het geslacht, de relatie tot index, telefoonnummer contactpersoon en e-mailadres contactpersoon, vastgelegd. Deze gegevens kwalificeren allemaal als gewone persoonsgegevens.

Brononderzoek

Persoonsgegeven	Gewoon persoonsgegeven	Bijzonder persoonsgegeven	Wettelijk identificerend persoonsgegeven
Contact met één of meerdere bewezen coronapatiënten?	Ja		
Volledige naam (geboorte- en partnernaam) bewezen coronapatiënt	Ja		
Geboortedatum bewezen coronapatiënt	Ja		
Indien bekend: HPzone-nummer en/of Osiris nummer van bewezen coronapatiënt	Ja		
Mensen in omgeving met klachten passend bij COVID-19	Ja		
Bezoek buitenland in 14 dagen voor aanvang EZD Zo ja: Noteren van data, land(en) en vervoersmiddel	Ja		

Tabel 2: Brononderzoek

Contactonderzoek

Huisgenoten

Persoonsgegeven	Gewoon persoonsgegeven	Bijzonder persoonsgegeven	Wettelijk identificerend persoonsgegeven
Voornaam en achternaam	Ja		
Geboortedatum	Ja		
BSN			Ja
Relatie tot index	Ja		
Telefoonnummer	Ja		
E-mailadres	Ja		
Laatste contactmoment	Ja		
Mogelijkheid isolatie		Ja	

Minimale datum einde quarantaine voor huisgenoten/gezin		Ja	

Tabel 3: Contactonderzoek huisgenoten

Nauwe contacten

Persoonsgegeven	**Gewoon persoonsgegeven**	**Bijzonder persoonsgegeven**	**Wettelijk identificerend persoonsgegeven**
Voornaam en achternaam	Ja		
Geboortedatum	Ja		
BSN			Ja
Telefoonnummer	Ja		
E-mailadres	Ja		
Datum laatste contact	Ja		
Aard laatste contact	Ja		

Tabel 4: Contactonderzoek nauwe contacten

Overige contacten

Persoonsgegeven	**Gewoon persoonsgegeven**	**Bijzonder persoonsgegeven**	**Wettelijk identificerend persoonsgegeven**
Voornaam en achternaam	Ja		
Datum laatste contact	Ja		
Soort contact	Ja		
E-mailadres	Ja		

Tabel 5: Contactonderzoek overige contacten

Voor de persoonsgegevens dient het volgende te worden opgemerkt. Indien een persoonsgegeven in de verzamelde set een bijzonder persoonsgegeven is, bijvoorbeeld een medisch gegeven, dan wordt de hele dataset gekwalificeerd als bijzondere persoonsgegevens. Dit betekent concreet bijvoorbeeld dat de naam dan ook wordt gekwalificeerd als een bijzonder gegeven als dit wordt verwerkt met een medisch gegeven.

3. Betrokken partijen en gegevensverwerking

Betrokken partijen en rolverdeling

In deze paragraaf wordt uiteengezet welke partijen betrokken zijn bij het bron- en contactonderzoek en in welke rol.

1. Ministerie van Volksgezondheid - Opdrachtgever

Het Ministerie van Volksgezondheid (in de vorm van de minister) is verantwoordelijk voor het leiding geven aan de bestrijding van epidemieën van infectieziekten categorie A (artikel 7 lid 1 Wpg). Op

basis hiervan zijn ze opdrachtgever aan GGD GHOR met betrekking tot de coördinering van de nationale opschaling van bron- en contactonderzoek. Er is hiervoor een formele opdracht opgesteld vanuit VWS aan GGD GHOR. Deze overeenkomst heet: *Dienstverleningsovereenkomst ARVODI-2018: Opdracht aan GGD-GHOR voor het realiseren in fte en coördineren van ondersteuning voor het telefonisch bron- en contactonderzoek*. De overeenkomst is getekend op 28 juni 2020 en is inwerking getreden met terugwerkende kracht per 1 juni 2020.

2. <u>GGD GHOR – Gezamelijke verwerkingsverantwoordelijke met GGD'en voor richtlijn en coördinatie – verwerker voor functioneel beheer</u>

GGD GHOR heeft van VWS de opdracht gekregen om een landelijke schil van BCO op te zetten die het mogelijk maakt dat landelijke BCO-medewerkers flexibel ingezet kunnen worden op momenten van capaciteitskrapte op regionaal niveau. Daarbij bepaalt GGD GHOR de landelijke richtlijnen op basis waarvan de landelijke BCO-medewerkers hun werk uitvoeren, coördineert ze incidenten en meldt deze in geval van landelijke incidenten, coördineert ze welke callcenters worden gecontracteerd en stelt ze eisen aan de beveiliging bij de callcenters en de inhuur van personeel. Omdat GGD GHOR een aandeel heeft in wie de werkzaamheden uitvoert en hoe de gegevens worden verwerkt door de landelijke procedures, wordt GGD GHOR hier gekwalificeerd als gezamenlijk verantwoordelijk met de GGD'en met betrekking tot de inzet en handelwijzen op basis van de landelijke richtlijnen van landelijke BCO-medewerkers.

GGD GHOR stemt de landelijke opschaling van bron- en contactonderzoek af met de GGD'en. Voor de opschaling zijn nog geen afspraken met de 25 GGD'en gemaakt, maar er wordt gewerkt aan een convenant waarin het proces en de verantwoordelijkheden worden vastgelegd.

Voor het fnunctioneel beheer, in dit geval het toekennen en intrekken van autorisaties, kan GGD GHOR gekwalificeerd worden als verwerker. GGD GHOR krijgt van de GGD of het callcenter het verzoek de autorisaties toe te kennen en deze ook weer in te trekken, zonder zelf een beoordeling te moeten uitvoeren met betrekking tot het toekennen van deze autorisaties.

3. <u>GGD – Gezamenlijk verantwoordelijk voor landelijke richtlijn en zelfstandig verantwoordelijk voor inzet medewerkers</u>

De regionale GGD'en zijn gezamenlijk verantwoordelijk voor de inzet van de landelijke BCO-medewerkers en de landelijke richtlijn.

GGD'en zijn zelfstandig verantwoordelijk voor het verstrekken en intrekken van autorisaties van de medewerkers en de uitvoering van de werkzaamheden volgens de richtlijnen van de eigen regio die de landelijke BCO-medewerker moet uitvoeren. Een BCO-medewerker van de landelijke schil wordt gedetacheerd bij een GGD op verzoek van desbetreffende GGD. De GGD'en bepalen dus de vraag naar nationale BCO-medewerkers en GGD GHOR, in samenwerking met een van de callcenters, coordineert het aanbod.

4. Callcenters – Verwerkers

De callcenter leveranciers stellen gezamenlijk de FTE-capaciteit voor de nationale opschaling van (telefonisch) bron- en contactonderzoek beschikbaar. Deze landelijke partners (callcenters) verwerken ten behoeve van de GGD'en persoonsgegevens van de index en contacten van de index om tijdige uitvoering van BCO te kunnen bewerkstelligen bij regionale capaciteitskrapte. Met de callcenters zijn verwerkersovereenkomsten gesloten, waarin onder andere is bepaald met welke systemen zij mogen werken en hoe personeel dient te worden gescreend.

De inzet van callcenters kan wisselen en is afhankelijk van de benodigde FTE-capaciteit. De huidige callcenters zijn: SOS International, ANWB, Eurocross, VHD, het Rode Kruis Yource en Teleperfomance.

5. RIVM – Zelfstandig verwerkersverantwoordelijke

Het RIVM krijgt gepseudominiseerde data aangeleverd om rapportages op te stellen die gebruikt worden als stuurinformatie voor indamming van de pandemie. Het RIVM bepaalt hoe deze gegevens worden geanalyseerd en worden ingezet voor rapportages/stuurinformatie. Osiris is het systeem van het RIVM waarin pseudoniem actuele infectie-en sterftecijfers bijgehouden worden. Osiris is gekoppeld aan HPzone Lite, maar de informatie moet wel actief naar het systeem verstuurd worden.

Om de effecten van het bron- en contactonderzoek te monitoren wordt dagelijks vanuit HPZone Lite informatie over contacten doorgegeven aan het RIVM. In HPZone Lite worden, in ieder geval, de volgende gegevens gerapporteerd per contact:

- persoonskenmerken (geslacht, geboortejaar, postcode);
- link aan index (Osiris-nummer) of situatie;
- categorie contact;
- eerste en laatste dag blootstelling;
- monitoringsperiode;
- belcontacten tijdens monitoringsperiode;
- ontstaan van klachten inclusief eerste ziektedag en soort klachten;
- afgenomen diagnostiek;
- GGD-regio.

6. Netherlands School of Public & Occupational Health (Hierna NSPOH) – Leverancier opleidingsmateriaal

NSPOH heeft het opleidingsprogramma ontwikkeld voor BCO-medewerkers en BCO-trainers. Daarnaast heeft NSPOH, in opdracht en met instructies van GGD GHOR, ter ondersteuning van het inwerken van nieuwe medewerkers voor bron- en contactonderzoek de e-learning 'bron- en contactonderzoek bij COVID-19' gemaakt. NSPOH levert enkel het opleidingsmateriaal, dit wordt door de betrokken organisaties geupload in de opleidingsomgeving. NSPOH verwerkt hierdoor geen persoonsgegevens.

7. Infact (leverancier HPZone Lite) – Verwerker

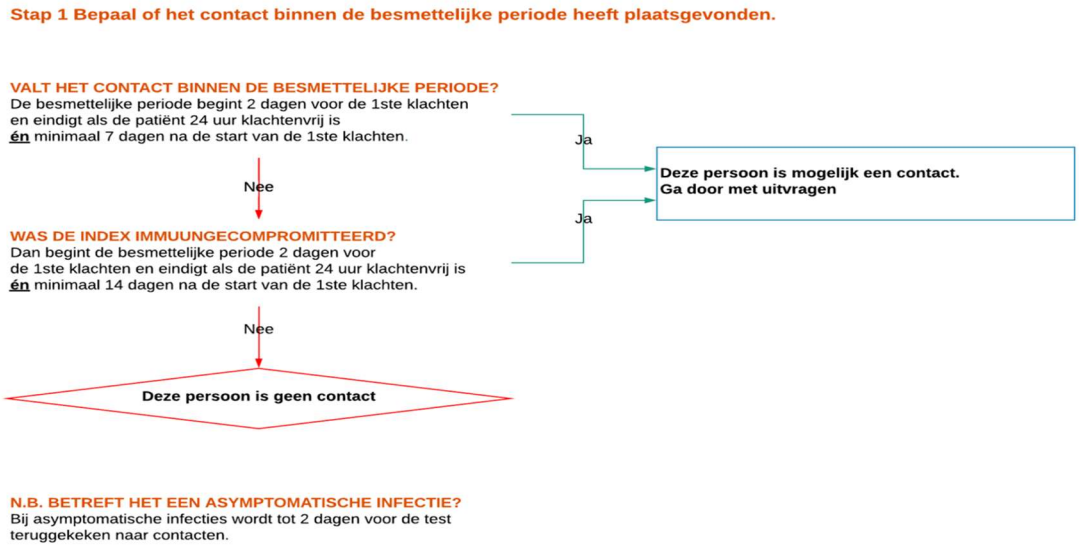
HPZone Lite is een product van Infact, een leverancier die gespecialiseerd is in 'Public Health Software'. Infact is een Brits bedrijf, maar HPZone Lite wordt gehost op een datawarehouse van KPN in Nederland. Er vinden geen dataverwerkingen plaats buiten de Europese Economische Ruimte (EER). HPZone is in beheer van de regionale GGD'en, zij zouden daarom een verwerkersovereenkomst moeten hebben afgesloten met deze leverancier.

8. Defensie – management ondersteuning

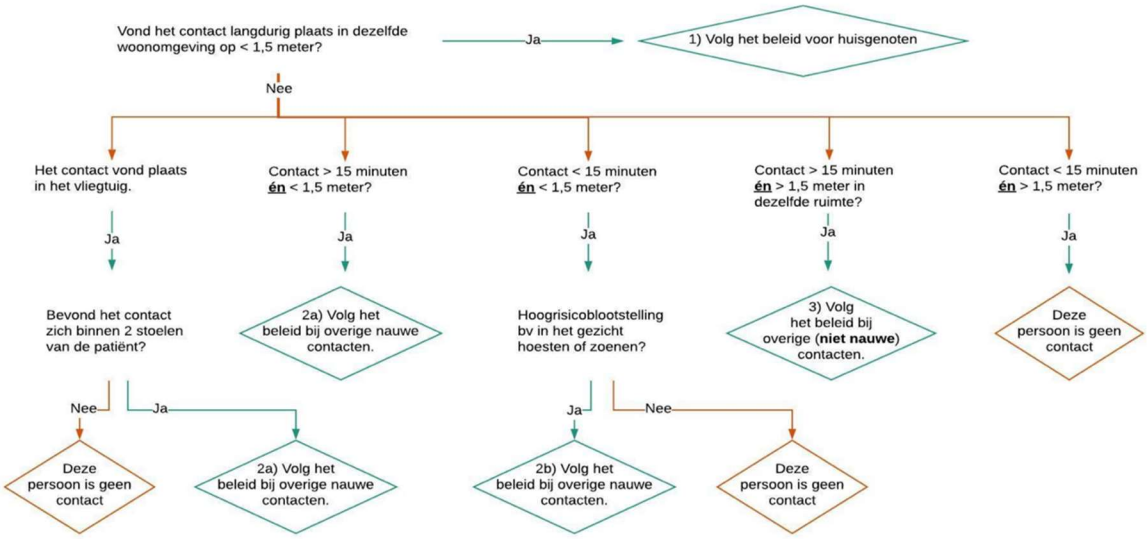
In de eerste helft van augustus 2020, is Defensie aangehaakt bij het landelijk programmateam BCO met de volgende doelen: ondersteuning van de landelijke schil van BCO, beschikbaarheid medische supervisie en algehele ondersteuning bij de coördinatie van/bij het landelijk coronateam van GGD GHOR, inclusief ondersteuning bij de aanpassing van het opschalingsplan. Het primaire doel is om te helpen met de organisatiestructuur van de landelijke BCO-inzet. Indien er nood is aan extra personeel is het mogelijk dat meer mankracht vanuit defensie wordt ingezet. Indien dat gebeurt, zullen daar de nodige overeenkomsten voor worden gesloten.

Gegevensverwerking

In deze paragraaf wordt weergegeven welke stappen worden genomen in het bron- en contactonderzoek.



Stap 2 Bepaal of het contact risico heeft gelopen op besmetting.



Disclaimer: het werkproces is continu onderhevig aan ontwikkeling. Voor de meest actuele werkwijze check de laatste versie van de landelijke BCO werkinstructie op Kennisnet. Voor het laatste nieuws over specificaties en termijnen zoals 'de besmettelijke periode' zie https://lci.rivm.nl/richtlijnen/covid-19

Het BCO op landelijk niveau heeft twee onderdelen: de landelijke inzet van medewerkers en de landelijke richtlijn die wordt opgezet door GGD GHOR en medewerkers uit de praktijk vanuit GGD'en. De landelijke richtlijn wordt hier beschreven om dit proces te schetsen. GGD'en zijn vrij dit deel van de DPIA over te nemen ter referentie voor een eigen DPIA, met de aanpassingen voor afwijkingen op regionaal niveau.

Landelijke inzet

GGD GHOR heeft overeenkomsten gesloten met landelijk ingezette callcentra. Deze callcentra zorgen voor het leveren van BCO-medewerkers aan GGD'en.

Selectie van medewerkers

BCO-medewerkers worden gelecteerd op basis van criteria die door GGD GHOR, in samenspraak met GGD'en, zijn opgesteld. Deze criteria worden opgesteld zodat medewerkers de richtlijnen duidelijk kunnen begrijpen en begrijpen dat zij hun taak zorgvuldig moeten uitvoeren. Door een tekort aan medisch geschoold personeel, wordt ook niet medisch personeel geselecteerd. Alle BCO-medewerkers staan onder supervisie van een arts. Van potentiële BCO-medewerkers wordt een VOG gevraagd. Als de medewerkers wordt ingehuurd, wordt een geheimhoudingsverklaring en een gedragscode thuiswerken getekend.

Training van medewerkers

De medewerkers worden getraind middels een training die is opgezet door NSPOH, waarbij GGD GHOR heeft aangegeven waar de training aan moet voldoen. Medewerkers worden via deze training getraind in de landelijke richtlijn en de omgang met gegevens.

Aanvraag inzet GGD

Indien een GGD behoefte heeft aan inzet van BCO-medewerkers uit de landelijke schil, vult de GGD een formulier in op een webpagina van SOS/CED. Dit kan op twee momenten in de week, maandag voor 10 uur in de ochtend en donderdag voor 10 uur in de ochtend. Op deze dagen wordt de capaciteit verdeeld.

De callcenters vullen eveneens een formulier in op een webpagina van SOS/CED, waarbij wordt gestreefd naar 100% capaciteit. GGD GHOR stelt voorwaarden op de inzet indien er niet voldoende capaciteit is. Dit gebeurt op basis van een eerlijke verdeling/het besmettingspercentage in de regio.

Via de mail wordt een de GGD'en en relatiemanagers gecommuniceerd welke partijen capaciteit zullen leveren. De callcenters krijgen een melding aan welke GGD ze BCO-medewerkers ze zullen leveren. De operationele invulling, dus hoe casussen aan GGD'en worden geleverd, verschilt per GGD.

Verdeling autorisaties

De GGD'en krijgen een lijst met BCO-medewerkers aangeleverd, die toegang moeten krijgen tot de systemen die zij nodig hebben om hun werkzaamheden uit te voeren. Deze lijst wordt handmatig verwerkt door een GGD medewerker. De aanlevering van autorisatiegegevens verschilt per GGD en kan per telefoon, mail of chat. Daarbij zijn er indicatoren om te verifiëren of er sprake is van een legitieme verzoeker tot autorisaties, namelijk:

- Domeinnaam van een van de alarmcentrales die callcenter capaciteit leveren.
- BIG-nummer: dit nummer is beschikbaar voor de medewerkers die medische supervisie verzorgen.
- Bekendheid van teammanagers en coördinatoren.

Nadat een BCO-medewerker niet meer werkzaam is voor een GGD, moeten de autorisaties door de GGD weer worden ingetrokken.

Inloggen en gebruik systemen

Medewerker loggen in via tweefactor authenticatie als het gaat om de systemen waar de contactgegevens in worden verwerkt.

BCO-medewerkers werken daarnaast met systemen van de callcentra. Het belangrijkste systeem dat wordt gebruikt is het mailsysteem om contact op te nemen met de index en de contacten.

Daarnaast wordt gebruik gemaakt van het eigen telefoonsysteem. GGD GHOR heeft eisen gesteld aan het gebruik van deze systemen. De callcentra dienen controle uit te oefenen op het juist gebruik van deze systemen en het correct uitvoeren van de gemaakte afspraken in de overeenkomsten met GGD GHOR met betrekking tot de inzet en het gebruik van deze systemen.

Het gebruikte e-mailadres en telefoonnummer dat wordt gebruikt om contact op te nemen met de index en contacten verschilt per callcentrum. Rode Kruis voert zelf geen intiële gesprekken met de index. Zij zetten de e-mail klaar en sturen deze naar de GGD'en om te laten versturen.

Multiple account access
In sommige gevallen beschikken BCO-medewerkers over accounts van meerdere GGD'en. Dit kan twee oorzaken hebben:

- De BCO-medewerker werkt op een dag voor verschillende GGD'en;
- De rechten van de BCO-medewerker met toegang tot de systemen voor een of meerdere GGD'en zijn nog niet ingetrokken.

Intrekken autorisaties
Autorisaties tot de systemen worden ingetrokken door de GGD'en. Hoe en wanneer dat gebeurt, is de verantwoordelijkheid van de GGD.

Landelijke richtlijn

0. Het BCO-proces wordt in gang gezet wanneer er een **melding is van een bevestigde COVID-19 patiënt**

De lokale GGD ontvangt een melding via CoronIT van een behandelend arts en laboratorium bij een positieve COVID-19 test. Het is dan de taak van de GGD om BCO zo snel mogelijk te initiëren, met een uiterlijke deadline van 24 uur. Vanwege capaciteitskrapte wordt deze deadline helaas niet altijd gehaald. Er wordt naar gestreefd om op regionaal niveau eerst een korte analyse te maken om vast te stellen of er sprake is van complexe casuistiek (voorbeeld indicatoren: risicogroep, minderjarig, taalbarriere). Indien dit het geval is, wordt het dossier bij voorkeur afgehandeld door de lokale GGD'en gezien die meer ervaring hebben met bron- en contactonderzoek. Een dossier wordt dus ofwel meteen doorgegeven aan de landelijke schil of er wordt besloten om het gesprek met de index op lokaal niveau af te handelen en het contactonderzoek uit te besteden aan landelijke BCO-medewerkers.

1. Casus oppakken en contact met de index

De GGD maakt vervolgens een dossier voor de index-patiënt aan in HPZone. Werknemers van de landelijke schil van BCO maken gebruik van HPZone Lite, zodat zij enkel gegevens die betrekking hebben op COVID-19 in kunnen zien. In beginsel is de index al op de hoogte van zijn/haar positieve uitslag, maar landelijke BCO-medewerkers verifiëren dit aan het begin van het gesprek. Het is verder

uiteraard van belang dat geverifieerd wordt of je de juiste persoon aan de lijn hebt, door actieve vragen te stellen.

De index wordt ondervraagd aan de hand van een vragenformulier dat BCO-medewerkers kunnen vinden onder 'Events' in HPZone Lite en/of op GGD GHOR Kennisnet. In dit vragenformulier staat een opsomming van vragen omtrent o.a.: klachten, ziekteverloop, verblijfplaats index, mogelijke bron, verblijfplaats, setting, contacten.

Huisgenoten, nauwe contacten en overige contacten waarmee de index in de besmettelijke periode in contact is geweest worden geinventariseerd en gecetagoriseerd. Deze besmettelijke periode begint 2 dagen voor start van de klachten, en eindigt als de patiënt 24 uur klachtenvrij is en minimaal 7 dagen na start symptomen.

Als een huisgenoot klachten overeenkomstig COVID-19 heeft, moet worden vastgesteld wat voor klachten en wanneer de eerste ziektedag was. Wanneer de klachten overeenkomen met de indicaties tot testen van contacten, moet dit contact verwezen worden naar de lokale GGD voor het aanmaken van een testaanvraag. Het HPzone nummer van de Index wordt dan verstrekt en het contact moet dat HPZone-nummer benoemen bij zijn/haar testaanvraag.

Tot slot, geven BCO-medewerkers voorlichting, instructies en advies op maat aan de Index-patient en huisgenoten.

Het is van belang om te controleren of het juiste e-mailadres is genoteerd om later de informatiebrieven naar te e-mailen. Het is van belang om in de instructies op te nemen dat een BCO-medewerker het emailadres nog een keer herhaald ter verificatie.

2. Informeren en adviseren

Bepalen en geven van advies op maat op basis van context en type contact. Versturen van e-mail met gemaakte afspraken (informatiepakket) naar index patiënt en contacten. Dit kan ook per post indien e-mail niet mogelijk is. De informatie wordt via reguliere mail verstuurd.

2A. Informeren van index en huisgenoten en brieven sturen

De index ontvangt vanuit de BCO-medewerker een e-mail met te nemen maatregelen. De BCO-medewerker moet vervolgens de volgende stappen doorlopen:

- Informeren van de index dat een medewerker/de GGD contact opneemt met de huisgenoten (als dat niet gelijk met de index kan) om passende maatregelen te bespreken. Deze worden ook per e-mail aan hen toegestuurd.
- Informeren van de index dat een medewerker/de GGD-contact opneemt met de overige nauwe contacten om passende maatregelen te bespreken. Deze worden ook per e-mail aan hen toegestuurd.

- Benoemen dat als men de brieven niet dezelfde dag hebben gekregen, ze mogen bellen met de eigen lokale GGD.
- De index verzoeken om de e-mail, bedoeld voor overige niet-nauwe contacten, door te sturen naar deze personen (afhankelijk wat er met de BCO-gesprekscoach is besproken).

2B. Bellen en informeren van nauwe contacten en brieven versturen

BCO-medewerkers nemen telefonisch contact op met alle huisgenoten (>16 jaar) en nauwe contacten. Voor de meest actuele definities van huisgenoten en nauwe contacten, zie https://lci.rivm.nl/COVID-19-bco. Nadat er telefonisch contact heeft plaatsgevonden, sturen BCO-medewerkers ook nog een e-mail met daarin de besproken adviezen.

Er is een standaard e-mailformat, maar het HPZone nummer en het telefoonnummer van de lokale GGD moeten handmatig worden ingevuld.

2C. Bellen en informeren van overige (niet nauwe) contacten en brieven versturen

BCO-medewerkers nemen tot slot telefonisch contact op met alle overige contacten. Nadat er telefonisch contact heeft plaatsgevonden, sturen ze ook nog een e-mail met daarin de besproken adviezen.

Ter ondersteuning van het doorlopen van stap 2 is in de landelijke werkinstructie BCO de volgende checklist opgenomen:

Informatievoorziening contacten	
Is de informatiemail verstuurd aan de index?	Let op: vul nummer lokale GGD in!!!
Zijn alle huisgenoten gebeld en is de informatiemail aan hen verstuurd?	
Zijn alle nauwe-contacten gebeld en is de informatiemail aan hen verstuurd?	
Is aan de index geadviseerd de informatiemail door te sturen aan zijn privé overige niet-nauwe contacten?	
Zijn de overige (niet nauwe) contacten buiten de privésfeer overgedragen aan de lokale GGD	
Vraag of de index zelf de huisarts wil informeren	

Osiris melding

De Osiris melding wordt door de GGD zelf afgehandeld en wordt daarom niet verder uitgewerkt in deze DPIA.

3. Telefonische nazorg en instructies

De contacten die zelf bellen met een vraag komen binnen bij de lokale GGD, dus niet bij het landelijke BCO-team. Dit wordt daarom niet uitgewerkt in deze DPIA.

4. Individuele monitoring

Beantwoording van contacten die zelf bellen in verband met koorts of andere klachten (hoesten en/of neusverkouden) en en eventuele doorverwijzing voor een test, wordt ook afgehandeld door de lokale GGD'en.

Bij een negatieve uitslag wordt het dossier afgesloten. De keuze om de huisarts in te lichten over de uitslag wordt bij het contact neergelegd.

5. Schema en afronden BCO

De index patiènt wordt gemonitord en aan het einde van de monitoring wordt het BCO afgerond voor de index en de huisgenoten. De betermelding van index-patiënt bij huisarts wordt bij de index neergelegd.

Er worden 3 vaste contactmomenten in HPZone ingebouwd: dag van eerste gesprek, dag 5 en een gesprek ter afsluiting van de quarantaineperiode (dag 10):

- Het 1e gesprek is voor uitleg en instructie
- Het 2e gesprek op dag 5 is om te informeren hoe het gaat en of er klachten zijn
- Het 3e gesprek checkt of er reden is om de quarantaine te verlengen. Als dat niet het geval is, is dit een afsluitend gesprek, waarmee de monitoring beëindigd wordt.

Let op: Als er tussen twee belmomenten minder dan 2 dagen (48 uur) zit, dan vervalt een gesprek, en wordt de inhoud van de twee gesprekken gecombineerd. HPzone zal aan deze uitgangspunten worden aangepast. Contacten kunnen uiteraard vaker worden gebeld als dat meerwaarde biedt bij de begeleiding van de quarantaine. Na afronding van het BCO-traject, wordt het dossier gesloten.

4. Verwerkingsdoeleinden

De landelijke flexibele schil verzorgt de mogelijkheid tot het inzetten van flexibele BCO-capaciteit, waarbij de medewerkers van die schil gegevens verwerken volgens de landelijke richtlijn. Het doel hiervan is dat snel medewerkers kunnen worden ingezet die op uniforme wijze volgens de landelijke richtlijn BCO uitvoeren bij GGD'en die capaciteit tekort komen. Op deze wijze wordt getracht BCO adequaat uit te kunnen voeren, ook tijdens piekmomenten.

Het doel van bron- en contactonderzoek is om zo snel mogelijk de bron van besmetting te achterhalen, contacten te identificeren, hen te informeren over de blootstelling en risico op besmetting, hen te wijzen op maatregelen die genomen moeten worden om verdere verspreiding te voorkomen en hen hierin te begeleiden. Voor de effectieve uitvoering van bron- en contactonderzoek is het noodzakelijk dat de landelijke BCO-medewerkers de persoonsgevens benoemd in **2. Persoonsgegevens** verwerken volgens de landelijke richtlijn.

5. Belangen bij gegevensverwerking

Samenleving als geheel

GGD'en voeren in geval van een infectieziekte altijd bron- en contactonderzoek uit. Daarmee spoor je op welke burgers positief testen, waar zij het virus hebben opgelopen, en met wie zij in contact zijn geweest. Het doen van bron- en contactonderzoek is een voorwaarde om te zorgen dat COVID-19 kan worden bestreden. De samenleving is er namelijk bij gebaat dat de juiste adviezen worden verstrekt en mensen worden geïnformeerd over de maatregelen die in acht moeten worden genomen, zodat verspreiding van COVID-19 wordt beperkt en COVID-19 wordt bestreden.

Betrokkenen

Effectief bron- en contactonderzoek zorgt dat betrokkenen tijdig op de hoogte worden gesteld van een kans op besmetting, waardoor deze beter kan monitoren of sprake is van klachten en zo sneller maatregelen kan treffen. Ook voorkomt de betrokkene op deze wijze dat hij/zij zelf contacten besmet.

GGD GHOR

GGD GHOR is een koepelorganisatie en dient dus de GGD'en in vragen/behoeftes. Het belang van GGD GHOR is om GGD'en te helpen en te zorgen dat ze hun taken kunnen uitvoeren, in dit geval het uitvoeren van het BCO. Vanuit die rol zorgt GGD GHOR, in opdracht van VWS, ervoor dat er op landelijk niveau afspraken worden gemaakt zodat GGD'en BCO kunnen uitvoeren.

GGD

GGD'en hebben tijdens deze pandemie de plicht om tijdig adequaat BCO uit te voeren, ondanks de grote schommelingen in besmettingspercentages. Daarom is het van belang dat voldoende medewerkers kunnen worden ingezet, waar de landelijke capaciteit aan kan bijdragen. Zo kan ook op piekmomenten snel bron- en contactonderzoek uitgevoerd blijven worden en voldoet de GGD aan haar wettelijke taak.

Ministerie van Volksgezondheid

Het ministerie, vertegenwoordigd door de minister, is op basis van de Wet publieke gezondheid (Wpg artikel 7.1) verantwoordelijk voor het coordineren van de bestrijding van epidemieën van infectieziekenten categorie A (zoals corona). Het ministerie (en de minister) hebben derhalve belang bij het op een verantwoorde manier opschalen van de landelijke BCO-capaciteit. In het kader daarvan is daarom ook de opdracht gegeven tot het opschalen van BCO-capaciteit op landelijk niveau.

6. Verwerkingslocaties

HPZone Lite, de applicatie waar BCO-medewerkers van de landelijke schil gebruik van maken in het kader van bron- en contactonderzoek, wordt gehost op KPN-datacentra in Nederland. Er worden geen gegevens verwerkt buiten de Europese Unie (EU).

7. Techniek en methode van gegevensverwerking

Voor deze verwerking wordt gebruik gemaakt van:

- HPZone Lite
- KPN datacenter voor hosting HPZone Lite
- Telefonietools ingezet door verwerkers
- Mailservers van de verwerkers
- Leermanagementsysteem Moodle

8. Juridisch en beleidsmatig kader

Voor de verwerking van persoonsgegevens in het kader van BCO is de volgende wet- en regelgeving van toepassing:

- Algemene Verordening Gegevensbescherming (AVG);
- Uitvoeringswet AVG (UAVG);
- Wet publieke gezondheid (Wpg);
- Opdracht van Ministerie van VWS aan GGD GHOR;
- Convenant gegevensuitwisseling inzake nationale opschaling bron- en contactonderzoek.

De volgende beleidsstukken zijn van toepassing op de verwerking van de persoonsgegevens door de BCO-medewerkers:

- BCO Landelijke werkinstructie
- Privacybeleid GGD GHOR
- Geheimhoudingsverklaring Bron- en Contactonderzoek
- Privacyverklaring Bron- en Contactonderzoek
- Trainingsmateriaal BCO-medewerkers
- Informatiepakket BCO
    - 5 gouden privacy regels
    - Meldplicht datalekken
    - Instructie GGD GHOR gebruik Social Media

9. Bewaartermijn

De GGD'en nemen de persoonsgegevens die verzameld zijn in het kader van bron- en contactverzoek op in een door hen gehouden registratie en bewaren deze gegevens ten hoogste vijf jaar (art. 29 lid 1 en lid 2 Wpg). Dit geldt voor in de meldplicht opgenomen persoonsgegevens (meldingsgegevens) zoals omschreven in artikel 24 lid 1 Wpg.

Uit de memorie van toelichting van artikel 29 Wpg blijkt dat de gegevens verwijderd dienen te worden zodra de GGD'en hebben vastgesteld dat deze niet langer noodzakelijk zijn, met een maximale bewaartermijn van 5 jaar. In het voorkomende geval is het bewaren van de betreffende persoonsgegevens in ieder geval noodzakelijk voor de gehele duur van de pandemie. Indien de pandemie minder lang duurt dan 5 jaar, zullen de gegevens dus eerder verwijderd worden.

Voor de persoonsgegevens die aanvullend op de hierboven vermelde gegevens worden verzameld, geldt dat deze voor dezelfde periode worden bewaard als de meldingsgegevens. Hiervoor is gekozen omdat dit gegevens betreft waarmee contact op kan worden genomen met betreffende personen (zoals telefoonnummer en e-mailadres). Tijdens de pandemie kan het voorkomen dat personen meerdere keren onderdeel uitmaken van een bron- en contactonderzoek. Ter voorkoming van het meermaals moeten uitvragen van de gegevens en het daarmee verkleinen van de kans op het verzamelen van onjuiste of dubbele gegevens, is ervoor gekozen alle tijdens het BCO verzamelde persoonsgegevens te bewaren zolang de pandemie duurt, met een maximum bewaartermijn van 5 jaar. Dit geldt ook voor alle persoonsgegevens die worden verzameld over contacten van de Index, aangezien deze niet vallen onder de meldplicht uit de Wpg.

Na deze bewaartermijn, worden de persoonsgegevens verwijderd of geanonimiseerd. De mogelijkheid bestaat dat gegevens in een geanonimiseerde vorm beschikbaar blijven om onderzoek mee te doen. In dat geval wordt gezorgd dat de gegevens niet herleidbaar zijn en op een adequate wijze worden afgeschermd.

B. Beoordeling rechtmatigheid gegevensverwerkingen

10. Rechtsgrond

De bestrijding van COVID-19 betreft een infectie behorend tot groep A waarvoor veiligheidsregio's verantwoordelijk zijn (art. 6 lid 2 Wpg). Om deze bestrijding te verwezenlijken, heeft de GGD de taak om tijdig bron- en contactonderzoek te doen (art. 6 lid 1 sub c Wpg). De uitvoering van BCO is een wettelijke taak en uitvoering van deze wettelijke taak wordt vorm gegeven volgens een protocol: https://lci.rivm.nl/COVID-19-bco (art. 6 lid 5 Wpg).

Het doel van BCO is om contacten te identificeren, hen te informeren over de blootstelling en risico op besmetting en het te wijzen op maatregelen die genomen moeten worden om verdere verspreiding te voorkomen en hen hierin te begeleiden. Om deze feitelijke uitvoering door de GGD'en te realiseren en zo te voldoen aan de wettelijke taak die voortkomt uit de Wet Publieke Gezondheid, is de verwerking van persoonsgegevens noodzakelijk. Het opvragen van persoonsgegevens door de GGD is derhalve noodzakelijk voor het vervullen van een taak van algemeen belang of een taak in het kader van de uitoefening van het openbaar gezag (art. 6 lid 1 sub e AVG). Deze noodzaak moet bij lidstatelijk recht zijn geregeld (art. 6 lid 3 sub b AVG) en in dit geval is deze wettelijke taak opgenomen in artikel 6 lid 1 sub c Wpg.

11. Bijzondere persoonsgegevens

Voor het verwerken van bijzondere persoonsgegevens, zoals gegevens over de gezondheid, is het noodzakelijk dat er een wettelijke uitzondering van toepassing is, zoals gesteld in art. 9 AVG. Het verbod op het verwerken van bijzondere persoonsgegevens kan worden doorbroken als de verwerking noodzakelijk is om reden van algemeen belang op het gebied van de volksgezondheid

zoals bescherming tegen ernstige grensoverschrijdende gevaren voor de gezondheid als dit ook nog in lidstatelijk recht is geregeld (art. 9 lid 2 sub i AVG).

Art. 9 lid 2 sub i AVG:

- De verwerking is noodzakelijk om redenen van algemeen belang op het gebied van de volksgezondheid, zoals bescherming tegen ernstige grensoverschrijdende gevaren voor de gezondheid of het waarborgen van hoge normen inzake kwaliteit en veiligheid van de gezondheidszorg en van geneesmiddelen of medische hulpmiddelen, op grond van Unierecht of lidstatelijk recht waarin passende en specifieke maatregelen zijn opgenomen ter bescherming van de rechten en vrijheden van de betrokkene, met name van het beroepsgeheim.

De Covid-19 pandemie is een grensoverschrijdende aanslag op onze volksgezondheid en valt dus te scharen onder de bovenstaande uitzondering. Het toepasselijke lidstatelijk recht waarin dit geregeld is, is de Wet publieke gezondheid. Deze specifieke wetgeving heeft daarnaast voorrang op algemene wetgeving zoals de UAVG.

Op basis van art. 7 Wpg heeft de minister de bevoegdheid sturing te geven bij een pandemie. GGD GHOR heeft daarom voor de verwerking een grondslag in de opdracht van de minister om een landelijke flexibele schil op te zetten. Afspraken met de GGD'en ondersteunen deze grondslag en dus de mogelijkheid voor GGD GHOR om de landelijke schil vorm te geven.

12. Doelbinding

Het uitvoeren van bron- en contactonderzoek verkort de duur tussen het onstaan van klachten en het starten van isolatiemaatregelen en reduceert daarmee transmissie. De verwerking van persoonsgegevens is noodzakelijk om de bron van besmetting te achterhalen en mogelijk besmette contacten in kaart te brengen. GGD GHOR en de GGD'en verwerken persoonsgegevens conform het BCO-protocol en verzamelen en verwerken enkel die gegevens die noodzakelijk zijn voor het uitvoeren van het bron- en contactonderzoek. Voor verdere toelichting, zie **4. Verwerkingsdoeleinden**.

13. Noodzaak en evenredigheid

De AVG bepaalt dat alle verwerkingen van persoonsgegevens moeten voldoen aan de vereisten van proportionaliteit en subsidiariteit. Dit houdt kort gezegd in dat: het doel en de aard en omvang van de gegevens die voor dat doel worden verwerkt met elkaar in verhouding moeten zijn en dat altijd moet worden gekozen voor de minst ingrijpende verwerking van persoonsgegevens.

Bij het inrichten van de BCO-procedure is als volgt rekening gehouden met de beginselen proportionaliteit en subsidiariteit:

Proportionaliteit

De GGD heeft de wettelijke taak tot het doen van BCO. BCO is vormvrij en moet breed worden opgevat. De GGD moet immers kunnen differentiëren naar wat afhankelijk van de omstandigheden van het geval de beste aanpak is. Voor de bestrijding van de pandemie geldt dat het doel van BCO het beste kan worden bereikt als zoveel mogelijk mensen die risicovol in de nabijheid van een geïnfecteerde persoon zijn geweest zo snel mogelijk kunnen worden gewaarschuwd.

Deze wettelijke taak van de GGD dient een algemeen belang op het gebied van volksgezondheid. Het door de GGD verrichtte bron- en contactonderzoek is essentieel voor het doorbreken van de keten van infecties en het voorkomen van verdere infecties en levert daarmee een cruciale bijdrage aan de bestrijding van COVID-19. Dit sluit aan bij het uitgangspunt van de EDPB dat 'het rechtskader voor gegevensbescherming is ontworpen met flexibiliteit voor ogen en als zodanig een efficiënte respons mogelijk maakt die de pandemie indamt en de fundamentele mensenrechten en vrijheden beschermt'.[4]

GGD GHOR stelt een landelijke werkinstructie op, op basis waarvan de BCO-medewerkers gegevens verwerken. Deze richtlijn sluit aan bij de gegevens die in de praktijk nodig zijn en de richtlijn die is opgesteld door het RIVM. Daarom is de verwerking proportioneel.

De verwerking van persoonsgegevens door invoering in HPZone Lite tijdens het bron- en contactonderzoek is daarom noodzakelijk en proportioneel.

Subsidiariteit
HPZone Lite is speciaal ontwikkeld zodat landelijke BCO-medewerkers in een applicatie werken die hen alleen inzicht verschaft in de relevante COVID-19 dossiers. Andere applicaties zijn daardoor overbodig in het BCO-proces, wat betekent dat een wildgroei aan applicaties en verscheidenheid aan gemelde informatie wordt vermeden. Dit zorgt ook voor rapportages die betrouwbaarder zijn en zorgen dat adequatere keuzes kunnen worden gemaakt.

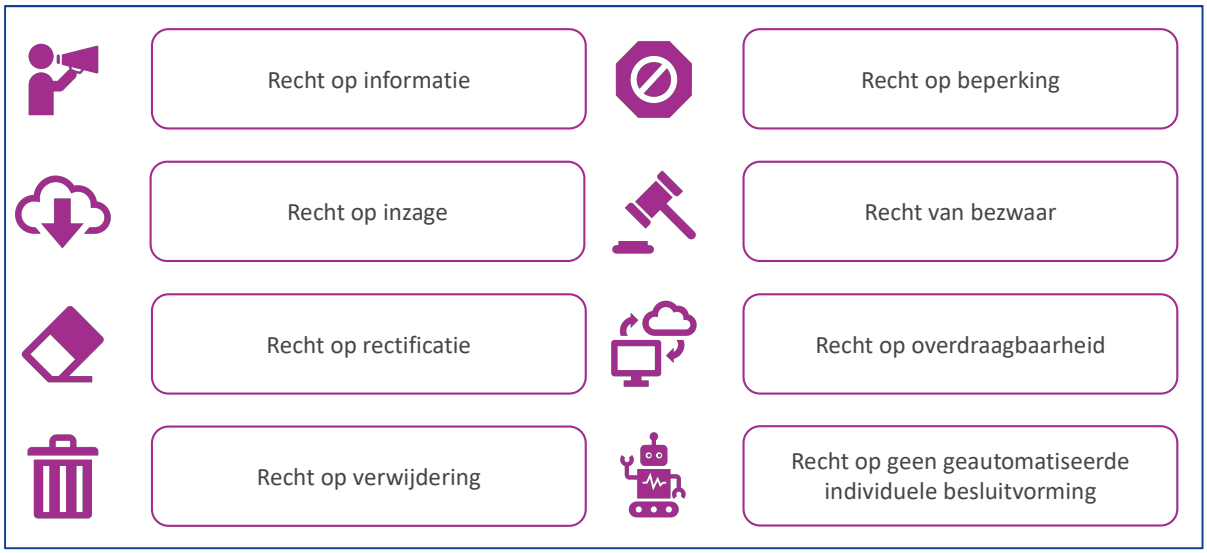
De verwerking van (persoons)gegevens is beperkt tot het strikt noodzakelijke. Daarnaast zijn ook verschillende andere passende technische en organisatorische beveiligingsmaatregelen getroffen (zie daarvoor ook onderdelen **15. Risico's** en **16. Maatregelen**).

In dit proces is het van belang dat BCO adequaat wordt uitgevoerd, ook als de GGD zelf niet voldoende capaciteit heeft. Het structureren van deze extra inzet volgens eenzelfde training en richtlijn, maakt dat de gegevens op een uniforme wijze worden verwerkt en dat wordt gezorgd dat de medewerkers worden gescreend en getraind. Dit voorkomt versnippering van werkwijzen van verschillende bureaus die anders op regionaal niveau zouden worden ingezet. Verwerking op landelijk niveau volgens de landelijke richtlijn door BCO-medewerkers is daarom subsidiair.

[4] Richtsnoeren 04/2020 voor het gebruik van locatiegegevens en instrumenten voor contacttracering in het kader van de uitbraak van COVID-19, EDPB, Vastgesteld op 21 april 2020.

14. Rechten van betrokkenen

In het kader van BCO worden zowel gewone als bijzondere persoonsgegevens verwerkt. Omdat die persoonsgegevens worden verwerkt, hebben betrokkenen een aantal rechten, zoals bepaald in hoofdstuk III AVG. De beoordeling van verzoeken gebaseerd op art. 15 tot en met 21 AVG is een verantwoordelijkheid van de regionale GGD.



Recht op informatie (art. 13/14 AVG):

De betrokkene heeft recht om informatie te ontvangen over de verwerking van zijn/haar persoonsgegevens. Op de website van GGD GHOR, onder het thema BCO, is een link naar de privacyverklaring geplaatst die informatie verstrekt over de gegevens die landelijke BCO-medewerkers uitvragen en verwerken. Voor meer informatie zie: https://ggdghor.nl/thema/bron-en-contactonderzoek/.

GGD'en dienen zelf een privacyverklaring te hebben voor het BCO dat zij zelf uitvoeren.

Recht op inzage en afschrift (art. 15 AVG)

De betrokkene heeft het recht om de gegevens in te zien. De gegevens kunnen worden opgevraagd bij de lokale GGD die verantwoordelijk is voor BCO inzake betrokkene en daar kan ook een afschrift worden verkregen. De GGD is verantwoordelijk voor de gegevens in HPZone Lite voor de personen uit de eigen regio, waardoor zij ook dit verzoek moeten afhandelen.

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 lokale GGD die verantwoordelijk is voor het BCO inzake betrokkene.

Indien de aanpassing kleine aanpassingen betreft, zoals telefoonnummer en e-mailadres, dan kunnen betrokkenen dit ook telefonisch laten aanpassen. Dit moet worden opgenomen in de landelijke richtlijn.

Recht op gegevenswissing (art. 17 AVG)
De betrokkene kan verzoeken persoonsgegevens te wissen. De GGD zal hierbij een afweging moeten maken of de gegevens kunnen worden gewist en de betrokkene van die beslissing op de hoogte moeten brengen met een motivering.

Recht op beperking van de verwerking (art. 18 AVG)
De betrokkene kan in de door de wet bepaalde gevallen verzoeken bij zijn/haar lokale GGD om de verwerking van zijn/haar gegevens te beperken. Dit is enkel het geval indien de gegevens mogelijk onjuist zijn.

Recht op overdraagbaarheid van de gegevens (art. 20 AVG)
Dit recht is alleen van toepassing bij toestemming of contract, daarvan is in dit proces geen sprake.

Recht van bezwaar (art. 21 AVG)
De betrokkene heeft het recht om in bepaalde gevallen bezwaar te maken tegen de verwerking van persoonsgegevens, wanneer de individuele omstandigheden van het geval dit rechtvaardigen en de verwerking plaatsvindt op basis van het algemeen of gerechtvaardigd belang. Het bezwaar kan worden ingediend bij de GGD die verantwoordelijk is voor de uitvoering van bron- en contactonderzoek inzake betrokkene. Desbetrefende lokale GGD zal het verzoek in behandeling nemen.

Recht om niet te worden onderworpen aan geautomatiseerde individuele besluitvorming (art. 22 AVG)
Er is in het kader van de uitvoering van bron- en contactonderzoek geen sprake van geautomatiseerde individuele besluitvorming overeenkomstig art. 22 AVG.

C. Beschrijving en beoordeling risico's voor de betrokkenen

15. Risico's

In deze paragraaf worden de risico's voor betrokkenen uiteen gezet, inclusief de risico's die door voorgenomen maatregelen reeds gemitigeerd zijn. Per risico wordt een inschatting gemaakt van het risiconiveau op basis van kans x impact. Vervolgens worden er verschillende mitigerende maatregelen voorgedragen en wordt ingeschat wat het risiconiveau betreft na toepassing van deze maatregelen. Aangezien er hier sprake is van een proces waarin veranderingen plaatsvinden, zullen eventuele nieuwe risico's in een register worden bijgehouden. Grote wijzigingen in het proces zullen in een addendum bij deze DPIA worden bijgevoegd.

Een deel van de risico's is inherent aan het uitvoeren van BCO. Een ander deel zijn aanvullingen in risico's die spelen in de landelijke opschaling.

1. **Veranderingen in werkinstructies, snelle training en lokale verschillen in werkwijzen, zorgen voor onrechtmatige verwerking van gegevens.**

Door de snelle veranderingen, snelle training en lokale verschillen in werkwijze, kan verwarring ontstaan bij medewerkers of kunnen oude werkwijzen worden gehanteerd. Hierdoor kunnen niet noodzakelijke persoonsgegevens worden verwerkt. Voorbeelden van onrechtmatige verwerkingen in de praktijk die het resultaat kunnen zijn van het gebruik van verkeerde werkinstructies of gebrek aan training zijn:

- Het niet vragen van toestemming aan de index om zijn naam te noemen aan contacten;
- Het verkeerd linken van contacten aan de index, waardoor clusters van contacten niet zichtbaar zijn of dubbele dossiers worden aangemaakt en mensen twee keer worden gebeld;
- Invullen van gegevens over contacten in het dossier van de index;
- Volgen van de verkeerde instructies (regionaal/verouderde landelijke instructies);
- Vergeten van het klaarzetten van acties, zodat iemand met de juiste autorisaties het dossier kan sluiten. Hierdoor blijft het dossier onnodig gemonitord.

Hoe groot is de kans dat dit risico zich manifesteert en indien het zich manifesteert, hoe groot schat men de impact voor de betrokkenen:

- De kans dat dit risico zich manifesteert is hoog. Er is een groot aantal medewerkers dat wordt ingezet voor BCO. Ze worden allemaal getraind, echter is deze training snel en is het lastig te controleren of iedereen alles heeft begrepen. Daarnaast veranderen richtlijnen regelmatig en hebben regio's hun eigen richtlijnen, waardoor verwarring kan ontstaan. Ten slotte kunnen medewerkers vergeten te kijken naar de laatste versie van de richtlijnen, waardoor ze met een verouderde versie werken.
- De impact van het risico is hoog. Het verkeerd verwerken van gegevens van de betrokkene, kan zorgen voor onrechtmatige verwerking. Als teveel gegevens in het systeem staan, blijven deze opgeslagen en verwerkt door meerdere mensen. als te weinig gegevens worden verzameld of gegevens verkeerd worden gekoppeld, kan dit gevolgen hebben voor de monitoring van de betrokkene. Ten slotte kan het noemen van de naam van de index, terwijl daar geen toestemming voor is, eveneens gevolgen hebben voor de betrokkene.

Geadviseerd wordt om de volgende maatregelen te nemen:

- Beoordeel welke vragen wel en niet nodig zijn. De naam van de index lijkt namelijk niet nodig om te delen. Laat deze keuze bij de index.
- Zorg voor goede en gestructureerde training van medewerkers. Dit betekent ook periodiek trainen door trainingssessies en/of bespreken van privacy en nieuwe richtlijnen bij een dagstart door een teamleider.

- Indien er een wijzigingen is in de richtlijnen, stel dan een pop-up in zodat medewerkers direct kunnen klikken naar de nieuwe richtlijn.
- Communiceer wijzigingen in de richtlijnen, zeker indien deze belangrijk zijn, ook in de dagstart om te controleren of medewerkers de wijzigingen begrijpen.
- Zorg voor steeksproefgewijs controleren van de werkzaamheden van de medewerkers om te achterhalen of ze hun werkzaamheden correct uitvoeren. Dit kan bijvoorbeeld door het beluisteren van gesprekken. Zo kan de kwaliteit worden verhoogd en kunnen trainingen worden verbeterd.
- Controleer de richtlijnen op het type gegevens dat wordt uitgevraagd en zorg voor een juridische afweging van de gegevens die worden gevraagd versus het doel waarmee ze worden opgevraagd.

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

Restrisico: door de omvang van de organisatie kan het zijn dat medewerkers nog niet goed begrijpen wat van hen wordt verwacht. Zelfs door het implementeren van de voorgestelde maatregelen, kan het voorkomen dat een klein percentage van de medewerkers nog niet begrijpt wat een richtlijn inhoudt of niet doorhebben wat van hen wordt verwacht bij communicatie van een nieuwe richtlijn. Het aantal medewerkers dat hier problemen bij ondervindt, zal echter drastisch worden verminderd.

2. Datalekken kunnen ontstaan door het niet volgen van de richtlijnen, onzorgvuldig handelen en onrechtmatig verwerken van persoonsgegevens.

In het BCO-proces zijn een aantal zaken die kunnen zorgen voor datalekken. Zo kan het wijzigen van een richtlijn waarvan medewerkers niet of niet voldoende op de hoogte zijn, leiden tot onrechtmatige verwerking van gegevens.
Daarnaast zijn er in het werkproces een groot aantal punten waar de medewerkers handmatige acties moeten verrichten, zoals met het invullen van formulieren, het verzenden van mails waarbij de naam van een ander in het template blijft staan, de mail in CC in plaats van BCC wordt verzonden, etc. Dit zorgt voor datalekken die onbewust en/of door te weinig controle worden veroorzaakt.

- De kans dat het risico zich manifesteert is hoog. Richtlijnen veranderen vaak, waardoor de medewerkers niet altijd handelen naar de laatste richtlijn en hierdoor gegevens onrechtmatig kunnen verwerken. Daarnaast doen medewerkers veel zaken handmatig en er is veel druk op het proces. Hierdoor wordt niet dubbel gecontroleerd of bijvoorbeeld gegevens goed zijn ingevuld.
- De impact van het datalek is hoog. Als persoonsgegevens onrechtmatig worden verwerkt en uitlekken, lekken medische gegevens uit. Daarnaast kan uitlekken wie potentieel besmet is door wie. Dit kan gevolgen hebben voor alle betrokkenen.

Geadviseerd wordt om de volgende maatregelen te nemen:

- Train medewerkers op het juist verwerken van persoonsgegevens en de risico's die bestaan bij een verkeerde verwerking van persoonsgegevens. Dit dient periodiek te gebeuren.
- Het besteden van aandacht aan veel voorkomende datalekken tijdens de dagstart.
- Het opstellen van duidelijke werkinstructies en een quick reference card met de belangrijkste zaken waar regelmatig fouten in worden gemaakt.
- Het invoeren van extra controle voor het verzenden van berichten of het invoeren van gegevens.

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

Restrisico: door de omvang van de organisatie kan het zijn dat medewerkers nog niet goed begrijpen wat van hen wordt verwacht. Zelfs door het implementeren van de voorgestelde maatregelen, kan het voorkomen dat een klein percentage van de medewerkers nog niet begrijpt wat een richtlijn inhoudt of niet doorhebben wat van hen wordt verwacht bij communicatie van een nieuwe richtlijn. Het aantal medewerkers dat hier problemen bij ondervindt, zal echter drastisch worden verminderd.

Daarnaast zijn er verschillende partijen, waarbij het moeilijk is te controleren of zij doen wat is overeengekomen en de medewerkers dus fouten kunnen maken in de uitvoering van de werkzaamheden.

3. Onvoldoende controle op en monitoring van logging leidt tot niet opsporen van onrechtmatige verwerkingen.

Voor de uitvoering van de werkzaamheden van de medewerkers is het noodzakelijk dat wordt gelogd wat de medewerkers in de dossiers doen. Dit betekent dat gecontroleerd wordt of de handelingen die zei uitvoeren met betrekking tot de persoonsgegevens rechtmatig zijn. Dit kan door controle van de logging. Indien deze controle niet wordt uitgevoerd, kunnen onrechtmatige verwerkingen niet worden opgespoord en afgehandeld.

- De kans dat het risico zich manifesteert is hoog. Medewerkers worden ingezet bij GGD'en, die zelf moeten monitoren. Het is niet bekend of deze logging bij iedere GGD wordt gecontroleerd en of wordt gekeken naar de BCO-medewerkers van de landelijke schil die worden ingezet.
- De impact van het datalek is hoog. Het aantal gegevens waar toegang toe wordt gekregen, bevatten gegevens die gevoelig zijn, zoals medische gegevens, maar ook gegevens die extra beschermd worden, zoals een BSN. Het uitlekken van deze persoonsgegevens kan grote gevolgen hebben, zoals fraude met deze persoonsgegevens.

Geadviseerd wordt om de volgende maatregelen te nemen:

- Zorg dat met iedere verwerker en met de GGD'en wordt afgesproken dat de is logging ingeschakeld en periodiek wordt gecontroleerd. Controle van de logging is een verantwoordelijkheid van de GGD'en. Voor de controle is een procedure nodig, waarbij rekening wordt gehouden met de omstandigheden waaronder wordt gewerkt, het aantal mensen dat werkt en het aantal persoonsgegevens dat wordt verwerkt.
- Zorg voor een uniforme werkwijze bij het opsporen van onrechtmatige activiteiten en indien opzettelijk, de sancties die worden gegeven.

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

Het restrisico is dat door de grote aantallen medewerkers, die constant wisselen en die thuis werken, de kans op fraude en onrechtmatig gebruik blijft bestaan. Er is geen controle op de werkvloer en met periodieke controle kan niet alles worden gecontroleerd. Zo kan iemand gemakkelijk niet worden opgemerkt.

4. Medewerkers werken vanuit huis met hun eigen apparaten, wat kan leiden tot situaties waarin persoonsgegevens onrechtmatig worden verwerkt.

Medewerkers werken thuis, wat betekent dat andere personen aanwezig kunnen zijn en gebruik kunnen maken van het thuisnetwerk. Dit betekent dat huisgenoten onrechtmatig gegevens kunnen horen of zien, indien de medewerker werkt op een locatie waar andere aanwezig zijn.
Daarnaast kunnen mensen die op hetzelfde netwerk werken, toegang krijgen tot de gegevens die via dat netwerk worden verstuurd. Hierdoor kan onrechtmatige inzage van gegevens mogelijk zijn.
Ten slotte gebruiken medewerkers eigen apparatuur om de werkzaamheden op uit te voeren. Medewerkers kunnen bestanden met vertrouwelijke informatie downloaden uit de beveiligde omgeving en niet/niet tijdig verwijderen. Indien deze apparatuur niet goed is beveiligd, kan worden meegekeken in de systemen van de medewerker of kunnen inloggegevens worden gestolen. Dit betekent dat fraude kan worden gepleegd met deze gegevens.

- De kans dat het risico zich manifesteert is hoog. Medewerkers werken thuis, maar vaak ook de huisgenoten. Dit betekent dat de medewerker zich altijd zal moeten afzonderen, wat voor sommige medewerkers niet mogelijk is. Ook kan een huisgenoot binnenlopen bij een gesprek. Vaak wordt door huisgenoten ook hetzelfde wifi-netwerk gebruikt, waardoor deze toegang kunnen krijgen tot de data-uitwisseling van de medewerker met het netwerk.
- De impact van het risico is hoog. Hoewel het gaat om huisgenoten, kunnen zij de persoonsgegevens opvangen. Hierdoor bestaat de kans dat wordt gesproken over de casus. Als een huisgenoot de data-uitwisseling kan volgen, betekent dat dat hij met de

persoonsgegevens kan doen wat hij wenst, terwijl het hier gaat om gegevens die gevoelig zijn en die gebruikt/verkocht kunnen worden om fraude mee te plegen.

Geadviseerd wordt om de volgende maatregelen te nemen:

- Stel een landelijke procedure met gedragsregels bij thuiswerken en de beveiliging van een device en het netwerk. Leg deze aan de medewerker voor en laat de medewerker deze ondertekenen/hiermee akkoord gaan. Benadruk dat deze documenten grondig moeten worden gelezen.
- Besteed bij de training aandacht aan dit onderwerp en laat dit tijdens periodieke trainingen terugkomen.
- Breng de gedragsregels voor thuiswerken en beveiliging van de device en het netwerk periodiek aan de orde bij de dagstart.
- Controleer of er opties bestaan om na te gaan of de medewerker zich aan de afspraken houdt.

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

5. Snelle ontwikkelingen in partijen om de snelgroeiende vraag naar capaciteit om tegemoet te komen leidt tot verlies van overzicht en het niet (adequaat) maken van afspraken.

Binnen BCO is er een snelgroeiende vraag naar capaciteit, zodat GGD'en BCO adequaat kunnen uitvoeren. Deze vraag stijgt continu, waardoor nieuwe partijen, zowel verwerkers als subverwerkers, worden aangesloten. Hiervoor is geen centraal overzicht welke partijen exact meewerken en met wie wel en niet afspraken zijn gemaakt.
Ook veranderd de werkwijze. Hierdoor kunnen verwerkersovereenkomsten achterlopen op de praktijk en dus niet de volledige verwerking bevatten. Dit betekent dat afspraken niet adequaat of volledig zijn gemaakt en dat persoonsgegevens onrechtmatig worden verwerkt, zowel in de wijze van verwerken, als de partij die deze persoonsgegevens verwerkt.

- De kans dat het risico zich manifesteert is hoog. Juist door de snelle ontwikkelingen wordt gefocust op het inschakelen van de partij en het zo snel mogelijk aan de gang krijgen van de medewerkers. Hierdoor kunnen afspraken over de verwerking van persoonsgegevens over het hoofd worden gezien, alsook het centraal registreren van de partijen en de overeenkomsten die zijn gesloten. Daarnaast kunnen verwerkers ook subverwerkers inschakelen. Hier kan in de haast worden vergeten dit te melden, waardoor GGD GHOR de voorgenomen subverwerker niet kan toetsen.
- De impact van het risico is hoog. Indien niet de juiste afspraken worden gemaakt, worden persoonsgegevens, waaronder ook persoonsgegevens van gevoelige aard, onrechtmatig

verwerkt, wat bijvoorbeeld kan betekenen dat medewerkers de persoonsgegevens onrechtmatig kunnen inzien, niet adequaat worden beveiligd en te lang en/of verkeerd worden bewaard.

Geadviseerd wordt om de volgende maatregelen te nemen:

- Stel een centraal overzicht op van alle verwerkers en vraag bij hen de subverwerkers op.
- Stel in de overeenkomsten vast dat de verwerkers GGD GHOR op de hoogte brengt van een (beoogde) nieuwe subverwerker. Zorg daarbij ook dat GGD GHOR dit periodiek uitvraagt bij de verwerker, zodat het eventueel vergeten van het doorgeven van een subverwerker wordt ondervangen.
- Stel periodieke controle in voor de verwerkersovereenkomsten om te controleren of deze nog adequaat zijn en passen bij de praktijk.
- Zet een beheersorganisatie op, zodat snel en adequaat kan worden opgeschaald, afgeschaald en overgedragen.

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

6. **Gebrek aan afspraken, onder andere met betrekking tot de rolverdeling, tussen regionale en landelijke partners kan leiden tot onduidelijkheid in de verwerking van persoonsgegevens.**

Voor het landelijke BCO traject heeft de intentie bestaan een convenant te sluiten tussen GGD GHOR en de GGD'en om duidelijke afspraken te maken over de taken van GGD GHOR en de GGD'en. De optie van het convenant is afgewezen, waardoor nu geen afspraken zijn gemaakt. Dit heeft een aantal nadelen. Zo is het niet duidelijk wie welke rollen heeft, maar bestaan er voor GGD GHOR ook problemen met de grondslag om contracten voor BCO te sluiten, omdat ze daar in eigen titel geen bevoegdheid en grondslag voor heeft.

Daarnaast zijn er verschillende richtlijnen. Er moeten afspraken worden gemaakt over de te volgen richtlijnen. Zo kan in ieder geval worden gezorgd dat medewerkers niet continu andere richtlijnen moeten volgen als ze bij een andere GGD worden ingezet.

- De kans dat het risico zich manifesteert is hoog. Door een gebrek aan afspraken is het onduidelijk wat de taken van de partijen zijn. Hierdoor kan verwarring bestaan in het verwerken van de persoonsgegevens.
- De impact van het risico is hoog. Onrechtmatige of onjuiste verwerking van de gegevens kan grote gevolgen hebben voor de persoonsgegevens van de betrokkene, maar ook de manier waarop zij op de hoogte worden gebracht over een eventuele besmetting.

Geadviseerd wordt om de volgende maatregelen te nemen:

- Stel een overeenkomst op, bij voorkeur een convenant, waarin wordt geregeld wie welke rol heeft en welke taken de partijen hebben.
- Indien een convenant niet kan worden opgesteld, kan worden geopteerd om een opdrachtverstrekking te krijgen. Dit is echter niet optimaal, omdat een aantal zaken, zoals het afhandelen van datalekken, daar niet in is opgenomen.
- Zorg voor landelijke richtlijnen om te zorgen dat GGD'en op een uniforme wijze BCO uitvoeren.
- Om uniformering van de BCO-werkwijze op korter termijn te bewerkstelligen, is het aangeraden dat de regionale GGD'en enkel werken volgens de landelijke BCO-werkinstructie.

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

7. Betrokkenen worden onvoldoende geïnformeerd over de verwerking van persoonsgegevens in BCO.

Voor betrokkenen is een privacyverklaring opgesteld naar de stand van zaken op dat moment. Indien er wijzigingen zijn, zullen die worden doorgevoerd in de privacyverklaring. Betrokkenen in het BCO traject worden echter gebeld, wat betekent dat ze vooraf niet weten of ze gebeld worden en dus niet vooraf kijken naar de privacyverklaring. Dit betekent dat betrokkenen in het gesprek op de hoogte moeten worden gebracht over de verwerking van hun persoonsgegevens en indien nodig toestemming moet worden gevraagd voor het opnemen van het gesprek en wat dit betekent voor de verwerking van de opname. Dit zal voor iedere GGD gelijk moeten zijn, zodat geen verwarring ontstaat in de uitleg.

Indien de betrokkene niet wordt geïnformeerd, wordt niet voldaan aan de verplichtingen uit de AVG. Indien de verwerking op toestemming berust en de betrokkene de toestemming niet geïnformeerd is gegeven, dan is de verwerking onrechtmatig.

- De kans dat het risico zich manifesteert is hoog. De callscripts zijn niet doorgenomen op de eisen de gesteld worden met betrekking tot de informatieplicht, waardoor het aannemelijk is dat de benodigde informatie niet wordt verstrekt.
- De impact van het risico is hoog. De persoonsgegevens van de betrokkene zullen worden verwerkt zonder dat de betrokkene op de hoogte is wat deze verwerking inhoudt. Dit betekent dat ze niet de keuze kunnen maken wat ze wel en niet verstrekken. Daarnaast geven ze toestemming voor een opname waarvan ze niet weten wat daarmee gebeurt.

Geadviseerd wordt om de volgende maatregelen te nemen:

- Stel callscripts op en laat ze controleren op de informatieverstrekking en de wijze waarop toestemming wordt gevraagd.
- Bespreek de callscripts met een aantal GGD'en en stel deze vast.
- Laat wijzigingen checken op de informatie en de verdeel deze aan de regionale GGD'en.

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

8. BCO medewerkers verwerken bijzondere persoonsgegevens, waarbij de gegevens niet op de meest adequate wijze worden verwerkt.

BCO medewerkers verwerken bijzondere en gevoelige gegevens. Hieronder vallen het BSN en medische gegevens, namelijk een besmetting met corona van de index en een potentiële besmetting van de contacten. BSN wordt door de BCO medewerkers actief uitgevraagd in outbound gesprekken. Dit is niet in lijn met de fraudebestrijdende richtlijn dat overheden niet om BSN vragen als de overheid zelf belt. Voor de medische gegevens geldt dat normaal een arts infectieziekten betrokken is bij het proces. Door de grote hoeveelheden van besmettingen, kan niet al het BCO door artsen of medewerkers die weten wat verwacht wordt worden uitgevoerd. Daarom is gezorgd voor training en het ondertekenen van geheimhoudingsverklaringen.

- De kans dat het risico zich voordoet is hoog. Medewerkers blijven BSN uitvragen, tegen de richtlijn in, waardoor gemakkelijk door een kwaadwillende fraude kan worden gepleegd. Daarnaast zijn medewerkers zich niet altijd bewust van de risico's van het verwerken van medische gegevens. Hierdoor kunnen de persoonsgegevens onrechtmatig worden verwerkt.
- De impact van het risico is hoog. Indien fraude wordt gepleegd, kan, met de gegevens die in het BCO traject normaal worden gebruikt, behoorlijk wat schade worden berokkent aan de betrokkene. Dit geldt ook als de medewerker de persoonsgegevens onrechtmatig verwerkt.

Geadviseerd wordt om de volgende maatregelen te nemen:

- Vraag geen BSN bij het outbound bellen.
- Indien geverifieerd moet worden met het BSN, zorg dan dat enkel wordt geverifieerd met de laatste drie cijfers van het BSN en communiceer dit ook helder in communicatie rond de uitvoering van BCO, zowel naar de medewerkers als de betrokkenen.
- Zorg voor periodieke training van medewerkers en heldere richtlijnen over de verwerking van de persoonsgegevens in het kader van BCO.

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

9. Er bestaat geen duidelijkheid over hoe de betrokkene zijn rechten kan uitoefenen.

In de privacyverklaring is kort een stuk opgenomen over de rechten van betrokkenen. Een procedure is echter niet opgesteld en BCO medewerkers worden hier niet in opgeleid. Daarnaast bestaan geen afspraken met de GGD'en wie welk verzoek opneemt. Dit kan ertoe leiden dat de betrokkene zijn rechten niet kan uitvoeren, of dat niet binnen de termijn aan het verzoek van de betrokkene wordt voldaan.

- De kans dat het risico zich voordoet is hoog. Betrokkenen zullen vooral spreken met BCO medewerkers, waarvan een deel uit de landelijke schil zal komen. Zij zijn het eerste aanspreekpunt. Daarnaast is niet iedere betrokkene even handig met het opzoeken waar deze een verzoek kan indienen.
- De impact is hoog. Een betrokkene heeft het recht in te kunnen zien welke gegevens over hem/haar worden verwerkt. Indien dit niet kan, kan de betrokkene niet weten wat er exact wordt verwerkt. Voor de andere rechten geldt dat de betrokkene deze heeft gekregen om over zijn gegevens te kunnen blijven beschikken. Indien dat niet kan, is de betrokkene de beschikking over gevoelige persoonsgegevens kwijt.

Geadviseerd wordt om de volgende maatregelen te treffen:

- Maak afspraken met de GGD'en en verwerkers wie welke verzoeken afhandelt.
- Leidt medewerkers op en stel quick reference card/FAQ's op waar medewerkers snel terug kunnen vinden waar een betrokkene terecht kan met een verzoek.

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

10. Vergeten van het intrekken van rechten van een BCO medewerker en het geven van rechten voor meerdere GGD'en, leidt tot onrechtmatige verwerking van persoonsgegevens.

Applicatiebeheerders bij GGD'en moeten medewerkers van de landelijke schil rechten geven om in de systemen van de GGD te kunnen werken. Dit wordt vaak wel gedaan, maar door de drukte wordt vergeten de rechten in te trekken als de medewerker niet meer werkt voor die GGD. Daarnaast wordt vergeten de rechten op inactief te zetten als de medewerker bij een andere GGD wordt ingezet, waardoor de medewerker actieve inloggegevens heeft bij meerdere GGD'en, terwijl deze maar bij een GGD werkt op dat moment. Ook blijken medewerkers met gegevens van een andere GGD voor een GGD te werken. Hierdoor wordt het moeilijk na te gaan voor welke GGD is gewerkt en of de verwerkingen die de medewerker heeft uitgevoerd rechtmatig zijn, waardoor de kans op onder andere fraude toeneemt en fouten minder snel kunnen worden opgespoord.

Dit geldt ook voor het geven van meerdere accounts aan een landelijke BCO-medewerker. Hierdoor hebben landelijke BCO-medewerkers toegang tot de omgevingen van meerdere GGD'en, wat betekend dat ze altijd in al deze omgevingen in kunnen loggen. Dit verhoogt de kans op onrechtmatige toegang en fraude, en verkleint die kans op detectie van deze onrechtmatige toegang en fraude.

- De kans dat het risico zich manifesteert is hoog. De medewerkers kunnen gewoon bij de gegevens tot het account wordt verwijderd of op inactief wordt gezet. Dit in combinatie met slechte tot geen monitoring van de logging, zorgt ervoor dat niet kan worden achterhaald dat er iets fout gaat en de kans op fraude die door blijft gaan groot is.
  Met de multiples accounts kunnen medewerkers gelijktijdig toegang krijgen tot de verschillende omgeving waarbij deze medewerkers toegang krijgen tot een groot aantal persoonsgegevens.
- De impact is hoog. Met de gegevens kan onrechtmatige inzage worden gegeven en fraude worden gepleegd. Hier kan de betrokkene grote gevolgen van ondervinden.

Geadviseerd wordt om de volgende maatregelen te treffen:

- Stel eenduidige maatregelen rond het intrekken en op inactief zetten van accounts, zodat medewerkers geen toegang blijven houden tot een of meerdere omgevingen van de GGD.
- Maak GGD'en bewust dat ook moet worden gezorgd voor voldoende capaciteit bij de functioneel beheerders die de activatie en deactivatie van accounts verzorgen.
- Maak GGD'en bewust van de risico's en promoot een adequate logging en monitoring daarvan.

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

Het restrisico is dat GGD'en focussen op de bestrijding van corona, en daarbij vergeten in de haast en door het niet verhogen van de capaciteit van het aantal functioneel beheerders, accounts onrechtmatig op actief blijven staan. Dit geldt ook voor medewerkers en GGD'en die medewerkers op een account laten werken. Hoe drukker het wordt met BCO, hoe hoger dit restrisico.

11. Inzet van vershillende callcentra betekent verschillende handelswijzen, wat leidt tot fraude, onrechtmatige verwerking en datalekken.

De inzet van verschillende callcentra bij verschillende GGD´en resulteert in verschillende methoden van aanmelding van landelijke BCO-werknemers volgens verschillende methodes. Dit kan leiden tot verwarring bij de aanvraag van autorisaties en daardoor kunnen mensen onrechtmatig toegang krijgen tot het systeem.

Daarnaast werken callcentra vanuit hun eigen mailsystemen en met hun eigen telefoonnummers. Dit kan leiden tot verwarring bij betrokkenen, maar ook tot fraude. Mensen kunnen zich namelijk een e-mailadres aanmaken dat lijkt op het e-mailadres van het callcenter of bellen met een nummer en zich voordoen als een medewerker van het callcenter. Het is moeilijker te onderscheiden of het echt een landelijke BCO-medewerker is, of een fraudeur, omdat er geen centraal e-mailadres of telefoonnummer is.

- De kans dat het risico zich manifesteert is midden. De GGD'en zijn op de hoogte van de contactgegevens van de landelijke partners. Daarnaast worden burgers steeds waakzamer op vreemde mails en verzoeken aan de telefoon.
- De impact van het risico is hoog. Als een persoon onrechtmatige toegang krijgt, kan deze onrechtmatig gegevens verwerken. Dit geldt ook indien een persoon een vals nummer of e-mailadres aanmaakt. In dat geval kan er sprake zijn van fraude met de gegevens.

Geadviseerd wordt om de volgende maatregelen te nemen:

- Stel een uniforme werkwijze op zodat GGD'en weten dat de aanmelding van een landelijke BCO-medewerker echt door een landelijke partner wordt gedaan en stel een eenduidige werkwijze voor verificatie vast.
- Communiceerd de e-mailadressen en telefoonnummers van waaruit kan worden gebeld en zorg dat betrokkenen op de hoogte zijn wat deze mailadressen en telefoonnummers zijn. Stel betrokkenen ook op de hoogte van de vragen die ze mogen verwachten en wat zeker niet wordt gevraagd.

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

De gegevens die verzameld kunnen worden door een fraudeur zijn omvangrijk. Dit betekent dat mensen altijd een reden kunnen zien om te frauderen. De groep potentiële slachtoffers is groot en niet iedereen weet op welke signalen moet worden gelet in een geval van fraude. Daarom zal het risico altijd blijven bestaan en gezien de groep mensen, de verschillende partners en de mogelijkheid om op deze wijze gegevens te bemachtigen.

D. Beschrijving voorgenomen maatregelen

16. Maatregelen

De uitwisseling van persoonsgegevens tussen de GGD'en, GGD GHOR en de externe partners, is onontkoombaar voor de effectieve uitvoering van de nationale schil van BCO. Het verwerken en delen van die persoonsgegevens brengt echter wel verschillende risico's met zich mee, zoals beschreven in de voorgaande paragraaf. Om deze risico's tijdig in kaart te brengen en, voor zover mogelijk, in te dammen, zijn er reeds een aantal maatregelen genomen. Deze kunnen worden opgedeeld in technische en organisatorische maatregelen.

Organisatorische maatregelen:

- Het uitvoeren van een Data Protection Impact Assessment (hierna DPIA). Een DPIA is een instrument dat ingezet wordt om de privacy-risico's van gegevensverwerking in kaart te brengen en vervolgens maatregelen te kunnen nemen om de risico's te verkleinen. De hectiek en acute crisissituatie van deze pandemie maakten het niet mogelijk om de volledige risico-inventarisatie op voorhand van BCO af te ronden en te publiceren; echter privacy is continue een pijler geweest welke geborgd is in beslismomenten tijdens het proces.
- Aansluiten van een privacy professional bij alle operationale overleggen zodat privacy risico's tijdig gesignaleerd en opgepakt kunnen worden en privacy bewustzijn een cruciaal component is van de dagelijkse werkprocessen.
- Er is een kwaliteitsmanager die de samenwerking en kwaliteit van de alarmcentrales monitort en zorgt voor tijdige bijsturing. Er zijn verschillende mechanisme ingericht om continu de kwaliteit te verbeteren en een belangrijke pijler is privacy.
- Er is een expertteam ingericht van artsen, verpleegkundigen en beleidsmedewerkers. Dit zijn ervaren medewerkers die primair de medische kwaliteit bewaken. Zij passen werkinstructie continu aan op basis van de praktijk. Opgeleide artsen en verpleegkundigen zijn over het algemeen bewust van privacy-richtlijnen. Hierdoor signaleren ze naar verwachting tijdig privacy risico's. Daarnaast verwerkt dit expertteam ook aanpassingen die nodig zijn vanwege privacy en zo wordt de kwaliteit van de landelijke werkinstructie constant herzien.
- Er zijn concrete afspraken over de verhouding tussen het aantal landelijke medewerkers en het aantal BCO-coaches, teammanagers en artsen. Hierdoor borgen we dat er voldoende oog voor kwaliteit is.
- Het opstellen van een privacyverklaring die specifiek gericht is op de verwerking van persoonsgegevens in het kader van BCO, zodat betrokkenen geinformeerd worden over de BCO-gegevensverwerking.
- Trainen van BCO-medewerkers en het opstellen van een informatiepakket voor BCO-medewerkers waarin zij instructies krijgen om op een verantwoorde manier om te gaan met persoonsgegevens en privacy te waarborgen in het doorlopen van het BCO-proces.
- Het toetsen van alle juridische zaken door de Functionaris Gegevensbescherming van GGD GHOR en consultatie van één of meerdere Functionarissen Gegevensbescherming van de GGD-en;
- Eén geheimhoudingsverklaring van GGD GHOR namens de 25 GGD-en waarbij GGD GHOR regie heeft op de uitvoering van een eventuele boeteclausule bij inbreuk op de geheimhoudingsverklaring;
- Eén afspraak over het VOG-screeningsprofiel voor alle landelijke BCO-medewerkers, namelijk screeningsprofiel 45: gezondheidszorg voor mens en milieu;
- Eén verwerkersovereenkomst per externe partner namens GGD GHOR en de 25 GGD-en zodat externe partners niet meerdere verwerkersovereenkomsten hoeven te tekenen en uniforme normen gehandhaafd worden. In deze verwerkersovereenkomsten worden de

landelijke informatiebeveiligingsstandaarden van GGD GHOR (Nen7510, 7512 en 7513 en ISO 27001) gehanteerd.

- Audits bij externe partners om te controleren of zij zich houden aan de overeengekomen afspraken.

Technische maatregelen:

- Informatiebeveiligingsrichtlijnen van de GGD GHOR NL worden gehanteerd conform landelijke richtlijnen. De standaarden zijn Nen7510, 7512 en 7513 en ISO 27001.
- Landelijke BCO-medewerkers gebruiken HPZone Lite, dat enkel toegang biedt tot COVID-19 data. Toegang wordt verleend op basis van toestemming van én door de ontvangende GGD, binnen HPZone.
- Wat betreft telefonie is alleen uitgaand belverkeer mogelijk.
- Er wordt gebruikt gemaakt van meerdere actieve datacentra, zodat er in het geval van een calamiteit snel uitgeweken kan worden.
- Oprichting van een aparte opleidingsomgeving, zodat nieuwe gebruikers getraind kunnen worden zonder toegang tot een test/acceptatie-omgeving die voor andere doelen is.
- Afsluiten van een Service Level Agreement met KPN waarbij de focus ligt op de verplichtingen rondom proactieve beheeractiviteiten aan de zijde van KPN.
- Inzet autorisatiematrix en monitoring inzet bij GGD'en.

E. Bijlagen

Bijlage 1: Advies Functionaris Gegevensbescherming

Advies Functionaris Gegevensbescherming GGD GHOR over nationale opschaling van BCO en de daarop uitgevoerde DPIA

<nog niet te vullen>

Bijlage 2: Toelichting risico niveaus

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 omgeschreven 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

Risico Calculatie

Deze stap gebruikt de kans en impact om het niveau van het risico te bepalen, op basis van de beschreven aspecten:

De kans (K) dat een risico effectueert; en

De impact (I) op de 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 mitigerende maatregelen. Indien na deze mitigerende maatregelen een hoog risico voor Betrokkene blijft bestaan, dient voorafgaande raadpleging plaats te vinden bij de Autoriteit Persoonsgegevens.
Midden	Als een waarneming wordt beoordeeld als gemiddeld risico, dienen mitigerende maatregelen te worden genomen. Indien na deze mitigerende maatregelen een gemiddeld risico voor Betrokkene blijft bestaan, dient te worden verantwoord waarom het accepteren van dit risico in dit geval noodzakelijk is.
Laag	Als een waarneming wordt beschreven als een laag risico, kunnen nog steeds mitigerende maatregelen worden genomen om het risico voor Betrokkene zo veel mogelijk te beperken.