5

DPIA CoronIT

Versie datum: mei 2021
Versie 1.1
Documenteigenaar: TM Sector Corona
Advies FG: DATUM
Evaluatiedatum:

Inleiding

CoronIT is een webapplicatie die is ontwikkeld in opdracht van GGD GHOR Nederland door Topicus om het testproces van COVID-19 te centraliseren, automatiseren, versnellen en vereenvoudigen. Hierdoor kan de testcapaciteit ten volle worden benut en kan de verspreiding van COVID-19 beter worden gecontroleerd en bestreden. De opdracht tot het ontwikkelen van CoronIT is gegeven door ministerie van Volksgezondheid, Welzijn en Sport (VWS) aan GGD GHOR Nederland en het implementeren van deze webapplicatie is door VWS uitdrukkelijk gevraagd aan alle GGD'en. Daarnaast dient CoronIT als basis voor statistieken om de verspreiding van COVID-19 te monitoren en stuurbeslissingen te nemen om de verspreiding van COVID-19 onder controle te houden.

CoronIT is een registratiesysteem, waarin het testproces van COVID-19 wordt gecentraliseerd, geautomatiseerd, versneld en vereenvoudigd. In CoronIT worden slechts die persoonsgegevens verzameld die noodzakelijk zijn om te bepalen of iemand klachten heeft en getest kan worden, de test uit te laten voeren en het resultaat terug te kunnen koppelen. CoronIT is geen medisch dossier in de zin van de Wet geneeskundige behandelovereenkomst (Wgbo) en zal ook niet als zodanig worden gebruikt. Dientengevolge is de Wpg van toepassing.

In CoronIT worden de gegevens verwerkt met betrekking tot de infectieziekte die verplicht zijn gesteld te melden aan de GGD door de arts die de infectieziekte vermoed of vaststelt. Dit betekent dat in CoronIT persoonsgegevens worden verwerkt, en daarbij ook bijzondere persoonsgegevens. De autoriteit Persoonsgegevens heeft een lijst gepubliceerd[1] van soorten verwerkingen waarvoor een DPIA verplicht is[2]. In deze lijst wordt gesteld dat voor gezondheidsgegevens een DPIA dient te worden uitgevoerd. Dientengevolge wordt voor de webapplicatie CoronIT een DPIA uitgevoerd.

DPIA: landelijke format voor GGD'en

Het model gegevensbeschermingseffectbeoordeling Rijksdienst (PIA) is gebruikt als uitgangspunt voor het opstellen deze DPIA.

GGD Zaanstreek-Waterland heeft met toestemming van GGD GHOR Nederland de door de laatste opgestelde en door de FG's van de regionale GGD'en (waaronder ook de FG van GGD Zaanstreek-Waterland) aangevulde DPIA als input voor deze lokale DPIA gebruikt. Dit is versie 1.0 van mei 2021.

[1] https://autoriteitpersoonsgegevens.nl/nl/zelf-doen/data-protection-impact-assessment-dpia#voor-welke-soorten-verwerkingen-is-het-uitvoeren-van-een-dpia-verplicht-6667

[2] Zie hiervoor ook: "Besluit inzake lijst van verwerkingen van persoonsgegevens waarvoor een gegevensbeschermingseffectbeoordeling (DPIA) verplicht is, Autoriteit Persoonsgegevens" in de Staatscourant 2019 nr. 64418 van 27 november 2019.

A. Beschrijving kenmerken gegevensverwerkingen

1. Voorstel

Voorstel

Verwerking van persoonsgegevens in CoronIT

Om te zorgen dat het testproces van COVID-19 en de verstrekking van de daaruit volgende uitslag centraal, automatisch, versneld en eenvoudig verloopt, is CoronIT (een webapplicatie) ontwikkeld. In de webapplicatie worden door de aanvrager (bedrijfsarts, instellingsarts, GGD medewerker) of de betrokkene zelf (via een callcenter of portaal) de persoonsgegevens die noodzakelijk zijn voor het testen van de betrokkene ingevuld en wordt vervolgens een afspraak gepland. Aanvullende gegevens worden ingevuld als de betrokkene dit wenst. De gemaakte afspraak wordt automatisch bevestigd aan de betrokkene en voor de afspraak plaatsvindt bevestigd via e-mail en SMS, indien van toepassing ontvangt betrokkene 48 uur voor de afspraak een SMS ter herinnering. De betrokkene wordt getest bij een teststraat van de GGD. Hier worden de door de aanvrager ingevulde gegevens gecontroleerd, waarna bij de betrokkene een monster wordt afgenomen. Het afgenomen monster van de betrokkene wordt door de GGD naar het laboratorium gestuurd. Het betreft hier laboratoria waarmee de GGD (via de Dienst Testen van VWS) afspraken heeft gemaakt inzake het opsturen van monsters. Na ontvangst, worden de monsters door het laboratorium getest en worden de daaruit volgende uitslagen in CoronIT geladen. De aanvrager kan inloggen in de webapplicatie CoronIT om de uitslag te raadplegen. De betrokkene krijgt de uitslag van de test telefonisch via het callcenter of de aanvrager en kan deze inzien via het beveiligde portaal dat is opgezet.

VWS heeft GGD GHOR Nederland de opdracht gegeven om het proces te stroomlijnen en CoronIT te ontwikkelen. GGD GHOR Nederland treedt voor CoronIT op als opdrachtgever voor de ontwikkeling van de applicatie, contactpersoon met Topicus en verantwoordelijke voor het functioneel beheer.

Het callcenter en de opzet van het portaal zijn geen onderdeel van deze DPIA. Deze onderdelen zullen in een aparte DPIA worden uitgewerkt.

Aanleiding

VWS heeft GGD GHOR Nederland de opdracht gegeven om een webapplicatie te laten ontwikkelen en deze door alle GGD'en te laten implementeren om zo het testproces van COVID-19 en het communiceren van de uitslag te centraliseren en te zorgen voor een gelijke handelswijze. Daarnaast wordt de data uit CoronIT gebruikt als stuurdata tegen de verspreiding van COVID-19 en, wellicht, voor wetenschappelijk onderzoek. De basis voor de verwerking in de webapplicatie is de Wet publieke gezondheid (Wpg)[3], die ook de uitwisseling van gegevens met RIVM beschrijft.

2. Persoonsgegevens

Binnen CoronIT worden persoonsgegevens verwerkt. De gegevens die optioneel zijn, worden enkel gevuld als dit de wens van de betrokkene is. In de onderstaande tabel is per persoonsgegeven

[3] Hoofdstuk II par. 4 en hoofdstuk V Wpg

weergegeven om wat voor type persoonsgegevens (gewone, bijzondere of wettelijke identificerende) het gaat.

Persoonsgegeven	**Gewoon persoonsgegeven**	**Bijzonder persoonsgegeven**	**Wettelijk identificerend persoonsgegeven**
Voornaam en achternaam	Ja		
Geboortenaam partner (optioneel)	Ja		
Voorletters/roepnaam (optioneel)	Ja		
Postcode	Ja		
Huisnummer	Ja		
Straatnaam	Ja		
Woonplaats	Ja		
Gemeente	Ja		
Land	Ja		
Gekoppelde GGD	Ja		
Telefoonnummer (optioneel)	Ja		
E-mail	Ja		
Geslacht	Ja		
BSN			Ja
Barcode buisje	Ja		
Patiëntnummer	Ja		
Of de persoon de laatste 2 weken heeft gewerkt en zo ja, waar	Ja		
Checklist klachten		Ja	
Aantal afspraken bij GGD locaties		Ja	
Testuitslag		Ja	

De checklist met klachten wordt door de aanvrager doorgenomen met de betrokkene of online ingevuld. De checklist wordt doorgenomen en als er sprake is van de klacht, wordt deze aangekruist. De klachten zijn de volgende:

- Koorts/verhoging
- Hoesten
- Keelpijn
- Benauwdheid of kortademigheid
- Heftige spierpijn

- Neusverkouden
- Reukverlies
- Smaakverlies
- Geen van deze

Indien er sprake is van andere klachten, wordt gevraagd contact op te nemen met de huisarts.
Daarnaast wordt gevraagd:

- Sinds wanneer de betrokkene de klachten heeft;
- Of de betrokkene direct intensief contact heeft gehad met mensen die besmet waren met corona (minder dan 1,5 meter, meer dan 15 minuten);
- Of de betrokkene de afgelopen 2 weken heeft gewerkt;
- Als de betrokkene in de afgelopen 2 weken heeft gewerkt: waar dat dan was (keuze uit een lijst).
- Of de betrokkene onderdeel is van een BCO
- Of de betrokkende een melding heeft gehad via de coronamelder-app
- Of de betrokkene de afgelopen twee weken is teruggekeerd van een buitenlandse reis naar een land met oranje of rood reisadvies
- Of de betrokkene gevaccineerd is
- Of de betrokkende toestemming geeft om een eventuele positieve testuitslag door te geven aan de huisarts

3. Betrokken partijen en gegevensverwerking

Betrokken partijen en rolverdeling
In deze paragraaf worden de betrokken partijen inclusief hun rol binnen de verwerking beschreven. Indien er tussen partijen een verwerkersovereenkomst nodig is, staat dat aangegeven in deze paragraaf.

1. Ministerie van Volksgezondheid - *opdrachtgever*
   Het Ministerie van Volksgezondheid (in de vorm van de minister) is verantwoordelijk voor het leiding geven aan de bestrijding van epidemieën van infectieziekten categorie A (art. 7.1 Wpg). In dat kader zijn ze opdrachtgever aan GGD GHOR Nederland met betrekking tot het ontwikkelen van een efficiënt en gecoördineerd testproces, dat is uitgewerkt in CoronIT.

2. GGD GHOR Nederland – verwerker
   GGD GHOR Nederland is de landelijke koepel van de GGD'en en heeft de opdracht van VWS gekregen om een applicatie te laten bouwen en landelijk binnen alle GGD'en te implementeren om het testproces van COVID-19 te centraliseren, automatiseren, versnellen en vergemakkelijken, om zo ervoor te zorgen dat meer mensen kunnen worden getest. Omdat GGD GHOR Nederland vanuit de coördinerende rol invloed heeft op de verwerking van persoonsgegevens door GGD'en, is GGD GHOR Nederland samen met alle GGD'en (voor de eigen gegevens van de GGD) verantwoordelijk voor de verwerking van de persoonsgegevens in CoronIT. De verantwoordelijkheden van GGD GHOR Nederland en de GGD'en zijn vastgelegd in het 'Convenant gegevensuitwisseling gezamenlijk verantwoordelijken'. GGD GHOR Nederland heeft daarbij enkel inzage voor het ondersteunen bij het functioneel beheer, als inzage in

gegevens noodzakelijk is voor dit functioneel beheer. Daarnaast hebben medewerkers van het callcenter toegang tot CoronIT, maar dat is geen onderdeel van deze DPIA.

GGD GHOR Nederland voert in het kader van beheer controle uit op de logging. Deze gebeurt automatisch. Indien vreemde patronen worden gevonden, worden de organisaties waar de medewerkers werken op de hoogte gesteld, zodat zij kunnen zorgen voor het vervolgtraject.

GGD GHOR Nederland is verwerker voor het aanleveren van rapportages naar het RIVM en de GGD´en. De GGD´en vragen databestanden uit CoronIT op en deze worden opgesteld naar de wensen van de GGD´en. Daarnaast worden rapportages opgemaakt voor het RIVM, zodat de GGD´en deze niet apart aan hoeven te leveren.

GGD GHOR Nederland is daarnaast verantwoordelijk voor de helpdeskfunctie in het kader van het functioneel beheer en de verwerking van persoonsgegevens in het kader van deze functie. GGD GHOR Nederland zou voor deze taken gekwalificeerd kunnen worden als verwerker.

De verantwoordelijkheden van GGD GHOR Nederland en de GGD'en zijn vastgelegd in het 'Convenant gegevensuitwisseling gezamenlijk verantwoordelijken'.

3. De lokale GGD'en – *zelfstandig verwerkingsverantwoordelijken en tevens gezamenlijk verantwoordelijk*
   De GGD'en zijn verwerkingsverantwoordelijk voor de verwerking van de persoonsgegevens van de geteste personen in hun regio in CoronIT. GGD GHOR Nederland zal deze gegevens niet verwerken zonder dat hiervoor aanleiding is. Die aanleiding kan een probleem in de applicatie zijn die wordt gemeld vanuit een GGD of een vraag van een GGD waarbij het noodzakelijk is dat de gegevens kunnen worden ingezien. De GGD beslist wie binnen de organisatie rechten toegekend krijgt en van wie rechten in moeten worden getrokken.

   De GGD'en zijn gezamenlijk verantwoordelijk met GGD GHOR Nederland voor ontwikkelingen in de applicatie, waarbij GGD GHOR Nederland het enkele aanspreekpunt is naar Topicus, zoals is vastgesteld in het convenant. Op deze wijze komen verzoeken via GGD GHOR Nederland binnen en kan worden dat Topicus indien nodig op de hoogte wordt gebracht en dubbele vragen worden voorkomen.

4. RIVM – *verwerker*
   Het RIVM krijgt een gepseudonimiseerde lijst met data aangeleverd door GGD GHOR Nederland op basis van art. 28 Wet publieke gezondheid. Het RIVM gebruikt deze gegevens om rapportages op te kunnen stellen, die dienen als stuurinformatie tijdens de COVID-19 pandemie voor VWS. Het RIVM bepaalt hoe deze gegevens worden geanalyseerd en gebruikt voor rapportages.

5. Topicus – *verwerker*

Topicus heeft de applicatie in opdracht van GGD GHOR Nederland ontwikkeld en zorgt voor het technisch beheer. Om de applicatie technisch te kunnen beheren, hebben ze toegang tot de data, die zij enkel in kunnen zien als dit noodzakelijk is voor het technisch beheer. Tussen Topicus en GGD GHOR Nederland (als vertegenwoordiger van de GGD'en zoals vastgesteld in het convenant) is een verwerkersovereenkomst gesloten.

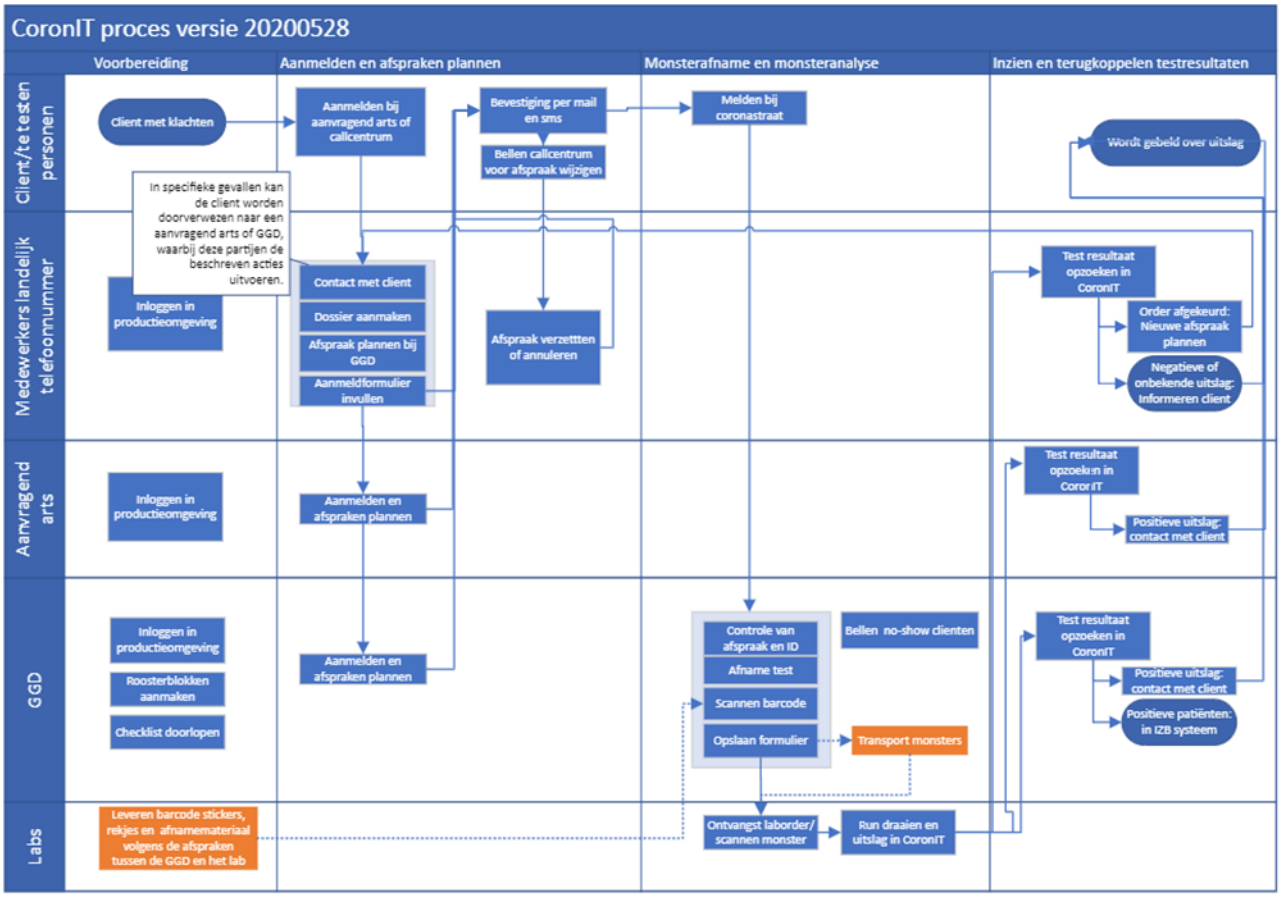
6. Externe aanvragers – *verwerkers*
   Externe aanvragers (nu nog enkel bedrijfsartsen) zijn in dit geval alle externen die gegevens invoeren voor de betrokkene. Zij krijgen allen inloggegevens om de betrokkene aan te melden voor een test en om de afspraak in de plannen. Vervolgens krijgen zij de uitslag ook teruggekoppeld. Zij zijn verantwoordelijk voor de gegevens die zij verwerken in dit proces. Hier zijn externe aanvragers arbo- en instellingsartsen.

7. Laboratoria – *verwerkers*
   Laboratoria ontvangen van de GGD'en monsters om te analyseren op besmetting met COVID-19. Er zijn verschillende labs in de keten, namelijk de labs die al voor de GGD'en werkten, maar ook labs die zijn bijgeschakeld om de hoge aantallen monsters te kunnen analyseren. Het landschap en de afspraken met de labs zijn daarom verspreid. Dat geldt ook voor de gegevens die naar de labs gaan. Landelijke labs ontvangen vaak enkel een barcode, soms aangevuld met een geboortedatum, terwijl labs bij GGD'en meer informatie over de persoon kunnen ontvangen.

Gegevensverwerking en rolverdeling
In deze paragraaf wordt weergegeven welke stappen worden genomen in het testproces in CoronIT en wie deze stappen uitvoert. Hieronder wordt grafisch weergegeven welke partijen welke stappen uitvoeren. De voorbereiding van de teststraat is niet meegenomen, omdat dit proces niet binnen CoronIT valt, maar wel illustreert hoe het testproces verloopt.

De verantwoordelijkheden zoals in hoofdstuk 3 zijn beschreven zijn niet conform het gestelde door GGD GHOR Nederland. De FG van GGD Zaanstreek-Waterland is hiertoe gekomen na een consultatie met de bedrijfsjurist en vele collega FG's .

Oorspronkelijk heeft GGD GHOR Nederland gekozen voor gezamenlijke verantwoordelijkheid voor GGD'en, GGD GHOR, zelfstandig verwerkingsverantwoordelijke [redacted] als verwerker en labs als zelfstandig verwerkingsverantwoordelijke.


CoronIT proces versie 20200528
Voorbereiding
Aanmelden en afspraken plannen
Monsterafname en monsteranalyse
Inzien en terugkoppelen testresultaten
Client/testen personen
Medewerkers landelijk telefoonnummer
Aanvragend arts
GGD
Labs
Client met klachten
Aanmelden bij aanvragend arts of callcentrum
Bevestiging per mail en sms
Bellen callcentrum voor afspraak wijzigen
Melden bij coronastraat
Wordt gebeld over uitslag
In specifieke gevallen kan de client worden doorverwezen naar een aanvragend arts of GGD, waarbij deze partijen de beschreven acties uitvoeren.
Inloggen in productieomgeving
Contact met client
Dossier aanmaken
Afspraak plannen bij GGD
Aanmeldformulier invullen
Afspraak verzetttten of annuleren
Test resultaat opzoeken in CoronIT
Order afgekeurd: Nieuwe afspraak plannen
Negatieve of onbekende uitslag: Informeren client
Inloggen in productieomgeving
Aanmelden en afspraken plannen
Test resultaat opzoeken in CoronIT
Positieve uitslag: contact met client
Inloggen in productieomgeving
Roosterblokken aanmaken
Checklist doorlopen
Aanmelden en afspraken plannen
Controle van afspraak en ID
Afname test
Scannen barcode
Opslaan formulier
Bellen no-show clienten
Transport monsters
Test resultaat opzoeken in CoronIT
Positieve uitslag: contact met client
Positieve patiënten: in IZB systeem
Leveren barcode stickers, rekjes en afnamemateriaal volgens de afspraken tussen de GGD en het lab
Ontvangst laborder/ scannen monster
Run draaien en uitslag in CoronIT

Voorbereidingen teststraat

De medewerkers van de GGD zorgen dat het rooster van de medewerkers van de teststraat het rooster uploaden in CoronIT. Hierbij wordt gezorgd dat de capaciteit in de teststraat overeenkomt met het rooster in CoronIT.
Daarnaast wordt gezorgd dat alle juiste afnamematerialen beschikbaar zijn op de teststraat. Het betreft hier:

- Buisjes met een barcode;
- Correcte swabs;
- PBM;
- Laptops en scanners.

Op locatie zijn mensen beschikbaar voor het aanmelden van de betrokkene en het koppelen van de betrokkene aan het correctie buisje via de scanners op locatie.
Voor het transport zijn transportafspraken gemaakt, waarin is vastgesteld wanneer en door wie de buisjes worden opgehaald voor analyse in het laboratorium (MML's en landelijke labs).
De medewerkers hebben, voordat zij in de teststraat zullen werken, instructies gekregen en een korte training gevolgd om de werkzaamheden correct uit te kunnen voeren.
De betrokkene komt op afspraak en heeft ook informatie gehad over wie moet worden gebeld om de afspraak te verzetten.

Stap 1: Verzoek betrokkene tot testen

De aanvraag tot testen kan op verschillende manieren worden ingediend. De volgende opties zijn beschikbaar:

- De betrokkene kan een verzoek indienen om een test te laten uitvoeren bij een aanvrager (arts, bedrijfsarts, GGD). De betrokkene dient het verzoek in en zal contact op moeten nemen met een aanvrager om te verzoeken te worden getest. Deze route is de minst gebruikte route voor testen bij de GGD.
- De betrokkene kan bellen naar het landelijke callcenter. Een medewerker zal eerst een boodschap horen over wanneer ze getest mogen worden en wat aanvullende informatie, waarna en medewerker de betrokkene te woord zal staan. De medewerker controleert of de betrokkene voldoet aan de in het beleid vastgestelde testeisen. Deze optie is verder uitgewerkt in de DPIA callcenter.
- De betrokkene kan een afspraak maken via het burgerportaal. Hierbij vult de betrokkene eerst een aantal vragen in met betrekking tot de mogelijkheid om de teststraat te bereiken en de klachten, waarbij vervolgens wordt beoordeeld of de betrokkene zelf de afspraak kan inplannen door in te loggen met DigiD en de testlocatie en tijd te kiezen. Deze optie is verder uitgewerkt in de DPIA burgerportaal.

Stap 2: Checklist klachten en plannen van de afspraak

Indien de betrokkene contact opneemt met een aanvrager, zal de aanvrager starten met het doornemen van een checklist met klachten. Aan de hand daarvan wordt besloten of de betrokkene mag worden getest. Indien uit de checklist blijft dat er klachten zijn en dat de betrokkene mag worden getest, zal de aanvrager in CoronIT de persoonsgegevens van de betrokkene invoeren in een dossier (zoals benoemd in 2. Persoonsgegevens), alsook de gegevens uit de anamnese die is

afgegeven en overeenkomen met de gegevens gesteld in art. 24 Wpg. Vervolgens opent de aanvrager het rooster van de GGD waar de persoon zal worden getest en een afspraak inplannen. Indien de betrokkene zich aanmeldt via het callcenter, zal de medewerker de gegevens van de betrokkene registreren en de checklist met klachten met de betrokkene doornemen. Indien er klachten zijn, zal de medewerker een afspraak inplannen. In sommige gevallen wordt de betrokkene direct doorverwezen naar de GGD, waar het proces verder wordt afgehandeld. De medewerker van het callcenter plant een test in voor de betrokkene.
De betrokkene ontvangt per mail een bevestiging van de afspraak met daarin de datum, tijd en locatie van de test. Tevens wordt in deze mail ook verwezen naar de privacyverklaring, zodat de betrokkene kan lezen wat met zijn/haar gegevens wordt gedaan. Daarnaast wordt een SMS verstuurd met daarin het tijdstip en de locatie van de afspraak.
Indien van toepassing, krijgt de betrokkene ook een SMS-herinnering 48 uur voor de afspraak.
Ook indien de betrokkene een afspraak maakt in het burgerportaal, worden dee-mail en de SMS verstuurd met de afspraakbevestiging, met daarin de datum, tijd en locatie van de test. Indien van toepassing, krijgt de betrokkene ook een SMS-herinnering 48 uur voor de afspraak.

Stap 3: Betrokkene meldt zich voor de test

De betrokkene meldt zich bij de receptie of de teststraat van de testlocatie. De medewerker van de receptie of testraat van de testlocatie controleert of de betrokkene aangemeld is in het systeem en controleert het ID.

Stap 4: Afname van het monster

De betrokkene meldt zich bij de ruimte waar het monster zal worden afgenomen. De bemonsteraar neemt het monster af en stopt dit in de buis met de streepjescode. De barcode wordt gescand en wordt in CoronIT geladen. Vervolgens wordt deze klaargelegd bij de andere monsters voor transport naar het lab.
Als de buis wordt gescand en deze is van een MML-lab, dan ontvangt de MML een laborder. Als de buis van een pandemielab is, dan wordt er niet gewerkt met lab orders. Bij de pandemielabs wordt enkel de de buis met barcode opgestuurd, op basis waarvan het monster wordt getest en de uitslag in het systeem wordt geladen.

Stap 5: Ophalen van het monster door transportdienst

De transportdienst zal, volgens afspraak met de betreffende GGD, de monsters ophalen om te worden vervoerd naar het lab dat het monster zal analyseren.

Stap 6: Aankomst in het laboratorium

Het monster wordt geregistreerd in het lab. Het MML heeft een laborder ontvangen en heeft daarbij de gegevens van de betrokkene. Een pandemielab heeft enkel de barcode.

Stap 7: Draaien run

Het lab analyseert de monsters.

Stap 8: Uitslag beschikbaar

Na analyse is de uitslag beschikbaar en wordt via een koppeling tussen de labsystemen en CoronIT in CoronIT geladen.
De verwerking van het lab valt niet onder de scope van deze DPIA.

Stap 9: Terugkoppelen

De wijze waarop de uitslag wordt teruggekoppeld, is afhankelijk van de manier waarop de test is aangevraagd en de uitslag.

- De uitslag wordt teruggekoppeld via de aanvrager van de test, indien deze door een aanvrager is aangevraagd. De aanvrager kan inloggen in CoronIT om de uitslagen in te zien en zal vervolgens de uitslag terugkoppelen aan de betrokkene.
- Indien de aanvraag is gedaan via het callcenter, zijn er twee opties afhankelijk van de uitslag:
    - Negatief resultaat: een callcenter medewerker geeft de uitslag door;
    - Positief resultaat: de GGD van de regio waar de betrokkene is getest geeft de uitslag door.
- Alle uitslagen zijn door betrokkene ook in te zien via het portaal. Betrokkene moet daarvoor inloggen met behulp van DigiD.

Rapportage

CoronIT kent zelf geen rapportage-functies. Ten behoeve van rapportages worden gegevens uit CoronIT doorgegeven aan het Healthcare Intelligence Platform van GGD GHOR Nederland. Vanuit dit platform worden verschillende rapportages aangeleverd. De gegevens helpen de partijen om een overzicht te houden van de pandemie en de ontwikkelingen daarin in hun werkveld. Deze rapportages zijn geanomiseerd. Voor de GGD en het RIVM zijn de gegevens gepseudonimiseerd, omdat een kans bestaat dat iemand herleid zou kunnen worden door de aangeleverde gegevens. De partijen ontvangen de volgende gegevens:

- De GGD ontvangt een complete dataset, zodat zij de data uit de eigen regio kunnen analyseren.
- Het RIVM ontvangt een rapportage met alle records van testen met geanonimiseerde patiëntgegevens (geen BSN of adres), PC3, klachten en testuitslag, op basis van art. 28 Wpg. Dit is een gespeundonimiseerde set, aangezien deze niet direct herleidbaar is.
- Het LCDK ontvangt productiecijfers, namelijk aantal (positieve) testuitslagen per dag, GGD, Laboratorium, beroepsgroep, leeftijdscategorie, geslacht en gemeente. Deze set is gepseudinimiseerd, echter lijkt de kans op herleiding zeer klein.
- LOTC
- Teleperformance, leverancier van het klantcontactcentrum ontvangt lijsten met betrokkenen die negatief zijn getest en moeten worden gebeld door medewerkers van Teleperformance.
- CBS
- GGD GHOR Nederland

4. Verwerkingsdoeleinden

Het doel van de verwerking is het centraliseren, automatiseren, versnellen en vergemakkelijken van het COVID-19 testproces en het geven van inzicht in de ontwikkeling van de pandemie. Met CoronIT kan het aanvragen van een test, het maken van een afspraak, het testen en het melden van de uitslag worden vergemakkelijkt en versnelt. Daarnaast krijgt de GGD direct de gegevens die verplicht gemeld moeten worden zoals beschreven in art. 24 Wpg. Ten slotte worden de gegevens

zo ook op een gelijke wijze gemeld aan het RIVM conform art. 28 Wpg, op basis waarvan stuurbeslissingen kunnen worden gemaakt. Door middel van deze stuurinformatie en stuurbeslissingen kan de verspreiding van COVID-19 worden beheerst.

5. Belangen bij gegevensverwerking

Samenleving als geheel

De samenleving als geheel heeft een aantal belangen bij het gebruik van CoronIT. Het centraliseert, automatiseert, vesnelt en vereenvoudigt het testproces, waardoor de volgende zaken gemakkelijker en betrouwbaar verlopen:

- Het testen van betrokkenen en het delen van de uitslag van de test zodat betrokkenen weten of ze maatregelen moeten nemen of niet;
- Melden van infectieziekten bij de GGD, zodat kan worden gestart met bron- en contactonderzoek indien dit nodig is;
- Het verstrekken van rapportages die inzicht geven in de verspreiding van COVID-19 en zo dienen om te sturen op het bestrijden van COVID-19;
- Door het snelle testen, weten mensen of ze kunnen blijven werken (bij een negatief resultaat) of maatregelen moeten nemen (bij een positief resultaat). Dit komt ten goede aan de volksgezondheid en de economie.

Betrokkenen

Door CoronIT kan snel en eenvoudig een betrokkene worden aangemeld en getest. De uitslag kan vervolgens snel worden teruggekoppeld aan de betrokkene, zodat deze de juiste maatregelen kan treffen om zijn/haar gezondheid te beschermen en verspreiding van COVID-19 te voorkomen. Het snelle testen kan de betrokkene ook geruststellen over de gezondheid.

GGD GHOR Nederland

Verzorgen van functioneel beheer van de applicatie, coördineren van de implementatie en het functioneren van de applicatie en het creëren van voldoende testcapaciteit. Daarnaast wordt ervoor gezorgd dat rapportages worden opgemaakt voor de GGD'en en het RIVM. Zij hebben een belang om de applicatie goed te laten lopen en de testen effeciënt te kunnen laten verlopen via CoroniT, samen met de GGD'en.

GGD

Door het inplannen van afspraken door het callcenter, een aanvrager of via het portaal, kan de GGD efficiënt testen in de teststraten en wordt het maken van afspraken uit handen genomen. De GGD zorgt voor teststraten en het doorsturen van monsters naar laboratoria, zodat de monsters snel geanalyseerd kunnen worden en de uitslagen kunnen worden gecommuniceeerd Daarnaast ontvangt de GGD snel de testresulaten van positief geteste betrokkenen, zodat ze snel kunnen starten met het bron- en contactonderzoek. Zij hebben er baat bij dat voldoende testcapaciteit bestaat om te weten wie besmet is met COVID-19 en aan de hand daarvan gericht Bron- en Contactonderzoek te kunnen doen.

RIVM

In kaart brengen van de stand van zaken en ontwikkeling van de verspreiding van COVID-19 in Nederland. De informatie uit CoronIT wordt gepseudonimiseerd verstrekt aan het RIVM en dient om te voorzien in stuurinformatie.

Ministerie van Volksgezondheid
Het ministerie, vertegenwoordigd door de minister, is op basis van de Wet publieke gezondheid (Wpg artikel 7.1) verantwoordelijk voor het coordineren van de bestrijding van epidemieen van infectieziekenten categorie A (zoals corona). Het ministerie (en de minister) hebben derhalve belang bij het op een verantwoorde manier uitbreiden van de capiciteit om testafspraken te maken.

6. Verwerkingslocaties
De gegevens die in CoronIT worden verwerkt, worden verwerkt in Nederland, dus binnen de Europese Unie.

Verwerkers is gesteld dat gegevens niet buiten de EER mogen worden verwerkt.

[redacted]

8. Juridisch en beleidsmatig kader
Voor de verwerking in CoronIT is de volgende wet- en regelgeving van toepassing:

- Algemene Verordening Gegevensbescherming (AVG);
- Uitvoeringswet AVG (UAVG);
- Wet publieke gezondheid (Wpg);
- Wet Geneeskundige Behandel Overeenkomst (WGBO);
- Archiefwet.

9. Bewaartermijn
Voor gegevens van een melding van een infectieziekte, is in art. 29 Wpg een bewaartermijn bepaald van 5 jaar. Dit is een maximale termijn. In praktijk zullen gegevens dus niet langer bewaard worden dan noodzakelijk is voor het in kaart brengen en bestrijden van de pandemie, met een maximum van 5 jaar. Periodiek zal worden bekeken of de gegevens nog noodzakelijk zijn.

B. Beoordeling rechtmatigheid gegevensverwerkingen

10. Rechtsgrond

Het proces in CoronIT verloopt tweeledig. Ten eerste is er een aanmelding door een arts. Deze arts vermoed een COVID-19 besmetting en wil de persoon graag aanmelden voor een test. De arts plant een afspraak in CoronIT en de betrokkene krijgt daar een afspraakbevestiging. De betrokkene meldt zich vervolgens bij de GGD en daar wordt een monster afgenomen. Het monster wordt geanalyseerd door het lab, en de arts krijgt de uitslag, die aan de betrokkene wordt gemeld. COVID-19 is gekwalificeerd als een infectieziekte in categorie A.
De arts is volgens art. 21 Wet Publieke gezondheid (Wpg) verplicht een melding te maken aan de GGD indien er sprake is van een vermoeden of een vaststelling van een infectieziekte bij een patiënt. Als een arts een betrokkene aanmeldt, wordt deze getest, waarna de testuitslag aan de GGD wordt doorgegeven, om zo verder te kunnen handelen. CoronIT is op zichzelf dus geen meldsysteem, maar vanuit de testresultaten wordt wel gemeld bij de GGD wat de uitslagen waren van de test. De arts meldt daarbij alle zaken in CoronIT als anamnese zoals gesteld in art. 24 Wpg.
De tweede route voor het aanmelden voor een test, is via een callcenter of een online portaal. Hierbij kan een betrokkene zichzelf aanmelden. Via de telefoon zal door een callcenter medewerker worden gevraagd welke klachten er zijn, zodat kan worden bepaald of een test noodzakelijk is. Als de betrokkene staat op een test, zal deze worden afgenomen. Via het portaal moet de betrokkene een formulier invullen met de klachten, gelijk aan de vragen die worden gesteld door het callcenter. Als er geen klachten zijn, wordt de betrokkene verzocht het callcenter te bellen.
Het hele proces in CoronIT is gericht op het snel kunnen testen en verstrekken van de uitslag van een COVID-19 test. In het proces worden daarna de resultaten gemeld aan de GGD, zodat zij kunnen voldoen aan de wettelijke plicht die uit de Wpg op hen rust, namelijk de bestrijding van infectieziekten.
De verwerking van niet-bijzondere persoonsgegevens is toegestaan o.b.v. minimaal één van de zes grondslagen van de AVG [4]. Voor de verwerking van (gewone) persoonsgegevens in CoronIT wordt een beroep gedaan op art. 6 lid 1 sub c en e AVG:

- De verwerking is noodzakelijk om te voldoen aan een wettelijke verplichting die op de verwerkingsverantwoordelijke rust. Dit geldt voor het waar de exacte gegevens zijn bepaald, namelijk art. 24 en 28 Wpg.
- De verwerking is noodzakelijk voor de vervulling van een taak van algemeen belang of van een taak in het kader van de uitoefening van het openbaar gezag dat aan de verwerkingsverantwoordelijke is opgedragen.

Er is sprake van een verplichting tot het bestrijden van de pandemie, vastgelegd in de Wet publieke gezondheid (Wpg), waarin wordt gesteld hoe moet worden gehandeld bij bestrijding van een infectieziekte. Deze bestrijding is in het algemeen belang. De Wpg biedt echter niet een specifieke handelwijze voor infectieziekten in de categorie A, waardoor niet alle verwerkingen binnen CoronIT direct beschreven zijn in de wet. De Wpg biedt echter de mogelijkheid aan de minister en veiligheidsregio's om maatregelen te nemen, waaronder de opdrachtverstrekking tot ontwikkeling van een landelijk testsysteem.

[4] Artikel 6 AVG.

11. Bijzondere persoonsgegevens

Voor het verwerken van bijzondere persoonsgegevens is het noodzakelijk dat er een wettelijke uitzondering van toepassing is, zoals gesteld in art. 9 AVG. De verwerking valt onder de uitzondering zoals bepaald in art. 9 lid i AVG:

Art. 9 lid 2 sub i AVG:

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

De Wpg is een lex specialis, de UAVG een lex generalis. Dit betekent dat de Wpg, die de mogelijkheid geeft tot het verwerken van (medische) persoonsgegevens voorrang heeft op de UAVG. Het is daarom niet noodzakelijk dat de UAVG een uitzondering biedt voor de verwerking in CoronIT, omdat de Wpg deze grondslag als lex specialis biedt.

De uitzonderingen in de AVG vereisen een grond in unierecht of lidstatelijk recht. Deze grond is te vinden in de Wpg en voor CoronIT in art. 6 lid 2 en 4 Wpg. Daarin is gesteld dat de veiligheidsregio zorg draagt voor de voorbereiding op de bestrijding en de bestrijding van een infectieziekte. Daarbij is door VWS besloten dat, om de bestrijding te stroomlijnen, GGD GHOR Nederland dit proces op te laten pakken en CoronIT te ontwikkelen.

In de memorie van toelichting is opgenomen dat *'de medewerking van de bevolking op vrijwillige basis aan te treffen noodzakelijke maatregelen staat immers voorop bij de infectieziektebestrijding'*. Gesteld kan worden dat dit ook geldt voor het vrijwillig aanmelden voor een coronatest.

In het kader daarvan kan worden gesteld dat in het kader van het algemeen belang (zoals gesteld in art. 9, lid 2 sub i AVG en art. 6 lid 1 sub e AVG) en op basis van de Wpg, kan worden gesteld dat het testen van de betrokkene en de registratie van eventuele symptomen wordt uitgevoerd in het algemeen belang in het kader van de bestrijding van een infectieziekte. Voor het testen en registratie is het echter noodzakelijk de betrokkene goed te informeren over de verwerking van de persoonsgegevens.

De persoonsgegevens die worden verwerkt in CoronIT, zijn enkel de gegevens die verplicht zijn om te worden opgenomen in de registratie van de GGD'en, zoals deze zijn bepaald in art. 24 Wpg als een arts een melding doet van een infectieziekte. Andere persoonsgegevens zijn optioneel, indien de betrokkene wenst dat deze gegevens ook worden opgenomen. Deze gegevens worden in de registratie opgenomen, omdat de GGD'en vanuit CoronIT de positieve uitslagen gemeld krijgen en

zo de juiste informatie verstrekt krijgen. Daarnaast stelt de Wpg stelt dat een (vermoeden van) een besmetting van een infectieziekte moet worden geregistreerd. Aangezien enkel wordt getest op basis van symptomen die overeen kunnen komen met een COVID-19 besmetting, mogen deze worden geregistreerd in CoronIT.

12. Doelbinding

CoronIT is een registratiesysteem waarin een betrokkene kan worden aangemeld of zichzelf kan aanmelden voor een coronatest. De betrokkene wordt geregistreerd, een afspraak kan worden gemaakt voor een test, de gegevens kunnen worden ingezien door de afnemer van de test bij het afnemen van het monster ter verificatie en de uitslag van de test kan worden geregistreerd, om zo weer te worden gemeld aan de betrokkene of de arts, indien de aanvraag door een arts is gedaan. Dit versnelt het proces en stroomlijnt de data. Het doel van de verwerking van gegevens in CoronIT is dus het uniform en efficiënt testen van mensen, door het hele proces in één systeem uit te voeren.

Daarnaast worden de gegevens verstrekt aan het RIVM volgens art. 28 Wpg, dat rapportages opstelt voor VWS. Hierdoor kan VWS adequatere beslissingen nemen in de bestrijding van COVID-19.

13. Noodzaak en evenredigheid

Bij de start van het ontwikkelen van CoronIT is nagedacht hoe de COVID-19 pandemie het best kan worden bestreden. Een van de oplossingen is het stroomlijnen van het testproces, waarbij tevens direct een melding bij de GGD wordt gedaan zoals verplicht is gesteld door de Wpg. Enkel het snel kunnen testen via een landelijk systeem, zorgt ervoor dat gecentraliseerd en snel inzicht wordt verkregen in de situatie rondom COVID-19 en dat adequate beslissingen kunnen worden genomen rond de bestrijding van COVID-19 door VWS.

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

Wat betreft de proportionaliteit: de applicatie is opgebouwd om te zorgen dat testen op een snelle en gecentraliseerde wijze worden afgenomen. Verder worden op deze wijze de GGD’en ontlast, waardoor zij zich kunnen richten op de andere taken die zij hebben in het kader van de bestrijding van de pandemie.

Daarnaast wordt gezorgd dat de gegevens op een eenduidige wijze worden doorgezet naar de laboratoria en wordt zo het testproces versneld, zodat de betrokkene snel de uitslag van de test krijgt. CoronIT zorgt dat het hele proces gestroomlijnd wordt omdat heel duidelijk is gesteld welke persoonsgegevens per stap nodig zijn en dit de enige manier is om de persoonsgegevens te melden voor een test en dus ook voor een wettelijk verplichte melding aan de betrokkene.
Voor elk gegeven dat wordt gevraagd is er of een wettelijke grondslag in art. 24 Wpg, of is er een afweging gemaakt waarvoor deze gegevens worden verwerkt en wat de impact is van het

uitvragen van dit gegeven op de persoonlijke levenssfeer van de betrokkene. Daarnaast is de betrokkene niet verplicht deze gegevens te verstrekken als hij/zij dat niet wenst.

Wat betreft de subsidiariteit: deze applicatie is gemaakt zodat het proces wordt gestroomlijnd en de gegevens snel en uniform worden gemeld. Andere applicaties zijn daardoor overbodig in het meld- en testproces, wat betekent dat een wildgroei aan applicaties en verscheidenheid aan gemelde informatie wordt vermeden. Dit zorgt ook voor rapportages die betrouwbaarder zijn en zorgen dat adequatere keuzes kunnen worden gemaakt. Daarnaast gaan er geen persoonsgegevens verloren, omdat alles in een systeem wordt verwerkt en niet overal en nergens in verschillende systemen worden verwerkt.

14. Rechten van betrokkenen

In CoronIT worden zowel gewone als bijzondere persoonsgegevens verwerkt. Omdat die persoonsgegevens worden verwerkt, hebben betrokkenen een aantal rechten, zoals bepaald in hoofdstuk III AVG. Verzoeken tot het uitoefenen van een van de rechten kunnen worden ingediend bij de GGD waar de betrokkene zich heeft laten testen. GGD'en beslissen zelf over het wel of niet uitvoering geven aan het verzoek van de betrokkene. Indien een verwijderingsverzoek is ingediend en de GGD besluit aan dit verzoek te voldoen, dan kan aan GGD GHOR Nederland worden gevraagd deze gegevens te verwijderen.

Recht op informatie (art. 13 AVG):

De betrokkene heeft recht om informatie te ontvangen over de verwerking van zijn/haar persoonsgegevens. Om deze informatie te verstrekken, wordt in de afspraakbevestiging en disclaimer vermeld dat in het kader van het testproces in CoronIT persoonsgegevens worden verzameld, waarbij wordt gelinkt naar de privacyverklaring van de gegevensverzameling in CoronIT.

Daarnaast is een privacyverklaring over de verwerking van gegevens in CoronIT online gepubliceerd op de website van GGD GHOR Nederland, waar GGD'en naar kunnen verwijzen op hun website.

Recht op inzage en afschrift (art. 15 AVG)

De betrokkene heeft het recht om zijn/haar gegevens in te zien. De gegevens kunnen worden opgevraagd bij de GGD waar de test is afgenomen en daar kan ook een afschrift worden verkregen.

Recht op rectificatie (art. 16 AVG)

De betrokkene heeft het recht om gegevens die niet (langer) juist zijn, te laten rectificeren. Een aanvraag daartoe kan de betrokkene indienen bij de GGD waar de test is afgenomen.

Recht op gegevenswissing (art. 17 AVG)

De betrokkene kan verzoeken persoonsgegevens te wissen. De GGD zal daar een zorgvuldige afweging voor moeten maken. Indien de GGD beslist dat de persoonsgegevens kunnen worden verwijderd, wordt een verzoek ingediend bij GGD GHOR Nederland om de gegevens te wissen.

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

Recht op overdraagbaarheid van de gegevens (art. 20 AVG)
De betrokkene kan bij de GGD waar hij getest is verzoeken om zijn gegevens over te dragen in een gangbare vorm. Indien de GGD dit direct kan doorsturen naar de gewenste ontvanger, zal dit worden verzorgd. Indien dit niet mogelijk is, zal de GGD de gegevens in een technisch gangbaar formaat aan de betrokkene overhandigen.

Recht van bezwaar (art. 21 AVG)
De betrokkene heeft het recht om in de wet bepaalde gevallen bezwaar te maken tegen de verwerking van persoonsgegevens, wanneer de individuele omstandigheden van het geval dit rechtvaardigen.

Het bezwaar kan worden ingediend bij de GGD waar de betrokkene is getest. De GGD zal het verzoek behandelen.

Recht om niet te worden onderworpen aan geautomatiseerde individuele besluitvorming (art. 22 AVG)
Er is geen sprake van geautomatiseerde besluitvorming in de zin van art. 22 AVG.

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 gedistilleerd. Hieronder is per risico kort uiteengezet wat het risico voor betrokkenen is en hoe dit risico gekwalificeerd dient te worden. In bijlage 2 wordt beschreven welke maatregelen zijn genomen indien de risico's in een update van deze DPIA zijn opgelost of gemitigeerd.

De kwalificatie wordt gemaakt op basis van kans x impact = risiconiveau. In bijlage 3 is een uitgebreide omschrijving opgenomen van de berekening en definities van kans, impact en risiconiveaus. Hieronder is aangegeven hoe de uiteindelijke risico calculatie plaatsvindt.

Risico Calculatie
We gebruiken de kans en impact om het niveau van het risico te bepalen, op basis van de beschreven aspecten:

- De kans (K) dat een risico effectueert; en
- De impact (I) op de organisatie of de Betrokkene als het risico is geëffectueerd.

Het risiconiveau wordt toegekend door een vooraf vastgestelde matrix die het belang van mitigerende maatregelen aangeeft. De combinaties van kans en impact zijn gegroepeerd in hoog (H, rood), midden (M, geel) en laag (L, groen). De matrix toont hoe de risico's zijn geclassificeerd gebaseerd op de impact en kans.

Kans → / Impact ↓	Laag	Middel	Hoog
Laag	Laag	Laag	Middel
Midden	Laag	Middel	Hoog
Hoog	Middel	Hoog	Hoog

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

Risico Niveau	Risico Beschrijving en te verwachten maatregel
Hoog	Als een waarneming of bevinding wordt geëvalueerd als een hoog risico, is er sterke behoefte aan corrigerende maatregelen. Een bestaand systeem kan blijven werken, maar een beveiligingsplan of andere risico-beperkende maatregel moet zo snel mogelijk worden geïmplementeerd.
Midden	Als een waarneming wordt beoordeeld als gemiddeld risico, moeten eventuele corrigerende maatregelen worden overwogen.
Laag	Als een waarneming wordt beschreven als een laag risico, kunnen corrigerende maatregelen nog steeds nodig zijn of kan het risico worden geaccepteerd.

1. *Geen logging van inzage afsprakenoverzicht*

Binnen CoronIT is geen logging aangezet op de inzage van het afsprakenoverzicht. In het afsprakenoverzicht is de naam, geboortedatum, geslacht, testlocatie, testdatum en testtijd te zien. Medewerkers kunnen zich hierdoor onrechtmatig inzage verschaffen in afspraakgegevens van betrokkenen.

- De kans dat dit risico zich manifesteert zonder maatregelen is hoog. Immers is het afsprakenoverzicht voor medewerkers toegankelijk en bijvoorbeeld snel worden gecontroleerd wanneer de afspraak van iemand is gepland.
- De impact van dit risico zonder maatregelen is middel. De gegevens bevatten geen medische gegevens, maar wel waar iemand op een exact moment te vinden is.

Geadviseerd wordt om de volgende maatregelen te nemen:

- Activeer logging op het afsprakenoverzicht, zodat duidelijk is wie zich wanneer toegang heeft verschaft tot het afsprakenoverzicht.
-

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

2. *Geen controle op de logging*

Binnen CoronIT is logging ingeregeld, maar de logging wordt niet actief op periodieke wijze en automatisch gecontroleerd. Voor deze controle is geen beleid opgezet, zodat niet is vastgelegd hoe en door wie deze controle zal worden uitgevoerd. Hierdoor is de kans groot dat misbruik wordt gemaakt van de gegevens in CoronIT, maar dat dit niet wordt opgemerkt.

- De kans dat het risico zich manifesteert zonder maatregelen is hoog. Er zijn veel autorisaties uitgegeven voor toegang tot CoronIT, waarbij medewerkers en externen toegang hebben tot (een bepaald deel van) de gegevens. Bij de aantallen medewerkers die in dienst zijn en zijn ingehuurd, is de kans groot dat iemand, kwaadwillend of niet, onrechtmatig dossiers opent.
- De impact van het risico is hoog. In CoronIT zijn medische gegevens en het BSN opgenomen, alsook contactgegevens. Hier kan op verschillende wijze misbruik van worden gemaakt.

Geadviseerd worden om de volgende maatregelen te nemen:

- Stem met de GGD'en af wie verantwoordelijk is voor welke deel van de controle van de logging. Dit kan worden opgenomen in het convenant/een addendum bij het convenant.
- Stel een beleid/procedure op voor de controle van de logging, dat voldoet aan de toepasselijke norm, de NEN 7513.
- Implementeer het beleid/de procedure in de organisatie en controleer zo snel mogelijk de logging. Indien dit niet met software kan, stel dan medewerkers aan die dit controleren tot de software wel beschikbaar is. Als met software wordt gecontroleerd, moet alsnog een menselijke controle worden uitgevoerd op een steekproef van de door de software gecontroleerde logbestanden.
- Zorg voor een sanctiebeleid waarin is opgenomen wat met de medewerker gebeurt indien hij niet werkt volgens de gestelde regels en zorg dat de medewerkers hiervan op de hoogte zijn.

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

Het restrisico na genomen maatregelen is dat de controle van logging niet iedere medewerker en iedere inzage van het dossier kan controleren. Hierdoor blijft een risico bestaan dat medewerkers toch onrechtmatig dossiers inzien en de gegevens misbruiken. De medewerkers werken in een groot deel van de gevallen thuis, waardoor ook geen onderling toezicht op de werkvloer bestaat.

3. Geen scheiding van toegang tussen regio's

Voor medewerkers van GGD'en is geen scheiding aangebracht tussen de regio's in CoronIT. Dit betekent dat medewerkers van de ene regio gegevens van betrokkenen in een andere regio kunnen opzoeken. Deze keuze is gemaakt op vraag van een aantal GGD'en, omdat mensen zich buiten hun regio kunnen laten testen en voor toegang tot die gegevens dan telkens een aanvraag moet worden ingediend, wat het proces vertraagd. Hierdoor is het echter mogelijk om onrechtmatig inzage te verkrijgen in de gegevens van alle inwoners van Nederland.

- De kans dat het risico zich manifesteert is groot. Er zijn veel medewerkers van GGD'en en ingehuurd personeel die gehele of beperkte toegang hebben tot CoronIT. De kans dat een van deze medewerkers zich, kwaadwillend of niet, toegang verschaft tot de gegevens.
- De impact van het risico is hoog. In CoronIT zijn medische gegevens en het BSN opgenomen, alsook contactgegevens. Hier kan op verschillende wijze misbruik van worden gemaakt.

Geadviseerd wordt om de volgende maatregelen te nemen:

- Besloten is dat het niet mogelijk is om CoronIT enkel voor de regio beschikbaar te stellen, omdat mensen zich ook regelmatig buiten de regio laten testen. Regel daarom dat, indien een dossier van iemand buiten de regio wordt geopend, breaking-the-glass is ingevoerd waarbij een reden moet worden ingegeven waarom de medewerker zich toegang wil verschaffen tot het dossier.
- Stel logging in op de breaking-the-glass inzages en controle elke toegang die via breaking-the-glass is verkregen. Op deze wijze kan worden beoordeeld of een medewerker rechtmatig inzage heeft gehad in de gegevens.
- Indien wordt gekozen breaking-the-glass niet in te stellen, dient strenge logging te worden toegepast op de verwerkingen in CoronIT.

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

Het restrisico na genomen maatregelen is dat als breaking-the-glass of een andere vorm van scheiding tussen regio's niet wordt aangezet en gecontroleerd, medewerkers toch onrechtmatig dossiers inzien uit andere regio's en de gegevens misbruiken. De medewerkers werken in een groot deel van de gevallen thuis (in het geval van het callcenter. Medewerkers van de GGD en in de teststraten werken vaker op locatie), waardoor ook geen onderling toezicht op de werkvloer bestaat. Logging kan daarbij niet iedere medewerker en iedere toegang tot de gegevens controleren.

4. *Medewerkers van worden snel opgeleid en werken, voor bij het callcenter, daarna thuis, waardoor niet adequaat kan worden gecontroleerd of ze begrijpen wat van hen wordt verwacht*

Medewerkers die extern worden ingehuurd, krijgen voor de start van de inhuur een training. Hierin wordt ook een stuk over privacy en informatiebeveiliging opgenomen. Ook krijgen ze een geheimhoudingsovereenkomst waar een en ander in wordt beschreven. Vervolgens beginnen ze met werken, in veel gevallen thuis. Hierdoor bestaat geen snelle controle of de medewerker alles begrijpt. Daarnaast is geen structuur opgezet, buiten de webinars als dit nodig blijkt, om periodiek kort het onderwerp privacy en informatiebeveiliging en dus de juiste omgang met gegevens aan te stippen. Hierdoor kunnen medewerkers, onbewust gegevens onrechtmatig verwerken.

- De kans dat het risico zich manifesteert is groot. Als enkel bij het begin van de inhuur een training wordt verzorgd, wordt in korte tijd veel informatie gegeven. Vervolgens wordt gestart met het nieuwe werk op de thuislocatie, waardoor het niet mogelijk is snel zaken na te vragen. Indien dit wel kan, kan dit gebeuren via digitale wegen, waar ook informatie kan worden meegestuurd over betrokkenen.
- De impact van het risico is hoog. Gegevens van betrokkenen kunnen op een verkeerde en/of onrechtmatige wijze worden verwerkt. Dit betekent dat er fouten in de gegevens kunnen ontstaan of gegevens onrechtmatig worden verwerkt. Hierdoor kunnen gegevens ook uitlekken, inclusief medische gegevens van de betrokkene.

Geadviseerd wordt om de volgende maatregelen te treffen:

- Stel een plan op om periodiek medewerkers te informeren over wat van hen wordt verwacht. Dit kan bestaan uit een korte presentatie, maar ook een vragenrondje. Dit moet in principe iedere organisatie zelf opstellen, echter kan ook worden gekeken in welke mate GGD GHOR Nederland hierin kan faciliteren. De vragenrondjes kunnen het best in het team worden georganiseerd.
- Stel duidelijke regels op waarin wordt gemeld wat medewerkers wel en niet mogen met de gegevens. Dit kan in de vorm van een korte lijst met gouden regels. Daarin kan bijvoorbeeld worden gemeld dat geen screenshots mogen worden gemaakt van de gegevens en dat gegevens niet via digitale media mogen worden gestuurd.
- Stel duidelijk waar medewerkers terecht kunnen met vragen en als wordt gemerkt dat een medewerker iets niet begrijpt, snel contact op wordt genomen.

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

5. *Medewerkers worden snel aangenomen en werken vaak, vooral bij het callcenter, thuis, waardoor het risico op fraude en onrechtmatige verwerking van gegevens verhoogd.*

Medewerkers worden gecontroleerd, maar werken daarna thuis en zijn nooit op locatie geweest. Ook wordt de werkplek niet gecontroleerd. Omdat geen controle op de werkplek of locatie van de werknemer/opdrachtgever bestaat, kan de medewerker sneller ongemerkt fraude plegen of de gegevens onrechtmatig verwerken. Een voorbeeld hiervan is dat huisgenoten mee kunnen kijken/luisteren met de medewerker.

- De kans dat dit risico zich manifesteert is hoog. Nadat de medewerker is aangenomen, worden weinig tot geen controles uitgevoerd over hoe de medewerker werkt en hoe zijn werkplek is ingericht.
- De impact van het risico is hoog. Gegevens van de betrokkene kunnen worden gebruikt voor fraude of op andere wijze onrechtmatig worden verwerkt. Dit kan ook door huisgenoten worden gedaan die de gegevens inzien/horen.

Geadviseerd wordt om de volgende maatregelen te treffen:

- Laat de medewerker een verklaring ondertekenen waarbij deze stelt een werkplek te hebben die aan in die verklaring opgenomen eisen voldoet.
- Laat de medewerker de juiste maatregelen treffen voor de beveiliging van zijn/haar systemen.
- Plan periodieke gesprekken met de medewerker om te vragen hoe het gaat en controleer daarbij of de medewerker werkt in een rustige ruimte zonder mensen in de buurt.
- Stel een sanctiebeleid op waarin wordt bepaald wat de sanctie is als niet aan de regels wordt voldaan en maak dit bekend bij de medewerkers.
- Voer de maatregelen met betrekking tot logging in.

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

Het risico blijft bestaan dat, zelfs met alle maatregelen, medewerkers zaken doen die niet mogen/wenselijk zijn. Als bovengenoemde maatregelen worden genomen, is de kans klein. Toch blijft de impact voor de betrokkene bij een kleine kans hoog, waardoor het risico voor de betrokkene als een medewerker toch iets onwettigs doet, bestaan.

6. *Uitwisseling van gegevens met verschillende partijen kan leiden tot onrechtmatige uitwisseling van gegevens en gebrek aan overzicht van de uitwisselingen*

De gegevens uit CoronIT zijn voor verschillende partijen interessant of van belang. Daarom vinden verschillende uitwisselingen plaats en worden vragen gesteld om uitwisselingen te starten. Sommigen daarvan zijn in de wet bepaald, voor anderen wordt een grondslag gezocht. De snelle ontwikkelingen en drukte kan leiden tot onzorgvuldige afweging van de uitwisseling, waardoor gegevens onrechtmatig kunnen worden uitgewisseld.

- De kans dat dit risico zich manifesteert is hoog. Over het algemeen worden de uitwisselingen op landelijk niveau aangevraagd, omdat dit voordelen oplevert. Binnen organisaties is vaak ook een lijn afgesproken om te beoordelen of de uitwisseling rechtmatig is. Er kunnen echter, door de drukte of door een medewerker die niet op de hoogte is dat een toetsing nodig is, gegevens worden uitgewisseld waar geen toetsing op is uitgevoerd.
- De impact van het risico is hoog. Vaak worden veel gegevens opgevraagd en daarbij ook de medische gegevens. Hier wordt vaak geen naam bij gegeven, maar sets kunnen naar personen worden herleid. Hoe meer informatie wordt gegeven, hoe sneller iemand kan worden herleid.

Geadviseerd wordt om de volgende maatregelen te treffen:

- Stel duidelijke richtlijnen op over de uitwisseling van data en neem daarin op dat eerst een toetsing moet plaatsvinden door iemand die daar in het kader van privacy een advies op kan geven.
- Wissel niet meer uit dan in het advies van de privacyspecialist is opgenomen. Het uitwisselen van (extra) gegevens kunnen namelijk leiden tot een ander advies.

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

7. *Wisselingen in partijen en verwerkingen kan leiden tot het niet maken van de juiste afspraken of onvoldoende grondslag*

CoronIT is gemaakt om te ondersteunen in het bestrijden van de coronapandemie. Dit betekent dat de verspreiding sneller of trager kan gaan, waardoor veranderingen in het beleid, de verwerking en de partijen die meewerken ontstaan. Deze veranderingen kunnen snel gaan. Voor nieuwe partijen kan dit betekenen dat ze snel gaan meewerken, maar dat daardoor geen afspraken worden gemaakt over de verwerking van de persoonsgegevens. Wijzigingen in het beleid en/of de verwerking kunnen leiden dat snel gehandeld moet worden, waardoor een onjuiste of geen grondslag bestaat voor de verwerking.

- De kans dat het risico zich manifesteert is hoog. Continue verandering is vaak onder tijdsdruk, waardoor niet altijd kan worden nagedacht over de gevolgen van de veranderingen. Daarnaast is het snel aansluiten van partijen om het proces vlot te kunnen laten verlopen vaak belangrijk. Het opstellen van de juiste documenten en de onderhandeling daarover, vooral met betrekking tot privacy, kan daardoor worden vergeten.
- De impact van het risico is hoog. Onjuiste afspraken en geen of onvoldoende grondslag kan leiden tot onrechtmatige verwerking en/of het uitlekken van (medische) gegevens.

Geadviseerd wordt om de volgende maatregelen te treffen:

- Stel een duidelijke communicatielijn in over uitwisselingen en het aansluiten van nieuwe partijen, zodat kan worden of een grondslag bestaat of kan worden bekeken of, en zo ja welke, afspraken moeten worden gemaakt.
- Controleer periodiek of er wijzigingen zijn in partijen, de verwerking of nieuw beleid/nieuwe inzichten.

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

8. *Door toename van medewerkers, tijdelijke inzet en wisseling van taken kunnen autorisaties verkeerd worden toegekend en vergeten worden in te laten trekken*

Door de grote vraag aan testen, is er een stijging in medewerkers, zowel eigen medewerkers als inhuur. Velen van hen moeten in meerdere of mindere mate rechten hebben om in te loggen in CoronIT. Door de drukte kan worden vergeten de juiste rechten voor CoronIT te verlenen, de rechten te laten wijzigen of de rechten te laten intrekken. Hierdoor kan onrechtmatige toegang worden verkregen tot de gegevens in CoronIT.

- De kans dat het risico zich voordoet is hoog. Organisaties staan onder grote druk en de medewerkers wisselen snel, waardoor een juiste administratie van autorisaties kan worden

vergeten en medewerkers over het hoofd kunnen worden gezien, vooral als de rollen wisselen of iemand niet meer hoeft te werken met CoronIT.
- De impact van het risico is hoog. Medewerkers die niet in (bepaalde delen van) het dossier hoeven, kunnen zich alsnog toegang verschaffen tot de gegevens.

Geadviseerd wordt om de volgende maatregelen te treffen:
- Stel een regeling op waarbij wordt bepaald wie wijzingen in rechten moet melden en waar dit moet worden gemeld in de organisatie.
- Meldt de wijzigingen zo snel mogelijk bij GGD GHOR Nederland zodat deze kunnen worden aangepast.

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

9. *Processen veranderen snel waardoor procesbeschrijvingen snel (kunnen) verouderen*

Het beleid rond testen verandert heel snel en is afhankelijk van ontwikkelingen rond de bestrijding van corona. Hierdoor kunnen processen en de daarbij behorende procesbeschrijving snel verouderen, waardoor het risico bestaat dat medewerkers niet zeker weten hoe ze moeten handelen of de update niet hebben gekregen van een verandering in het proces. Dit kan leiden tot fouten in de verwerking van persoonsgegevens.

- De kans dat dit risico zich manifesteert is hoog. Dit door de snelle wijzigingen, die niet altijd direct kunnen worden gecommuniceerd naar alle medewerkers en niet altijd direct kunnen worden omgezet in nieuwe/aangepast procesbeschrijvingen.
- De impact van het risico is middel. De aanpassingen kunnen klein zijn, waardoor de handeling vaak geen grote gevolgen hebben voor de verwerking van persoonsgegevens. Grote wijzigingen worden vaak ook via andere kanalen bekend gemaakt en zullen ook sneller en met meer aandacht door de organisatie worden gecommuniceerd.

Geadviseerd wordt om de volgende maatregelen te treffen:
- Stel een systeem op waarbij medewerkers direct op de hoogte worden gesteld van een verandering van werkwijze en dat daarbij ook dat medewerkers die thuis werken en/of medewerkers die op de dag geen dienst hebben alsnog hiervan op de hoogte worden gebracht als zij weer aan het werk gaan.

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

10. *Een overzicht van alle partijen, datastromen en uitwisselingen is niet opgesteld, waardoor gegevensstromen niet in kaart zijn, persoonsgegevens onrechtmatig worden verwerkt en uitlekken.*

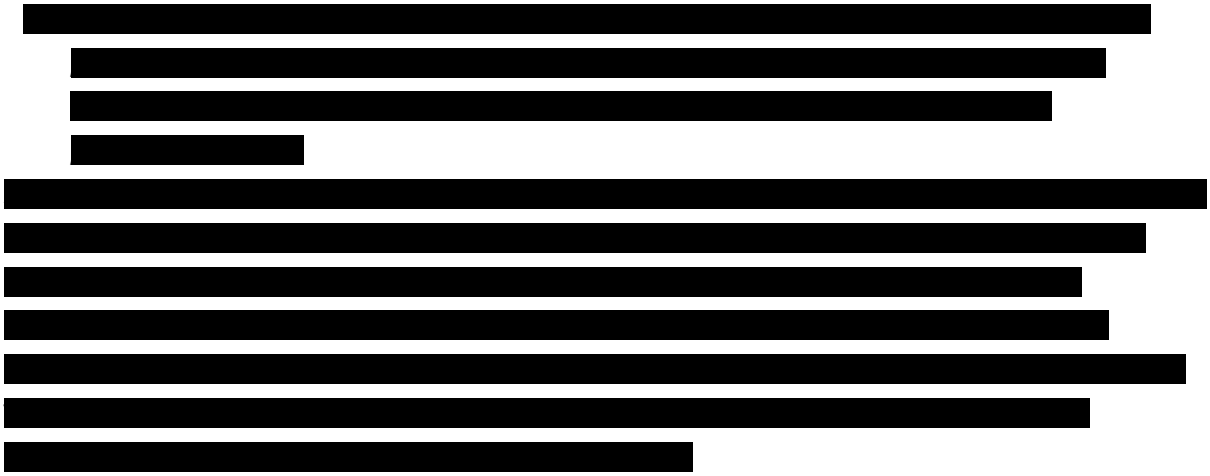
CoronIT is gelinkt met veel systemen. Daarnaast lopen nog processen langs CoronIT. Binnen GGD GHOR is geen totaaloverzicht van waar alle data wordt verwerkt en waar dat naar wordt

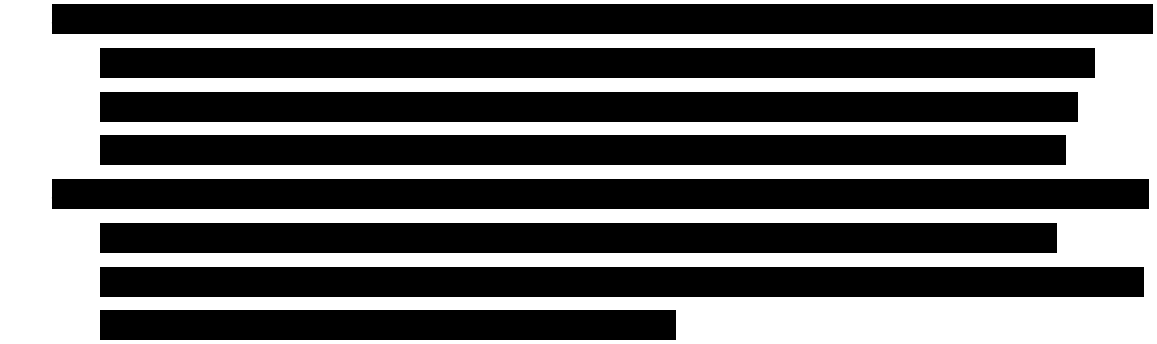
uitgewisseld. Dit kan leiden tot het missen van stromen en onrechtmatige uitwisselingen, maar ook van het ontbreken van afspraken met partijen die de persoonsgegevens verwerken.

- De kans dat het risico zich voordoet is hoog. Er is geen totaal overzicht en daarom kan niet worden gezegd of alles is getoetst en of alles rechtmatig wordt uitgewisseld.
- Het impact van het risico is hoog. Gevoelige persoonsgegevens kunnen uitlekken, wat grote gevolgen heeft voor de betrokkene van wie de data is gelekt.

Geadviseerd wordt om de volgende maatregelen te nemen:

- Breng de datastromen en afhankelijkheden rond de corona-applicaties in kaart.
- Toets na het in kaart brengen alle uitwisselingen en controleer of alle koppelingen zijn getoetst op beveiliging.





D. Beschrijving voorgenomen maatregelen

16. Maatregelen

Ter bescherming van de persoonsgegevens, zijn een aantal maatregelen genomen. Deze kunnen worden opgedeeld in technische en organisatorische maatregelen.

Organisatorische maatregelen

Informatiebeveiligingsbeleid

Binnen GGD GHOR Nederland is een informatiebeveiligingsbeleid opgesteld.

Topicus heeft een Informatiebeveilgingsbeleid, waarin 27 beleidspunten zijn opgenomen en waarin de ISO 27001 en NEN 7510 worden benoemd.

Privacybeleid

GGD GHOR Nederland heeft een privacybeleid. Dit is in 2018 opgesteld.

Geheimhoudingsverklaring

Geheimhoudingsverklaringen zijn ondertekend door personeel van GGD GHOR en externen die zijn ingehuurd door GGD GHOR Nederland voor het functioneel beheer. De geheimhoudingsverklaring wordt voorgelegd als een medewerker in dienst treedt. Voor externe medewerkers wordt de geheimhoudingsverklaring voorgelegd voor inhuur.

Van verwerkers wordt geëist dat medewerkers een geheimhoudingsverklaring hebben getekend voor hun dienstverband.

Bewustwording

Voor medewerkers van GGD GHOR Nederland die worden ingezet voor Corona, worden bij de start van het dienstverband trainingen georganiseerd. Daarnaast worden periodiek webinars gehouden over de werkwijze binnen CoronIT, waar telkens een ander deel uit de keten of nieuws wordt besproken. Daarbij wordt ook aandacht besteed aan hoe met de gegevens moet worden omgegaan.

Bij Topicus wordt in het onboardingstraject al bewustwording gecreëerd voor privacy en informatiebeveiliging. Daarnaast worden bewustwordingspresentaties gehouden en wordt minimaal eens per jaar een activiteit ingepland in het kader van bewustwording.

Autorisatiematrix

Een autorisatiematrix is opgesteld waarin de rollen en rechten zijn bepaald. Deze rollen en rechten zijn opgesteld voor de volgende organisaties:

- **GGD GHOR Nederland**

Een kleine groep medewerkers van de servicedesk hebben toegang tot CoronIT. Zij mogen geen gegevens inzien tenzij dit absoluut noodzakelijk is om de vraag die hen wordt gesteld op te kunnen lossen. Daarnaast zijn er twee medewerkers die brede rechten hebben in CoronIT, waarbij ze bij alle gegevens kunnen en zaken kunnen wijzigen/verwijderen. Zo kan bijvoorbeeld worden gezorgd dat voor GGD'en gegevens kunnen worden verwijderd als ze een verwijderingsverzoek toekennen.

- **Callcenter**
  Medewerkers van het callcenter hebben toegang tot de gegevens in CoronIT om de gegevens van betrokkenen in te vullen die een afspraak willen maken en voor het terugbellen van betrokkenen, waarbij controle kan worden uitgevoerd op de juistheid van de gegevens en het resultaat. Dit is verder uitgewerkt in de DPIA callcenter.
- **Topicus**
  Medewerkers van Topicus hebben enkel toegang tot CoronIT als ze daar door GGD GHOR Nederland rechten voor hebben gekregen. Deze mogen alleen worden gebruikt om problemen op te kunnen lossen.

  Voor het synaps platform, waar CoronIT op is gebouwd, is wel toegang voor een aantal medewerkers als superuser om schermen te kunnen definiëren.
- **GGD**
  Voor medewerkers van de GGD zijn verschillende rollen gedefinieerd. Deze zijn uitgewerkt in een autorisatiematrix. De GGD heeft deze ontvangen. Als mensen toegang nodig hebben tot het systeem, kan de GGD bij GGD GHOR Nederland de autorisaties aanvragen die de nieuwe medewerker nodig heeft.

  Als een medewerker niet meer in CoronIT hoeft te werken of uit dienst gaat, moet de GGD dit melden bij GGD GHOR Nederland, zodat de autorisaties worden ingetrokken.

Overeenkomsten

Met de verschillende partijen zijn passende afspraken gemaakt over de verwerking van gegevens, zodat de gegevens niet onrechtmatig worden gebruikt. Daarnaast is, waar nodig, bepaald welke beveiligingsmaatregelen moeten worden genomen.

Met **verwerkers** zijn verwerkersovereenkomsten gesloten waarin duidelijk is gesteld welke gegevens zij mogen verwerken en hoe deze gegevens mogen worden verwerkt. Daarnaast is bepaald welke beveiligingsmaatregelen worden vereist.

Met **gezamenlijk verantwoordelijken** is een convenant gesloten waarin is bepaald welke verwerkingen worden uitgevoerd en wie verantwoordelijk is voor welke verwerkingen.

Procedure datalekken

GGD GHOR Nederland beschikt over een datalekkenprocedure. Deze procedure wordt op dit moment herzien.

Met de verwerkers is afgesproken dat datalekken of beveiligingsincidenten waarbij twijfel bestaat of persoonsgegevens betrokken zijn bij het beveiligingsincident altijd moeten worden gemeld aan GGD GHOR Nederland.

Met de GGD'en is afgesproken in het convenant dat GGD'en GGD GHOR Nederland op de hoogte brengen als zich een datalek (of beveiligingsincident waarbij (vermoedelijk) persoonsgegevens zijn betrokken) heeft voorgedaan. In onderling overleg wordt dan besloten wie het datalek meldt en welke maatregelen worden getroffen.

Logging en monitoring
Voor de controle van logging is geen procedure opgesteld. Controle vindt ad hoc plaats, na een vermoed of vastgesteld incident.

Wel zijn plannen opgesteld voor hoe logging dient te worden gecontroleerd voor ten minste medewerkers van het callcenter. Daarbij wordt onderzocht hoe dit geautomatiseerd kan worden.

Gedragscodes
In de coronatijd is het niet altijd mogelijk om op een werklocatie te werken. Daarom zijn gedragscodes opgesteld over hoe moet worden omgegaan met thuiswerken en waar de beveiliging van de gebruikte computer aan moet voldoen, evenals de netwerkverbinding die wordt gebruikt.

Daarnaast zijn gedragscodes opgesteld over het gebruik van IT-middelen die zijn uitgegeven door GGD GHOR Nederland.

Van de verwerkers is geëist dat zij gedragscodes hebben opgesteld met betrekking tot IT-middelen en correct gebruik daarvan. Daarnaast wordt geëist dat afspraken zijn gemaakt met medewerkers over thuiswerken. De aanwezigheid van stukken hieromtrent bij Topicus is gecontroleerd. De verbinding voor thuiswerken verloopt via VPN. In coronatijd is herhaald wat wordt verwacht bij thuiswerken.

Rechten van de betrokkenen en verwijdering van dossiers
Binnen CoronIT kunnen betrokkenen hun rechten uitvoeren. De verzoeken moeten worden ingediend bij de GGD waar de betrokkene is getest. De GGD maakt de afweging om het verzoek toe te kennen of af te wijzen. De GGD kan zelf inzage geven en gegevens wijzigen. De gegevens kunnen echter niet door de GGD verwijderd worden. Indien een verwijderingsverzoek wordt ingediend, moet de GGD een afweging maken of de gegevens verwijderd kunnen worden en vervolgens opdracht geven aan GGD GHOR Nederland om deze te verwijderen. Dit kan via de servicedesk. GGD'en zijn daarom zelf verantwoordelijk voor het hebben van een beleid of richtlijn met betrekking tot de rechten van betrokkenen.

Voor de verwijdering van dossiers, zijn er twee opties:

- Het dossier inactiveren: het dossier wordt dan op inactief gesteld, maar dat kan ongedaan worden gemaakt.

- Het dossier verwijderen: in dit geval is het dossier echt verwijderd.

Synaps maakt elke dag een snapshot. Deze blijven 7 dagen bewaard. Daarnaast blijven gegevens nog in de back-up bewaard tot deze worden vervangen. Pas daarna zijn de gegevens echt verwijderd.

Na de bewaartermijn moeten dossiers worden verwijderd. Dit is nog niet geautomatiseerd, maar de automatisering staat wel op de ontwikkellijst.

Procedures en plannen

Topicus heeft verschillende procedures en plannen opgezet. Dit zijn de volgenden:

- **CMDB**
  Is aanwezig.
- **Uitgifte werkmiddelen en bijbehorende gedragsregels**
  Is aanwezig. Dit wordt gedaan door facilitair beheer. Voor gebruik van de werkmiddelen worden op dat moment ook de gedragsregels verstrekt. De apparatuur wordt periodiek vervangen. Elke 3 jaar wordt een nieuwe laptop verstrekt en elke 2 jaar een nieuwe telefoon.
- **Classificatiebeleid.**
  Is aanwezig.
- **Wijzigingenbeheer.**
  Is aanwezig en opgenomen in de DAP.
- **Capaciteitsmanagement.**
  Is opgesteld en opgenomen in de DAP.
- **Continuïteitsregeling.**
  Is opgesteld en deels opgenomen in de DAP. Voor continuïteit is gezorgd voor een redundant datacenter. Als er iets bij een datacenter gebeurt, kan het andere datacenter het direct overnemen. Hierdoor is er geen down time in de applicatie.

  Voor business continuity is een bankgarantie opgesteld bij Previder. Als er iets misgaat, hebben klanten een half jaar om op zoek te gaan naar een andere oplossing.
- **Problem management**
  Is opgesteld en opgenomen in de DAP.
- **Calamiteitenplan**
  Is opgesteld.
- **Vulnerability management en patch en release management**
  Is opgesteld. Er zijn periodieke updates en er zijn bouwomgevingen voor dead code. Op deze wijze kan de dead code weg worden gehaald.

  Indien uit testen toch kwetsbaarheden blijken, worden plannen opgesteld om de kwetsbaarheden op te lossen.

Daarnaast worden in bouwstraten testen op de code uitgevoerd en wordt gekeken of de componenten nog up-to-date zijn.

- **Procedure uitwisseling data**
  Voor personeel wordt duidelijk gemaakt dat data niet zomaar mag worden uitgewisseld. Er wordt beschreven welke data wel mag worden uitgewisseld, op welke wijze en hoe dit beveiligd dient te worden. Dit wordt vastgelegd in een interne norm, die wordt opgesteld op basis van opdrachten van de labs en GGD'en. Voorbeeld hiervan is de uitlagenlijst.
- **Hardening**
  Is aanwezig op het platform. Wordt gebouwd op basis van standaard.
- **Procedure risico analyse**
  Risico-analyses worden uitgevoerd in een cyclus van 3 jaar. Dat bestaat uit:
  - Distant risk assessments
  - Interne en externe audits
  - Continue risicobeheersing als onderdeel van de wijzigingsprocedure
- **Test management**
  Is aanwezig. Hierin is uitgeschreven hoe, welke tooling, visie en strategie. Daarnaast wil Topicus nog meer automatisch geen testen. Dat wordt nu uitgeschreven. Verder wordt bij elke release automatisch een test uitgevoerd op de code en is er een testmiddag waarbij allerlei scenario's worden doorlopen in de modules. Ook is er een smoketest waarbij de app op hoog niveau wordt doorlopen. Bij elke release krijgt GGD GHOR Nederland vervolgens 2 weken om de release te testen.
- **Leveranciersmanagement**
  Is opgenomen in een interne norm.
- **Beheersmaatregelen**
  Er wordt gewerkt naar een interne en externe norm, bovenop de certificering. Hiervoor worden action plans opgesteld. Dit is ook voor externe audits of pen-testen. Alles wordt centraal geregeld en aan acties worden deadlines gehangen. Dit wordt opgevolgd via een ticket dat wordt gekoppeld aan een team.

  Een corrective action plan is ook aanwezig.
- **Netwerkdiagram**
  Is opgesteld.

Technische maatregelen

Inregelen van autorisaties

De rechten en rollen die zijn bepaald in de autorisatiematrix, zijn ingeregeld in het systeem. Voor GGD´en is geregeld dat GGD GHOR Nederland het beheer van het systeem voert en dat GGD´en aan GGD GHOR Nederland de opdracht kunnen geven autorisaties te geven of in te trekken.

Normen

GGD GHOR Nederland tracht voor de systemen in eigen beheer te voldoen aan de voor hun toepasselijke normen, NEN 7510, 7512 en 7513.

Met verwerkers wordt overeen gekomen dat deze minstens werken volgens de NEN 7510, 7512 en 7513. De leverancier van CoronIT en het platform waarop dit draait, heeft een certificering voor de NEN 7510 en ISO 270001. Deze certificeringen zijn ingezien. Verder is met Topicus afgesproken dat zij werken volgens de NEN 7512 en 7513.

Logging

Op CoronIT wordt logging toegepast. Daarbij worden twee soorten logging bijgehouden:

- **Functionele logging (of audit trail).**
  In deze logging is te zien wat in het dossier is gebeurt. Dit betekent dat kan worden gezien welke delen van het dossier zijn geopend, door wie en wanneer. Daarnaast is te zien of er wijzingen of andere bewerkingen zijn geweest in de gegevens.

  Deze logging kan door GGD GHOR Nederland zelf worden ingezien. Ook het inzien van de logging wordt daarbij gelogd.

  Op deze logging worden geen signalen gegeven bij afwijkingen. Er zijn hiervoor geen afwijken gedefinieerd.

  De functionele logging wordt nooit verwijderd.

- **Technische logging**
  De techinsche logging geeft weer wat de applicatie wegschrijft. In principe worden hier geen persoonsgegevens in opgeslagen. Bij uitzondering kunnen echter wel zaken als een IP-adres worden opgeslagen.

  De technische logging is bij Topicus op te vragen indien GGD GHOR Nederland deze in wil zien.

  Op de technische logging is signalering ingericht, die in werking treedt als een drempelwaarde wordt bereikt.

  [redacted]

Scheiding tussen systemen

Tussen de regio's van GGD'en is geen scheiding aangebracht tussen de omgevingen. Deze keuze is gemaakt omdat mensen zich buiten de regio kunnen laten testen en het dus noodzakelijk kan zijn om snel toegang te hebben tot de gegevens van een betrokkene. Er is voor gekozen geen breaking-the-glass procedure in te zetten, omdat door GGD'en is aangegeven dat dit belemmerend werkt.

PEN-test

Om te controleren of het systeem veilig is en niet kan worden gehackt of op een andere manier kan worden gecompromitteerd, zijn PEN-testen uitgevoerd. Deze test heeft zowel gecontroleerd of de omgeving zonder credentials niet kan worden gehackt, als met (gedeeltelijke) credentials. Daarnaast zijn alle aangesloten applicaties en koppelingen getest om te controleren of daar ook geen kwetsbaarheden bestaan waarmee toch toegang kan worden gekregen tot CoronIT.

Daarnaast voert Topicus periodiek PEN-testen uit om te controleren of de omgeving up-to-date en veilig blijft.

Back-up en restore

Van CoronIT worden back-ups gemaakt. Hiervoor is een procedure vastgesteld door Topicus, waarbij back-ups over verschillende periodes worden gemaakt.

Voor CoronIT is point in time recovery mogelijk, waarbij uit de database de transactielogging wordt gehaald en waarmee de back-up wordt aangevuld, om zoveel mogelijk te kunnen herstellen als dat nodig is.

De datacenters voor CoronIT zijn redundant. Als een datacanter uitvalt, kan het andere datacenter dit overnemen. [redacted].

Beveiliging

Ter beveiliging van het systeem is gezorgd voor een Firewall en anti-malware software, die up-to-date wordt gehouden.

Het webverkeer is encrypted met een HTTPS-protocol. Voor data in transit wordt SSL gebruikt. Op schijfniveau wordt alles geëncrypt, wat betekent dat dit ook op file niveau gebeurt.

Zaken die worden aangeleverd door Topicus, worden standaard geëncrypt, zoals bitlocker op windows laptops die worden uitgegeven.

Multifactor authenticatie

Voor CoronIT is tweefactor authenticatie ingericht. Dit is gedaan door een gebruikersnaam en wachtwoord en een authenticatie applicatie. Er zijn twee opties:

1. Er kan worden ingelogd via het Zorgportaal van Topicus. of
2. Er kan worden ingelogd via The Identity Hub van GGD GHOR Nederland Van de laatste route wordt op dit moment vooral gebruik gemaakt door het landelijke callcentrum. Binnenkort zullen ook de overige partijen uit de keten op deze route worden overgezet.

Scheiding met schema's op database applicaties Synaps platform

CoronIT is gebouwd op het Synaps-platform. Op dit platform draait ook de applicatie iTBC. Op de databases zijn daarom schema's ingesteld, zodat mensen met een autorisatie voor een applicatie geen toegang krijgen tot de gegevens in de andere applicatie.

Laboratoria en koppelingen

Labonline koppelt met de labsystemen en is onderdeel van synaps. De communicatie met laboratoria verloopt altijd via een VPN verbinding.

Er is een lijst opgesteld met de laboratoria, de koppelingen en het type data. Er zijn namelijk verschillende koppelingen met de verschillende labs. Ook is er een verschil tussen labs die enkel het nummer van het testbuisje van het monster krijgen en er zijn labs die een laborder krijgen met informatie over de geteste persoon, zoals dat bij regulier onderzoek ook gebeurt. De inrichting verandert echter elke dag. Via de labkoppeling en Labonline wordt de uitslag vervolgens weer in CoronIT geladen.

Bijlage 1: Achtergrond Risiconiveaus

Kans

Bij het bepalen van de kans (K) dat een risico zich voordoet worden de volgende factoren in acht genomen:

- Het bestaan van gemotiveerde en bekwame actoren met bijbehorend hun motivaties en vaardigheden;
- Aard van de kwetsbaarheid; en
- Aanwezig zijn van bestaande maatregelen en hun effectiviteit

De kans dat een potentiele kwetsbaarheid kan worden uitgebuit door een actor zal worden omgeschreven als hoog, midden, of laag. De onderstaande tabel beschrijft deze drie lagen.

Impact

Kans	Kans beschrijving
Hoog	De actor is zeer gemotiveerd en bekwaam en maatregelen ter preventie van de uitbuiting van de kwetsbaarheid zijn ineffectief.
Midden	De actor is zeer gemotiveerd en bekwaam, maar er zijn maatregelen geïmplementeerd die de uitbuiting van de kwetsbaarheid belemmeren.
Laag	De actor mist motivatie of bekwaamheid, of maatregelen zijn geïmplementeerd om de uitbuiting van de kwetsbaarheid te voorkomen of significant te belemmeren.

De impact van een geëffectueerd risico wordt beschreven in termen van verlies of beperking van beschikbaarheid, integriteit of vertrouwelijkheid van gegevens op een schaal van laag, midden en hoog. De onderstaande beschrijvingen geven een korte omschrijving van deze aspecten en de consequentie (of impact) die daaraan verbonden is als dit doel niet behaald wordt.

Verlies van integriteit – Systeem en data integriteit verwijst naar de eis dat de juistheid en volledigheid van informatie geborgd moet zijn. De integriteit is verloren als incorrecte wijzigingen zijn aangebracht in de informatie door opzettelijk of onopzettelijk handelen. Als verlies van integriteit niet (tijdig) verholpen wordt kan verder gebruik van het gecompromitteerde systeem of data resulteren in onnauwkeurigheid, fraude of beveiligingsincidenten. Verlies van integriteit kan een eerste stap zijn in een aanval op systemen met verlies van beschikbaarheid of vertrouwelijkheid tot gevolg.

Verlies van Beschikbaarheid – Als een dienst (of gegevens aangeboden door een dienst) niet beschikbaar is voor de eindgebruikers, raakt dit mogelijk de missie van de organisatie. Verlies van systeemfunctionaliteit en operationele effectiviteit kunnen leiden tot beveiligingsincidenten of verlies van productiviteit.

Verlies van Vertrouwelijkheid – Systeem en data vertrouwelijkheid verwijst naar de bescherming tegen ongeautoriseerde openbaarmaking van gegevens (o.a. verlies van bedrijfsgeheimen, intellectueel eigendom (software, protocollen, documenten, etc.), of persoonsgegevens). Ongeautoriseerde, onverwachte, of onopzettelijk openbaarmaking van persoonsgegevens kan leiden tot het schenden van wet en regelgeving.

Impact niveau	Impact Beschrijving
Hoog	Misbruik van een kwetsbaarheid: 1. Kan resulteren in het kostbare verlies van kritische assets of middelen; 2. Kan de missie, reputatie of belang van de organisatie of Betrokkene significant schaden, compromitteren of belemmeren; 3. Kan een schending van wettelijke richtlijnen veroorzaken; 4. Kan resulteren in sterfte of ernstig letsel; 5. Kan een grote inbreuk opleveren in de fundamentele rechten en vrijheid van Betrokkene

Midden	Misbruik van een kwetsbaarheid: 1. Kan resulteren in het kostbare verlies van materiële assets of middelen; 2. Kan de missie, reputatie of belang van de organisatie of Betrokkene schaden, compromitteren of belemmeren; 3. Kan resulteren in persoonlijk letsel. 4. Kan een inbreuk opleveren in de fundamentele rechten en vrijheid van Betrokkene
Laag	Misbruik van een kwetsbaarheid: 1. Kan resulteren in het verlies van bepaalde assets of middelen; 2. Kan de missie, reputatie of belang van de organisatie of Betrokkene schaden 3. Kan een kleine inbreuk opleveren in de fundamentele rechten en vrijheid van Betrokkene

Risico Calculatie

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

- De kans (K) dat een risico effectueert; en
- De impact (I) op de organisatie of Betrokkene als het risico is geëffectueerd.

Het risiconiveau wordt toegekend door een vooraf vastgestelde matrix die het belang van mitigerende maatregelen aangeeft. De combinaties van kans en impact zijn gegroepeerd in hoog (H, rood), midden (M, geel) en laag (L, groen). De matrix toont hoe de risico's zijn geclassificeerd gebaseerd op de impact en kans.

Kans → / Impact ↓	Laag	Middel	Hoog
Laag	Laag	Laag	Middel
Midden	Laag	Middel	Hoog
Hoog	Middel	Hoog	Hoog

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

Risico Niveau	Risico Beschrijving en te verwachten maatregel
Hoog	Als een waarneming of bevinding wordt geëvalueerd als een hoog risico, is er sterke behoefte aan corrigerende maatregelen. Een bestaand systeem kan blijven werken, maar een beveiligingsplan of andere risico-beperkende maatregel moet zo snel mogelijk worden geïmplementeerd.
Midden	Als een waarneming wordt beoordeeld als gemiddeld risico, moeten eventuele corrigerende maatregelen worden overwogen.
Laag	Als een waarneming wordt beschreven als een laag risico, kunnen corrigerende maatregelen nog steeds nodig zijn of kan het risico worden geaccepteerd.

Bijlage 2 – Genomen maatregelen naar aanleiding van initiële risico's

Risico	Genomen maatregel
1	Controle op de logging is ingericht. In eerste instantie gebeurde dit handmatig. Nu is de controle ingericht. Daarnaast wordt een SIEM-oplossing ingericht binnen GGD GHOR Nederland, en is een SOC-team ingericht om te handelen bij (vermoede) incidenten. [redacted]
3	[redacted]
7	Er is besloten om CoronIT alleen nog maar voor de GGD-keten te gebruiken. De laat de kansen op nieuwe partijen afnemen. Daarnaast wordt voor ieder aan CoronIT gerelateerd systeem weer een DPIA opgesteld, waar de verwerking en de partijen in kaart worden gebracht. Dit betekent echter niet dat het risico niet meer bestaat. In de huidige keten kunnen namelijk ook partijen wisselen, al is dat wel sneller bekend en zichtbaar.
8	Er is een regeling ingesteld, maar dat heeft niet altijd het gewenste effect. Daarom is het nu van belang om te zorgen dat partijen actief worden begeleid bij het aanvragen van rechten. Bindende landelijke afspraken zou ook een optie bieden, maar de GGD'en blijven zelf verantwoordelijk en vrij om de autorisaties te bepalen.
10	Voor CoronIT zijn de datastromen bekend bij het project. De privacy lead heeft ze nog niet allemaal in beeld, dus hier moet de DPIA nog op worden aangevuld. Wel is bekend dat iedere nieuwe datastroom beoordeeld moet worden door een privacyspecialist.
11	Dienst testen van VWS sluit landelijke contracten met de laboratoria. Zo worden eenduidige afspraken gemaakt met de laboratoria. Afspraken met betrekking tot de verwerking van persoonsgegevens worden uitgewerkt in een overeenkomst die landelijk zal worden gesloten met alle laboratoria.

Bijlage 3 – Versiegeschiedenis

Versie	Auteur	Verspreiding bij	Activiteiten
1	GGD GHOR NL	Via Teams platform	Input voor GGD Zaanstreek Waterland
1.1	A. Rosendahl FG	K. van den Hoek	Onderdelen model DPIA Zaanstreek Waterland opgenomen.

GGD Zaanstreek-Waterland

Zaanstreek-Waterland

Postbus 2056 • 1500 GB Zaandam
Vurehout 2 • 1507 EC Zaandam
Telefoon (0900) 254 54 54 • Fax (075) 616 30 16
info@ggdzw.nl • www.ggdzw.nl