GGD Amsterdam

Data Protection Impact Assessment (DPIA)

Inleiding **2**

A. Beschrijving kenmerken gegevensverwerkingen **3**

2. Persoonsgegevens 4

3. Gegevensverwerkingen 6

4. Verwerkingsdoeleinden 15

5. Belangen bij gegevensverwerking 18

6. Verwerkingslocaties 19

7. Techniek en methode van gegevensverwerking 19

8. Juridisch en beleidsmatig kader 21

9. Bewaartermijn 22

B. Beoordeling rechtmatigheid gegevensverwerkingen **23**

10. Rechtsgrond 23

11. Bijzondere persoonsgegevens 26

12. Doelbinding 30

13. Noodzaak en evenredigheid 31

14. Rechten van betrokkenen 35

C. Beschrijving en beoordeling risico's voor de betrokkenen **36**

15. Risico's 36

D. Beschrijving voorgenomen maatregelen **50**

16. Maatregelen 51

E. Bijlagen **53**

Bijlage 1: Grafische weergave fases vaccinatieproces 53

Bijlage 2: Advies Functionaris Gegevensbescherming GGD GHOR Nederland over Gezondheidsmonitor V&O 2020 en de daarop uitgevoerde DPIA ..... **Fout! Bladwijzer niet gedefinieerd.**

Bijlage 3: Overzicht Proportionaliteit en Subsidiariteit .... **Fout! Bladwijzer niet gedefinieerd.**

Bijlage 4: Overzicht Risico's en Maatregelen 57

Inleiding

Om de verspreiding van het coronavirus binnen Nederland onder controle te houden en het gewone maatschappelijke leven weer op gang te brengen, is het van belang dat er op grote schaal gevaccineerd kan worden door de verschillende GGD'en.

Gezien de grote schaal waarop deze vaccinaties uitgevoerd moeten worden en de snelheid waarmee dit moet gebeuren, is het niet mogelijk om aanmeldingen voor de vaccinaties enkel via de (huis)arts te laten verlopen. In dat kader is besloten een landelijk vaccinatieproces op te zetten. De GGD is als partij betrokken bij dit proces en draagt zorg voor de vaccinatie van een (groot) deel van de bevolking. In dat kader is het bestaande callcenter uitgebreid, welke de vaccinatieafspraken zal gaan plannen en de melding en registratie in CoronIT zal doen. Daarnaast is CoronIT doorontwikkeld om niet alleen testafspraken en uitslagen te registeren, maar ook de vaccinatieafspraken en vaccinatiegegevens te registeren. De lokale GGD'en, voor wie dit een wettelijke taak is op basis van de Wet publieke gezondheid (Wpg) hebben GGD GHOR gemachtigd voor het opzetten en beheren van dergelijke processen. GGD GHOR Nederland heeft hiervoor op 16 december 2020 ook een formele opdracht ontvangen van het Ministerie van Volksgezondheid, Welzijn en Sport (VWS).

Deze DPIA ziet op de inzet van de callcenters voor het verwerken van afspraken, het beantwoorden van medische vragen, het gebruik van CoronIT voor de registratie van de vaccinatiegegevens, en de overige onderdelen van het vaccinatieproces waarbij er sprake is van verwerkingen van persoonsgegevens door GGD Amsterdam, de andere landelijke GGD'en en GGD GHOR.

Tot slot is het van belang om te vermelden dat deze DPIA kan worden gezien als een 'DPIA on the go'. Het proces is veranderlijk, waardoor ook de DPIA regelmatig zal moeten worden bijgewerkt. Er wordt daarom gewerkt met versies. In bijlage 5 zijn de versies te raadplegen.

Definitie Betrokkene

Voor deze DPIA is uitgegaan van de volgende definitie van het woord 'betrokkene': Betrokkene betreft de persoon, wiens gegevens worden verwerkt. In vrijwel alle gevallen betreft dit de aanvrager zelf, enkele uitzonderingen (aanvragen voor wilsonbekwame personen) daargelaten.

CoronIT

CoronIT is een webapplicatie die oorspronkelijk is ontwikkeld in opdracht van GGD GHOR Nederland door Topicus om het testproces van COVID-19 te centraliseren, automatiseren, versnellen en vereenvoudigen. In het kader van de uitvoering van het vaccinatieprogramma is in opdracht van GGD GHOR CoronIT uitgebreid om de uitvoering van het vaccinatieprogramma te kunnen faciliteren.

Ten aanzien van vaccinaties is CoronIT een zorginformatiesysteem (artikel 1 sub m Wet aanvullende bepalingen verwerking persoonsgegevens in de zorg) waarin het vaccinatieproces van COVID-19 wordt gecentraliseerd, geautomatiseerd, versneld en vereenvoudigd. In CoronIT worden slechts die persoonsgegevens verzameld die noodzakelijk voor de uitvoering van vaccinaties. Het dossier dat ten aanzien van de betrokkene wordt aangemaakt in CoronIT kan worden gezien als een medisch dossier.

In CoronIT worden de vaccinatiegegevens verwerkt. 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'en kunnen de inhoud van deze DPIA gebruiken en, indien nodig, DPIA aanpassen en/of aanvullen op basis van de situatie binnen de GGD.

A. Beschrijving kenmerken gegevensverwerkingen

1. Voorstel

Aanleiding

Op 16 december 2020 heeft VWS de opdracht gegeven aan GGD GHOR in samenwerking me de landelijke GGD'en om de eerste fase van de vaccinatiecampagne en de vaccinatie van de bevolkingsgroep tussen de 18-60 jaar op zich te nemen. CoronIT is daarom doorontwikkeld om zo in opdracht van VWS het vaccinatieproces uit te kunnen voeren. 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 en de Wet op de geneeskundige behandelingsovereenkomst (WGBO). Daarnaast wordt er, net als bij testen, gebruik gemaakt van het landelijke callcenter. Ook dit callcenter is daarom uitgebreid om verwerkingen t.b.v. vaccinaties te verrichten. Tot slot is er een callcenter ingericht, waar betrokkene terecht kunnen met medische vragen of voor hulp bij het invullen van de gezondheidsverklaring.

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

Voorstel
Om te zorgen dat het vaccinatieproces van COVID-19 centraal, automatisch, versneld en eenvoudig verloopt, is CoronIT (de webapplicatie voor het testproces) doorontwikkeld. In de webapplicatie worden de persoonsgegevens die noodzakelijk zijn voor het maken van een afspraak en het vaccineren van de betrokkene ingevuld.

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

Daarnaast wordt er een callcenter opgezet (door Teleperformance). Deze callcenter-medewerkers nemen de vaccinatie-aanvragen van betrokkenen in behandeling en registreren deze in CoronIT. Callcenter-medewerkers zullen expliciet geen medische adviezen geven of beoordelen of een vaccinatie al dan niet kan worden toegediend. Hiervoor is een apart medisch callcenter opgericht.

2. Persoonsgegevens
Binnen CoronIT worden door het callcenter en door de administrator of arts/verpleegkundige op de vaccinatielocatie persoonsgegevens verwerkt. De gegevens die optioneel zijn, worden enkel gevuld als dit de wens van de betrokkene is. In de onderstaande
tabel is per persoonsgegeven weergegeven om wat voor type persoonsgegevens
(gewone, bijzondere of wettelijke identificerende) het gaat.

Persoonsgegeven	**Gewoon persoonsgegeven**	**Bijzonder persoonsgegeven**	**Wettelijk identificerend persoonsgegeven**
Voornaam en achternaam	Ja		
Geboortenaam partner (optioneel)	Ja		
Voorletters/roepnaam	Ja		
Postcode	Ja		
Huisnummer	Ja		
Straatnaam	Ja		
Woonplaats	Ja		
Gemeente	Ja		
Land	Ja		
Gekoppelde GGD	Ja		
Telefoonnummer	Ja		

e-mail	Ja		
Geslacht	Ja		
BSN			Ja
Beroepsgroep/sector (dropdown)	Ja		
Type zorgverlener (dropdown)	Ja		
Type contactberoep (dropdown)			
Batchnummer vaccin		Ja	
Vaccinnaam		Ja	
Documentnummer identiteitsbewijs			Ja
V-nummer			Ja
Type identiteitsbewijs	Ja		
Patiëntennummer		Ja	
Naam arts	Ja		
Huisarts	Ja		
Doelgroep (vastgesteld door het RIVM bijv.: leeftijd, risicogroep, etc.)	Ja		
Medische triagevragen		Ja	
Vaccinatiebewijs		Ja	
Bijwerkingen		Ja	

Wanneer de betrokkene belt om een afspraak te maken, dan stelt de callcenter-medewerker de volgende triage vragen:

- Bent u de afgelopen 4 weken positief getest op corona?
- Heeft u Corona-gerelateerde klachten?
- Thuisquarantaine?
- Binnen 7 dagen voor of na afspraak andere vaccinatie?
- Onder behandeling bij trombosedienst?
- Binnenkort een operatie onder narcose? Zo ja, wanneer?

Daarnaast worden de volgende aanvullende vragen gesteld:

- Eerdere tegen Corona gevaccineerd?
- Zo ja, 1 of 2 vaccinaties gehad?
- Datum laatste vaccinatie

In de afspraakbevestiging die de betrokkene ontvangt is de gezondheidsverklaring[4] in de bijlage toegevoegd. Deze gezondheidsverklaring wordt op de vaccinatielocatie of door het medische callcenter overgenomen in CoronIT en bevat de volgende vragen:

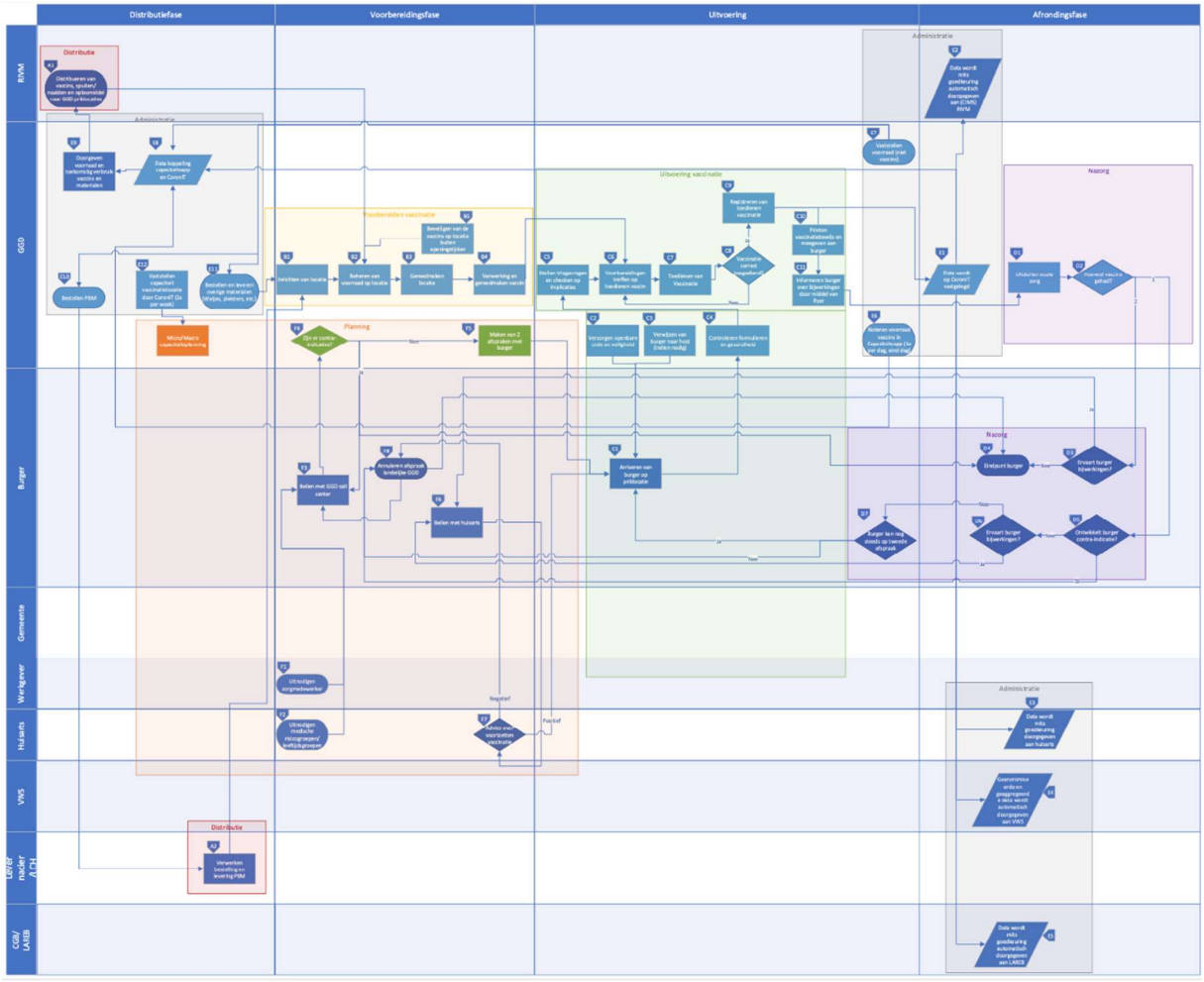
- Bent u in de afgelopen 4 weken positief getest op corona?
- Heeft u nu koorts van 38.5 graden Celsius of hoger?
- Heeft u nu andere corona-gerelateerde klachten en/of zit u in quarantaine?
- Krijgt u binnen 7 dagen voor of na de afspraak een andere vaccinatie?
- Is er 2 dagen voor of na de vaccinatie een operatie gepland?
- Valt u wel eens flauw na vaccinatie?
- Heeft u eerder een ernstige allergische reactie gehad op medicatie of een vaccinatie?
    - Waarop en bent u daarvoor behandeld?
    - Draagt u een EpiPen of geneesmiddelenpaspoort bij u?
- Heeft u borstkanker?
    - Rechts of links?
- Gebruikt u antistollingsmedicatie of bloedverdunners?
    - Welk medicijn en welke dosering afgelopen 7 dagen?
- Bent u bij de trombosedienst onder behandeling?
- Heeft u last van een stollingsstoornis?
    - Hemofilie
    - Ziekte van Von Willebrand
    - Tekort aan bloedplaatjes
    - Anders
- Epilepsie én aanval gehad bij koorts of vaccinatie?

Daarnaast is in CoronIT bij de gezondheidsverklaring de vraag opgenomen of er toestemming wordt gegeven voor het opvragen van medische informatie bij de behandelend arts. Het medisch callcenter zal gebruik maken van deze toestemmingsvraag.

3. Gegevensverwerkingen

In deze paragraaf wordt weergegeven welke stappen worden genomen in het vaccinatieproces en wie deze stappen uitvoert. In dit grafisch overzicht zijn alle fases meegenomen. Ook de fases waarop deze DPIA geen betrekking heeft. Hierdoor wordt er een compleet beeld gegeven van het gehele proces. In bijlage 1 zijn de stappen per fase waarop deze DPIA betrekking heeft opgenomen. Het gaat dan om de fases planning, uitvoering vaccinatie, administratie en nazorg.

[4] De gezondheidsverklaring zal tussentijds wijzigen. De uitgewerkte gezondheidsverklaring is de huidige verklaring die vanaf 27-1-2021 gebruikt wordt. De oude versie blijft in gebruik tot het moment dat iedere betrokkene waarbij deze verklaring gebruikt is, de tweede vaccinatie heeft ontvangen.



1. Afspraak maken

Onder verantwoordelijkheid van het RIVM is een uitnodigingsbrief opgesteld welke wordt verstuurd naar de doelgroep. De eerste burgers die gevaccineerd gaan worden zijn de zorgmedewerkers. De uitnodiging van deze medewerkers geschiedt via de werkgever. De werkgever deelt deze brieven vervolgens uit aan de werknemers. Bij de doelgroep 90-plussers worden de brieven aan de huisartsen verstuurd en verstrekt de huisarts de brief aan de betrokkene. Met deze brief kan de betrokkene contact opnemen met het callcenter voor het maken van een afspraak. De callcenter-medewerker doorloopt de volgende stappen:

Allereerst gaat de callcenter-medewerkers na voor wie er gebeld wordt. Wanneer dit voor een ander is, maar er wordt gebeld door een mantelzorger, medewerker in het verpleeghuis, kind van een ouder, doventolk of gevolmachtigde dan wordt de afspraak ingepland namens de betrokkene. In dat geval dient de beller de gegevens van de betrokkene te verstrekken. Op vaccinatielocatie wordt de identiteit van de betrokkene gecontroleerd.

Vervolgens worden de gegevens gecontroleerd. Er wordt gevraagd naar het BSN om te controleren of de betrokkenen reeds een dossier heeft in CoronIT, omdat deze persoon zich eerder heeft laten testen of wellicht eerder heeft gebeld voor het maken van een vaccinatie-afspraak. Om te verifiëren of het dossier van de beller is, worden er verificatievragen gesteld.

Vervolgens worden de vragen zoals genoemd op p. 5 van deze DPIA gesteld.

Indien de uitkomst van de vragen zodanig is dat een afspraak kan worden ingepland, wordt er nog gevraagd of de gegevens gedeeld mogen worden met de huisarts en of de gegevens gedeeld mogen worden met het RIVM. Deze toestemming wordt vervolgens geregistreerd in het dossier in CoronIT.

Tot slot wordt nog gevraagd of iemand eerder gevaccineerd is tegen Corona, en wordt het formulier opgeslagen in CoronIT.

Vervolgens kan er een afspraak worden ingepland. Hier wordt nog geregistreerd binnen welke doelgroep de betrokkene valt. Er worden twee afspraken ingepland. Ook wordt er alleen een eerste afspraak ingepland, wanneer het zeker is dat de persoon ook een tweede prik kan ontvangen. Wanneer de afspraak is ingepland, krijgt de betrokkene een afspraakbevestiging per sms en een e-mail met daarin de afspraakbevestiging toegestuurd. In deze e-mail staat de datum, tijd, locatie en algemene toelichting omtrent de afspraak. Ook wordt in de afspraakbevestiging de medische verklaring opgenomen, welke moet worden ingevuld en meegenomen naar de locatie. Daarnaast wordt in de afspraakbevestiging aangegeven welk vaccin de betrokkene krijgt toegediend. Er wordt hiervoor gebruik gemaakt van verschillende afspraakbevestigingen die worden gekoppeld aan het zorgdomein.

Het kan ook zijn dat een betrokkene belt om een afspraak af te zeggen. In dat geval wordt de reden van annulering vastgelegd in CoronIT.

Er komt een moment waarop er geen vaccins meer voorradig zijn. In dat geval kunnen de betrokkene die een uitnodiging hebben ontvangen, niet meer gevaccineerd worden. Om deze groep zo snel mogelijk in aanmerking te laten komen voor een vaccinatie wordt gevraagd om het telefoonnummer en de postcode te registreren in Quandago (programma van TelePerformance). Op die manier kan er een SMS worden uitgestuurd wanneer er in de desbetreffende regio weer vaccins voorradig zijn. Deze lijsten worden tevens gebruikt om betrokkene die op de lijst staan actief te benaderen, wanneer dit nodig is om spillage te voorkomen.

2. Medisch callcenter

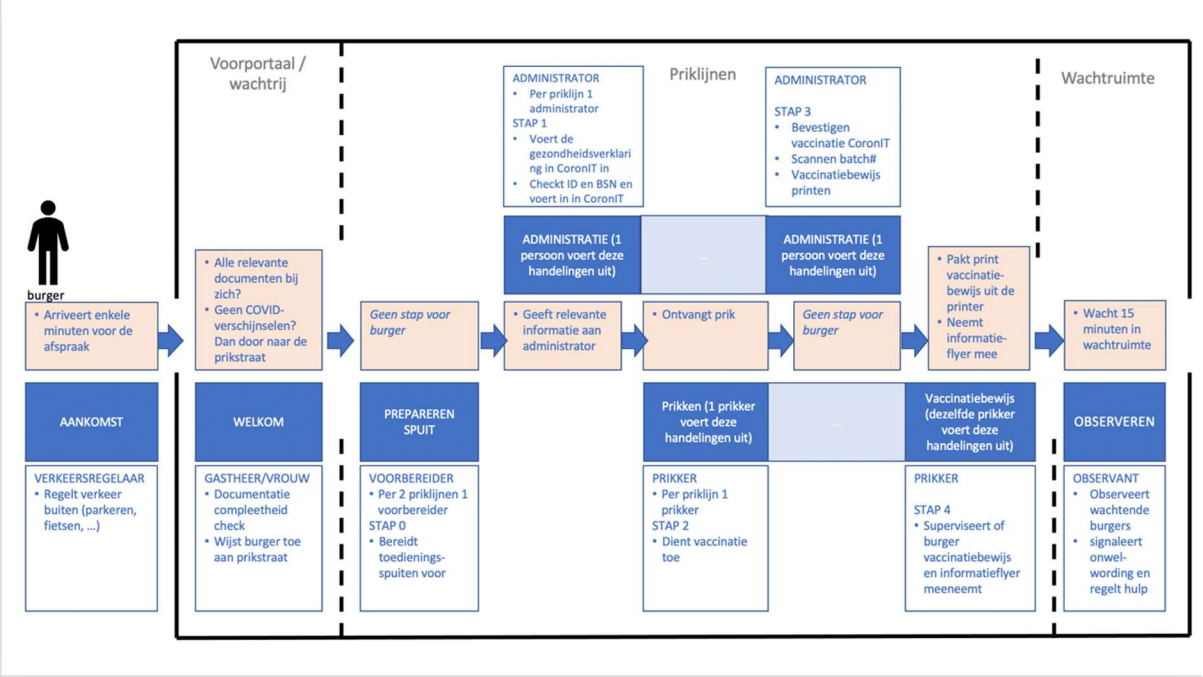
Vanuit betrokkenen worden er medisch inhoudelijk vragen gesteld over het wel of niet kunnen krijgen van een vaccinatie. Daarnaast stellen betrokkene vragen over het invullen van de gezondheidsverklaring. Deze vragen kunnen niet door het landelijke callcenter dat de afspraken

maakt, worden beantwoord omdat zij geen medisch advies geven. Om ervoor te zorgen dat de betrokkene wel ergens met hun vragen terecht kunnen is er een medisch callcenter opgezet. Beantwoorde vragen worden aan een dossier gekoppeld en opgeslagen in CoronIT.

Burgers kunnen contact opnemen met het medisch callcenter bij vragen of een coronavaccinatie in hun situatie wel of niet te adviseren is. Dit kunnen zowel burgers zijn waarbij al afspraken gepland staan, als burgers die nog geen afspraak hebben.

Voor het uitvoeren van de werkzaamheden hebben de medewerkers van SOS International toegang tot CoronIT. Hierin kunnen zij dossiers aanmaken (in geval er nog geen afspraak gemaakt is) of bestaande dossiers aanvullen door het invullen van de gezondheidsverklaring. Wanneer uit de medische beoordeling blijkt dat een afspraak niet door kan gaan, moeten deze afspraken afgezegd worden.

3. Uitvoeren vaccinatie



De burger meldt zich bij de locatie waar hij/zij een afspraak heeft laten inplannen. Een burger kan alleen toegelaten worden tot de locatie wanneer deze persoon beschikt over een uitnodigingsbrief van de werkgever, huisarts, arbodienst of instelling en een afspraakbevestiging kan overhandigen.

Bij aankomst controleert de gastheer/vrouw of de burger de afspraakbevestiging, gezondheidsverklaring en de brief van de werkgever bij zich heeft. Mocht de gezondheidsverklaring nog niet zijn ingevuld, dan dient de burger dit op locatie in te vullen. Hiervoor verstrekt de host een print van de lege gezondheidsverklaring.

Vervolgens controleert de administrator de identiteit van de burger en de documenten. De administrator verwerkt het soort document en het documentnummer van het identiteitsbewijs in CoronIT. Vervolgens wordt de ingevulde gezondheidsverklaring ingevoerd in CoronIT. Wanneer de ingevulde verklaring is doorgevoerd in CoronIT, hierna wordt deze verklaring teruggegeven aan de betrokkene. Deze is nodig voor een (mogelijk) tweede prikmoment. Na dit tweede prikmoment wordt de verklaring weer aan de betrokkene meegegeven.
Er zijn twee mogelijkheden bij het invullen/overnemen van de gezondheidsverklaringen:

- Alle vragen kunnen met nee beantwoord worden: in dat geval kan de administrator die de registratie uitvoert de antwoorden die by default staan ingevuld, overnemen in CoronIT en opslaan. De burger kan dan door naar de prikker.
- Wanneer een van de vragen met ja beantwoord wordt, wordt de burger verzocht om met de aanwezige arts te overleggen wat de juiste vervolgstappen zijn. De arts zal de gezondheidsverklaring doorlopen en de by default ingevulde 'nee' veranderen naar ja. Bij het opslaan van het formulier moet dan ook de naam van de arts die het formulier heeft ingediend worden vermeld. Zo is achteraf zichtbaar welke arts de triage heeft uitgevoerd bij de betrokkene. Daarna informeert hij de burger over het type vaccin en de verantwoordelijke arts.

Voordat de prik is gezet, scant de administrator de batchcode. Deze batchcode wordt op tafel geplakt zodat het gescand kan worden. De batchcode wordt gekoppeld aan de burger die het vaccin heeft ontvangen.

Voordat de prik is gezet, registreert de administrator het toedienen van de vaccinatie in CoronIT na afstemming met de prikker. Daarbij wordt tevens de naam van de arts geregistreerd. Vervolgens wordt er een vaccinatieregistratiebewijs uitgeprint. Gevaccineerde deelnemers krijgen na administratie een vaccinatiebewijs uitgereikt, voorzien van de datum, productnaam, batchnummer van het vaccin, naam en geboortedatum van de gevaccineerde. Dit wordt bij zowel de eerste als tweede vaccinatie gedaan. Degene die de printopdracht geeft, is dezelfde persoon als degene die de administratie vooraf doet. Deze persoon heeft dus toegang tot CoronIT. Daarnaast wordt de burger geïnformeerd over eventuele bijwerkingen door middel van een flyer en moet de betrokkene voor 15 minuten plaatsnemen in een wachtruimte.

Wanneer de vaccinatie niet goed is toegediend, wordt de persoon doorgestuurd naar de arts voor advies. In gevallen waarbij de fout wordt ontdekt als de burger de locatie al heeft verlaten, dient er contact met de burger worden opgenomen. Hiervoor wordt een recall procedure opgesteld. Indien het vaccin verkeerd is gegeven (te veel verdund, helemaal niet verdund of alleen oplosvloeistof) dan dient de administrator deze accidenten te registreren in het dossier van de burger. Er dient dan tevens een FOBO-melding (Fouten Bijna Ongelukken-melding) micmelding gemaakt te worden. Als een foutieve menging of hoeveelheid vaccin ook is toegediend, moet dit eveneens gemeld worden bij Bijwerkingencentrum Lareb (hierna: Lareb).

4. Administratie/nazorg

Na vaccinatie dient de burger 15 minuten in een wachtruimte plaats te nemen om acute post-vaccinale verschijnselen uit te kunnen sluiten.

5. Verstrekken gegevens huisartsen

Na elke vaccinatie-afspraak wordt, na toestemming van de burger, de eigen huisarts geïnformeerd over het type (merk) vaccinatie en de datum waarop deze is gegeven. De berichten worden in het HIS via Edifact verstuurd naar de huisartsen. Om na te gaan bij welke huisarts de betrokkene staat ingeschreven wordt de ION database geraadpleegd met gebruik van het BSN. Hiervoor wordt aan de betrokkene toestemming gevraagd. Wanneer toestemming is gegeven, gaat er een automatische aanvraag naar de ION-database om de AGB-code op te vragen van de huisarts. Hiervoor wordt het BSN en de geboortedatum van de betrokkene meegestuurd. Als de AGB-code wordt gevonden, wordt automatisch een bericht klaargezet. Dit bericht wordt beveiligd verstuurd naar het HIS van de huisarts, die een pushbericht ontvangt. Er wordt geen bericht teruggekoppeld aan de GGD. Het bericht komt via de beveiligde oplossing van Enovation in het HIS op praktijkniveau binnen en moet worden doorgezet naar de individuele huisarts. Voor nadere uitleg over de wijze waarop de gegevens verstrekt worden aan de huisarts, wordt verwezen naar de DPIA aansluiten huisartsen.

6. Verstrekken persoonsgegevens RIVM

Nadat het vaccin gezet is, gaan de gegevens van de toedieningen naar het RIVM voor centrale registratie. Hiervoor wordt de toestemming van de gevaccineerde gevraagd (opt-in). Deze toestemming wordt gevraagd bij het callcenter. De betrokkene wordt over deze verstrekking geïnformeerd middels een brief die als bijlage bij de uitnodiging is verstrekt door het RIVM. Op deze wijze is de betrokkene geïnformeerd voordat de betrokkenen een afspraak maakt en de toestemming wordt gevraagd.

De uitvoerende organisaties geven de vaccinatiegegevens, samen met een aantal persoonsgegevens die nodig zijn om de vaccinatie aan de juiste persoon in CIMS (COVID-vaccinatie Informatie- en Monitoringsysteem) te koppelen door aan het RIVM. Voorkeur heeft de aanlevering van gegevens via het LSP. Indien dit niet mogelijk is, heeft aanlevering door middel van CSV-bestanden middels Zorgmail de voorkeur. Gegevens kunnen ook via een Secure File Transfer protocol-connectie (SFTP-connectie) aangeleverd worden. Vaccinaties van mensen zonder BSN kunnen via CSV-bestanden doorgegeven.[5]

De persoonsgegevens die verstrekt worden zijn:

- Persoonsgegevens: naam, geboortedatum, geslacht, BSN, adres, woonplaats;

[5] https://lci.rivm.nl/richtlijnen/covid-19-vaccinatie onder 10.5

- Vaccinatiegegevens: productnaam, batchnummer, datum van 1ste vaccinatie en idem van 2e vaccinatie; uitvoerende instantie (naam GGD);
- Indien van toepassing: Indicaties over een persoon: de indicatie 'COVID medische indicatie'; 'COVID leeftijd indicatie' of 'COVID beroep indicatie', die door een zorgverlener zijn aangeleverd;
- Indien van toepassing: De AGB-code van de GGD.

7. Rapportage

Uit CoronIT worden verschillende rapportages aangeleverd. De gegevens helpen de partijen om een overzicht te houden van de pandemie en de ontwikkelingen daarin in hun werkveld. Deze rapportages zijn geanonimiseerd. 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 de eigen gegevens via datafeed, op eenzelfde wijze als dit gebeurt als bij testen.
- Het RIVM ontvangt een rapportage met alle records van vaccinaties met geaggregeerde gegevens namelijk: geboortejaar, weeknummer en tijd vaccinatie, vaccinnaam, batchnummer, aantal no-shows, beroepsgroepen medewerkers langdurige zorg, geslacht, eerste drie cijfers postcode en of er al dan niet toestemming is gegeven voor uitwisseling naar het CIMS. Dit is een gespeundonimiseerde set, aangezien deze niet direct herleidbaar is.

4. Betrokken partijen

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 vaccinatieproces.

2. De lokale GGD'en – *zelfstandig verwerkingsverantwoordelijken en tevens gezamenlijk verantwoordelijk*
   De GGD' en zijn zelfstandig verantwoordelijk voor de verwerking van de persoonsgegevens van de gevaccineerde personen in hun regio in CoronIT. GGHD GHOR Nederland zal deze gegevens niet verwerken zonder dat hiervoor aanleiding is. Die aanleiding kan een probleem in de

applicatie zijn die wordt gemeld vanuit een GGD of een vraag van een GGD waarbij het noodzakelijk is dat de gegevens kunnen worden ingezien.

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

Op basis van de wet zijn de lokale GGD' en belast met het plannen en uitvoeren van het vaccinatieprogramma. Zij zijn derhalve verantwoordelijk voor de verwerking van persoonsgegevens die voor dit proces worden opgevraagd. De inzet van het landelijke callcenter en het medisch callcenter verandert niet de rol van de lokale GGD' en, met uitzondering dat het plannen en verzetten van afspraken wordt uitgevoerd door het callcenter. De GGD' en hebben GGD GHOR Nederland aangewezen als aanspreekpunt voor dit proces en vertegenwoordiger van de GGD' en in relatie tot verwerker Teleperformance en SOS International. De verantwoordelijkheden van GGD GHOR Nederland en de GGD' en zijn vastgelegd in het 'Convenant gegevensuitwisseling gezamenlijk verantwoordelijken'.

3. GGD GHOR Nederland – *verwerker*
GGD GHOR Nederland voert voor alle GGD' en een coördinerende rol uit en beheert CoronIT. 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 landelijk callcenter en het medisch callcenter toegang tot CoronIT. Alle GGD'en stellen daarbij de doelen en middelen vast.

GGD GHOR Nederland is verwerker voor het aanleveren van rapportages aan 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 zelfstandig verantwoordelijk voor de helpdeskfunctie in het kader van het functioneel beheer en de verwerking van persoonsgegevens in het kader van deze functie.

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

Opmerking: het is op dit moment nog onduidelijk hoe de rol van GGD GHOR gekwalificeerd dient te worden. GGD GHOR heeft in principe te veel invloed gehad in de invulling van de procedures/doelen om als verwerker beschouwd te worden, maar heeft tegelijkertijd geen

wettelijke grondslag voor de verwerking van (bijzondere) persoonsgegevens als het verwerkingsverantwoordelijke wordt beschouwd.

4. RIVM – *zelfstandig verwerkingsverantwoordelijke*
   Het RIVM krijgt een gepseudonimiseerde lijst met data aangeleverd door GGD GHOR Nederland. Het RIVM gebruikt deze gegevens om rapportages op te kunnen stellen, die dient als stuurinformatie. Het RIVM bepaalt hoe deze gegevens worden geanalyseerd en gebruikt voor rapportages. Daarnaast ontvangt het RIVM, indien hiervoor toestemming is verleend door de betrokkene, de vaccinatiegegevens van de betrokkene met als doel deze op te nemen in het CIMS. In de gegevens transfer overeenkomst tussen de GGD' en, GGD GHOR Nederland en het RIVM worden afspraken gemaakt over deze gegevensuitwisseling.

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. Teleperformance- *verwerker*
   Teleperformance is leverancier van het callcenter. Zij sturen de callcenter-medewerkers aan en zijn verantwoordelijk voor kwaliteitscontrole en klachtafhandeling (m.u.v. klachten m.b.t. rechten van betrokkenen) Er is met Teleperformance een verwerkersovereenkomst afgesloten. Deze verwerkersovereenkomst is afgesloten met GGD GHOR Nederland en Teleperformance.

7. SOS International- *verwerker*
   SOS International is leverancier van het medisch callcenter. Zij sturen de callcenter-medewerkers aan en zijn verantwoordelijk voor kwaliteitscontrole en klachtafhandeling (m.u.v. klachten m.b.t. rechten van betrokkenen) Er is met SOS International een verwerkersovereenkomst afgesloten. Deze verwerkersovereenkomst is afgesloten met GGD GHOR Nederland en SOS International.

8. Huisartsen- *zelfstandig verwerkingsverantwoordelijke*
   De huisartsen krijgen, indien de betrokkene hiervoor toestemming verleend, de vaccinatiegegevens aangeleverd door GGD GHOR Nederland. Het doel van deze gegevensverstrekking is dat de huisarts op de hoogte is van de vaccinatie en efficiënt en adequaat acute zorg kan verlenen in geval er bijwerkingen optreden.

9. Olympia Nederland B.V.- *leverancier uitzendkrachten*

Olympia Nederland is een uitzendbureau welke callcenter-medewerkers levert aan Teleperformance. Deze callcenter-medewerkers vewerken de persoonsgegevens volgens instructies van Teleperformance. De callcenter-medewerkers die worden ingehuurd, worden voor het callcenter gezien als medewerkers van Teleperformance.

10. Young Capital Flex B.V.- *leverancier uitzendkrachten*
Young capital Flex is een uitzendbureau welke callcenter-medewerkers levert aan Teleperformance. Deze callcenter-medewerkers verwerken de persoonsgegevens volgens instructies van Teleperformance. De callcenter-medewerkers die worden ingehuurd, worden voor het callcenter gezien als medewerkers van Teleperformance.

4. Verwerkingsdoeleinden

Het algemene doel van de verwerkingen is het centraliseren, automatiseren, versnellen en vergemakkelijken van het COVID-19 vaccinatieproces en het geven van inzicht in de ontwikkeling van de pandemie. Met CoronIT kan het maken van een afspraak, het vaccineren en de nazorg van het vaccinatieproces worden vergemakkelijkt en versnelt.

1. Telefonisch opvragen van persoonsgegevens ten behoeve van het maken (of verzetten) van een afspraak.

Het doel van het verwerken van de persoonsgegevens van betrokkenen, is om na te gaan of iemand reeds een dossier heeft in CoronIT en deze aan te vullen ten aanzien van vaccinatie of om een dossier aan te maken wanneer er nog geen dossier aanwezig is van de betrokkenen. Daarnaast is het doel van deze verwerking om een afspraak te kunnen maken voor de betrokkene.

2. Registreren van contra-indicaties

Het doel van het registreren van contra-indicaties is om vast te leggen of iemand medisch gezien gevaccineerd kan worden.

3. Registreren e-mailadres en telefoonnummer

Het doel van deze verwerking is om per e-mail de afspraakbevestiging te versturen en per sms een herinnering te sturen voor de afspraak.

4. Registreren telefoonnummer en postcode in Quandago

Het doel van deze verwerking is om de betrokkene die een uitnodiging hebben ontvangen, maar geen afspraak kunnen maken te kunnen informeren indien het vaccin weer op voorraad is. Daarnaast kunnen de betrokkene die hun telefoonnummer hebben achtergelaten actief worden benaderd voor het maken van een afspraak, wanneer dit nodig is om spillage te voorkomen.

5. Uitvragen van toestemming voor delen data aan RIVM en huisarts

Het doel van deze verwerking is om vast te leggen of iemand toestemming geeft voor het verstrekken van de data aan het RIVM of de huisarts.

6. Identificatie en verificatie van de betrokkene op locatie en de registratie daarvan

Het doel van deze verwerking is om vast te stellen of de juiste persoon verschijnt bij de vaccinatie locatie en of deze persoon dus de gerechtigde persoon is om het vaccin te ontvangen.

7. Registreren vragen gezondheidsverklaring

Het doel van deze verwerking is om na te gaan of de persoon een vaccin mag ontvangen. Dit moet worden vastgelegd, omdat er een medische handeling wordt verricht. De behandeling kan tevens ontzegd worden op basis van de antwoorden die gegeven worden.

8. Registreren vaccinatiegegevens

Het doel van deze verwerking is om betrokkenen te kunnen informeren op het moment afwijkingen zijn ontdekt bij een batch vaccins.

9. Aanmaken vaccinatieregistratiebewijs

Het doel van deze verwerking is om een vaccinatieregistratiebewijs te kunnen verstrekken op verzoek van de betrokkene.

10. Registreren naam arts

Het doel van deze verwerking is om later aan te kunnen tonen welke arts het medische advies verstrekt heeft indien een van de vragen op de gezondheidsverklaring met ja is beantwoord. Daarnaast wordt te allen tijde de naam van de arts genoteerd, omdat er met het zetten van een vaccinatie een medische handeling wordt verricht.

11. Opname van de telefoongesprekken voor kwaliteitsdoeleinden en klachtafhandeling

Het doel van deze verwerking is het faciliteren van klachtenafhandeling, verbeteren van de efficiëntie van processen en het uitvoeren van kwaliteitscontroles. Hierbij kan worden gedacht aan het opsporen van fraudeleus gedrag of het onrechtmatig geven van medisch advies.

12. Het aanmaken van een dossier in CoronIT, invullen van de gezondheidsverklaring of het annuleren van een afspraak door SOS International.

Het doel van deze verwerking is de betrokkene de mogelijkheid te geven om met behulp van een medisch specialist de gezondheidsverklaring in te vullen. Hierdoor kan beoordeeld worden of de persoon een vaccinatie kan krijgen of niet en indien nodig de afspraak worden geannuleerd of de persoon worden doorverbonden om een afspraak te maken.

13. Doorverbinden betrokkene naar GGD indien nodig.

Het doel van deze verwerking is de betrokkene doorverbinden naar de GGD wanneer dit nodig is, bijvoorbeeld bij algemene vragen. Hiermee wordt de betrokkene gefaciliteerd omdat ze niet zelf de GGD hoeven te bellen.

14. Verstrekken gegevens huisarts

Het doel van deze verwerking is dat de huisarts geïnformeerd wordt over het feit dat de betrokkene gevaccineerd is. Deze informatie kan de huisarts helpen bij het verlenen van acute zorg, wanneer er bijvoorbeeld post-vaccinale bijwerkingen optreden.

15. Raadplegen ION database

De ION database wordt geraadpleegd om te achterhalen bij welke huisarts de betrokkene staat ingeschreven. Hiervoor wordt het BSN gebruikt.

16. Verstrekken gegevens aan het RIVM

Centrale registratie van COVID-19-vaccinatie is van groot belang voor de individuele deelnemer, voor de uitvoering van het programma, voor de bewaking van de volksgezondheid en voor de monitoring van de effectiviteit en veiligheid. RIVM-DVP verzorgt de centrale registratie van de vaccinaties en de toegediende vaccins en controleert de gegeven vaccinaties op juistheid wat betreft gehanteerd interval, merk vaccin en expiratiedatum.

De algemene doelen van gegevensverstrekking aan de centrale registratie zijn: *bestrijding van de pandemie, effectiviteitsonderzoek, veiligheidsbewaking van en voor de cliënt/patiënt en het vaccinatieprogramma.*

De operationele doelen die met het centraal registreren worden beoogd zijn de volgende:

a. Bestrijding van de pandemie door snel en nauwkeurig inzicht in de bijdrage van vaccinatie hieraan in verband met al dan niet kunnen afschalen van de (*landelijke of lokale*) maatregelen.

b. Inzicht in de vaccinatiegraad van de bevolking (de verschillende doelgroepen voor vaccinatie) om maatschappelijke vragen hierover te beantwoorden en om het programma bij te sturen als doelgroepen onvoldoende bereikt blijken te worden.

c. Inzicht in de effectiviteit van de verschillende vaccins (bij de verschillende doelgroepen) om het vaccinatieprogramma in samenhang met andere maatregelen voor de bestrijding van de pandemie te kunnen bijsturen.

d. Ten aanzien van veiligheid: het verbeteren van betrouwbaarheid van data om de veiligheid te kunnen monitoren en te kunnen ingrijpen bij calamiteiten. Deze situatie kan zich bijvoorbeeld voordoen bij ernstige bijwerkingen of wanneer blijkt dat vaccinbatch niet/zeer beperkt effectief is.

e. Vaccinatiestatus is eenvoudig in te zien of opvraagbaar voor de gevaccineerde en (na toestemming gevaccineerde) in bepaalde gevallen via een verzoek aan de beheerder (die het verzoek zal toetsen op rechtmatigheid) voor diens zorgverlener.

f. De arts die een positieve COVID-19 diagnose vaststelt kan eenvoudig de vaccinatiestatus opvragen om te voldoen aan de wettelijke meldplicht die op hem rust (signalering vaccinfalen).

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 vaccinatieproces, waardoor de volgende zaken gemakkelijker en betrouwbaar verlopen:

- Het vaccineren van betrokkenen;
- 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 vaccineren, weten mensen dat zijzelf of de omgeving beter beschermd is tegen het virus. Dit komt ten goede aan de volksgezondheid en de economie.

Betrokkenen

Door CoronIT kan snel en eenvoudig een betrokkene worden aangemeld en gevaccineerd. De vaccinatiegegevens kunnen vervolgens snel worden teruggekoppeld aan de betrokkene. Het snelle vaccineren kan de betrokkene ook geruststellen over de gezondheid.

Mensen kunnen door de aanwezigheid van het COVID-19 virus stress en onzekerheid ervaren en mogelijk gehinderd worden in het uitvoeren van werkzaamheden. Derhalve is het voor de betrokkene van belang dat zij zich zo snel mogelijk kunnen laten vaccineren.

De betrokkene heeft als belang dat de huisarts hulp kan verlenen indien dit noodzakelijk is naar aanleiding van een gegeven vaccinatie tegen COVID-19. De betrokkene heeft echter zelf de keuze of de gegevens zullen worden doorgegeven aan de huisarts en dus onderdeel zullen uitmaken van het medisch dossier dat wordt gehouden door de huisarts.

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 vaccinatiecapaciteit. 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 het vaccineren effeciënt te kunnen laten verlopen via CoronIT, samen met de GGD'en.

GGD

Door het inplannen van afspraken door het callcenter, kan de GGD efficiënt vaccineren op de vaccinatie locaties en wordt het maken van afspraken uit handen genomen. De GGD zorgt voor vaccinatie locaties. Zij hebben er baat bij dat zoveel mogelijk betrokkenen worden gevaccineerd, waardoor het aantal positieve testen zal verminderen en daarmee de druk op de GGD'en ten aazien van de uitvoering van het testproces en het Bron- en Contactonderzoek zal verminderen.

RIVM

In kaart brengen van de stand van zaken en ontwikkeling van de verspreiding van COVID-19 in Nederland. De informatie uit CoronIT wordt geanonimiseerd verstrekt aan het RIVM en dient om te voorzien in stuurinformatie. Voor onder meer bestrijding van de pandemie, evaluatie van het programma, onverwachte bijwerkingen of een recall is het belangrijk dat alle vaccinaties geregistreerd worden in CIMS.

Ministerie van Volksgezondheid
De minister draagt via het RIVM zorg voor de regie op en de coordinatie van de uitvoering, alsmede de registratie, bewaking en evaluatie van het vaccinatieprogramma (Wpg artikel 6b). Daarnaast is het ministerie, vertegenwoordigd door de minister, 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 uitvoeren van het vaccinatieprogramma.

Huisartsen
Huisartsen hebben er een belang bij om een zo volledig mogelijk dossier van de betrokkene te hebben en op de hoogte te zijn van een een gegeven vaccinatie voor COVID-19. Het doorkrijgen van de vaccinatie is van belang om dit te kunnen linken aan eventuele symptomen die iemand vertoont. Op deze manier kan de huisarts snel zorg verlenen als dat nodig blijkt. Daarnaast zijn deze zaken opgenomen in het medisch dossier van de betrokkene, zodat deze informatie bij complicaties altijd kan worden nagezocht.

6. Verwerkingslocaties

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

Voor het callcenter vinden de verwerkingen plaats in Nederland en Duitsland:

- De callcenter-medewerkers verwerken de gegevens in CoronIT, welke in Nederland wordt gehost.
- De hosting van de telefonietool en de opnames van de gesprekken vindt plaats in Frankfurt, Duitsland.
- De ingekochte software van Tableau draait in de eigen rapportage omgeving van GGD GHOR Nederland op servers (van Vancis) in Nederland.

7. Techniek en methode van gegevensverwerking

Voor de verwerking in CoronIT wordt gebruik gemaakt van:

- CoronIT (webapplicatie, geleverd door Topicus);

- Synaps (platform waarop CoronIT is gebouwd, geleverd door Topicus);
- Barcode van de vaccins;
- Servers (Previder);
- Tableau (tijdelijke oplossing voor oplevering rapportages, geleverd door Topicus);
- The Identity Hub (Authenticatie platform, in beheer van GGD GHOR);

Tableau is een reporting tool van de GGD. Het betreft ingekochte software, die draait in de eigen rapportage-omgeving. Er worden geen persoonsgegevens getoond in deze rapportages.

Doorgifte RIVM

Voor de verwerking wordt gebruik gemaakt van:

- CoronIT (geleverd door Topicus)
- HIP
- CIMS (RIVM)
- VPN-verbindingen met het RIVM

Het HIP bestaat uit:

- Data warehouse voor het ontvangen van de gegevens vanuit de datamart/etl van CoronIT. (GGD GHOR in beheer (technisch) bij Vancis)
- Python scripts voor het verwerken en klaarzetten van de data (Servers in beheer bij Vancis maken onderdeel uit van het GGD GHOR domein)
- Datahub: Omgeving met script en dataviews voor het ophalen van data. Doormiddel van dataview wordt bepaald welke data er opgehaald kan worden. Voor het CIMS is dit de lijst uit de requirements voor de koppelingen. Voor de anonieme data is dit de afgestemde lijst. Deze omgeving is onderdeel van het GGD GHOR domein en in beheer (technisch) bij Vancis
- Site to site VPn (Vancis) naar het RIVM om het ophalen van de data mogelijk te maken.

Doorgifte huisartsen

Voor de verwerking wordt gebruik gemaakt van:

- CoronIT (geleverd door Topicus)
- HIP
- ION-database (Vecozo – wordt gebruikt om een BSN nummer aan een huisarts te koppelen)
- Edifact-oplossing (Enovation)
- HIS (huisarts informatie systeem, geleverd door diverse levanciers)
- HPZone (Infact)

Callcenter

Er worden verschillende tools gebruikt voor de verwerking van de persoonsgegevens door callcenter-medewerkers en de inzet van deze medewerkers door Teleperformance. De belangrijkste in het kader van vaccinaties zijn QuandaGo en CoronIT. Voor een volledig overzicht van de tools die bij het callcenter worden gebruikt, wordt verwezen naar de DPIA van het Callcenter.

Enkel in QuandaGo en CoronIT worden persoonsgegevens verwerkt van de Betrokkene. De overige systemen worden onder andere gebruikt voor urenregistratie door (ingehuurde) medewerkers van Teleperformance, het hosten van een intranet voor (ingehuurde) medewerkers van Teleperformance enzovoort.

QuandaGo is een "cloud contact center", callcenter-medewerkers kunnen hiermee telefoongesprekken aannemen en terugbellen (WebRTC oplossing). Daarnaast bevat deze tool een dashboard (wachtrij overzicht, etc.) en de verschillende belscripts waar de callcenter-medewerker gebruik van maakt (welke vragen, wat te doen met antwoorden, welke stap na een bepaald antwoord, etc.).

Voor de verwerkingen die worden uitgevoerd door het callcenter is er geen sprake van geautomatiseerde besluitvorming, profilering of big dataverwerkingen.

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);
- Besluit publieke gezondheid;
- Wet op de geneeskundige behandelovereenkomst;
- Wet aanvullende bepalingen gebruik BSN in de zorg;
- Uitvoeringsrichtlijn COVID-19-vaccinatie 2021;
- Opdracht van Ministerie van VWS aan GGD GHOR Nederland;
- Mandaat GGD'en aan GGD GHOR Nederland.

Op de verwerking van de persoonsgegevens door de callcenter-medewerkers is de volgende wet- en regelgeving van toepassing:

- Algemene Verordening Gegevensbescherming (AVG);
- Uitvoeringswet AVG (UAVG);
- Wet publieke gezondheid (Wpg);
- Besluit publieke gezondheid;
- COVID-19-Vaccinatie richtlijn RIVM;
- Opdracht van Ministerie van VWS aan GGD GHOR Nederland
- Mandaat GGD'en aan GGD GHOR Nederland.

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

- Privacybeleid GGD GHOR Nederland
- Privacybeleid Teleperformance
- Werkinstructie Outbound
- Werkinstructie Inbound
- GECSP - Global essential compliance & security policies Teleperformance
- TISPS - Teleperformance Information Security and Privacy Standards Gedragsregels thuiswerken & BYOD Teleperformance
- Geheimhoudingsverklaring incl. gedragsregels social media Teleperformance
- Geheimhoudingverklaring uitzendpartners

9. Bewaartermijn

Gegevens in CoronIT:

De bewaartermijn is afhankelijk van de kwalificatie van het dossier in CoronIT ten aanzien van vaccinaties. In geval van vaccinaties kan CoronIT worden gezien als een medisch dossier. In dat geval is de bewaartermijn 20 jaar op grond van artikel 7:454 lid 3 BW. Betrokkene kan wel verzoeken om het dossier eerder te verwijderen. In dat geval dient een afweging gemaakt te worden of de gegevens verwijderd kunnen worden of niet.

Opnames telefoongesprek:

- Het telefoongesprek wordt binnen 14 dagen gecheckt en gemarkeerd, anders wordt na 14 dagen het telefoongesprek verwijderd.
- Telefoongesprekken waarbij een incident is vastgesteld, dan wel op basis van controle, dan wel op basis van een binnengekomen klacht, worden bewaard totdat het incident volledig is afgerond. Na volledige afhandeling van het incident wordt de opname binnen 14 dagen verwijderd.

Speech analysis transcripten:

- De transcripten worden 6 weken bewaard, in verband met het kunnen controleren van de transcripten indien er een klacht wordt ingediend.
- Indien een transcript onderdeel wordt van een (juridische) procedure, bijvoorbeeld naar aanleiding van een klacht van Betrokkene, of bij constatering van fraudeleus gedrag, wordt het transcript bewaard voor de duur van de juridische procedure.
- De geaggregeerde rapportages worden bewaard voor 14 maanden, in verband met de noodzaak van de GGD'en en GGD GHOR Nederland om seizoensanalyses te kunnen maken en vergelijken.

Telefoonnummer en postcode in Quandago

Zodra een SMS wordt verstuurd dat het vaccin weer op voorraad is, worden de gegevens verwijderd uit Quandago.

B. Beoordeling rechtmatigheid gegevensverwerkingen

10. Rechtsgrond

Verwerkingen in CoronIT

Het COVID-19 vaccinatieprogramma is onderdeel van de bestrijding van de infectieziekte COVID-19. De bestrijding van infectieziekten is een wettelijke plicht uit de Wpg die rust op de GGD. Daarnaast is er een wijzigingsbesluit ingediend voor het Besluit publieke gezondheid. Door deze wijziging zal het COVID-19 vaccinatieprogramma onder het Rijksvaccinatieprogramma vallen. In dat geval is artikel 6, eerste lid jo artikel 6b, derde lid Wpg jo art. 11 eerste lid, sub h Besluit Wpg van toepassing. Daarnaast is de Wet op de geneeskundige behandelovereenkomst (WGBO) van toepassing.

De verwerking van niet-bijzondere persoonsgegevens is toegestaan o.b.v. minimaal één van de zes grondslagen van de AVG [6]. 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.
- 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 wettelijke verplichting, 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. Daarnaast bevat de Wpg specifieke bepalingen die zien op de uitvoering van het vaccinatieprogramma. De Wpg bevat omissies, waardoor niet alle verwerkingen binnen CoronIT direct beschreven zijn in de wet. In dat geval wordt gesteund op de intentie van de Wpg en het algemeen belang om infectieziektes te bestrijden. Daarnaast berust verwerking van persoonsgegevens op de WGBO. Dit betekent dat zowel de Wpg als de WGBO de grondslag vormen voor de verwerking van persoonsgegevens gedurende het vaccinatieprogramma.

Voor het registreren van de aard en het nummer van het identiteitsbewijs bij de identificatie van de betrokkene op de vaccinatielocatie is artikel 6 van de Wabvpz van toepassing. De verwerkingsgrondslag voor deze gegevens is dan ook art. 6 lid 1 sub c AVG jo art. 6 Wabvpz.

Verwerkingen callcenter

De verwerking van persoonsgegevens die plaatsvindt door het opnemen van de gesprekken in het kader van kwaliteitscontrole, vindt plaats op basis van:

[6] Artikel 6 AVG.

- De toestemming (opt-in/opt-out) van de betrokkene, gegeven alvorens een opname wordt gestart. (AVG artikel 6 lid 1 sub a)

De verwerking van persoonsgegevens uit opgenomen telefoongespreken door middel van speech analysis en handmatige controles vindt plaats op basis van:

- Het gerechtvaardigd belang van zowel GGD GHOR Nederland als Teleperformance. (AVG artikel 6 lid 1 sub f)
- Opmerking: deze grondslag hangt af van de discussie of GGD GHOR verwerkingsverantwoordelijk is of verwerker. Indien GGD GHOR als verwerker beschouwd moet worden, moet naar een andere grondslag worden gezocht (aangezien GGD Amsterdam geen beroep op een gerechtvaardigd belang kan doen).

Het opvragen en registreren van het telefoonnummer en de postcode in Quandago en het versturen van een SMS wanneer er weer vaccins voorradig zijn, vindt plaats op basis van:

- art. 6 lid 1 sub c AVG: De verwerking is noodzakelijk om te voldoen aan een wettelijke verplichting die op de verwerkingsverantwoordelijke rust.

Door middel van het versturen van een SMS worden de betrokkene die als eerste in aanmerking zouden komen voor het ontvangen van een vaccinatie in de gelegenheid gesteld om alsnog een afspraak te maken voor een vaccinatie. Hiermee wordt er invulling gegeven aan de wettelijke taak van de GGD om op grond van de Wpg de infectieziekte te bestrijden en het vaccinatieprogramma uit te voeren.

Doorgifte persoonsgegevens aan RIVM

De verstrekking van herleidbare persoonsgegevens aan het RIVM met als doel deze op te nemen in het CIMS, geschiedt op grond van toestemming zoals bedoeld in artikel 6 lid 1 sub a AVG. Wanneer het COVID-19 vaccinatieprogramma wordt toegevoegd aan het Rijksvaccinatieprogramma, dan blijkt uit de memorie van toelichting (hierna: MvT) welke gegevens met het RIVM gedeeld moeten worden in het kader van centrale registratie. Hierbij wordt expliciet genoemd dat het BSN verstrekt moet worden aan het RIVM in het kader van de centrale registratie. De grondslag voor het verstrekken van het BSN is dan ook art. 6 lid 1 sub c AVG. Onder punt 11 van deze DPIA wordt nader ingegaan op de wijze waarop voldaan wordt aan de vereisten van toestemming.

Doorgifte persoonsgegevens aan huisartsen

De verwerking van niet-bijzondere persoonsgegevens is toegestaan o.b.v. minimaal één van de zes grondslagen van de AVG [7]. Voor de verwerking van (gewone) persoonsgegevens in het burgerportaal wordt een beroep gedaan op art. 6 lid 1 sub a AVG:

[7] Artikel 6 AVG.

- *"De betrokkene heeft toestemming gegeven voor de verwerking van zijn persoonsgegevens voor een of meer specifieke doeleinden"*

De betrokkene geeft uitdrukkelijke en ook actieve toestemming om de gegevens uit te wisselen met de arts.

Voor het gebruik van het BSN voor het ophalen van de AGB-code van de huisarts is geen directe grondslag in de wet te vinden. De toestemming voor de verwerking van gegevens kan geen toestemming voor de verwerking van het BSN inhouden. Een verwerking van een BSN moet zijn vastgelegd in een wet.

Art. 10 Wet algemene bepalingen Burgerservicenummer (Wabb) stelt dat overheidsorganen bij het verwerken van persoonsgegevens in het kader van de uitvoering van hun taak gebruik kunnen maken van het BSN.

Daarnaast bepaalt art. 4 wet aanvullende bepalingen verwerking persoonsgegevens in de zorg (Wabvpz) dat een zorgaanbieder het BSN van een cliënt gebruikt met het doel te waarborgen dat de in het kader van de verlening van zorg te verwerken persoonsgegevens op die cliënt betrekking hebben.

GGD GHOR Nederland voert taken uit voor overheidsorganen. Daarnaast kunnen GGD'en, waarvoor GGD GHOR Nederland het systeem beheert en de gegevens uitwisselt, worden gekwalificeerd als zorgverlener. Het gebruik van het BSN om de AGB-code van de huisartsen op te zoeken, heeft een aantal positieve effecten. Ten eerste wordt de tijd dat een telefoongesprek duurt om de huisarts uit te vragen, verkort. Dit betekent een aanzienlijke verhoging van de efficiëntie. Daarnaast zorgt de raapleging voor het vinden van de huisarts waar de persoon is ingeschreven. Dit proces gebeurt automatisch, waardoor de kans dat de gegevens bij de verkeerde huisarts terecht komen zeer klein is.

Hier kan dus worden beargumenteerd dat het gebruik van het BSN voor het opzoeken van de AGB-code van de huisarts, kan worden gezien als het uitvoeren van een publieke taak, namelijk het bestrijden van infectieziekten en het verzorgen van de juiste nazorg, op basis van toestemming van de betrokkene. Daarnaast kan worden gesteld dat het opzoeken van de juiste AGB-code en zo het doorgeven van deze zeer relevante informatie aan de juiste huisarts, kan worden gezien als een vorm van goed hulpverlenerschap.

Voor het doorgeven van het BSN aan de huisarts kan worden teruggevallen op art 4 Wabvpz. Er wordt een bericht gestuurd met medische gegevens over een patiënt van de huisarts. Om te kunnen verifiëren dat de gegevens aan het juiste dossier worden toegevoegd, is het BSN het enige unieke nummer dat daarvoor kan worden gebruikt.

- Opmerking: ook deze grondslag is sterk afhankelijk van de uitkomst van de discussie over de kwalificatie van GGD GHOR.

11. Bijzondere persoonsgegevens

Verwerking bijzondere persoonsgegevens in CoronIT

Daarnaast worden in CoronIT bijzondere persoonsgegevens verwerkt. In dat geval moet er een beroep worden gedaan op een van de uitzonderingsgronden van artikel 9 AVG. De verwerking valt onder de uitzondering zoals bepaald in art. 9 lid 2 sub g, h en i AVG:

Art. 9 lid 2 sub g AVG:

- De verwerking is noodzakelijk om redenen van zwaarwegend algemeen belang, op grond van Unierecht of lidstatelijk recht, waarbij de evenredigheid met het nagestreefde doel wordt gewaarborgd, de wezenlijke inhoud van het recht op bescherming van persoonsgegevens wordt geëerbiedigd en passende en specifieke maatregelen worden getroffen ter bescherming van de grondrechten en de fundamentele belangen van de betrokkene;

Art. 9 lid 2 sub h AVG:

- De verwerking is noodzakelijk voor doeleinden van preventieve of arbeidsgeneeskunde, voor de beoordeling van de arbeidsgeschiktheid van de werknemer, medische diagnosen, het verstrekken van gezondheidszorg of sociale diensten of behandelingen dan wel het beheren van gezondheidszorgstelsels en -diensten of sociale stelsels en diensten, op grond van Unierecht of lidstatelijk recht, of uit hoofde van een overeenkomst met een gezondheidswerker en behoudens de in lid 3 genoemde voorwaarden en waarborgen;

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.

Art. 30 lid 3 sub a Uitvoeringswet AVG (UAVG) bepaalt dat bijzondere gegevens mogen worden verwerkt met het oog op een goede behandeling of verzorging van de betrokkene dan wel het beheer van de betreffende instelling. De GGD kan daaronder worden geschaard.

De verwerking met een zwaarwegend algemeen belang en het zwaarwegend algemeen belang op het gebied van volksgezondheid is in de UAVG niet verder uitgewerkt voor epidemieën. Sub h is

niet voor epidemieën uitgewerkt en sub i is in zijn geheel niet opgenomen in de UAVG. Dit lijkt een omissie in de UAVG.

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 jo artikel 6b lid 3 Wpg. Daarin is gesteld dat de veiligheidsregio zorgdraagt voor de voorbereiding op de bestrijding en de bestrijding van een infectieziekte en het deel van het vaccinatieprogramma dat daartoe bij algemene maatregel van bestuur is aangewezen. Daarbij is door VWS besloten dat, om de bestrijding te stroomlijnen, de GGD GHOR 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'*.

In het kader daarvan kan worden gesteld dat in het kader van het algemeen belang (zoals gesteld in art. 9, lid 2 sub g, h en i AVG en art. 6 lid 1 sub e AVG) en op basis van de Wpg, kan worden gesteld dat het vaccineren van de betrokkene en de registratie van medische gegevens wordt uitgevoerd in het algemeen belang in het kader van de bestrijding van een infectieziekte, waarbij de bevolking zelf maatregelen kan treffen. Deze maatregel kan bijvoorbeeld inhouden het aanmelden voor een vaccin en het verstrekken van de gegevens die daarvoor nodig zijn. Voor het vaccineren en registratie is het echter noodzakelijk de betrokkene goed te informeren over de verwerking van de persoonsgegevens. Daarnaast is er bij vaccinaties mogelijk sprake van een medische behandelrelatie, waardoor een beroep kan worden gedaan op artikel 9 lid 2 sub h voor de verwerking van bijzondere persoonsgegevens.

Doorgifte bijzondere persoonsgegevens aan het RIVM
Bij de doorgifte aan het RIVM met als doel de gegevens op te nemen in het CIMS, worden ook bijzondere gegevens verstrekt, namelijk medische gegevens. De grondslag voor deze verstrekking is toestemming zoals bedoelt in artikel 6 lid 1 sub c en e jo artikel 9 lid 2 sub a AVG. De toestemming die wordt gegeven voor het verstrekken van de gegevens aan het RIVM is tevens bedoeld voor de doorbreking van het beroepsgeheim in de zin van art. 7:457 BW.

Betrokkene wordt vooraf geïnformeerd over het feit dat zijn of haar toestemming wordt gevraagd en wordt daarbij nader geïnformeerd over de verstrekking die in dat geval zal plaatsvinden.

Omdat de grondslag voor de verwerking toestemming in de zin van de AVG is, zijn er eisen verbonden aan de manier waarop deze toestemming gevraagd wordt. Er zijn adviezen opgesteld waarbij op de eisen van toestemming is ingegaan en waarbij de risico's ten aanzien van deze vereisten in beeld zijn gebracht. Deze risico's zijn voorgelegd bij de landsadvocaat, welke deze

risico's grotendeels heeft weerlegd. Hieronder worden de overwegingen beschreven en wordt verwezen naar het standpunt van de landsadvocaat.

1. Al dan niet aanwezig zijn van een Wanverhouding

De GGD'en geven bij het vaccineren uitvoering aan de aan hen opgedragen taak op grond van de Wpg. Hierdoor is de GGD te kwalificeren als overheid. De AVG geeft aan dat er in bepaalde gevallen een wanverhouding kan bestaan wanneer er sprake is van de relatie tussen burger en overheid. Daarbij moet het gaan om een duidelijke wanverhouding. Er kan geen gebruik worden gemaakt van toestemming in die gevallen waarin een duidelijk wanverhouding ertoe leidt dat de toestemming niet vrijelijk is gegeven. De overheid, en dus de GGD, kan gebruik maken van toestemming als verwerkingsgrondslag, als is voorzien in voldoende maatregelen om te waarborgen dat die toestemming inderdaad vrijelijk is gegeven.[8]

Om een duidelijke wanverhouding te voorkomen zijn enkele maatregelen genomen. De betrokkene wordt over de doeleinden van verwerking geïnformeerd middels een brief die gelijktijdig met de uitnodiging tot vaccinatie wordt verstrekt. De betrokkene wordt duidelijk geïnformeerd over het feit dat weigeren van toestemming geen negatieve gevolgen heeft.[9] Het weigeren van toestemming staat de mogelijkheid tot vaccineren daardoor niet in de weg.

Een van de doelen van het verstrekken aan de gegevens is dat de betrokkene snel gewaarschuwd kan worden bij eventuele bijwerkingen en dat de betrokkene een kopie van het vaccinatieregistratiebewijs kan opvragen bij het RIVM. Wanneer de betrokkene geen toestemming geeft voor het verstrekken van de gegevens, wordt hij/zij door de GGD geïnformeerd in geval van bijwerkingen en kan hij/zij een kopie van het vaccinatieregistratiebewijs opvragen bij de GGD. Tot slot wordt de betrokkene in de informatiebrief geïnformeerd over het gegeven dat toestemming kan worden ingetrokken en de wijze waarop dat kan. Hierdoor zitten er geen negatieve gevolgen aan het weigeren van toestemming. Er kan beargumenteerd worden dat er gezien bovenstaande geen sprake is van een duidelijke wanverhouding.

2. Granulariteit/specifiek

De AVG geeft aan dat de toestemming niet 'vrijelijk' is wanneer er geen afzonderlijke toestemming kan worden gegeven voor verschillende persoonsverwerkingen.[10]

Er zijn meerdere doeleinden waarvoor de gegevens in het CIMS worden verwerkt. Deze doeleinden zijn in de informatiebrief samengevoegd tot een korte uitleg aan de betrokkene.[11] Het is voor de betrokkene niet mogelijk om afzonderlijk toestemming te geven voor de verschillende doeleinden. Dit omdat er dan verschillende datastromen moeten zijn waarbij onderscheid wordt gemaakt in de

[8] Zie punt 4.6 van het advies van de landsadvocaat.
[9] Zie punt 4.7 van het advies van de landsadvocaat.
[10] Zie overweging 43 AVG.
[11] Zie onder 'doeleinde' van dit advies de tekst die is opgenomen in de informatiebrief die door het RIVM is opgesteld.

doeleinden waarvoor toestemming is gegeven. Bovendien zal de informatie daardoor onnodig complex worden en als gevolg daarvan niet voldoen aan de criteria dat informeren eenvoudig en begrijpelijk dient te zijn.

Om deze redenen is ervoor gekozen om de informatie samen te vatten. Zo wordt de betrokkene wel geïnformeerd over de doeleinden van de verwerking en wordt er zo goed mogelijk invulling gegeven aan de vereisten van toestemming in de zin van de AVG. In het convenant wordt aandacht besteedt aan de doelen waarvoor de gegevens worden verwerkt.

3. Aantoonbaarheid

De toestemming moet uitdrukkelijk worden gegeven. Dit kan schriftelijk, maar ook mondeling. In het geval van de voorgestelde aanpak is er sprake van mondelinge toestemming. Mondelinge toestemming ligt niet vast, anders dan na de vraagstelling in het callcenter wat het vereiste "aantoonbaarheid" uit de AVG bemoeilijkt.

Wel kan worden aangetoond dat er een vast proces wordt gevolgd. De betrokkene wordt geïnformeerd, waarna de callcenter medewerker toestemming vraagt en vastlegt in CoronIT als deze wordt gegeven. Dit strikte proces toont aan dat toestemming altijd op dezelfde wijze wordt uitgevraagd en vastgelegd. Door middel van een steekproef zal worden gecontroleerd of dit proces juist wordt uitgevoerd.

Middels steekproeven worden gecontroleerd of de toestemming wordt gevraagd volgens de instructies uit het callscript en of het antwoord van de betrokkene overeenkomst met de toestemming die is geregistreerd in CoronIT. In een latere fase wordt verder onderzocht of en hoe zorgvuldigheidsmaatregelen al dan niet uitgebreid kunnen worden.

4. Toepassing van andere grondslagen dan toestemming

Er is onderzocht in hoeverre het mogelijk is om een beroep te doen op een andere grondslag dan toestemming. In eerdere adviezen is de vraag aan VWS gesteld om een wettelijke basis te creëren voor de gegevensverstrekking aan het RIVM. Hiertoe ziet VWS vooralsnog geen aanleiding. Mede vanuit het ministerie wordt toestemming als passende grondslag gezien, waarbij is aangegeven dat enkel wanneer er onvoldoende toestemming wordt verleend deze wetswijziging opnieuw wordt overwogen.

Alles overwegende is toestemming op dit moment de best passende grondslag voor de uitwisseling met het RIVM. Dit gezien het belang van de gegevensverwerking door het RIVM dat bij wet is bepaald en is gemotiveerd in de MvT en het belang van de bestrijding van de pandemie. Daarbij wordt meegenomen dat er advies is gegeven door de Landsadvocaat, welke ook het advies heeft verzorgd over de gegevensuitwisseling tussen huisartsen en het RIVM evenals voor de ziekenhuizen en het RIVM. Hiermee wordt bereikt dat gelijke uitgangspunten van beoordeling geborgd zijn.

Doorgifte bijzondere persoonsgegevens aan de huisarts

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 2 sub a AVG:

- *"De betrokkene heeft uitdrukkelijke toestemming gegeven voor de verwerking van die persoonsgegevens voor een of meer welbepaalde doeleinden, behalve indien in Unierecht of lidstatelijk recht is bepaald dat het in lid 1 genoemde verbod niet door de betrokkene kan worden opgeheven"*

De betrokkene kan toestemming geven voor de uitwisseling van de medische gegevens met de huisarts. Deze toestemming is tevens bedoeld voor het doorbreken van het beroepsgeheim in de zin van artikel 7:457 BW.

12. Doelbinding

CoronIT

CoronIT is een registratiesysteem waarin een betrokkene kan worden aangemeld voor een vaccinatie. De betrokkene wordt geregistreerd, een afspraak kan worden gemaakt voor de vaccinatie, de gegevens kunnen worden ingezien door de administrator bij de vaccinatielocatie en de vaccinatiegegevens kunnen door dezelfde administrator worden geregistreerd. Dit versnelt het proces en stroomlijnt de data.

Daarnaast bieden vaccinatiegegevens zoals de vaccinatiegraad de mogelijkheid om inzicht te krijgen in het verloop van de pandemie, waardoor VWS adequatere beslissingen kan nemen in de bestrijding van COVID-19.

Ook in de richtlijn van het RIVM voor de COVID-19 vaccinaties, wordt aangegeven dat iedere zorgmedewerker zijn/haar medische verrichting conform de wet WGBO vastlegt in het eigen medische dossier van de cliënt, in principe op de dag van de vaccinatie. [12] De GGD registreert in een eigen systeem, namelijk CoronIT.

Verstrekken gegevens huisarts

De gegevens worden verwerkt om de AGB-code van een arts op te halen zodat de gegevens naar de juiste arts worden gestuurd. Daarna worden gegevens over de vaccinatie tegen COVID-19 gedeeld met de huisarts. Op deze wijze kan adequate zorg worden verleend indien iemand meer klachten krijgt of bijwerkingen krijgt van het vaccin. Daarnaast zijn deze zaken dan aangetekend in het dossier van de huisarts, zodat deze in het medisch dossier van de betrokkene zijn opgenomen, wat relevant kan zijn bij latere klachten of bijwerkingen en het traceren van de oorzaak daarvan.

[12] https://lci.rivm.nl/richtlijnen/covid-19-vaccinatie onder 10.5

Verstrekken gegevens RIVM

In opdracht van de minister van VWS is het Centrum Infectieziektebestrijding van het RIVM (RIVM-CIb) verantwoordelijk voor de regie van het COVID-19-vaccinatieprogramma. Daaronder valt de ontwikkeling van de richtlijn voor de uitvoering, het opzetten en de coördinatie van de communicatie over de COVID-19-vaccinatie naar professionals en de controle en evaluatie van het vaccinatieprogramma.

Vaccinatiegegevens zoals de vaccinatiegraad bieden de mogelijkheid om inzicht te krijgen in het verloop van de pandemie, waardoor VWS adequatere beslissingen kan nemen in de bestrijding van COVID-19. Voor dit doel worden anonieme gegevens verstrekt.

Centrale registratie van COVID-19-vaccinatie is van groot belang voor de individuele deelnemer, voor de uitvoering van het programma, voor de bewaking van de volksgezondheid en voor de monitoring van de effectiviteit en veiligheid. RIVM-DVP verzorgt de centrale registratie van de vaccinaties en de toegediende vaccins en controleert de gegeven vaccinaties op juistheid wat betreft gehanteerd interval, merk vaccin en expiratiedatum. Dat is belangrijk voor de veiligheid, voor onderzoek om te kijken of het vaccin goed werkt, en om te besluiten of er bij een voldoende hoge vaccinatiegraad maatregelen kunnen worden versoepeld. Ook kan de betrokkene bijvoorbeeld snel gewaarschuwd worden bij eventuele bijwerkingen.

Na vaccinatie krijgt de betrokkene een vaccinatiebewijs mee met informatie over het vaccin dat hij/zij gekregen heeft. Deze kunt u bij de tweede vaccinatie opnieuw gebruiken. Als de gegevens zijn doorgegeven aan het RIVM, dan kan de betrokkene later een kopie van uw vaccinatiebewijs bij het RIVM opvragen.

13. Noodzaak en evenredigheid

CoronIT

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 vaccinatieproces. Enkel het snel kunnen vaccineren 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.

De gegevens die worden verwerkt, zijn alle noodzakelijk voor de doeleinden waarvoor zij worden verwerkt. Zo zijn de contra-indicaties die worden gevraagd afkomstig uit de richtlijnen vanuit het RIVM.

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?’).

Proportionaliteit

De applicatie is opgebouwd om te zorgen dat er op een snelle en gecentraliseerde wijze kan worden gevaccineerd. 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.

CoronIT zorgt dat het hele proces gestroomlijnd wordt omdat heel duidelijk is gesteld welke persoonsgegevens per stap nodig zijn.

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 vaccinatieproces, 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.

Administratie is een essentieel onderdeel van de vaccinatie. Alleen bij een zorgvuldige registratie kunnen in het geval van een incident adequate maatregelen genomen worden.

Gegevensverstrekking huisarts

Voor een verwerking kan worden gestart, dient de noodzaak en evenredigheid te worden bepaald.

Noodzaak

Het is noodzakelijk dat een arts op de hoogte is van een vaccinatie tegen COVID-19 zodat de arts adequate zorg kan verlenen indien er sprake is van bijwerkingen. Aangezien deze gegevens onderdeel worden van het medisch dossier, kan ook op een later moment worden gekeken of later ontstane klachten of bijwerkingen het gevolg zijn van een besmetting en/of de vaccinatie. Het systeem dat daarvoor is opgezet, is hierbij beveiligd, efficiënt en verkleind de kans op fouten. Het raadplegen van de ION-database zorgt dat de gegevens naar de huisarts gaan waar de betrokkene is ingeschreven en het systeem zorgt voor het veilig versturen van de gegevens naar de huisarts.

Evenredigheid

Evenredigheid kan worden ingedeeld in proportionaliteit en subsidiariteit.

Proportionaliteit

De verwerking is proportioneel. He BSN wordt enkel gebruikt om te controleren of de gegevens naar de juiste huisarts gaan en om te zorgen dat de gegevens in het juiste dossier terechtkomen. Dit gebeurt automatisch, wat betekent dat minder mensen die gegevens inzien.

Subsidiair

De verwerking is subsidiair. Het gebruik van andere gegevens in de ION-database leidt tot een groter uitvalpercentage en dus medewerkers die de gegevens gaan verwerken, wat inzage en een grotere kans op fouten kan betekenen. Voor het uitwisselen van de gegevens met de huisarts is het BSN de enige manier om iemand met een uniek nummer te kunnen identificeren. In de zorg is dat erg belangrijk, gezien de impact die een foute registratie kan hebben. Daarom is gebruik van andere gegevens voor het bericht naar de huisarts niet aan te raden.

Gegevensverstrekking RIVM

Noodzaak

Het RIVM verwerkt de gegevens in het CIMS. Centrale registratie van COVID-19-vaccinatie is van groot belang voor de individuele deelnemer, voor de uitvoering van het programma, voor de bewaking van de volksgezondheid en voor de monitoring van de effectiviteit en veiligheid. RIVM-DVP verzorgt de centrale registratie van de vaccinaties en de toegediende vaccins en controleert de gegeven vaccinaties op juistheid wat betreft gehanteerd interval, merk vaccin en expiratiedatum. Dat is belangrijk voor de veiligheid, voor onderzoek om te kijken of het vaccin goed werkt, en om te besluiten of er bij een voldoende hoge vaccinatiegraad maatregelen kunnen worden versoepeld. Ook kan de betrokkene bijvoorbeeld snel gewaarschuwd worden bij eventuele bijwerkingen.

Centrale registratie van COVID-19-vaccinatie is van groot belang voor de individuele deelnemer, voor de uitvoering van het programma, voor de bewaking van de volksgezondheid en voor de monitoring van de effectiviteit en veiligheid. RIVM-DVP verzorgt de centrale registratie van de vaccinaties en de toegediende vaccins en controleert de gegeven vaccinaties op juistheid wat betreft gehanteerd interval, merk vaccin en expiratiedatum.

Voor onder meer bestrijding van de pandemie, evaluatie van het programma, onverwachte bijwerkingen of een recall is het belangrijk dat alle vaccinaties geregistreerd worden in CIMS. RIVM-DVP heeft de taak de toegediende vaccinaties vast te leggen in CIMS.

Proportionaliteit

Hiervoor worden niet meer gegevens verstrekt dan noodzakelijk. Dit zijn tevens de gegevens die genoemd worden in de Memorie van Toelichting op de Wpg.[13]

Subsidiariteit

De verwerking is subsidiair. Het RIVM heeft ervoor gekozen om het CIMS als centrale register te gebruiken, vanwege het gebrek aan capaciteit van het bestaande systeem Praeventis. Daarnaast kan bij het ontwerp van het CIMS de privacy by design en default worden meegenomen. De grondslag voor de verwerking is toestemming, waardoor er geen verplichting is om de gegevens te verstrekken. Hierdoor is het ook mogelijk voor de betrokkene om zich te laten vaccineren zonder dat de gegevens verstrekt worden. Er is dan ook bewust niet gekozen voor een wettelijke

[13] https://www.parlementairemonitor.nl/9353000/1/j9vvij5epmj1ey0/vk3zjuymwjzs

grondslag vanuit VWS. Dit om de betrokkene een keuze te geven en zo min mogelijk verplichtingen te stellen aan het al dan niet ontvangen van een vaccinatie.

Inzet landelijk callcenter
De persoonsgegevens die worden verwerkt zijn allen noodzakelijk voor het bereiken van verwerkingsdoeleinden. Het is niet mogelijk om de doelen te bereiken door gebruik van minder of gepseudonimiseerde gegevens. De gegevens die worden verzameld zijn of noodzakelijk voor het kunnen opnemen van contact met de Betrokkene, de verificatie van de identiteit van de Betrokkene en het aanvragen (of verzetten/annuleren) van een vaccinatie voor Betrokkene.

De inbreuk is derhalve proportioneel aan het doel, daar het doel is het faciliteren van het maken (of verzetten/annuleren) van vaccinatie afspraken.

De inbreuk op de persoonlijke levenssfeer door de inzet van het callcenter, is ook niet groter dan de inbreuk die gemaakt wordt bij gebruik regionale callcenters. Aanvullende risico's door inzet callcenter zijn in de DPIA van het callcenter opgenomen en er zijn maatregelen getroffen om deze risico's te beperken.

Er wordt nog gewerkt aan een is sinds het opstellen van de eerste concept DPIA ook nog een derde mogelijkheid voor het aanvragen van een test opgezet voor Betrokkenen, namelijk de aanmelding voor een testafspraak via een beveiligd online portal, met identificatie door gebruik van DigiD.

Inzet medisch callcenter
De persoonsgegevens die worden verwerkt zijn noodzakelijk voor het doel, namelijk medische ondersteuning bieden bij vragen over de gezondheidsverklaring en het invullen van de gezondheidsverklaring.

De inbreuk is proportioneel aan het doel. Alleen medisch geschoolde personen hebben toegang tot het dossier. Deze toegang hebben zij nodig om op te zoeken of er al een dossier is aangemaakt voor de persoon die belt en zo niet, om een dossier aan te maken en zo de gezondheidsverklaring in te vullen.

De inbreuk op de persoonlijke levenssfeer door de inzet van het callcenter is niet groter dan de inbreuk bij het invullen van de gezondheidsverklaring op de vaccinatielocatie. Door de inzet van het medisch callcenter wordt de vaccinatielocatie ontlast waardoor er een snellere doorstroom kan plaatsvinden. Dit is belangrijk gezien het volume mensen dat dagelijks gevaccineerd moet worden. Daarnaast kan er indien nodig overleg plaatsvinden met de behandelend arts, waarna de persoon wel of niet gevaccineerd kan worden. Dit is op de vaccinatielocatie niet mogelijk. Hierdoor wordt voorkomen dat personen naar de vaccinatielocatie komen die uiteindelijk niet gevaccineerd kunnen worden omdat er geen volledige medische beoordeling kan plaatsvinden. De inzet van het medisch callcenter is hierdoor niet alleen in het belang van de GGD' en, maar ook van de betrokkenen.

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.

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 vaccinatieproces in CoronIT persoonsgegevens worden verzameld, waarbij wordt gelinkt naar de privacyverklaring van de gegevensverzameling in CoronIT. Over de verstrekking van de gegevens aan het RIVM worden de betrokkene geïnformeerd in een brief die wordt toegevoegd aan de uitnodiging. Over de uitwisseling met de huisarts wordt de betrokkene telefonisch geïnformeerd.

Daarnaast is een privacyverklaring over de verwerking van gegevens 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 de gegevens in te zien. De gegevens kunnen worden opgevraagd bij de GGD waar de vaccinatie is uitgevoerd. Daar kan ook een afschrift worden verkregen. Het is nog niet mogelijk om elektronisch inzage te verkrijgen. Wanneer CoronIT een medisch dossier is, dan moet elektronische inzage wel mogelijk zijn. Het is de bedoeling om deze mogelijkheid op termijn te realiseren. Tot die tijd kan de betrokkene wel inzage krijgen in zijn/haar gegevens die in CoronIT worden verwerkt. Er kan een print gemaakt worden van deze gegevens en deze kan verstrekt worden aan de betrokkene. De betrokkene dient hiervoor een verzoek in te dienen bij de regionale GGD waar de vaccinatie is uitgevoerd.

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 vaccinatie is gezet.

Recht op gegevenswissing (art. 17 AVG)
Voor de vaccinatiegegevens geldt in principe een bewaartermijn van 20 jaar. Wel kan de betrokkene bij de locatie waar hij/zij gevaccineerd is een verzoek doen om zijn/haar persoonsgegevens eerder te verwijderen. In dat geval dient er een afweging te worden gemaakt of dit verzoek gefaciliteerd kan worden. Zo kan het verzoek bijvoorbeeld worden geweigerd als het verwijderen van gegevens een belemmering is voor goed hulpverlenerschap. Voor vaccinaties kan dit bijvoorbeeld het geval zijn wanneer er een verzoek wordt gedaan voor verwijdering van de persoonsgegevens tussen de eerste en tweede vaccinatie. Er wordt een richtlijn opgesteld hoe om te gaan met verwijderverzoeken ten aanzien van vaccinatiegegevens.

M.b.t. de gegevens die aan het RIVM zijn verstrekt, kan de betrokkene hiervoor een verzoek indienen bij het RIVM.

Voor de verstrekking aan de huisartsen geldt dat de betrokkene het verzoek bij de huisarts kan indienen.

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 overeenkomstig art. 22 AVG.

Recht op intrekken toestemming
Voor het verstrekken van de gegevens aan de huisarts en het RIVM wordt toestemming gevraagd. Wanneer de betrokkene zijn toestemming intrekt, dan heeft dat tot gevolg dat de gegevens van de betrokkene verwijderd moeten worden. Hiervoor kan de betrokkene een verzoek indienen bij de huisarts of het RIVM.

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.

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. *Maatregelen voor informatiebeveiliging zijn onvoldoende ingericht wat leidt tot datalekken, imagoschade en financiële schade in de vorm van opgelegde boetes/sancties en claims van betrokkenen.*

Het is voor de projectgroep onbekend of de back-ups van CoronIT alleen lokaal worden bewaard of (ook) op een externe locatie, of back-ups fysiek of digitaal worden opgeslagen, hoe lang de gemaakte back-ups worden bewaard en tot op welk detailniveau de back-ups te restoren zijn. Daarnaast is het onbekend wat de leverancier verstaat onder het periodiek uitvoeren van restoretesten of in de 2 datacenters de data realtime wordt gerepliceerd en welke beveiligingsmaatregelen hierbij zijn getroffen voor het borgen van de vertrouwelijkheid van gegevens in opslag en transport. Het tijdig of in zijn geheel niet meer beschikbaar hebben van persoonsgegevens is een datalek op basis van de bepalingen in de AVG. Daarnaast bestaat het risico op onrechtmatige verwerkingen.

- De kans dat het risico zich manifesteert zonder maatregelen is midden. In de verkregen documentatie staat beschreven dat er maatregelen getroffen zijn voor back-up en restore. Het is onbekend op welke wijze deze zijn getroffen en door de hoge tijdsdruk is het mogelijk dat een aspect als vertrouwelijkheid over het hoofd is gezien.
- De impact van het risico is hoog. Indien de maatregelen die getroffen zijn niet effectief zijn dan gaan gegevens verloren of worden deze te lang bewaard en dus onrechtmatig verwerkt.

Geadviseerd wordt om de volgende maatregelen te nemen:

- Zet in de technische documentatie op welke wijze back-up en restore wordt uitgevoerd en welke maatregelen voor beschikbaar, vertrouwelijkheid en integriteit van de gegevensverwerking in acht worden genomen (gegevens en opslag/transport).
- Stel dat Topicus zich moet houden aan de afspraken in de verwerkersovereenkomst met betrekking tot standaarden voor back-up en restore.

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

2. *Logging wordt niet automatisch gecontroleerd, wat leidt tot onrechtmatige verwerking*

Binnen CoronIT wordt toegang tot persoonsgegevens gelogd. De logging in CoronIT wordt op basis van handmatige logging gecontroleerd. Door de grote hoeveelheden loggegevens, kan met de handmatige controle niet alles worden gecontroleerd, waardoor niet alle gevallen van potentieel

onrechtmatige verwerking wordt gespot. Dit leidt tot onrechtmatige verwerking van persoonsgegevens en potentieel fraude.

- De kans dat het risico zich manifesteert is hoog. Er werken veel mensen in CoronIT. De kans dat iemand een onrechtmatige inzage heeft, en daar een patroon in bestaat, kan met handmatige controle niet snel worden gevonden.
- De impact is hoog. Indien onrechtmatige verwerkingen niet worden gevonden en sprake is van fraude, heeft dit grote gevolgen voor de betrokkene.

Geadviseerd wordt om de volgende maatregelen te nemen:

- Richt de geplande SIEM-oplossing in met regels die fraude kunnen opsporen.

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

Restrisico: Zelf bij automatische controle van de logging, zijn er medewerkers die een patroon van onrechtmatige inzage kunnen hebben dat moeilijk als fraude te kwalificeren is. Deze gevallen zijn nooit uit te sluiten en zijn moeilijk te vinden, zelfs met strikt gespecificeerde regels.

3. *Het systeem is voor vaccinaties niet getest op kwetsbaarheden en bij nieuwe ontwikkelingen is nog niet gesteld dat wordt getest, wat kan leiden tot onrechtmatige toegang tot en gebruik van de persoonsgegevens.*

CoronIT is voor het stuk testen uitgebreid getest door Fox-IT. kwetsbaarheden die daarin naar voren zijn gekomen zijn meegenomen in de nieuwe releases om deze op te lossen. Vaccinaties werkt grotendeels hetzelfde, maar een ontwikkeling in een systeem kan toch leiden tot achterdeurtjes waarbij hackers of andere kwaadwillenden persoonsgegevens uit het systeem kunnen halen. Dit leidt tot onrechtmatige verwerking van persoonsgegevens en fraude.

- De kans dat het risico zich manifesteert is midden. Het systeem is al uitgebreid getest en vaccinaties betreft een kleine wijziging in CoronIT. De kans dat hierbij een kwetsbaarheid is ontstaan, is klein.
- De impact is hoog. Indien persoonsgegevens van een betrokkene uitlekken of onrechtmatig worden gebruikt, heeft dit gevolgen voor de betrokkene, namelijk dat zijn/haar gegevens kunnen worden misbruikt.

Geadviseerd wordt om de volgende maatregelen te nemen:

- Laat een security assessment en test op kwetsbaarheden uitvoeren, zodat alle nieuwe delen van CoronIT worden doorgelicht en zo alle kwetsbaarheden duidelijk zijn.
- Wanneer er nieuwe koppelingen of (grote) ontwikkelingen worden gerealiseerd in CoronIT, dient er een security assessment te worden uitgevoerd.

- Voer een hertest uit als de kwetsbaarheden zijn opgelost, zodat kan worden onderzocht of de risico's nog bestaan.

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

4. *Overeenkomsten met leveranciers zijn niet opnieuw beoordeeld op de verwerking met betrekking tot vaccinatiegegevens, waardoor persoonsgegevens onrechtmatig kunnen worden verwerkt.*

De gegevens met betrekking tot vaccinaties moeten worden bijgevoegd bij de bestaande overeenkomsten. Voor sommige leveranciers is dit ook een moment om de overeenkomsten die onder tijdsdruk zijn afgesloten, opnieuw te onderhandelen. Als vaccinaties niet wordt meegenomen als verwerking, zijn hier formeel geen afspraken over gemaakt, wat kan leiden tot onrechtmatige verwerkingen.

- De kans is middel. Er zijn reeds afspraken gemaakt over de verwerkingen in CoronIT. Daarbij kan worden gesteld dat die afspraken ook gelden voor de nieuwe verwerkingen.
- De impact is middel. De leveranciers zijn gebonden aan standaarden. De persoonsgegevens zullen voor de nieuwe verwerkingen in opdracht van GGD GHOR Nederland worden verwerkt volgens instructies van GGD GHOR Nederland.

Geadviseerd wordt om de volgende maatregelen te nemen:

- Vul de huidige overeenkomsten aan en update de overeenkomsten indien nodig.

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

5. *Volledige technische informatie is niet beschikbaar, waardoor niet kan worden gecontroleerd hoe de datastromen lopen, wat leidt tot onrechtmatige verwerkingen.*

Processen om de vaccinatiegegevens te verwerken en te communiceren (gehele keten) zijn niet eenduidig gedefinieerd en zijn onderhavig aan wijzigingen, wat leidt tot datalekken, imagoschade en financiële schade in de vorm van opgelegde boetes/sancties en kosten voor herstelwerkzaamheden.

- De kans is midden. Er mist echter een overzicht van zowel de datastromen (in de vorm van procesplaten) waardoor niet direct kan worden overzien wat exact waar naartoe gaat. Daarnaast zijn er vaak wijzigingen in de processen, waardoor het overzicht op de datastromen kan worden verloren.

- De impact is hoog. Indien de persoonsgegevens onrechtmatig worden verwerkt, kunnen deze worden gebruikt om te frauderen of komen deze op straat te liggen.

Geadviseerd wordt om de volgende maatregelen te nemen:

- Stel procesplaten op die de datastromen weergeven.
- Houdt de procesplaten up-to-date en informeer het privacy- en informatiebeveiligingsteam over wijzigingen.

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

6. *Rechten van betrokkenen zijn onvoldoende ingericht en procedures zijn onvoldoende helder, wat leidt tot niet-naleving van de in de AVG en andere wetgeving gestelde plichten richting de betrokkene.*

CoronIT is een medisch dossier. Daarom moet de mogelijkheid om elektronische inzage te verkrijgen wettelijk gezien worden ingericht. Op dit moment is er voor de betrokkene geen mogelijkheid om elektronisch inzage te krijgen in het dossier.

Daarnaast zijn er nog geen duidelijke werkinstructies over de wijze waarop de rechten van betrokkenen worden uitgevoerd. Vaccinaties zijn de verantwoordelijkheid van de GGD. De GGD'en dienen zelf procedures ingericht te hebben t.a.v. de uitvoering van de rechten van betrokkenen. In de gevallen waar GGD GHOR Nederland ondersteuning moet bieden, moet worden afgesproken hoe dit zal worden uitgevoerd.

Dit leidt tot financiële schade in de vorm van boetes/sancties, imagoschade en het niet voldoen aan de plicht tot informatie.

- De kans is hoog. Het is een gegeven dat elektronische inzage niet mogelijk is, hierdoor wordt direct niet voldaan aan het recht om een medisch dossier elektronisch in te zien. Daarnaast zullen betrokkenen ook andere rechten uit willen oefenen, waarbij de GGD’en allemaal anders handelen en verzoeken op een juiste wijze moeten worden doorgeleid.
- De impact is midden. Elektronische inzage is niet mogelijk, maar een betrokkene kan wel inzage krijgen in zijn/haar persoonsgegevens. Bijvoorbeeld door middel van prints uit CoronIT. De rechten van betrokkenen zullen wel gefaciliteerd worden, maar mogelijk zal de reactietermijn moeten worden verlengd.

Geadviseerd wordt om de volgende maatregelen te nemen:

- Verschaf inzage door prints te maken van de gegevens die geregistreerd worden in CoronIT. Dit geldt tot de tijd dat een optie tot elektronische inzage is gerealiseerd.
- Realiseer een oplossing waarmee elektronische inzage mogelijk is.

- Bepaal de uitvoering van rechten van betrokkenen in het convenant CoronIT als dit wordt aangepast voor vaccinaties.
- Sluit een convenant met het RIVM wanneer er gegevens verstrekt worden aan het RIVM. Hierin moeten afspraken worden opgenomen over het intrekken van toestemming voor deze verstrekking.
- Verstrek algemene richtlijnen over de uitvoering van rechten van betrokkenen.

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

7. *Er is geen scheiding tussen test- en vaccinatiegegevens, waardoor medewerkers onrechtmatig medische gegevens (testgegevens) in kunnen zien.*

Er wordt voor iedere betrokkene een dossier aangemaakt, waarin zowel test- als vaccinatiegegevens zijn opgenomen. Dit is nodig om dubbele dossiervorming te voorkomen. Medewerkers die met testgegevens werken, horen echter geen vaccinatiegegevens in te zien en omgekeerd. Indien dat wel het geval is, is sprake van onrechtmatige inzage.

- De kans is hoog. Indien de omgeving openstaat, kunnen medewerkers heel makkelijk in het volledige dossier en dus de persoonsgegevens inzien.
- Impact is midden. De medewerkers zijn gehouden aan geheimhouding en werkinstructies. Toch kunnen zij persoonsgegevens inzien en deze vervolgens lekken en/of misbruiken.

Geadviseerd wordt om de volgende maatregelen te nemen:

- Beoordeel in hoeverre de dossiers afgescheiden kunnen en moeten worden. Draag zorg voor afgescheiden dossiers. Indien alle of delen van de persoonsgegevens van beide onderdelen (testen en vaccinaties) moeten worden ingezien, dient hier een verantwoording voor te worden opgesteld.

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

8. *Toegang tot persoonsgegevens is geregeld via een autorisatiematrix, echter zijn partijen niet voldoende zorgvuldig in de toekenning daarvan.*

In CoronIT worden veel gegevens verwerkt en veel medewerkers met verschillende rollen hebben toegang tot (delen van) deze gegevens. De rollen moeten duidelijk zijn en wanneer bepaalde personen geen toegang nodig hebben tot bepaalde gegevens voor de uitvoering van de werkzaamheden, moet toegang tot deze gegevens worden afgeschermd. Daarnaast lijkt de in- en uitstroom van medewerkers bij de GGD'en en verwerkers erg hoog te zijn, waardoor medewerkers wel worden aangemeld, maar niet direct worden afgemeld, waardoor ze toegang behouden tot de (medische) gegevens in CoronIT. Toegang tot persoonsgegevens lijkt onvoldoende te zijn geregeld,

waardoor onbevoegden gegevens in kunnen zien. Dit leidt tot imagoschade, negatieve publiciteit en financiële schade in de vorm van boetes/sancties.

- De kans is hoog. De autorisaties zijn in beeld gebracht en technisch doorgevoerd. Gezien de omvang en aard van de verwerking en de snelheid waarin het proces wijzigt kan er een fout in de autorisatie treden. Dit geldt vooral voor een verkeerde aanvraag en voor het afmelden van medewerkers en dus het intrekken van de autorisaties, gezien hier sprake is van veel druk op het proces en het aanmelden van medewerkers meer prioriteit heeft dan het afmelden van deze medewerkers. Daarnaast worden rollen vaak breed toegekend, zodat medewerkers snel van taken kunnen wisselen.
- De impact is hoog. Wanneer er onbevoegd toegang wordt verkregen, dan wordt dit gezien als een datalek. Indien er niet voldoende technische en organisatorische maatregelen worden genomen om dit voorkomen, dan kan dit resulteren in een boete en zware imagoschade.

Geadviseerd wordt om de volgende maatregelen te nemen:

- Meldt GGD'en dat zij zorgvuldig moeten zijn in de toekenning van rollen aan personeel en het intrekken daarvan. GGD'en hebben echter de verantwoordelijkheid te zorgen voor de juiste interne procedures en de capaciteit om te zorgen dat autorisaties op tijd en juist worden aangevraagd en op tijd worden ingetrokken.
- Laat medewerkers geheimhoudingsverklaringen tekenen en train ze voldoende en periodiek, zodat zij weten wat zij wel en niet mogen doen met de persoonsgegevens en, indien zij zich hier niet aan houden, sancties kunnen worden getroffen.

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

Restrisico: De GGD'en hebben beperkt capaciteit voor het toekennen van rollen. Hierdoor blijft de kans bestaan dat niet wordt gecontroleerd of iemand inderdaad een bepaalde rol moet hebben en worden de autorisaties niet tijdig ingetrokken.

9. *Persoonsgegevens in CoronIT dienen enkel inzichtelijk te zijn per regio zodat de GGD van die regio kan werken met de vaccinatiegegevens. Indien dit niet gebeurt, worden gegevens onrechtmatig ingezien.*

CoronIT is voor het deel van vaccinaties een medisch dossier. Dit betekent dat een andere zorgverlener geen toegang mag hebben tot dit medisch dossier zonder toestemming van de betrokkene. Iedere GGD kan worden gezien als afzonderlijke zorgverlener. In dat geval mag GGD A niet de gegevens van betrokkene inzien die gevaccineerd zijn in de regio van GGD B.

- De kans is hoog. Wanneer CoronIT wordt gezien als een medisch dossier, dan is deze inzage onrechtmatig.
- De impact is hoog. Wanneer er onbevoegd toegang wordt verkregen, dan wordt dit gezien als een onrechtmatige inzage. Indien er niet voldoende technische en organisatorische maatregelen worden genomen om dit voorkomen, dan kan dit resulteren in een boete en zware imagoschade.

Geadviseerd wordt om de volgende maatregelen te nemen:

- Weeg af of scheiding tussen de regio's noodzakelijk is. Zo niet, motiveer dit.
- Voor de uitvoering van vaccinaties is het niet noodzakelijk dat regio's onderling inzage hebben in de gegevens van de betrokkene. Een positieve testuitslag is een contra-indicatie voor het krijgen van een vaccinatie, maar dit gegeven wordt bij de betrokkene zelf uitgevraagd. Hierdoor kunnen de dossiers van de regio's niet worden afgescheiden. In de toekomst kan worden gekeken naar een 'breaking glass' oplossing.
- De eerste prik kan op een andere locatie worden gezet dan de tweede prik. Hierdoor moeten de dossiers inzichtelijk zijn voor de afzonderlijke locaties. Mogelijk kan hiervoor gebruik worden gemaakt van een 'breaking glass'.
- Er dient na te worden nagegaan of toegang tot de gegevens in de regio noodzakelijk is voor de melding die de GGD' en moeten doen op grond van artikel 28 Wpg. Hiervoor moet de vaccinatiestatus worden doorgegeven. Wanneer een betrokkene in de ene regio wordt getest en in de andere regio is gevaccineerd, dan moeten deze gegevens beide inzichtelijk zijn om de status door te kunnen geven aan het RIVM.

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

Restrisico: Het is de vraag of de GGD' en moeten worden gezien als afzonderlijke zorgverleners in deze situatie. Zolang er geen 'breaking glass' wordt ingesteld, hebben GGD'en in feite onrechtmatig toegang tot alle dossiers wanneer iedere GGD als afzonderlijke zorgverlener moet worden gezien. Wel is het noodzakelijk om de regio's toegang te houden, voor de werkbaarheid van de processen.

10. *Rechtmatigheid van de verstrekking van vaccinatiegegevens aan het RIVM is in het gedrang, wat leidt tot een onrechtmatige verstrekking van persoonsgegevens.*

De grondslag voor het verstrekken van gegevens aan het RIVM is toestemming zoals bedoeld in art. 6 lid 1 sub a jo art. 9 lid 1 sub a AVG. Aan deze toestemming zijn strenge voorwaarden gesteld. Aan deze voorwaarden kan mogelijk niet volledig worden voldaan. Daarnaast dient er een andere grondslag te zijn voor het verstrekken van het BSN, omdat toestemming geen grondslag kan bieden voor het verstrekken van het BSN.

De rechtmatigheid van de verwerking is in het gedrang omdat grondslagen (nog) niet zijn vastgelegd. Dit leidt tot een onrechtmatige verwerking en daarmee zware imagoschade en financiële schade in de vorm van boetes/sancties.

- De kans is hoog. Het is een proces dat in de schijnwerpers staat. Naar aanleiding van de pers of kamervragen kunnen er vragen gesteld worden over de rechtmatigheid van de verstrekking van deze gegevens. Ook kan er een verzoek tot handhaving worden ingediend bij de Autoriteit Persoonsgegevens, waardoor de Autoriteit Persoonsgegevens gedwongen kan worden om een onderzoek in te stellen. De Autoriteit Persoonsgegevens heeft ook ambtshalve de bevoegdheid om een onderzoek in te stellen.
- De impact is hoog. Het gaat om de verstrekking van een grote omvang persoonsgegevens met een bijzondere aard. Wanneer niet volledig wordt voldaan aan de vereisten van toestemming, dan bestaat de kans dat achteraf geoordeeld wordt dat de gegevens onrechtmatig zijn verstrekt. Dit kan leiden tot een boete, imagoschade en een vermindering van de vaccinatiebereidheid.

Geadviseerd wordt om de volgende maatregelen te nemen:

- Stel een informatiebrief op waarin de betrokkene zo goed mogelijk geïnformeerd wordt over de verwerking van zijn/haar persoonsgegevens.
- Neem kwaliteitsmaatregelen om ervoor te zorgen dat de mondelinge toestemming op een juiste wijze verkregen wordt en kan worden aangetoond, zodat de rechtmatigheid van de verwerking vastligt.
- Leg de grondslag voor het verstrekken van de gegevens aan het CIMS aan de Autoriteit Persoonsgegevens.
- Maak een goede technische inrichting voor het waarborgen van het vereisten dat de toestemming aantoonbaar moet zijn.
- Er is een wijzigingsbesluit waarmee Covid-19 vaccinatie wordt toegevoegd aan het RVP. In dat geval biedt dit de grondslag voor de uitwisseling van het BSN. Dit besluit is nog niet gepubliceerd en in werking.
- Er wordt geadviseerd om de toestemmingsvraag op te nemen in de IVR en deze te koppelen met CoronIT, waardoor de betrokkene actief toestemming geeft en deze toestemming ook wordt vastgelegd en gelinkt aan het telefoonnummer/dossier in CoronIT.

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

Restrisico: achteraf kan worden geconcludeerd dat informatiebrief niet voldoende aan de eisen hiervoor voldoet. Daarnaast zijn er op dit moment zijn er nog onvoldoende kwaliteitsmaatregelen genomen. Daarnaast is het besluit op grond waarvan het BSN verstrekt kan worden nog niet in werking.

11. *Grondslag voor verstrekking van data aan huisartsen is onduidelijk, waardoor persoonsgegevens onrechtmatig worden gedeeld.*

Er worden gegevens verstrekt aan de huisarts, indien de betrokkene daarvoor toestemming verleent. Het BSN mag niet verwerkt worden op grond van toestemming. Het BSN mag wel gebruikt worden in het kader van de communicatie tussen zorgverleners. In dit geval wordt het BSN echter gebruikt om de ION database te raadplegen, waarvoor geen duidelijke grondslag is. Rechtmatigheid voor het raadplegen van de ION database door middel van het BSN is onduidelijk. Daarnaast kunnen de gegevens van betrokkenen die geen BSN hebben, niet worden verstrekt aan de huisarts.

- De kans is midden. De betrokkenen wordt geïnformeerd over het feit dat de ION database wordt geraadpleegd met BSN om na te gaan wie de huisarts is. Daarnaast geeft de betrokkene toestemming voor het verstrekken van de gegevens. De noodzakelijkheid is ook te motiveren. De kans is midden dat dit als een onrechtmatige verwerking wordt gezien.
- De impact is midden. De gegevens worden alleen verstrekt wanneer toestemming is verleend. Het BSN mag gebruikt worden als dit noodzakelijk is voor het verlenen van goede zorg. Hieruit blijkt niet de grondslag voor het raadplegen van de ION database door middel van het BSN, echter voor het verlenen van de goede zorg (waarmee de betrokkenen instemt) is het noodzakelijk om de ION database te raadplegen. Dit kan alleen door middel van het gebruik van het BSN.

Geadviseerd wordt om de volgende maatregelen te nemen:

- Duidelijke informatie dient beschikbaar te worden gemaakt aan de betrokkene, zodat deze weet waar de toestemming voor wordt gegeven en hoe wordt gezorgd dat de gegevens aan de huisarts worden verstrekt zodat adequate zorg kan worden geleverd aan de betrokkene.
- Het raadplegen van de ION-database dient adequaat te worden gemotiveerd, zodat de noodzaak voor het verlenen van zorg duidelijk is. Dit kan door het opstellen van een memo in samenwerking met Stichting ION.
- Met de huisartsen dienen heldere afspraken te worden gemaakt over de verstrekking van de gegevens aan de huisartsen. De vorm waarin deze afspraken worden gemaakt moet worden bepaald.

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

12. *Bij weigering van een vaccinatie wordt een dossier aangemaakt omdat dit een weigering van een behandeling is. Dit leidt tot bovenmatige verwerking van persoonsgegevens.*

Het is nodig om ook de mensen waarvoor geen afspraak wordt ingepland omdat zij niet door de eerste fase van vragen komen (de contra indicaties), te registreren. Dit omdat je een medische handeling ontzegt en je later moet kunnen bekijken waarom deze ontzegd is wanneer iemand daartegen bezwaar maakt. Dit betekent dat voor iedereen die belt een dossier aangemaakt wordt, ongeacht of zij een vaccinatie ontvangen. Echter, de AVG kent een beginsel van dataminimalisatie wat inhoudt dat je alleen gegevens mag verwerken die noodzakelijk zijn voor het doel. Dit zijn twee vereisten die op gespannen voet staan.

- Kans is midden: Werkinstructies waren in het begin van het proces zo ingericht dat er altijd een dossier wordt aangemaakt.
- Impact is hoog: Wanneer een dossier onnodig wordt aangemaakt worden de gegevens van betrokkene 20 jaar bewaard. Zo kunnen er gegevens van betrokkene die niet bij de GGD gevaccineerd zijn, wel twintig jaar bewaard worden. Wanneer blijkt dat er onnodig dossiers worden aangemaakt, dan is er daarnaast sprake van een bovenmatige verwerking.

Geadviseerd wordt om de volgende maatregelen te nemen:

- Enkel wanneer er geen afspraak wordt ingepland omdat er sprake is van een contra-indicatie dient er een dossier worden aangemaakt. Wanneer iemand geen uitnodiging heeft, nog niet tot de doelgroep behoort of wanneer er geen vaccins meer voorradig zijn is dit niet noodzakelijk.
- Het onderscheid wanneer er wel of geen dossier moet worden aangemaakt, moet duidelijk zijn opgenomen in de instructies voor het callcenter.

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

13. Gebrek aan duidelijke en organisatorische maatregelen, leidt tot onrechtmatige verwerking.

De betrokkene wordt gevraagd een medische verklaring in te vullen en mee te nemen. Deze wordt op de vaccinatielocatie overgenomen in CoronIT. Daarbij bestaat een risico op dubbele registraties of dat formulieren rondslingeren. Dubbele registraties gaan tegen dataminimalisatie in, terwijl rondslingerende formulieren tot datalekken en verlies van vertrouwelijkheid van gegevens kan leiden. Het gebrek aan duidelijke organisatorische maatregelen leidt tot onrechtmatige verwerking, datalekken en financiële schade in de vorm van boetes/sancties.

Daarnaast missen in de snelheid van het proces nog een aantal procedures, zoals het terugkoppelen van een probleem met een batch vaccinaties. Indien deze procedures niet zijn vastgesteld en gecommuniceerd, leidt dit tot onrechtmatige verwerking.

- Kans is midden. De papieren worden vernietigd waardoor de kans klein is dat de formulieren gaan rondslingeren.
- Impact is hoog. Op de gezondheidsverklaring staan medische gegevens en het kan zijn dat deze gegevens herleidbaar zijn. Wanneer de verklaringen niet vernietigd worden, is er een kans dat de papieren rond gaan slingeren wat kan worden gezien als een datalek.

Geadviseerd wordt om de volgende maatregelen te nemen:

- Zet een procedure op waarin wordt opgenomen dat wanneer de verklaring is overgenomen in CoronIT, de papieren versie kan worden vernietigd. Vernietiging wordt aangeraden te laten verlopen via speciale containers die door een gespecialiseerd bedrijf worden afgevoerd. Indien dit niet mogelijk is om dit snel te regelen, wordt aangeraden een papierversnipperaar te gebruiken en te zorgen dat de documenten niet meer aan elkaar kunnen worden geplakt.
- Op elke locatie is een papierversnipperaar aanwezig. In het landelijke draaiboek wordt de instructie gegeven dat de gezondheidsverklaringen in de papierversnipperaar moeten na overname in CoronIT.

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

Restrisico: Er blijft een risico dat een gezondheidsverklaring niet wordt vernietigd, ondanks de instructies.

14. *Versturen van een afspraakbevestiging is niet altijd mogelijk omdat niet iedereen over een e-mailadres beschikt. In de afspraakbevestiging is informatie opgenomen, die de betrokkene in dat geval niet ontvangt en dus niet wordt voldaan aan de informatieplicht.*

Indien iemand geen e-mailadres heeft, ontvangt hij geen afspraakbevestiging met daarin informatie over het vaccin dat ze krijgen.

- Kans is middel: de meeste betrokkene zullen in het bezit zijn van een e-mailadres
- Impact is middel: telefonisch kan worden aangegeven welk vaccin de betrokkene ontvangt.

Geadviseerd wordt om de volgende maatregelen te nemen:

- Zet een procedure op waarin wordt opgenomen hoe een betrokkene geïnformeerd wordt in het geval hij/zij de afspraakbevestiging met daarin bepaalde informatie niet kan ontvangen. Te denken valt aan een script voor callcenter-medewerkers waarin zij de betrokkene verwijzen naar een website bijvoorbeeld.

Risico voor Betrokkene (voor maatregelen)	Middel

Risico voor Betrokkene (na maatregelen)	Laag

15. *Informatie voor gegevensverstrekking aan huisartsen wordt niet in alle gevallen verstrekt omdat callcentermedewerkers dit niet altijd juist uitvragen, wat leidt tot verstrekken van gegevens zonder dat de betrokkene juist is geïnformeerd.*

Wanneer er toestemming wordt gevraagd voor de informatieverstrekking aan huisartsen, dan moet de betrokkene op een juiste wijze en voldoende specifiek geïnformeerd worden over de verwerking. Op dit moment wordt deze informatie telefonisch bij het maken van de afspraak verstrekt en achteraf in de privacyverklaring. Er bestaat echter een kans dat de informatie niet op een goede wijze verstrekt wordt aan de telefoon.

- Kans is middel: Er is een callscript waarin de informatieverstrekking is opgenomen, maar callcenter-medewerkers zouden hiervan af kunnen wijken.
- Impact is hoog: Toestemming is niet op een geldige manier verkregen, waardoor er sprake is van een onrechtmatige verwerking.

Geadviseerd wordt om de volgende maatregelen te nemen:

- De informatie die aan de telefoon verstrekt wordt, moet worden opgenomen in de uitnodiging die de betrokkene ontvangt voor het maken van een afspraak.

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

16. *Bij het inplannen van een afspraak voor een derde wordt niet altijd toestemming gevraagd aan de derde. Dit leidt tot onrechtmatig ingeven van persoonsgegevens.*

Gezien het feit dat de GGD' en ook oudere vaccineert wordt er regelmatig gebeld door een kind of mantelzorger van deze oudere om een afspraak te maken. In dat geval is het niet wenselijk om toestemming te vragen aan de betrokkene, omdat die niet altijd aanwezig is. Dit is ook niet wenselijk wanneer de betrokkene bijvoorbeeld beginnend dementerend is. Hierdoor wordt er in deze gevallen geen toestemming gevraagd aan de oudere voor het plannen van een afspraak door een derde. Wanneer de derde contact opneemt met het medisch callcenter kan er niet aan de betrokkene om toestemming worden gevraagd om met de behandelend arts te overleggen.

- Kans is hoog: Veel oudere van 80 plus zijn niet in staat zelf een afspraak in te plannen.
- Risico is middel: het risico bestaat dat zonder toestemming/medeweten een afspraak wordt ingepland voor de oudere. Echter, de oudere moet daarna nog verschijnen op de vaccinatielocatie. Wanneer de oudere daar verschijnt kan daaruit worden afgeleid dat hij/zij akkoord gaat met de vaccinatie en dus met de verwerking van de persoonsgegevens.

Geadviseerd wordt om de volgende maatregelen te nemen:

- Wanneer een derde belt om een afspraak te maken, moet deze derde zelf de gegevens van de oudere kunnen verstrekken inclusief BSN.
- Wanneer de ouder verschijnt op de vaccinatielocatie moet de identiteit zorgvuldig worden vastgesteld.
- Wanneer de ouder niet verschijnt op de vaccinatielocatie, moeten de gegevens alsnog verwijderd worden uit CoronIT.
- Wanneer het medisch callcenter wordt benaderd door een derde, dan moeten zij bij overleg met de behandelend arts wel toestemming vragen aan de betrokkene. Deze toestemming is niet geldig wanneer deze door een derde is gegeven.

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

Restrisico: De kans op verwerking van persoonsgegevens zonder toestemming of medeweten van de betrokkene blijft bestaan. Echter, het vragen van toestemming roept veel verontwaardiging en onrust op in de maatschappij.

D. Beschrijving voorgenomen maatregelen

1. Wijze backup en restore verantwoorden

In de technische documentatie dient verantwoord te worden op welke wijze back-up en restore wordt uitgevoerd.

2. Logging conform Privacy by Design

De logging dient conform Privacy by Design te worden ingericht (logging bevat geen live gegevens) en opgeslagen te worden met in acht name van maatregelen voor vertrouwelijkheid. Met de GGD'en moet worden vastgelegd wie de loggingcontrole uitvoert. De SIEM-oplossing biedt hier uitkomst.

3. Uitvoering pentest

De nieuwe ontwikkelingen in CoronIT moeten worden getest om te controleren of er geen achterdeur is gecreëerd in CoronIT. Indien kwetsbaarheden worden gevonden, moet een schema worden opgesteld voor het oplossen van deze kwetsbaarheden.

4. Wijzigingen testen

Wijzigingen in het systeem moeten, zeker als dit grote wijzigingen betreft, worden getest door Topicus en GGD GHOR Nederland.

5. Heronderhandelen verwerkersovereenkomst

De verwerkersovereenkomst met Topicus moet heronderhandeld worden naar de standaard van GGD GHOR. Daarnaast moet worden gecontroleerd met welke partijen nog meer nieuwe afspraken moeten worden gemaakt.

6. Updaten technische documentatie

Technische documentatie updaten, in kaart brengen welke koppelingen van toepassing zijn, risico inschatting per koppeling in kaart brengen.

7. Inzage door prints

Tot de mogelijkheid er is om inzage elektronisch te verkrijgen, kan er inzage verschaft worden door prints te maken van de gegevens die geregistreerd worden in CoronIT. Dit neemt echter niet weg dat er niet wordt voldaan aan het direct inzage verschaffen in een medisch dossier.

8. Convenant tussen GGD GHOR en GGD'en

Er worden convenanten gesloten tussen GGD GHOR Nederland en de GGD'en waarbij afspraken gemaakt worden over de gevallen waar GGD GHOR Nederland ondersteuning biedt.

9. Regio's onderling inzage

Voor de uitvoering van vaccinaties is het noodzakelijk dat regio's onderling inzage hebben in de gegevens van de betrokkene. Dit omdat een betrokkene zich kan laten vaccineren. Beoordelen of breaking-the-glass moet worden ingeschakeld.

10. Afspraken met huisartsen verstrekking van gegevens

Met de huisartsen dienen heldere afspraken te worden gemaakt over de verstrekking van de gegevens aan de huisartsen. De vorm waarin deze afspraken worden gemaakt moet worden bepaald. Hiervoor zijn gebruiksvoorwaarden opgesteld, maar het portaal is nog niet in gebruik.

16. Maatregelen

Om de risico's zoals in dit document omschreven te beperken zijn verschillende maatregelen getroffen. Voor maatregelen die genomen zijn t.a.v. CoronIT en het callcenter wordt verwezen naar de DPIA's die reeds zijn opgesteld voor CoronIT en het Callcenter.

1. Professor ingeschakeld voor toelichting

Er wordt op dit moment gekeken naar de mogelijkheden om duidelijkheid te krijgen over de grondslag, zodat de bewaartermijn en de mogelijkheden tot verzoeken tot verwijdering kunnen worden bepaald. Er is een professor ingeschakeld die gespecialiseerd is in het gezondheidsrecht om hier oordeel over te geven.

2. Autorisatiematrix

Er wordt gebruik gemaakt van een autorisatiematrix waarin de rollen worden toegekend. Op basis van deze matrix worden de rollen technisch toebedeeld.

3. Convenant gesloten met het RIVM

Er wordt een convenant gesloten met het RIVM wanneer er gegevens verstrekt worden aan het RIVM.

4. Informatiebrief voor betrokkene

Stel een informatiebrief op waarin de betrokkene zo goed mogelijk geïnformeerd wordt over de verwerking van zijn/haar persoonsgegeven.

5. Procedure voor vernietiging papieren versie

Er dient een procedure te worden opgezet waarin wordt ogenomen dat wanneer de verklaring is overgenomen in CoronIT, de papieren versie kan worden vernietigd.

6. Aanmaken dossiers

Werkinstructies zijn aangepast zodat er enkel dossiers worden aangemaakt wanneer de vaccinatie vanwege medische redenen wordt ontzegd.

7. Organisatorische beveiligingsmaatregelen

Er zijn verwerkersovereenkomsten gesloten met de verwerkers waarin afspraken zijn gemaakt over hoe er moet worden omgegaan met de persoonsgegevens. Daarnaast zijn er geheimhoudingsverklaringen gesloten met medewerkers en is er een gedragscode verstrekt aan de medewerkers. Middels trainingen worden medewerkers er telkens op gewezen wat wel en niet is toegestaan ten aanzien van de verwerking van persoonsgegevens. Tot slot worden medewerkers gewezen op de gevolgen van het onrechtmatig openen van dossiers.

8. Richtlijnen met betrekking tot verzoeken met betrekking tot rechten van betrokkenen zijn opgesteld.

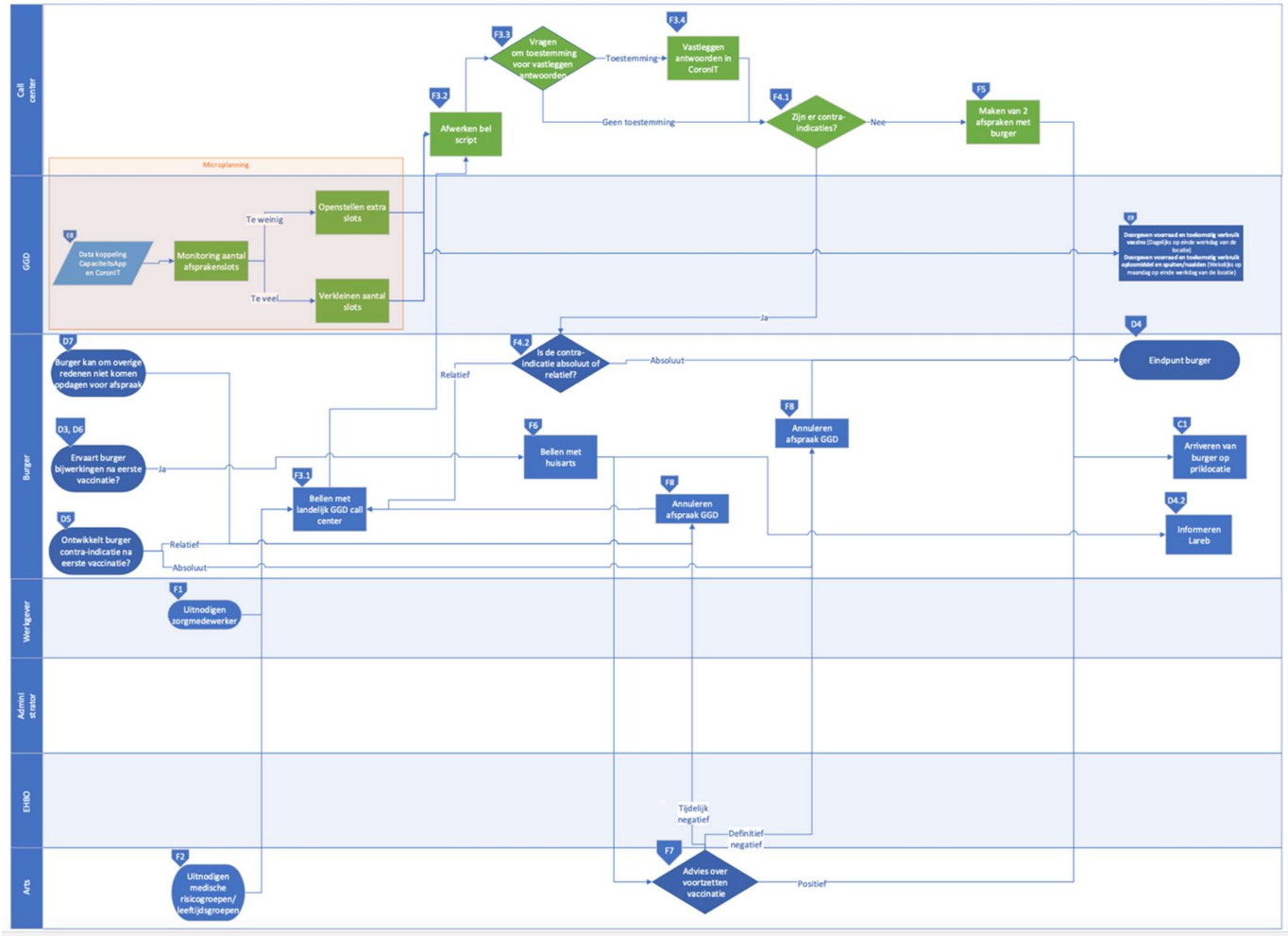
Richtlijnen voor inzage en verwijdering zijn opgesteld, zodat GGD'en deze kunnen nagaan bij deze verzoeken.

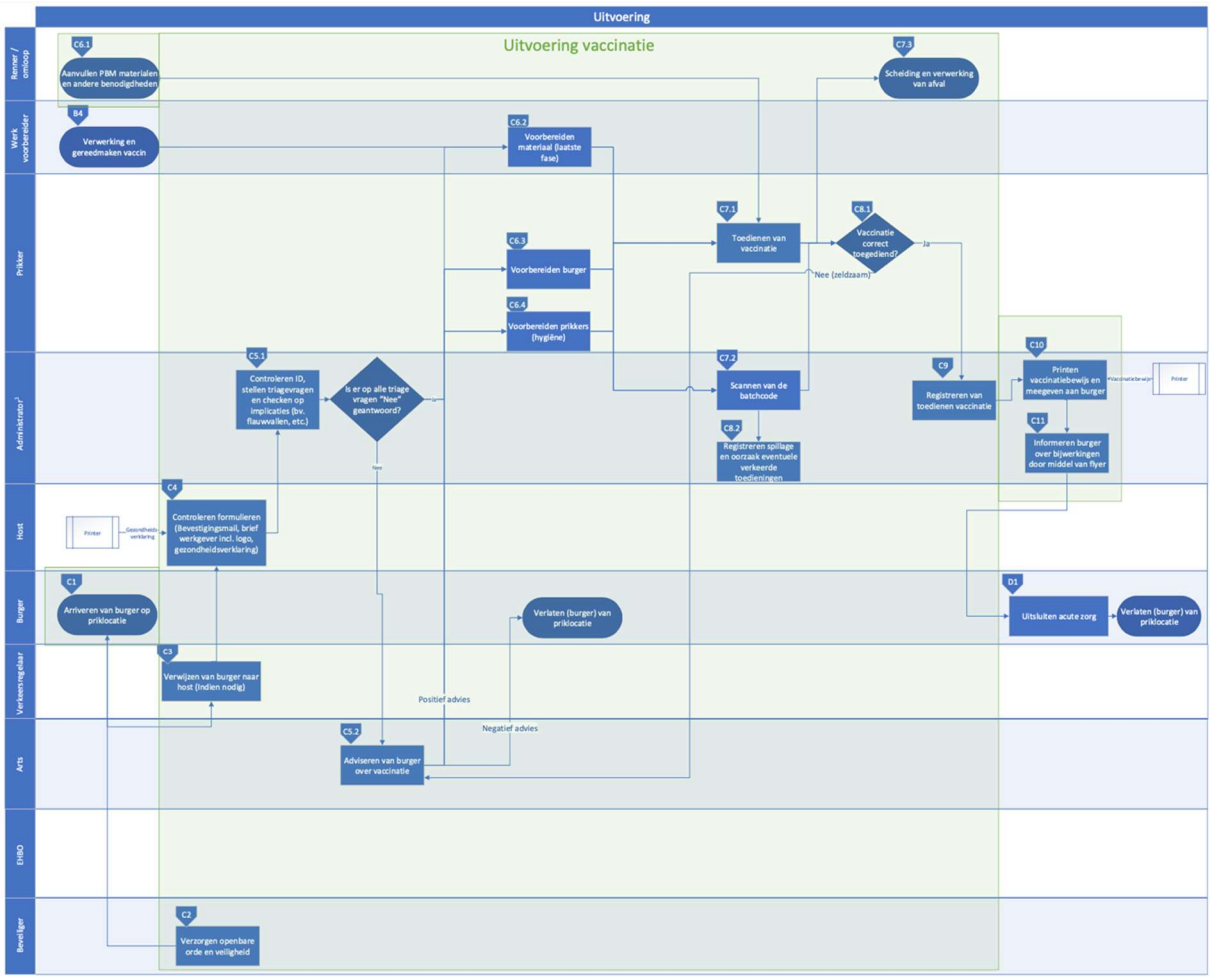
9. AP is geraadpleegd met betrekking tot uitvraag toestemming RIVM ter registratie van persoonsgegevens in CIMS.

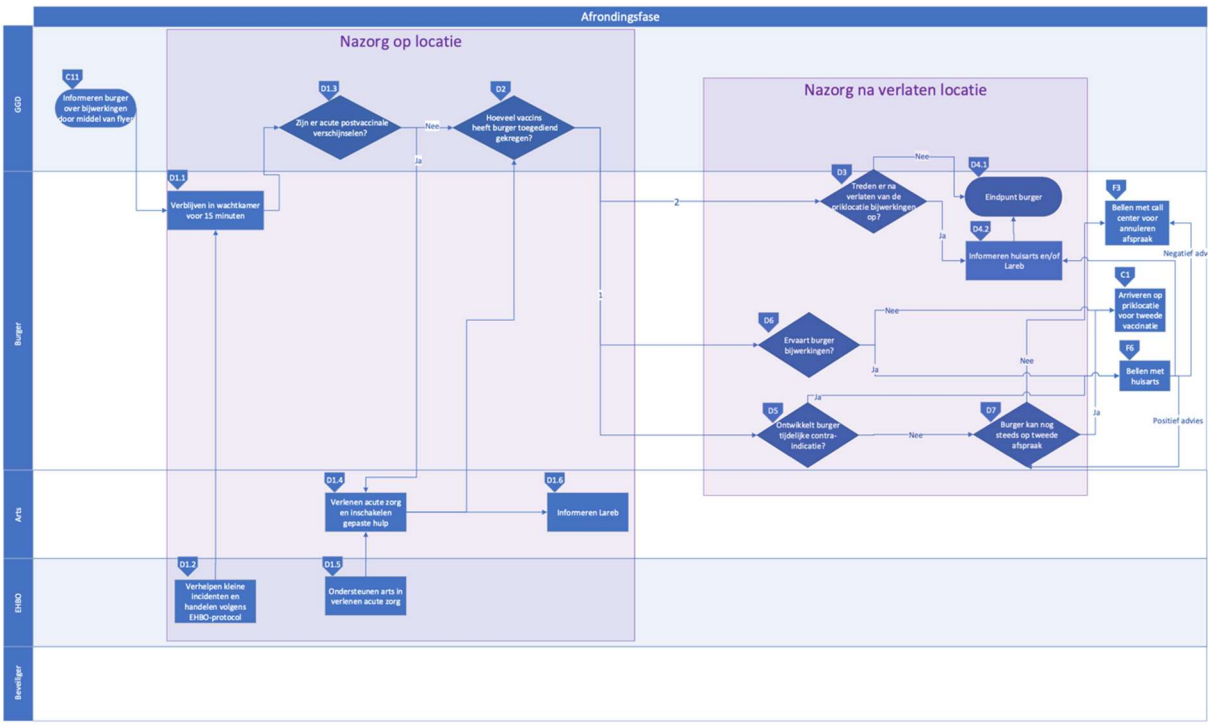
RIVM heeft een document opgesteld waarop de AP een memo heeft geschreven. Daarnaast is telefonisch contact geweest met de AP, maar hierbij is verder geen advies gegeven.

E. Bijlagen

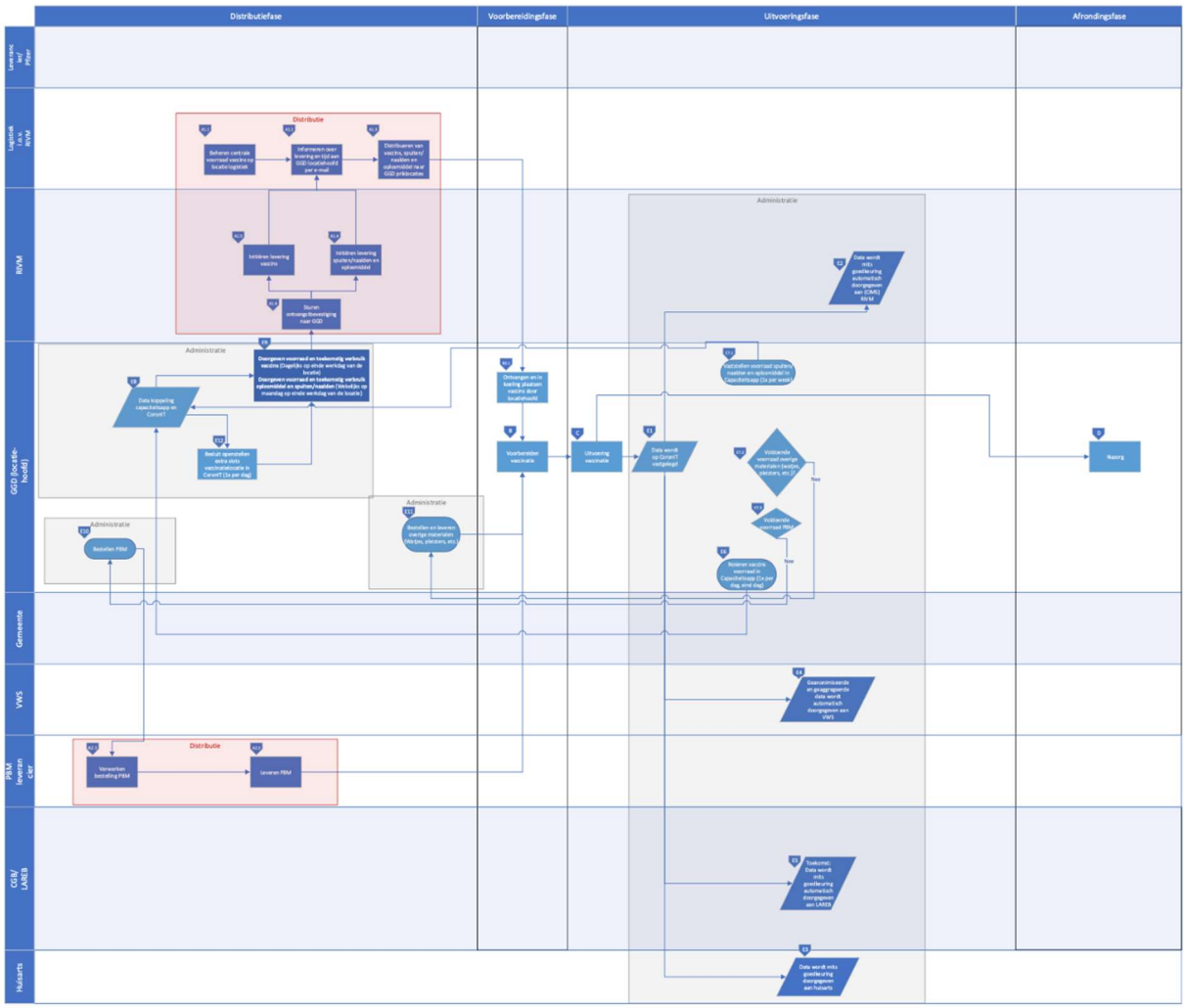
Bijlage 1: Grafische weergave fases vaccinatieproces




Uitvoering
Uitvoering vaccinatie
Renner / omloop
Werk voorbereider
Prikker
Administrator¹
Host
Burger
Verkeersregelaar
Arts
EHBO
Beveiliger
C6.1 Aanvullen PBM materialen en andere benodigdheden
B4 Verwerking en gereedmaken vaccin
C6.2 Voorbereiden materiaal (laatste fase)
C6.3 Voorbereiden burger
C6.4 Voorbereiden prikkers (hygiëne)
C7.3 Scheiding en verwerking van afval
C7.1 Toedienen van vaccinatie
C8.1 Vaccinatie correct toegediend?
Ja
Nee (zeldzaam)
C5.1 Controleren ID, stellen triagevragen en checken op implicaties (bv. flauwvallen, etc.)
is er op alle triage vragen "Nee" geantwoord?
Ja
Nee
C7.2 Scannen van de batchcode
C8.2 Registreren spillage en oorzaak eventuele verkeerde toedieningen
C9 Registreren van toedienen vaccinatie
C10 Printen vaccinatiebewijs en meegeven aan burger
C11 Informeren burger over bijwerkingen door middel van flyer
Printer
Vaccinatiebewijs
C4 Controleren formulieren (Bevestigingsmail, brief werkgever incl. logo, gezondheidsverklaring)
Printer
Gezondheids verklaring
C1 Arriveren van burger op priklocatie
Verlaten (burger) van priklocatie
D1 Uitsluiten acute zorg
Verlaten (burger) van priklocatie
C3 Verwijzen van burger naar host (Indien nodig)
Positief advies
Negatief advies
C5.2 Adviseren van burger over vaccinatie
C2 Verzorgen openbare orde en veiligheid


Afrondingsfase
Nazorg op locatie
Nazorg na verlaten locatie
GGD
Burger
Arts
EHBO
Beveiliger
C11 Informeren burger over bijwerkingen door middel van flyer
D1.3 Zijn er acute postvaccinale verschijnselen?
Nee
Ja
D2 Hoeveel vaccins heeft burger toegediend gekregen?
D1.1 Verblijven in wachtkamer voor 15 minuten
2
1
D3 Treden er na verlaten van de priklocatie bijwerkingen op?
Nee
Ja
D4.1 Eindpunt burger
D4.2 Informeren huisarts en/of Lareb
F3 Bellen met call center voor annuleren afspraak
Negatief adv
C1 Arriveren op priklocatie voor tweede vaccinatie
D6 Ervaart burger bijwerkingen?
Nee
Ja
F6 Bellen met huisarts
D5 Ontwikkelt burger tijdelijke contra-indicatie?
Ja
Nee
D7 Burger kan nog steeds op tweede afspraak
Ja
Positief advies
D1.4 Verlenen acute zorg en inschakelen gepaste hulp
D1.6 Informeren Lareb
D1.2 Verhelpen kleine incidenten en handelen volgens EHBO-protocol
D1.5 Ondersteunen arts in verlenen acute zorg

GGD
Amsterdam



GGD Amsterdam

Bijlage 4: Overzicht Risico's en Maatregelen

#	Risico's	Risiconiveau voor maatregel	Risiconiveau na maatregel	Maatregelen
1	Maatregelen voor informatiebeveiliging zijn onvoldoende ingericht	Middel		1
2	Onbekend op welke wijze logging wordt toegepast	Middel		2
3	Vastgestelde kwetsbaarheden	Middel		3
4	Vastgestelde kwetsbaarheden II	Middel		4
5	Afspraken omtrent beheer CoronIT onduidelijk en/of niet geformaliseerd	Middel		5
6	Overeenkomsten met betrokken partijen en leveranciers en afspraken over verantwoordelijkheid zijn niet duidelijk en/of niet geformaliseerd	Middel		6
7	Communicatie vaccinatiegegevens niet eenduidig gedefinieerd	Middel		7

8	Rechten van betrokkenen onvoldoende ingericht	Hoog		8
9	Geen duidelijke werkinstructies	Hoog		9 en 10
10	Bewaartermijnen CoronIT zijn nog niet onderbouwd	Middel		11
11	Toegang tot persoonsgegevens onvoldoende geregeld	Hoog		12
12	Inzage in CoronIT door elke regio is onrechtmatig indien medisch dossier	Hoog		13
13	Rechtmatigheid van de verwerking in het gedrang	Hoog		14
14	Onduidelijke grondslag data verstrekking aan huisartsen	Middel		15
15	Aanmaken dossier bij vaccinatieweigering			
16	Gebrek aan duidelijk en organisatorische maatregelen	Middel		16
17	Dossier aangemaakt voor iedere beller			

	Maatregelen	**Helpt bij risico**

1	Wijze backup en restore verantwoorden	1
2	Logging conform Privacy by Design	2
3	Schema met kwetsbaarheden en security assessement	3
4	Wijzigingen testen	4
5	Toegankelijke data	5
6	Heronderhandelen verwerkersovereenkomst	6
7	Updaten technische documentatie	7
8	Inzage door prints	8
9	Convenant tussen GGD GHOR en GGD'en	9
10	Convenant gesloten met RIVM	9
11	Professor inschakelen voor toelichting	10
12	Autorisatimatrix	11
13	Regio's onderling inzage	12

14	Informatie voor betrokkene	13
15	Afspraken met huisartsen vertrekking van gegevens	14
16	Procedure voor vernietiging papieren versie	16

GGD Amsterdam

Versie	Datum	Auteur	Verspreiding bij	Opmerkingen
0.1	15 januari 2021	Privacy adviseur GGD GHOR	GGD GHOR/FG'en regionale GGD'en	Dit is de conceptversie. Deze versie is nog niet geschikt voor het verlenen van commentaren, maar is enkel ter kennisname om zo een beeld te krijgen van het proces vanuit het oogpunt van gegevensverwerking.
0.2	29 juli 2021	Privacy Officer GGD Amsterdam	GGD Amsterdam	De conceptversie is aangepast naar versie voor GGD Amsterdam.