Departementaal Vertrouwelijk

Rijksinstituut voor Volksgezondheid
en Milieu
Ministerie van Volksgezondheid,
Welzijn en Sport

AANVRAAGFORMULIER RISICOACCEPTATIE – 25 februari 2021 –

Betreft:	Bestelproces COVID vaccins (aanvullende acceptatie)	
Aanvrager:	5.1.2e	
Aanvraagnummer:	**20210225-01 RACC Bestelproces COVID Vaccins**	
Datum aanvraag:	28-12-2020 (initieel)	
Centrum/dienst:	DVP	CvB
Systemen	DVP-SAP en Movianto SAP	SNPG Webapp
Verantwoordelijk lijnmanager:	5.1.2e 5.1.2e	5.1.2e
Verantwoordelijk centrum- of afdelingshoofd:	5.1.2e	5.1.2e 5.1.2e 5.1.2e 5.1.2e
Informatiemanager:	5.1.2e -> waargenomen door 5.1.2e	5.1.2e
Doel:	Vaststellen risico's en te nemen maatregelen c.q. uit te stellen maatregelen	
Aan:	5.1.2e 5.1.2e 5.1.2e 5.1.2e 5.1.2e 5.1.2e 5.1.2e 5.1.2e 5.1.2e 5.1.2e 5.1.2e 5.1.2e	
T.b.v. vergadering:	**Besluitvormend overleg 25 februari 2021, 10u-11u**	
Aantal pagina's:	**19**	
Notitie toegevoegd:	**Bijlage: spreadsheet 'Maatregelen Bestelproces 20210024'**	
Versienummer:	**0.9**	
Datum laatst gewijzigd:	**24-02-2021**	

Quickscan resultaat COVID-19 vaccin bestelproces *Neem hier de resultaten van de Quickscan over*	**Datum Quickscan: 28 december 2020**

I Samenvatting

	STAP 1		STAP 2			STAP 3					
(X)	Rubricering	(X)	Classificatie proces	(X)	Classificatie systeem	(X)	B	(X)	I	(X)	V
	Openbaar		Ondersteunend		Nuttig		Laag		Laag		Laag
	RIVM Intern (besloten)		Bijdragend		Belangrijk		Midden		Midden		Midden
X*	RIVM Vertrouwelijk	X	Strategisch	X	Vitaal	X	Hoog	X	Hoog	X	Hoog
X*	Departementaal Vertrouwelijk		Kritisch strategisch								
	Staatsgeheim Confidentieel										
	Staatsgeheim Geheim										
	Staatsgeheim Zeer Geheim										

*exacte rubricering nog nader vast te stellen. Voor SNPG webapp is de rubricering initieel RIVM vertrouwelijk en zijn daarop de risico's en maatregelen ingeschaald. Voor de bestelketen van de

COVID-19 vaccins wordt Departementaal Vertrouwelijk voorgesteld.
Update: voor de gehele keten is het uitgangspunt Departementaal Vertrouwelijk

BBN *1, 2, 3 of VIR-BI*	*BBN3*	*Voor de Covid19-vaccinvoorziening geldt: commercieel vertrouwelijke informatie, ieveranciersinformatie, grootschalige opslag, beheer en vervoer. Voor statelijke actoren of crimineien is het interessante informatie welke bestellingen/voorraden er waar zijn. Daarom wordt BBN3 als passend beschouwd.*

Aanvraagnummer
Geef aan onder welk nummer de aanvraag al in het risk register staat of dat het een nieuwe aanvraag betreft

20210225-01 RACC Bestelproces COVID Vaccins
Vorige versie: 20210128-01 RACC Bestelproces COVID Vaccins

Aanleiding
Gerelateerd proces of informatiesysteem (+doelstelling)
Korte omschrijving van proces(sen) en informatiesyste(e)m(en) waar de risicoacceptatie betrekking op heeft en de doelstelling ervan

Achtergrond en urgentie
In dit document wordt het bestelproces van de COVID-vaccins en de bijbehorende risico's, maatregelen en restrisico's beschreven.

De vaccinatiestrategie wordt gaandeweg duidelijk. Wie gevaccineerd gaat worden en door welke partij dit gebeurt kan per dag wijzigen, wat invloed heeft op het bestelproces. Om deze reden is dit een groeidocument dat bij relevante wijzigingen aangepast zal worden. Op dit moment worden de vaccins al uitgeleverd aan de GGD'en die personeel uit de acute zorg vaccineert. Vanaf maandag 18 januari 2021 kunnen de verpleeghuizen ook gaan bestellen via de SNPG Webapp en vanaf 25 januari de huisartsen. Vanwege de hoge eisen die aan informatiebeveiliging van het bestelproces worden gesteld en omdat veel zaken nog uitgezocht moeten worden, zijn op dit moment een aantal risico's nog niet bekend, in detail beschreven en/of generiek als hoog of midden ingeschat. De consequentie van het niet accepteren van de risico's is, dat per direct een mailing naar de verpleeghuizen gestuurd moet worden dat er maandag niet besteld kan worden. Het bestellen en uitleveren van de vaccins aan de verpleeghuizen valt dan stil en deze doelgroep kan dan niet op korte termijn gevaccineerd worden. Dit betreft tevens een risico voor de volksgezondheid, omdat dat niet spoedig een groter percentage Nederlanders gevaccineerd kan worden tegen COVID-19.

Beschrijving van het bestelproces
Voor een eerste systeemdecompositie / procesplaat van het proces wordt verwezen naar pagina 3 van dit document. Er zijn verschillende manieren om vaccins te bestellen.

De SNPG-webapp wordt gebruikt voor bestellen vaccins, bestellen informatiemateriaal en declareren en melden van vaccinaties. De SNPG-webapp wordt gebruikt door huisartsen, Arboartsen en zorginstellingen.
SNPG staat voor: Stichting Nationaal Programma Grieppreventie.

De bestelgegevens vanuit de SNPG-webapp worden in SAP-DVP ingelezen. Hieruit worden vervolgens salesorders voor de logistiek dienstverlener Movianto gemaakt die de vaccins naar de klanten brengt.

SAP-Movianto krijgt via beveiligde zorgmail een met password beveiligd Excelbestand van DVP waarna zij de gegevens in hun eigen SAP-systeem invoeren. Met deze gegevens kunnen Movianto-chauffeurs de bestelde vaccins en toebehoren bij de klanten afleveren.

Voor het bestellen en distribueren van de COVID-vaccins zijn drie ketens uitgewerkt, zie onderstaand overzicht. Voor alle ketens geldt dat het om gegevens gaat over hoeveelheid vaccins en toebehoren (optrek/toedieningsnaalden en -spuiten en oplosmiddelen) en NAW-gegevens van de klant (GGD, huisarts, zorginstellingen waar de vaccins bezorgd zullen worden). Er worden geen gegevens van te vaccineren personen gebruikt.

Buiten scope van deze risico-acceptatie:

- De SAP portal welke zal worden gebruikt als keten 3. Deze is nog in ontwikkeling. Onbekend

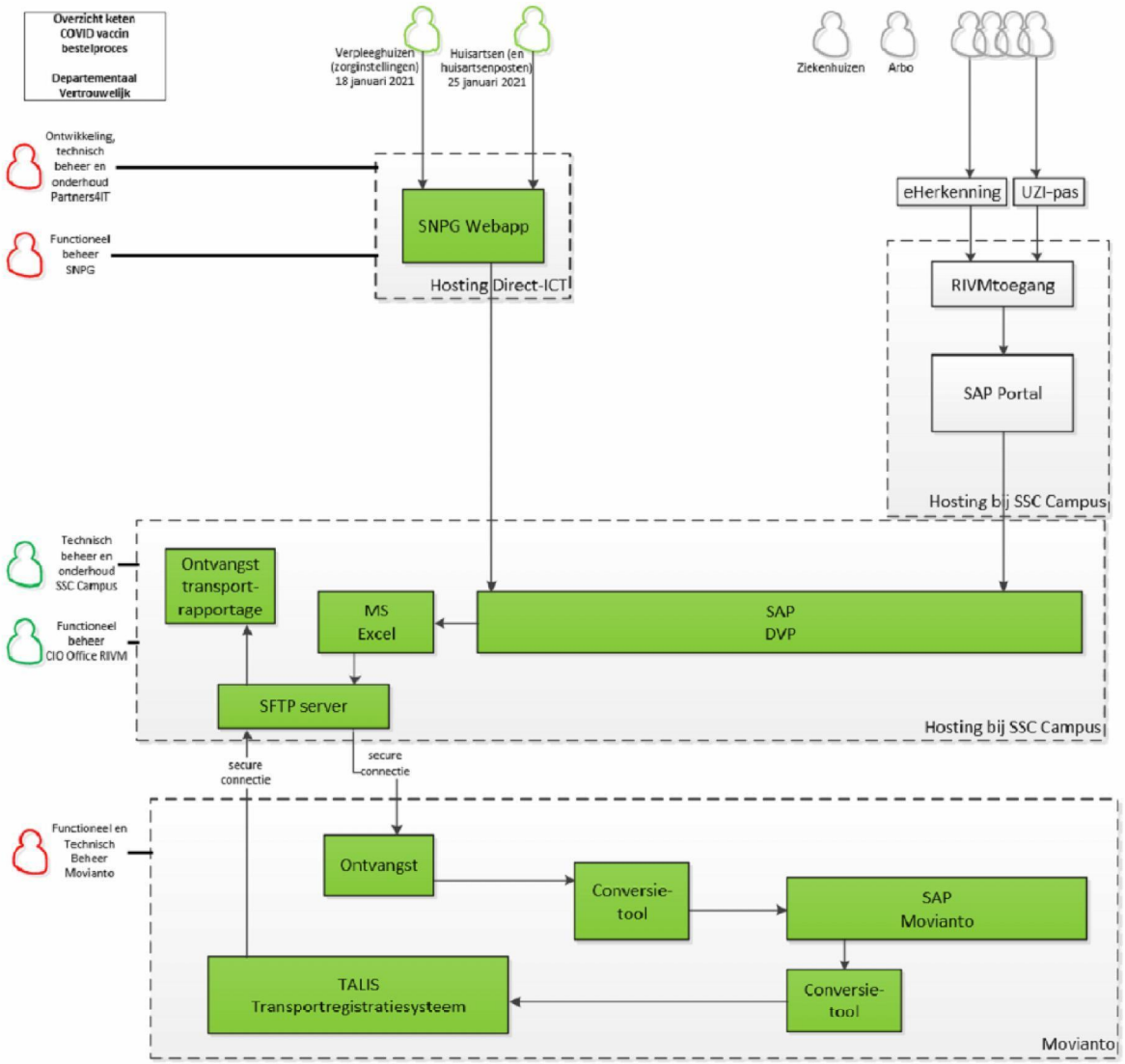
is wanneer deze klaar is.
- De 'DVP-chauffeursapp' is een interne app gekoppeld aan SAP waarmee de DVP-regiokantoren werken. Deze app wordt niet voor de COVID-vaccins gebruikt en zal dus niet meegenomen worden in de risicoanalyse.
- Het logistieke (fysieke) proces van aflevering van de vaccins op de priklocaties aan geautoriseerde/geauthentiseerde personen. Dit valt binnen scope van de COVID-19-projecten rond beveiliging. Hierbij is ook de IGJ (inspectie) betrokken.

Verantwoordelijkheden
- De COVID-programmadirecteuren zijn verantwoordelijk voor het bestelproces van de COVID-vaccins.
- CvB is verantwoordelijk voor de SNPG Webapp. Met deze app bestelden huisartsen en een groot deel van de zorginstellingen al de griep- en pneumokokkenvaccins. Deze app zal nu ook gebruikt worden voor het bestellen van de COVID-vaccins. De uitvoering van de griep- en pneumokokkencampagne is belegd bij SNPG. CvB is eigenaar van de app, SNPG verzorgt het functioneel beheer en Partners4IT verzorgt het technisch en applicatiebeheer en de doorontwikkeling.
- De distributie vindt plaats door logistiek dienstverlener Movianto.
- DVP is proceseigenaar van alles wat loopt via SAP-DVP en het opdrachtgeverschap richting Movianto.

Bijzonderheden:
- **Met Movianto is frequent afstemming over de voortgang op de risico's.**
- **Tijdens de risicoanalyse sessie op 12 februari heeft het kernteam samen met de IM-ers voor het vaccinatieprogramma** 5.1.2e **de systeemdecompositie van het COVID-19 vaccin bestelproces en IT/IB technische versie van Movianto besproken en zijn (additionele) risico's en de maatregelen besproken.**
- **Op maandag 15 februari is door LCC besloten om Formdesk niet in te gaan zetten voor het COVID-19 bestelproces.**
- **Op basis van het gesprek op 22 februari met SNPG en Partners4IT is de systeemdecompositie voor SNPG webapp omgeving uitgewerkt in twee varianten; op proces level en IT/IB technisch in detail. Eerstgenoemde is aan dit document toegevoegd.**

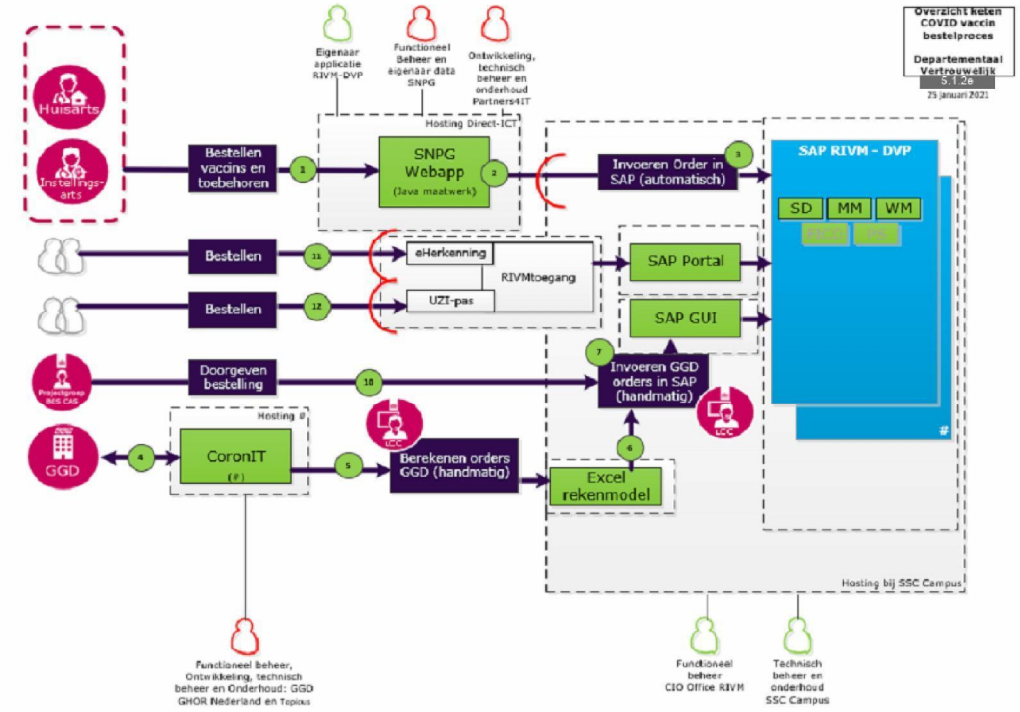
Rijksinstituut voor Volksgezondheid
en Milieu
*Ministerie van Volksgezondheid,
Welzijn en Sport*

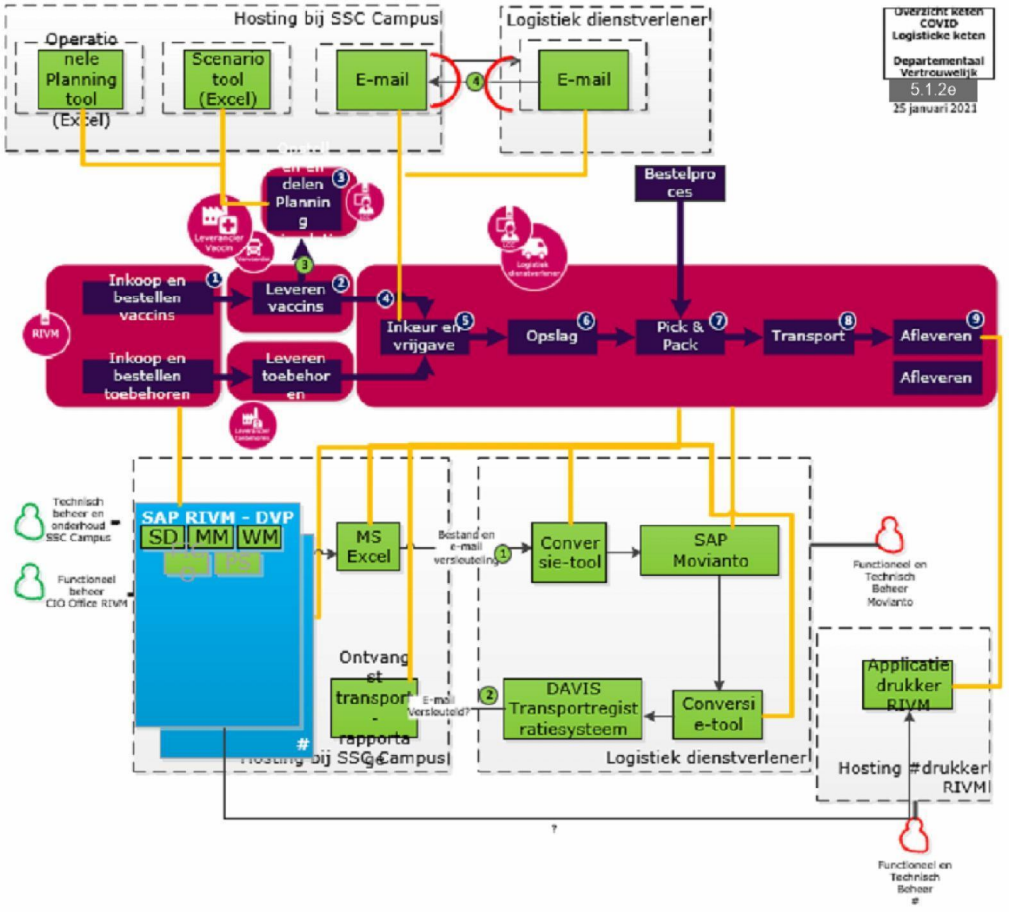
Systeemdecompositie keten COVID vaccin bestelproces
Systeemdecompositie van het betreffende informatiesyste(e)m(en) ***(updated!)***



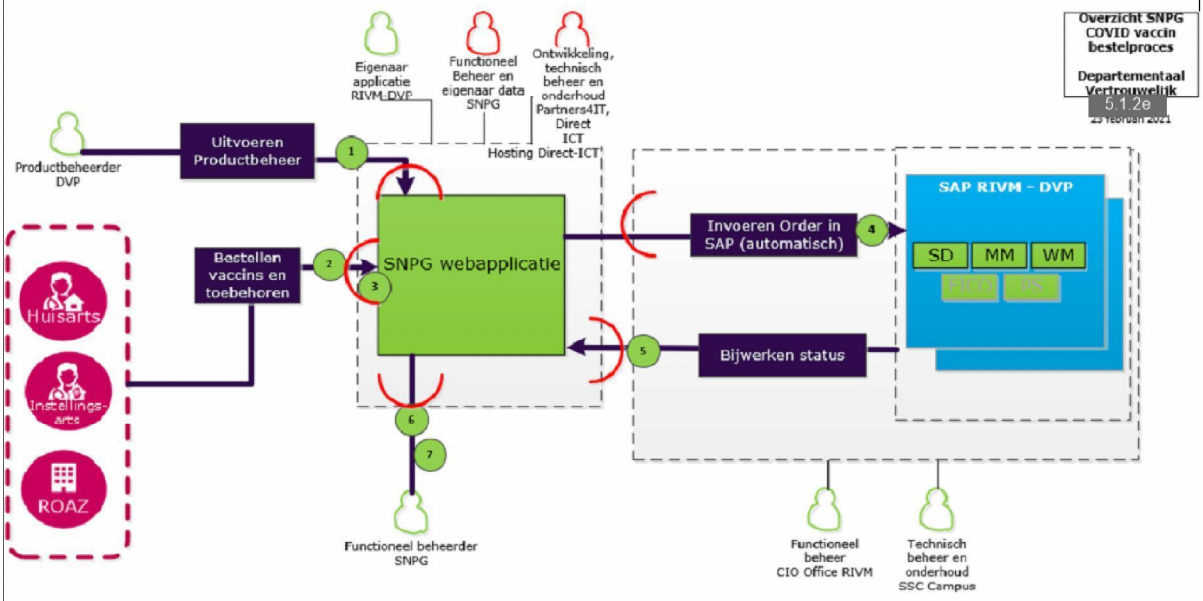
Overzicht bestelproces COVID vaccins.

Nadere uitwerking bestelproces COVID vaccins (bestelproces en logistieke keten)





Overzicht SNPG bestelproces COVID-19 vaccins (23 februari 2021)



Informatiebeveiliging en risico's

Voor het proces van de NSPG-webapp is op 6 oktober 2020 de Quickscan BIO uitgevoerd en een risicoanalyse uitgevoerd (22, 29 oktober en 11 november 2020) en in basis een risicoacceptatie opgesteld. De aanvraag voor risicoanalyse van de SNPG webapp was nog niet ingediend.

Nu gaat de omgeving gebruikt worden voor de COVID-19 vaccinatie, gebruik makend van Formdesk* en SAP Movianto. Op 24 december 2020 is gestart met de risicoanalyse op basis van de uitbreiding op de scope. Daarbij zijn op hoofdlijnen de risico's in kaart gebracht en actiepunten benoemd. Voor het bestelproces vaccins is de Quickscan BIO opgesteld.

Op 30 december 2020 zijn de openstaande issues rond informatiebeveiliging (IB) en privacy, mede vanwege de verhoogde IB-eisen als gevolg van gebruik voor COVID-19 besproken in een bestuurlijk overleg, waarbij aanwezig o.a. de CFO RIVM en het hoofd DVP. Gezien de haast te starten met het leveren van de COVID-vaccins aan de GGD-en voor de eerste vaccinatietranche is tijdens de bestuurlijke risicoacceptatie besloten om, ondanks de openstaande issues, de bestellingen en distributie in deze keten vanaf eind december 2020 in gang te zetten. Formdesk* kan hierbij (alleen) door DVP-medewerkers gebruikt worden (alleen intern gebruik).

Inmiddels zijn veel acties uitgevoerd, vragen beantwoord en is het risicoacceptatieformulier verder uitgewerkt. De volgende vaccinatietranches via huisartsen en zorginstellingen gaan binnenkort starten via de SNPG Webapp. Daarom wordt de huidige stand van het risicoacceptatieformulier voorgelegd voor de ketens 1 en 2.

***LCC heeft op 15 februari besloten Formdesk niet in te gaan zetten voor het bestelproces.**

Privacy

De contactgegevens/persoonsgegevens binnen het proces worden uitsluitend in het kader van de afhandeling van de bestelling verwerkt.
De 5.1.2e ; 16 november) en 5.1.2e ; 17 december) hebben de Quickscan PIA doorlopen en gesteld dat tot op heden een PIA niet nodig is. Oordeel PO: dan lijkt de privacy impact van de verwerking beperkt en is een PIA niet direct noodzakelijk.
De kijkend naar de negen beoordelingscriteria AVG wordt het uitvoeren van een DPIA niet nodig geacht. Wel is er de noodzaak om de onderbouwing ervan uit te werken.

Er moet een DPIA worden uitgevoerd als aan twee of meer van onderstaande criteria wordt voldaan:

nr	Criterium	Verwerking in het bestelproces voldoet ja / nee	Onderbouwing
1	Beoordelen van mensen op basis van persoonskenmerken	Nee	Er worden geen mensen beoordeeld met de verzamelde ordergegevens
2	Geautomatiseerde beslissingen	Nee	De orderverwerking heeft geen gevolgen voor mensen
3	Stelselmatige en grootschalige monitoring	Nee	Niet van toepassing
4	Gevoelige gegevens	Nee	Er worden geen bijzondere persoonsgegevens verzameld. Beperkt tot NAW gegevens
5	Grootschalige gegevensverwerking	Nee	Niet van toepassing, er worden alleen ordergegevens en NAW gegevens van een beperkte groep klanten verwerkt
6	Gekoppelde databases	Nee	Niet van toepassing: Er worden geen gegevensverzamelingen gecombineerd of gekoppeld.
7	Gegevens over kwetsbare personen	Nee	Niet van toepassing: Alle betrokken professionals kunnen in vrijheid hun toestemming gegeven voor het verwerken van hun vaccinorder
8	Gebruik van nieuwe technologieën	Nee	Niet van toepassing
9	Blokkering van een recht, dienst of contract	Nee	Het gevolg van de orderverwerking is het uitleveren van vaccins en producten. Geen gevolg van de orderverwerking dat de betrokkene geen uitlevering krijgt

Conclusie: Er hoeft geen DPIA te worden uitgevoerd: De voorgenomen verwerking van de niet-bijzondere persoonsgegevens leveren een laag privacy risico op voor de betrokken personen.

Probleemstelling, risicobeschrijving en mitigatie
Geef hierbij aan welk risico geaccepteerd wordt dan wel voor welk beleid een ontheffing aangevraagd wordt. Geef duidelijk aan wat het risico is, welke mitigerende maatregelen getroffen zijn en wat het managed risico is

Twee weken geleden geraakte bekend dat het computernetwerk van het Algemeen Medisch Labo in Antwerpen was gehackt. — © BELGA

Cyberaanval legt labo's over heel België plat

De complexe cyberaanval op een Antwerps medisch labo dat coronatests analyseert, heeft ook verschillende andere medische labo's in ons land platgelegd.

Werner Rommers, Dirk Coosemans en Steven Leenknegt

Vrijdag 8 januari 2021 om 18:36

Met het RIVM vergelijkbare actoren zoals de EMA en labs in België liggen onder vuur van cyberaanvallen van statelijke actoren. Recentelijk heeft een hack bij de EMA plaatsgevonden; documenten van de EMA staan inmiddels op Russische fora. Daarnaast hebben zeer recent gerichte aanvallen op Belgische laboratoria plaatsgevonden. Naast statelijke actoren behoren ook activisten zoals antivaxxers tot de mogelijke actoren. Hoewel het hier gaat om andersoortige informatie (over de veiligheid en toepassing van vaccins) dan die in het bestelproces (logistieke informatie over hoeveelheden, locaties, et cetera) geeft dit een beeld van de context waarin het RIVM op dit moment opereert. In de hierna volgende tabel worden de risico's een voor een beschreven.

Het overzicht aan risico's met mitigatie bestaat uit twee delen.
Het eerste deel bestaat uit de indeling op risicogroep zoals gebruikt in de vorige risicoacceptatie. Deze is nu geüpdatet m.b.t. de mitigatie en de risicolevels.
Het tweede deel bestaat uit de inhoudelijke risico's met daarbij de relevante maatregelen.

Ref.	Omschrijving	Risico	Mitigerende maatregelen aanwezig	Uit te voeren acties/te implementeren maatregelen

R-A	Dreigingen vanuit statelijke actoren (en activisten/ antivaxxers) t.a.v. het bestelproces van vaccins	Het (mogelijke) doel hierbij varieert van het verspreiden van misleidende informatie (m.b.t. de vaccindistributie en -campagne) tot pogingen de vaccindistributie te ontregelen.	- BBN3 dreigingsniveau is in acht genomen op COVID vaccin bestelproces - Er is intensief contact IB RIVM met AIVD (NBV) en NCSC t.b.v. dreigingsinformatie en concrete aanwijzingen - Er is direct contact met ketenpartners - Er is voor het RIVM verhoogde dijkbewaking in de vorm van o.a. monitoren op verdacht verkeer, verkeerde inlogpogingen etc. - Binnen het bestelproces zijn de resterende systemen Departementaal Vertrouwelijk gerubriceerd. - Informatieclassificatie Departementaal Vertrouwelijk (DepV) en het bijbehorend normenkader zijn gehanteerd en assessments zijn uitgevoerd - Set aan relevante maatregelen voor BBN3 zijn gedefinieerd - **Met inachtneming van BBN3 dreigingsniveau nadere risicoanalyses uitvoeren; *NB. BBN3-maatregelen staan qua zwaarte meer naast dan boven BBN2***	- Maatregelen beleggen, najagen en risico's oplossen - Voor nadere details zie beveiligingsniveau per systeem

R-B	Tijdsdruk en ad hoc besluitvorming	De vaccinatiestrategie verandert steeds. Daarnaast verandert het transport door o.a meer kennis en eigenschappen van de vaccins. Een aantal activiteiten binnen het programma zijn later dan gewenst van start gegaan.	- Recentelijk is awareness voor het dreigingsniveau gecreëerd - Intensieve afstemmingen hebben plaatsgevonden om de hoofdrisico's in kaart te brengen - Een (eerste) overall procesplaat/systeemdecom positie van het bestelproces is gemaakt - De opzet voor de systeemdecompo-sitie is uitgewerkt - Dagelijks is er een update met het kernteam voor de risicoacceptatie waarin ook IB vertegenwoordigd - **Een gedetailleerde systeemdecompositie uitwerken waarin de gehele keten in scope wordt nemen (w.o. ook de ontwikkeling van de SAP portal)**	- Bij het nemen van besluiten dient het management van belang van de consequenties voor informatiebeveiliging meenemen, de juiste partijen aanhaken en dit tijdig communiceren.
R-C	Beveiligingsnive au SNPG webapp	De SNPG webapp gaat gebruikt worden door huisartsen, huisartsenposten en zorginstellingen om COVID vaccins te bestellen en dient weerbaar te zijn tegen dreigingen vanuit statelijke actoren. **Ook partijen zoals de ROAS-en, GGZ, DJI etc. gaat ook via SNPG.**	- Uitgevoerde risicoanalyse op SNPG webapp - BBN2 - Pentest is uitgevoerd en er is hertest; de meest belangrijke bevindingen zijn opgelost – er resteren bevindingen op niveau midden en laag - SNPG en Partner4IT zijn ISO 27001 gecertificeerd - DepV assessment is uitgevoerd - Actiepunten uit DepV assessment zijn benoemd en geadresseerd - **Nadere risicoanalyse uitvoeren met inachtneming van BBN3 dreigingsniveau, maatregelen implementeren (of zo nodig accepteren)**	- Monitoren, najagen en oplossen openstaande midden en laag bevindingen pentest en risico's verder mitigeren - **Partners4IT is gestart met ISO27001 certificering. Het ISMS is opgezet vanuit verkiezingen applicatie. Na de verkiezingen wordt het weer opgepakt. (dan certificaat en toepasselijk-heidsverklaring opvragen)**
R-D	Beveiligingsnive au Formdesk formulier COVID bestellingen.			- **Voor Formdesk is vanuit LCC besloten dit niet in te gaan zetten voor het bestelproces** - Geen acties.

R-E	Beveiligings-niveau SAP DVP	SAP DVP is onderdeel van het bestelproces voor COVID vaccins en dient weerbaar te zijn tegen dreigingen vanuit statelijke actoren. Voor het bestellen van de griepvaccins wordt al meerdere jaren gebruik gemaakt van deze systemen, het betreft interne systemen.	- DepV assessment is afgerond, actiepunten zijn benoemd en geadresseerd - **Nadere risicoanalyse uitvoeren met inachtneming van BBN3 dreigingsniveau, maatregelen implementeren (of zo nodig accepteren)**	- Monitoren beleggen, najagen en risico's mitigeren
R-F	Beveiligingsni-veau Movianto	Naast griepvaccins gaat Movianto nu de COVID-19 vaccins distribueren. De bestelinformatie en de details over transporten e.d. worden tussen RIVM en Movianto uitgewisseld. In 2020 is vanuit NCTV is een assessment uitgevoerd voor de fysieke beveiliging. De risico's en maatregelen ten aanzien van informatiebeveiliging/cybersecurity zijn toen niet beoordeeld. *NB: de vaccinatie- en preventieprogramma's lopen al geruime tijd via Movianto.*	- Kennis maken, relatie opbouwen en een eerste inventarisatie uitvoeren van kwetsbaarheden en verbeterpunten - Assessment door IB RIVM - Assessment door de AIVD (NBV) - DepV assessment is afgerond, actiepunten zijn benoemd en geadresseerd - Maatregelen uit site visit IB RIVM en rapport NBV (AIVD) zijn opgenomen in de actielijst - **Nader risicoanalyse BBN3 uitvoeren, maatregelen implementeren (of zo nodig accepteren)** - **Interfacing (koppeling) tussen SAP RIVM en SAP Movianto realiseren** - **Beveiliging e-mail verkeer transport-gegevens (van Movianto naar DVP)**	- Logging en actief monitoring e.d. (SIEM-SOC functies) realiseren i.s.m. NCSC of commerciële partij - ISO27001 certificering door Movianto - Maatregelen beleggen, najagen en risico's mitigeren

Kwantitatief overzicht voortgang actiepunten

Het overzicht van openstaande maatregelen staan beschreven in spreadsheet 'Maatregelen Bestelproces 20210224' (bijlage).

De huidige status van de openstaande operationele actiepunten:

Risicogroep	Aantal openstaande acties 27/1/2021	Aantal openstaande acties 24/2/2021
- Set statelijke actoren (BBN3)	27	25
- DepV – SNPG webapp (incl. findings RA – BBN2 en pentest findings)	40	36*
- DepV – Formdesk	5	0
- DepV – SAP DVP	20	14
- DepV – SAP Movianto	13	5
- Site visit Movianto + analyse NBV (AIVD)	15	10

***een groot deel van de openstaande acties zijn bijna gereed!**

Rijksinstituut voor Volksgezondheid
en Milieu
*Ministerie van Volksgezondheid,
Welzijn en Sport*

Risicomatrix
Geef in de matrix aan waar het risico zich bevindt (dit op basis van de risicoanalyse; in te vullen door CISO of FCC/S&S)

Status risico's bestelproces COVID vaccins per 27 januari 2021

Risicomatrix					
kans / impact	1 < 1 keer per 10 jaar	2 Minimaal 1 keer 5 jaar	3 Minimaal 1 keer per jaar	4 Elk kwartaal	5 Een keer per maand of vaker
3 (hoog)		C E D	B F A		
2 (midden)					
1 (laag)					

A: Dreiging statelijke actoren (BBN3 dreigingsniveau)
B: Tijdsdruk en ad hoc besluitvorming
C: Beveiligingsniveau SNPG webapp
D: Beveiligingsniveau Formdesk formulier COVID bestellingen
E: Beveiligingsniveau SAP DVP en Winshuttle
F: Beveiligingsniveau Movianto

Status risico's bestelproces COVID vaccins per 24 februari 2021

Risicomatrix					
kans / impact	1 < 1 keer per 10 jaar	2 Minimaal 1 keer 5 jaar	3 Minimaal 1 keer per jaar	4 Elk kwartaal	5 Een keer per maand of vaker
3 (hoog)		F B E	A C		
2 (midden)					
1 (laag)					

A: Dreiging statelijke actoren (BBN3 dreigingsniveau)
B: Tijdsdruk en ad hoc besluitvorming
C: Beveiligingsniveau SNPG webapp
E: Beveiligingsniveau SAP DVP en Winshuttle
F: Beveiligingsniveau Movianto

Toelichting:
Vanwege uitkomsten van het gesprek met SNPG en Partners4IT is (tijdelijk) het groepsrisico C hoger ingeschaald.

Overzicht inhoudelijke risico's

Onder elk risico staat de relevante risicogroep weergegeven.

Ref.	Risico	Maatregel	Gerelateerde BIO norm	Status *(CISO RIVM)*	Bijzonderheden *(CISO RIVM)*
R01 CEF	Gebruik van de onrechtmatig verkregen inloggegevens van een medewerker of andere belanghebbende; zowel binnen RIVM als bij ketenpartner.	- Inrichten van toegang middels twee factor authenticatie (2FA) - Awareness bij medewerkers	9.3.1 9.4.2.1	SNPG webapp: 2FA is ingericht voor bestellers. SAP DVP: is standaard ingericht; voor (functioneel) beheerder nog nader onderzoek. SAP Movianto: Voor VPN is dit ingericht (eind februari gereed), voor beheerders loopt.	
R02 CEF	Misbruik van een kwetsbaarheid in het toegangssysteem van een applicatie	- Testen op kwetsbaarheden en bij doorgevoerde wijzigingen - Overweeg red teaming (initiatief vanuit VWS werkend met ethical hackers)	12.6.1	SNPG: Voordat wijzigingen in productie worden genomen wordt er getest. Movianto: Afstemming met NCSC en met de moedermaatschappij loopt. SAP DVP: aansluiting op SIEM-SOC SSC Campus loopt. (planning: voor 25/3 gereed)	
R03 CEF	Rechtstreeks misbruik van een kwetsbaarheid (ontbreken patch in de software)	- De SNPG webapp goed laten testen voordat deze in productie genomen wordt. - Inrichten dat inbreuken op de beveiliging worden gedetecteerd	12.6.1	SNPG: pentest en hertest. Status-update pentest-findings ontvangen. Bij Movianto moet dit nog plaatsvinden.	
R04 CF	Denial-of-Service DOS/DDOS aanval	- Inrichten limiet per IP adres. - Anti DDOS dienst inrichten/afnemen.	13.1.2	SNPG: limiet per IP adres is ingericht. Aanvullend onderzoek.	Mitigatie is nu nog onvoldoende.
R05 CEF	Diefstal, lezen, lekken van (gevoelige) gegevens	- Encryptie op database server inrichten - Autorisatiebeheer	8.2.3	Movianto: wordt dit getest. SNPG: nog te onderzoeken.	Mitigatie is nu nog onvoldoende.
R06 CEF	Misbruik van informatie door het ontbreken van classificatie, rubricering, werkinstructies en bewustzijn.	- Instructie aan RIVM medewerkers en medewerkers bij ketenpartners binnen het bestelproces COVID-19 Dit betreft 20 maatregelen uit de actielijst		Zowel een interne als externe werkinstructie is opgesteld.	Nog te implementeren binnen de keten.
R07 CE	Ten onrechte vaccins kunnen bestellen.	- Controles uitvoeren op authenticatie bij onboarding proces voor nieuwe bestellers	12.2.1 9.4.2	SNPG/SAP DVP: is in opzet goed ingericht.	Nog te controleren op bestaan en werking

R08 CEF	Aanpassing van gegevens, manipulatie van programmatuur voor na ingebruikname	- Inrichten van toegang middels twee factor authenticatie (2FA). - Testen bij wijzigingen - Bij wijzigingen in de code 4 ogen principe toepassen en code review uit laten voeren		Zie R01 Zie R02	
R09 CEF	Niet juist vernietigen van gegevens	- Vanuit handleiding centraal archief RIVM opnemen in werkinstructie.		Wordt opgenomen in de werkinstructie.	
R10 CF	Installatie malware met als doel, toegang tot de omgeving te verschaffen, gegevens te lekken, te vernietigen en/of "losgeld" te vragen	- Antivirus en anti malware detectie		Nog nader te onderzoeken.	
R11 CEF	Phishing (phishing, spear-phishing, whaling)	- Awareness kweken bij medewerkers (en laten doen door ketenpartners)	7.2.2 9.4.2	Op te nemen in de werkinstructie.	
R12 CEF	Afpersing van individuen om informatie beschikbaar te stellen of om bepaalde activiteiten uit te voeren (gijzeling, charge) door verbaal of fysiek agressief/gewelddadig gedrag.	- Bij poging tot afpersing contact opnemen met RIVM.	7.2.2	Op te nemen in de werkinstructie.	
R13 C	Fouten door foutgevoelige/complexe bediening	- Toepassen vier-ogen principe bij doorvoeren wijzigingen - Bijhouden wijzigingen - Waar mogelijk terughoudendheid betrachten bij verzoeken	12.1.1	SNPG/Partners4IT: in de webapp worden veel tabellen gebruikt die handmatig moeten worden onderhouden (foutgevoeligheid).	
R14 CF	Fouten door onvoldoende kennis/training; het borging van kennis	- Borgen van kennisoverdracht en voorkomen van single points of failure. - Goed documenteren van de IT en de IB omgeving en inrichting.		Vanuit het RIVM zijn adviesgesprekken gestart.	SNPG en Partners4IT zijn kleine organisaties. Movianto NL heeft maar 1 IT beheerder.
R15 CF	Verlies van informatie die misbruikt kan worden (op papier, op gegevensdragers zoals USB-sticks etc.)	- Instructie- en awareness sessies aan medewerker en door ketenpartners aan hun medewerkers		Op te nemen in de werkinstructie.	Binnen Movianto zijn en worden awareness trainingen gegeven. SNPG besluit om DepV niet te exporteren.

R16 CE	Procesfouten (onjuiste uitvoering van een procedure/richtlijnen, waardoor bijvoorbeeld een systeem foutief wordt geconfigureerd, een softwarewijziging onjuist wordt geïmplementeerd en dergelijke). Niet werken volgens voorschriften/procedures (gebrek motivatie/loyaliteit)	Testen met productiegegevens SD11, 12 en 13 + SN 12 en 27: Het volgende moet in gang gezet worden: 1. Afspraak maken met functioneel beheer SNPG om een set van 10 fakeadressen aan te maken. 2. De productiedata blijft weliswaar in SAP aanwezig in de testomgeving, maar daar wordt niet mee getest. 3. Ter informatie: aan zowel SNPG kant als aan SAP kant, zijn de functioneel beheerders betrokken die reeds toegang hebben tot de productieomgeving. 4. Printen of downloaden van data is geen onderdeel van de ketentest. Deze werkafspraak dient nogmaals te worden gemaakt.	12.1.1	De afspraken over het toepassen van 10 fakeadressen worden thans gemaakt. Voor SNPG webapp nog acties te ondernemen.	
R17 CF	Misconfiguratie van een systeem of beveiligde verbinding, waardoor een kwetsbaarheid met gevolgen voor de beveiliging van de ICT-omgeving van RIVM ontstaat (ketenpartner wordt 'stepping stone')	- Toepassen architectuurprincipes, ontwerp, toepassen segmentering en documentatie van de IT omgeving en de beveiliging ervan (oa. systeemdecompositie)		Movianto: afspraken hierover gemaakt, rechtsreeks ook advies vanuit NSCS en gezamenlijk systeemdecompositie uitgewerkt. SNPG/Partners4IT: situatie besproken en systeemdecompositie in concept uitgewerkt.	
R18 CE	Ontwerpfouten in de ontwikkeling van de software (waaronder evt. achterdeur in de programmatuur)	- Toepassen van Secure Software Development (SSD)	14.2.1	SNPG/Partners4IT: indruk is dat men de applicatie erg goed kent en daar veel in aan kan passen. Ook voor SAP DVP relevant.	
R19 CEF	Verstrekken van vertrouwelijke bestelinformatie via telefoon en/of e-mail	- Interne en externe instructie - Awareness sessies - Richtlijnen en oplossingsrichtingen voor beveiligd e-mailen (ook voor de ketenpartners)		Opnemen in werkinstructie. Adviesgesprekken kunnen bijdragen aan goed oplossingen.	
R20 A CEF	Dreiging tegen statelijke actoren (eigen set aan BBN3 maatregelen)	- Risicomanagement tijdens de gehele levenscyclus - Minimalisatie ICT omgevingen - Minimale privileges - Zelfbehoud ICT-componenten - Bescherming in lagen (defense in depth) - Actuele beveiliging technieken toepassen - Weerbaarheid en herstelvermogen		Deze maatregelen worden reeds in delen toegepast. In de komende maanden zal verdere implementatie plaatsvinden.	

Generieke maatregelen	Doorlooptijd	Opmerkingen	Status gereed
Geheimhoudingsverklaring	Weken	Voor SNPG en Movianto gereed, nog niet voor Partners4IT	70%
VOG	Weken	Voor SNPG gereed, nog niet volledig voor Movianto en Partners4IT	60%
Werkinstructie voor intern en extern (beslaat in totaal 20 maatregelen)	Dagen/weken	Er is op hoofdlijnen een werkinstructie geschreven, dit zou eigenlijk een procedure moeten zijn.	60%
ISO certificering leverancier	Maanden	SNPG -> Partners4IT: planning is om Q2 2021 ISO 270001 gecertificeerd te zijn voor ander systeem. Daarna wordt bekeken wat nodig is om de certificering ook voor SNPG te doen. Movianto: nog geen ISO27001 certificering	2%
Systeemaudit door externe partij (of verklaring van onafhankelijke derde toetsende partij; TPM)	Maanden	Voor SNPG/Partners4IT en Movianto. We halen nu de status van opzet en bestaan op. Later kan worden getoetst op werking. (de 2 punten die nog op te plannen staan)	0%

Risicomatrix

Geef in de matrix aan waar het risico zich bevindt (dit op basis van de risicoanalyse; in te vullen door CISO of FCC/S&S)

Samenvatting huidige risico's

Status risico's bestelproces COVID vaccins per 24 februari 2021

Risicomatrix

kans / impact	1 < 1 keer per 10 jaar	2 Minimaal 1 keer 5 jaar	3 Minimaal 1 keer per jaar	4 Elk kwartaal	5 Een keer per maand of vaker
3 (hoog)	R07 R08 R11 R12	R01 R02 R05 R06 R09 R10 R13 R14 R15 R16 R18	R03 R04 R17 R19 R20		
2 (midden)					
1 (laag)					

Mitigerende maatregelen niet van toepassing

Geef aan waarom geen additionele maatregelen getroffen kunnen worden en/of waarom het beleid niet geïmplementeerd kan worden

Geef dit bij voorkeur per risico aan

Niet van toepassing

Consequenties andere partijen

Geef aan of andere partijen (domeinen, centra, leveranciers, klanten) consequenties kunnen ondervinden van dit risico

Geef dit bij voorkeur per risico aan

Mogelijke issues of incidenten kunnen de beeldvorming / het imago van de leveranciers (Movianto en Partners4IT) negatief beïnvloeden.

Periode

Geef aan voor welke periode de risicoacceptatie moet gaan gelden en wat de einddatum van deze acceptatie is

Deze risicoacceptatie geldt vanaf 25 februari 2021 en is geldig tot en met maandag 1 mei 2021. In de komende maanden zullen (continuerend en deels iteratief) nadere analyses en testen worden uitgevoerd.

Evaluatie

Geef aan wanneer en op welke wijze evaluatie van het restrisico zal gaan plaatsvinden

In doorloop zullen de komende weken gapanalyses en risicoanalyses plaatsvinden, maatregelen geïmplementeerd en testen uitgevoerd worden en daarbij afstemming met de verantwoordelijken. Relevante restrisico's worden geregistreerd in het risicoregister, de voortgang op mitigerende maatregelen wordt actief bewaakt. Er wordt een coördinator aangesteld om het IB&P-proces te begeleiden en maatregelen te implementeren.

Gevraagd besluit:	**Akkoord te gaan met het accepteren van de benoemde (rest)risico's voor informatiebeveiliging zoals deze nu bekend zijn van het bestelproces van de COVID vaccins.**		
Partij	***Naam***	***Mening*** *(invullen door Hoofd centrum, CISO, CIO, Compliance, Legal, Privacy en DR)*	***Akkoord***
Hoofd DVP	5.1.2e 5.1.2e		Akkoord: ja/nee
Centrumhoofd CvB	5.1.2e		Akkoord: ja/nee
CISO *(mandatory voor alle risk levels)*	5.1.2e		Akkoord: ja
Privacy Officer	Nvt		Akkoord: nvt
CIO *(mandatory voor medium en hoger risico)*	5.1.2e		Akkoord: ja/nee
Programmadirecteur COVID-19 vaccinatie	5.1.2e 5.1.2e		Akkoord: ja/nee
CFO/Hoofd Bedrijfsvoering/Plv. DG	5.1.2e 5.1.2e		Akkoord: ja/nee
DR *(mandatory voor hoog en zeer hoog risico)*			