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

AANVRAAGFORMULIER RISICOACCEPTATIE – 17 januari 2021 **Departementaal Vertrouwelijk**

Betreft:	Bestelproces COVID vaccins (aanvullende acceptatie)	
Aanvrager:	5.1.2e	
Aanvraagnummer:	20210114-01 RACC Bestelproces COVID Vaccins	
Datum aanvraag:	28-12-2020 (initieel)	
Centrum:	DVP	CvB
Systemen	Formdesk, DVP-SAP, Winshuttle en Movianto SAP	SNPG Webapp
Verantwoordelijk lijnmanager:	5.1.2e 5.1.2e	
Verantwoordelijk centrum- of afdelingshoofd:	5.1.2e 5.1. 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	
T.b.v. vergadering:	Besluitvormend overleg 17 januari 2021	
Aantal pagina's:	8	
Notitie toegevoegd:	Actielijst	
Versienummer:	0.5	
Datum laatst gewijzigd:	17-01-2021	

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, leveranciersinformatie, grootschalige opslag, beheer en vervoer. Voor statelijke actoren of criminelen 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

20210114-01 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 vanag 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 veel risico's nog niet in detail beschreven en 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.

Beschrijving van het bestelproces
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 Griepppreventie.

Formdesk wordt enerzijds als rekentool gebruikt waarmee DVP-medewerkers bij het bestelde aantal vaccins het correcte naalden, spuiten en oplosmiddel e.d. kunnen berekenen voordat ze het in Excel inlezen.
Anderzijds kan Formdesk in de toekomst als bestelformulier gebruikt worden door externe klanten die nog niet binnen de SNPG Webapp vallen.

De bestelgegevens vanuit de SNPG Webapp of uit Formdesk 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 e-mail een Excelbestand van DVP waarna zij de gegevens in hun eigen SAP-systeem invoeren. Met deze gegevens kunnen chauffeurs de bestelde vaccins en toebehoren bij de klanten afleveren.

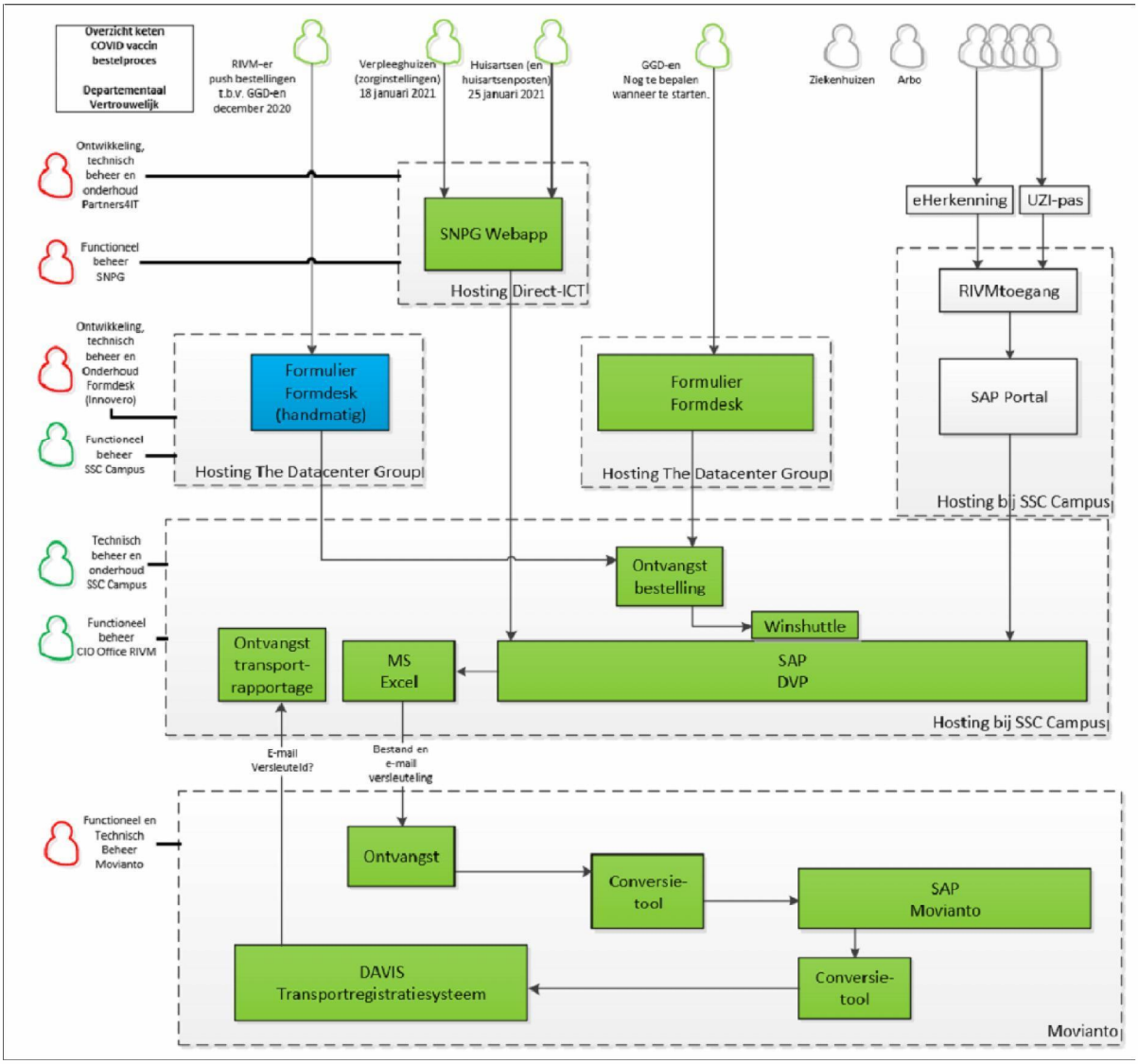
Voor het bestellen en distribueren van de COVID-vaccins zijn drie ketens uitgewerkt, zie onderstaand overzicht. Voor alle ketens geldt dat het om gegevens gaat over hoeveelheid vaccins en toebehoren (optrek/toedieningsnaalden en -spuiten en oplosmiddelen) en NAW-gegevens van de klant (GGD, huisarts,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

Buiten scope:
De SAP portal welke zal worden gebruikt als keten 3. Deze is nog in ontwikkeling.
De 'chauffeursapp' is een interne app gekoppeld aan SAP waarmee de regiokantoren werken. Deze app wordt niet voor de COVID vaccins gebruikt en zal dus niet meegenomen worden in de risicoanalyse.

Verantwoordelijkheden

- De COVID-programmacoördinator is 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.

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



Informatiebeveiliging en risico's

Voor het proces van de NSPG webapp op 6 oktober 2020 de Quickscan BIO uitgevoerd en een risicoanalyse uitgevoerd (22, 29 oktober en 11 november) 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, is op 24 december 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. Gezien de haast te starten met het leveren van de COVID-vaccins aan de GGD-en voor de eerste vaccinatietranche is besloten om, ondanks de openstaande issues, de bestellingen en distributie volgens keten 2 (zie figuur 1 hieronder) vanaf eind december 2020 in gang te zetten. Formdesk kan hierbij door DVP 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.

Privacy

De contactgegevens/persoonsgegevens binnen het proces worden uitsluitend in het kader van de afhandeling van de bestelling verwerkt.
De privacy coördinatoren van CvB (5.1.2e ; 16 november) en DVP (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.

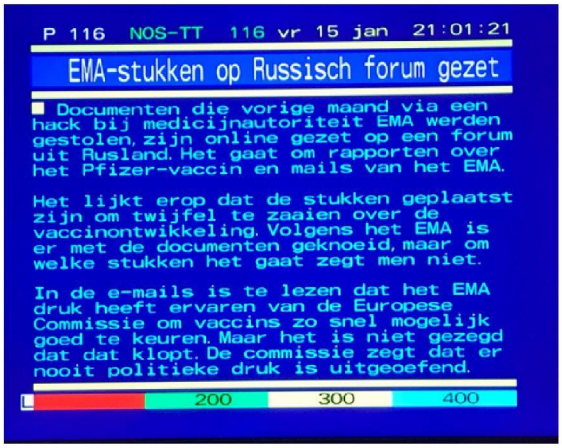
Er moet een DPIA worden uitgevoerd als aan twee of meer van onderstaande criteria wordt voldaan:

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

Ref.	Omschrijving	Risico	Mitigerende maatregelen aanwezig	Uit te voeren acties/te implementeren maatregelen
R-A	Dreigingen vanuit statelijke actoren (en activisten/ antivaxxers)	Dreigingen vanuit statelijke actoren manifesteren zich steeds meer. 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. Het doel hierbij varieert van het verspreiden van misleidende informatie (m.b.t. de vaccindistributie) 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.	- Met inachtneming van BBN3 dreigingsniveau nadere risicoanalyses uitvoeren; NB, BBN3 maatregelen staan qua zwaarte meer naast dan boven BBN2 - Informatieclassificatie Departementaal Vertrouwelijk (DepV) en het bijbehorend normenkader hanteren en assessments uitvoeren - 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 overall procesplaat van het bestelproces is gemaakt	- Bij het nemen van besluiten dient het management van belang van de consequenties voor informatiebeveiliging meenemen, de juiste partijen aanhaken en dit tijdig communiceren. - Een gedetailleerde systeemdecompositie uitwerken waarin de gehele keten in scope wordt nemen (w.o. ook de ontwikkeling van de SAP portal)

R-C	Beveiligingsniveau 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.	- Uitgevoerde risicoanalyse op SNPG webapp - BBN2 - Pentest is uitgevoerd en er is hertest. De meest belangrijke bevindingen zijn opgelost - SNPG en Partner4IT zijn ISO 27001 gecertificeerd - DepV assessment is uitgevoerd	- Nadere risicoanalyse uitvoeren met inachtneming van BBN3 dreigingsniveau, maatregelen implementeren (of zo nodig accepteren) - Monitoren openstaande midden en laag bevindingen pentest - Toepasselijkheidsverklaring opvragen
R-D	Beveiligingsniveau Formdesk formulier COVID bestellingen.	Formdesk gaat door GGD-en gebruikt worden om COVID vaccins te bestellen en dient weerbaar te zijn tegen dreigingen vanuit statelijke actoren.	- Voor Formdesk is een risicoanalyse uitgevoerd en zijn meerdere pentesten uitgevoerd - De formulieren van het RIVM staan bij Formdesk op een dedicated server - DepV assessment is deels uitgevoerd	- DepV assessment afronden - Nadere risicoanalyse uitvoeren met inachtneming van BBN3 dreigingsniveau, maatregelen implementeren (of zo nodig accepteren)
R-E	Beveiligingsniveau SAP DVP en Winshuttle	SAP DVP en Winshuttle zijn 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.	- Een versneld assessment voor deze applicaties is in gang gezet. Winshuttle is ISO 27001 gecertificeerd. Zowel de scope als de toepasselijkheids-verklaring geven in eerste instantie een goed en vertrouwd beeld.	- DepV assessment uitvoeren - Nadere risicoanalyse uitvoeren met inachtneming van BBN3 dreigingsniveau, maatregelen implementeren (of zo nodig accepteren)
R-F	Beveiligingsniveau 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/cybersecuri ty zijn toen niet beoordeeld. NB: de vaccinatie- en preventieprogramma's lopen al jaren 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 uitvoeren en risicoanalyse BBN3 uitvoeren, maatregelen implementeren (of zo nodig accepteren) - Interfacing (koppeling) tussen SAP RIVM en SAP Movianto realiseren - Beveiliging e-mail verkeer transportgegevens (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 - PM maatregelen (o.a. uit rapport AIVD)

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)

Overzicht huidige risico's:

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 G	B D 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
G: Afgifte vaccins

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

De beoogde datum van gebruik is 18 januari 2021.

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 Formdesk) 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 livegang per 18 januari 2021 en is geldig tot en met 31 januari 2021.
In de komende weken zullen (deels iteratief) 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.

Gevraagd besluit:	- Akkoord te gaan met het accepteren van de benoemde (rest)risico's voor informatiebeveiliging zoals deze nu bekend zijn voor de start van het bestelproces van de COVID vaccins; het bestellen door verpleeghuizen vanaf maandag 18 januari en huisartsen vanaf 25 januari 2021.		
Partij	***Naam***	***Mening** (invullen door Hoofd centrum, CISO, CIO, Compliance, Legal, Privacy en DR)*	***Akkoord***
Hoofd DVP	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/nee
Privacy Officer	nvt		Akkoord: nvt
CIO *(mandatory voor medium en hoger risico)*	5.1.2e		Akkoord: ja/~~nee~~
CFO/Hoofd Bedrijfsvoering	5.1.2e		Akkoord: ja/nee
DR *(mandatory voor hoog en zeer hoog risico)*	5.1.2e		Akkoord: ja/nee