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

A. van Leeuwenhoeklaan 9
3721 MA Bilthoven
Postbus 1
3720 BA Bilthoven
www.rivm.nl

KvK Utrecht 30276683

T 5.1.2e
5.1.5 @rivm.nl

nota

Risicoacceptatie IB&P bestelproces Covid-19 vaccins

Nota nummer	DPV_211i Besluitnota risicoacceptatie IB&P bestelproces Covid-19 vaccins
Aan	5.1.2e
Van	5.1.2e

Datum
26 mei 2021

Ons kenmerk
DVP-211i Risicoacceptatie IB&P bestelproces Covid-19 vaccins

Classificatie
Departementaal Vertrouwelijk

Gevraagd besluit:
Er wordt gevraagd om:

- Kennis te nemen van de gehanteerde systematiek waarmee gekozen wordt om de openstaande maatregelen uit te voeren of voor langere termijn te accepteren
- Een besluit te nemen over het nog uitvoeren van de maatregelen of niet (en dus de restrisico's voor langere termijn te accepteren)
- De restrisico's van het bestelproces van de Covid-19 vaccins accepteren tot 1 augustus 2021 (voor maatregelen die nog uitgevoerd gaan worden)
- De overige restrisico's voor accepteren tot 1 april 2022 (voor maatregelen die niet uitgevoerd gaan worden)
- sturing te geven aan de implementatie van resterende maatregelen bij externe partijen

Achtergrond
Historie risicoacceptatie
Het bestelproces Covid19-vaccins moet zoals bekend voldoen aan strikte beveiligingsmaatregelen vanwege de BBN3-classificatie die voor dit proces geldt. De extra complicerende factor hierin betreft het feit dat er in een keten gewerkt wordt waarbij RIVM-DVP, Movianto en SNPG de belangrijkste spelers zijn. Geconstateerd zijn diverse tekortkomingen bij deze ketenpartners waar melding van is gemaakt en opgenomen in de lijst 5.1.2h De afgelopen periode is door het projectteam bestelproces hard gewerkt aan het vaststellen van de aard van de maatregelen, het plannen en tot uitvoer brengen (waar mogelijk) van deze maatregelen en het adviseren over maatregelen die (nog) niet kunnen worden opgepakt. Een belangrijk aspect hierbij is de vraag: in hoeverre is RIVM sturend in het laten oppakken van mitigerende maatregelen door ketenpartners, in het bijzonder Movianto en de hostingpartij van SNPG, P4IT?

Datum
26 mei 2021

Ons kenmerk
DVP-211i Risicoacceptatie IB&P bestelproces Covid-19 vaccins

Classificatie
Departementaal Vertrouwelijk

Te nemen maatregelen: opzet systematiek tbv business case
Er is een indeling gemaakt van de lijst met risico's op basis waarvan een besluit kan worden genomen over het al of niet te accepteren risico's. De indeling is als volgt:

1. Voortgang groen (voldoende voortgang/maatregel bijna gereed): risico mitigeren (maatregel implementeren).
2. Basisniveau maatregelen die elk volwaardig (IT) bedrijf geïmplementeerd zouden moeten hebben: risico mitigeren (maatregel implementeren).
3. Overig – voorstel risico mitigeren of accepteren op basis van criteria met puntentelling.

Om meer duiding te kunnen geven aan de implicaties van de te nemen maatregelen is een systematiek opgezet waarbij gekeken wordt naar:

1. Restrisico na implementatie (geen/klein/groot) - 0/5/10p pnt
2. Impact op organisatie (klein/middel/groot) - 0/5/10 pnt
3. Kosten eenmalig (1K/10K/50K/100K) - 0/5/10/15 pnt
4. Tijd eenmalig (dg/wk/mnd) - 0/5/10 pnt
5. Kosten jaarlijks (1k/10K/50K/100K) - 0/5/10/15 pnt
6. Tijd jaarlijks (dg/wk/mnd) - 0/5/10 pnt
7. Meerwaarde onder BBN2 (ja/nee) - 0/10 pnt
8.

Voor elk van deze onderwerpen zijn punten gegeven per risico waarvan aangegeven is dat de maatregelen nog niet zijn uitgevoerd of waarvan duidelijk is dat de maatregel tot het basisniveau IT behoort.

Uitwerking
Het document *Gebruikte systematiek en voorstel* geeft op basis van het totaaloverzicht zoals opgenomen in de excel *Maatregelen bestelproces 20210528 v0.1* een handzaam overzicht van de risico's die om specifieke aandacht vragen. De specifieke aandacht richt zich dan op 2 zaken:

1. Een ketenpartner is betrokken, in hoeverre gaat het RIVM hierin sturend optreden.
2. Geld speelt een grote rol bij het evt. mitigeren van het risico. Dit geldt zowel voor een aantal activiteiten bij het RIVM als bij de ketenpartner.

Tabel 3 in het document *Gebruikte systematiek en voorstel* bijvoorbeeld geeft duidelijk aan dat er gevraagd wordt om een basisniveau van informatiebeveiliging bij de ketenpartners.

Vervolgstappen
Het verdient aanbeveling de volgende stappen in overweging te nemen na vaststelling van de restrisico's:

1. Stel per te nemen maatregel een verantwoordelijke aan
2. Met Movianto en SNPG worden contractuele afspraken gemaakt
3. Vanuit RIVM vindt sturing plaats
4. Het risico-acceptatieformulier is leidend en wordt in beheer genomen.