



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

nota

Risicoacceptatie IB&P bestelproces Covid-19 vaccins

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

KvK Utrecht 30276683

T 5.1.2e
info@rivm.nl

Nota nummer	DPV_211h Besluitnota risicoacceptatie IB&P bestelproces Covid-19 vaccins 29-04-2021 v0.1
Aan	5.1.2e, 5.1.2e, 5.1.2e, 5.1.2e, 5.1.2e, 5.1.2e, 5.1.2e
Van	5.1.2e, 5.1.2e, 5.1.2e, 5.1.2e, 5.1.2e, 5.1.2e, 5.1.2e Projectteam bestelproces: 5.1.2e, 5.1.2e, 5.1.2e 5.1.2e, 5.1.2e, 5.1.2e, 5.1.2e, 5.1.2e

Datum
28 april 2021

Ons kenmerk
DVP-211h Risicoacceptatie
IB&P bestelproces Covid-19
vaccins 29-04-2021 v1

Classificatie
Departementaal Vertrouwelijk

Beste lezer,

Gevraagd besluit:

Er wordt gevraagd om:

- de 20 restrisico's van het bestelproces van de Covid-19 vaccins te accepteren tot 1 juli 2021,
- een besluit te nemen over het gebruik van UPS voor de opslag en de uitlevering van Covid-19 vaccins aan uitvoerders (groepsrisico 21)
- sturing te geven op de implementatie van resterende maatregelen bij externe partijen
- in te stemmen dat het bestelproces onverminderd gebruikt kan worden voor het bestellen van de Covid-vaccins.

Achtergrond

Doel en uitbreiding scope

De scope van de risicoanalyse betreft de logistieke keten die binnen de invloedssfeer van het RIVM valt. Dit betreft het bestellen van de Covid-19 vaccins via de SNPG Webapp, via push-bestellingen waarbij DVP'ers de bestelling zelf in SAP plaatsen, of via telefoon. Ten opzichte van de vorige risicoacceptatie (d.d. 25 februari 2021) is de scope uitgebreid met de SAP Bestelmodule waarmee uitvoerders zelf vaccins kunnen bestellen. IB is vanaf het begin betrokken geweest bij de opzet. Op termijn moet de bestelmodule achter RIVM Toegang gaan draaien, maar voor de huidige risicoacceptatie valt RIVM Toegang nog buiten scope.

De bestelinformatie wordt vervolgens doorgezeten en verwerkt door logistiek dienstverlener Movianto. Het afleveren van de vaccins bij de uitvoerders valt buiten scope van de risicoanalyse. De scope is verder uitgebreid met UPS als tweede logistiek dienstverlener. VWS heeft RIVM opdracht gegeven een tweede partij in te huren om de continuïteit van het uitleveren van de vaccins te garanderen, mochten zich logistieke problemen voordoen bij Movianto. Zomer 2020 (ruim voor aandacht

Datum

6 april 2021

Ons kenmerkDVP-211h Risicoacceptatie
IB&P bestelproces Covid-19
vaccins 29-04-2021 v1

Classificatie

Departementaal Vertrouwelijk

kwam voor IB&P van het bestelproces) werd UPS ingehuurd als extra opslaglocatie voor de Covid-19 vaccins. Het is niet haalbaar om de twee delen van de logistieke keten (opslag en levering) bij verschillende partijen onder te brengen. Daarom is het streven de eerste opdracht aan UPS (opslag) uit te breiden met het uitleveren van vaccins aan de uitvoerende partijen. Bij de laatste audit t.b.v. het fysieke proces is een kritische bevinding gevonden. Het formele audittraject wordt gevolgd en de verwachting is dat eind april kan worden besloten of de opdracht aan UPS verleend kan worden. Het al dan niet accepteren van de restrisico's voor IB&P moet worden meegenomen in dit besluit.

Analyse van de informatiebeveiligingsrisico's

In bijlage 1 is het risicoacceptatieformulier gegeven. Sinds de vorige risicoacceptatie van 25 februari 2021 heeft VKA de systeemdecompositie uitgebreid met de SAP Bestelmodule en UPS. In tabel 1 staan de openstaande actiepunten t.o.v. de vorige risicoacceptatie.

Tabel 1. Huidige status van de actiepunten.

Risicogroep	Aantal openstaande acties 24/2/2021	Aantal openstaande acties 28/4/2021
- Set statelijke actoren (BBN3)	- 25	- 25
- DepV – SNPG webapp (incl. findings RA – BBN2 en pentest findings)	- 36*	- 20
- DepV – SAP DVP	- 14	- 14
- DepV – SAP Movianto	- 5	- 5
- Site visit Movianto + analyse NBV (AIVD)	- 10	- 11**
- UPS	-	- ?

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

- **status SFTP server

In de hieronder gegeven risicomatrices zijn de risico's per februari 2021 en per 28 april 2021 gegeven. Voor UPS kan enkel nog een groepsrisico aangegeven worden. Het overall risicobeeld is vrijwel constant gebleven. Het projectteam constateert dat de voortgang in het realiseren van maatregelen stagneert (zie bespreekpunt 2 hieronder).

Datum

6 april 2021

Ons kenmerkDVP-211h Risicoacceptatie
IB&P bestelproces Covid-19
vaccins 29-04-2021 v1**Risicomatrix IB Risicoanalyse – analyse per 24.01.2021**Status risico's bestelproces COVID vaccins per 24 februari 2021

Risicomatrix					
kans	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)					

Classificatie

Departementaal Vertrouwelijk

Risicomatrix IB Risicoanalyse – analyse per 28.04.2021Status risico's bestelproces COVID vaccins per 28 april 2021

Risicomatrix					
kans	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 R10 R11 R12	R01 R02 R06 R09 R13 R14 R15 R16 R17 R18 R19	R03 R04 R05 R20	R21	
2 (midden)					
1 (laag)					

Bespreekpunten**1. Openstaande IB-risico's UPS**

IB&P is sinds 14 april betrokken bij het traject van opdrachtverlening aan UPS. Hierop heeft VKA de systeemdecompositie uitgebreid met UPS. Op dit moment kan voor UPS enkel een (hoog) groepsrisico voor IB ingeschat worden. Ook voor privacy bestaat een risico. UPS is een Amerikaans bedrijf waarvan de relevante servers enkel in de VS staan. Het kan daardoor niet uitgesloten worden dat data opgevraagd zal worden door de Amerikaanse staat. Het gaat om NAW-gegevens, waardoor het privacy-team het risico als laag inschaalt. De gegevens zijn met weliswaar ook vindbaar via bv. internet, maar in hun totaliteit geven ze wel een overzicht van het Nederlandse zorgsysteem.

Het alternatief voor UPS is geen back-up voor Movianto inregelen. De opdracht bij een Nederlandse of Europese partij onderbrengen vraagt maanden voorbereidingstijd. Daarnaast bleek uit het Europees aanbestedingstraject dat er nauwelijks (geen) partijen zijn die op grote

Datum

6 april 2021

Ons kenmerkDVP-211h Risicoacceptatie
IB&P bestelproces Covid-19
vaccins 29-04-2021 v1

schaal en met voldoende kwaliteit de logistiek van vaccins kunnen organiseren.

2. Afnemen voortgang in realisatie van IB maatregelen

Uit de risicomatrix wordt duidelijk dat het overall risicobeeld vrijwel constant is t.o.v. de vorige risicoacceptatie. In Discussienota DPV_211g van 6 april 2021 (zie bijlage 3) heeft het projectteam al gesignaleerd dat de voortgang in de realisatie van de oplossingen voor informatiebeveiliging afneemt. De vraagstukken die hierbij spelen zijn:

Classificatie
Departementaal Vertrouwelijk

- Wegen de kosten die gemaakt worden op tegen de waarschijnlijkheid dat dreigingen zich manifesteren? Dit vooral vanuit het beeld van het mogelijke tijdelijke karakter van de dreigingen
- Daar waar nu samengewerkt wordt met relatief kleinschalige partners/leveranciers, wordt capaciteit die ingezet wordt voor mitigerende maatregelen/oplossingen van risico's op het gebied van informatiebeveiliging weggehaald bij de uitvoering. Dit geldt bijvoorbeeld bij SNPG en partners 4 IT. Is dit wenselijk?
- Hoe lang blijft dit proces op BBN3 niveau en/of classificatie departementaal vertrouwelijk en worden geen acties in gang gezet die gereed zijn op moment risico's niveau's mogelijk weer worden afgeschaald?
- Een aantal partners ziet de noodzaak voor een aantal maatregelen niet. Het RIVM zal indien RIVM ze de acties noodzakelijk acht, dit als opdracht moeten uitzetten.
- Ook binnen het projectteam zien we dat tijd en aandacht in toenemende mate verdeeld moeten worden tussen activiteiten t.b.v. de uitvoering van het vaccinatieprogramma en activiteiten om IB-risico's te mitigeren. Daarbij breidt het werk zich uit door acties die voortkomen uit nieuwe onderdelen van het bestelproces (de SAP-bestelmodule en UPS).

Inmiddels is bekend dat de NBV het dreigingsniveau voor het bestelproces als onverminderd hoog ziet wat betekent dat maatregelen niet kunnen worden afgeschaald. De directeuren wordt gevraagd sturing en prioritering te geven aan de implementatie van resterende maatregelen bij externe partijen.