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

AANVRAAGFORMULIER RISICOACCEPTATIE

Betreft:	Ad hoc oplossing CIMS-IT/ oproepen en (doen) verzenden oproepbrief door Xerox B.V. [batch 19/20 januari 2021] (verlenging aanvraag voor batch 28 januari 2021). Extra verlening voor batch 75-80 jarigen (mat-datum 18 februari)
Aanvrager:	Stuurgroep CIMS o.l.v. 5.1.2e (CFO)
Telefoonnummer:	
Aanvraagnummer:	
Datum aanvraag:	18-1-2021. Verlenging 26-01-201. Tweede verlenging 08-02-2021
Naam verantwoordelijk lijnmanager:	Nader te bepalen
Naam centrum- of afdelingshoofd:	Nader te bepalen
Centrum:	Nader te bepalen
Naam informatiemanager:	N.v.t.
Doel:	risicoacceptatie
Aan:	Stuurgroep COVID registratie
T.b.v. vergadering:	Stuurgroep COVID registratie – maandag 18 januari 2021 12u30 (in aanwezigheid van andere aanwezigen RIVM)
Aantal pagina's:	4
Notitie toegevoegd:	20210115 concept Versnelde IB en P analyse voorlopige oplossing selecteren en oproepen.docx & advies privacy officer 15.1.2021 keuze drukker 20210128 Verlenging op deze risico acceptatie aangevraagd voor tweede batch uitnodigingen bestaande uit een oplagen van 450.000 20210209 Verlenging op deze risico acceptatie aangevraagd voor derde batch uitnodigingen bestaande uit een oplagen van ~800.000 20210222 Gemaakte mitigerende maatregelen voor opstaande risico's
Versienummer	1.4
Datum laatst gewijzigd	22-2-2021

Context

Veranderde vaccinatiestrategie
De vaccinatiestrategie is aan verandering onderhevig. RIVM is gevraagd om versneld een selectie en oproep van een nog nader vast te stellen doelgroep mogelijk te maken.

Nog te bepalen doelgroep
De vaststelling om welke doelgroep het gaat, wordt op 19.1.2021 verwacht. Hierover worden ten tijde van het opstellen van onderhavig risico-acceptatieformulier, nog onderhandelingen gevoerd met stakeholders (bron: R. Riesmeijer). Het is belangrijk vast te stellen dat onderhavige risicoacceptatie *alleen* betrekking heeft op deze eerste batch van te printen brieven. Bij vervolgbatches zal de IB&P nader uitgewerkt en de risico's opnieuw geaccepteerd moeten worden.

CIMS nog niet gereed
De bouw van de functionaliteit selecteren & oproepen in CIMS is gepland met inachtneming van het oorspronkelijke vaccinatieschema. Deze functionaliteit is nog niet gereed. Een ad hoc oplossing moet de versnelde selectie en oproep mogelijk maken.

Doorlooptijd tussen VWS opdracht en verzending oproepbrief
Tussen het moment van het geven van een opdracht tot selecteren en oproepen en het moment dat de oproepbrieven worden verzonden, zit minimaal 2 weken. Het RIVM heeft – wanneer het testbestand goed verloopt – naar verwachting 2 dagen nodig voor het selecteren van de doelgroep. De drukker heeft 2 weken nodig om de oproep te printen en te (laten) verzenden.

Wijziging mantelpartijen
De inkoop van o.a. drukwerkdiensten geschiedt Rijksbreed. Dit is belegd bij het Ministerie van VenJ.
Het lopende contract (uit 2014) is geëxpireerd. Het nieuwe contract is op dinsdag 19 januari 2021 getekend door Xerox en min. JenV en in het bezit van het RIVM, inclusief een aanvullende verklaring over de werkwijze van Xerox.

Verscherpte eisen
Uit recente jurisprudentie blijkt dat het door de Verenigde staten geboden beschermingsniveau niet passend wordt geacht in de zin van de AVG. Freedom Act is ook een punt van aandacht.

Stuurgroep Registratie besluit d.d. 15.1.2021
De Stuurgroep Registratie heeft op 15.1.2021 besloten om onder de gegeven omstandigheden een versnelde risico-analyse Informatiebeveiliging en privacy te laten uitvoeren nu op zo'n korte termijn een uitvoerige(r) analyse zoals verdere IB analyse en een DPIA niet mogelijk waren. De scope van deze analyse bestaat uit het door CIMS IT ondersteunde deel van het proces selecteren en oproepen en beslaat dus (nog) niet het gehele proces van uitnodigen van A tot Z. Deze IB&P-analyse dient uitgebouwd te worden tot het gehele proces en op korte termijn (eind januari / begin februari 2021) dient er opnieuw een risico-acceptatie plaats te vinden.

Resultaat versnelde risico-analyse Informatiebeveiliging en privacy

- Xerox B.V. is 100 % (indirect) eigendom van Xerox Corporation, gevestigd in de VS.
- Versnelde risico-analyse IB & P versie 14.1.2021
- Als bijlage: '20210115 concept Versnelde IB en P analyse voorlopige oplossing selecteren en oproepen.docx'; als bijlage advies keuze drukker 15.1.2021.

Aanvullende opmerkingen of randvoorwaarden

- Risico-acceptatie ziet op de verwerkingen / dat deel van het proces selecteren en oproepen voor zover deze door CIMS IT worden ondersteund.

- In de risico-acceptatie wordt uitgegaan (**aanname**) van AVG en BIO conforme afspraken in de mantelovereenkomst tussen VenJ en Xerox (inclusief subverwerkers).

  Niet gebleken is dat in de volgende punten is voorzien:

- Er is een vernieuwde versie van de Patriot Act in werking getreden, genaamd Freedom Act. Amerikaanse autoriteiten hebben onder bepaalde voorwaarden toegang tot persoonsgegevens die zijn opgeslagen buiten de VS. Mitigerende maatregelen kunnen niet worden getroffen om de toepasselijkheid van de Freedom Act verhinderen.

- Het risico voor rechten en vrijheden van betrokkenen wordt ingeschat als laag omdat de kans dat deze situatie zich zal voordoen, verwaarloosbaar lijkt. De impact kan wel groot zijn, gezien de grootschaligheid (aantal burgers) van de verwerking.

- Het risico voor min. VWS & RIVM: wordt ingeschat als gemiddeld/hoog. Het gunnen van een dergelijke opdracht aan Xerox is slecht te rechtvaardigen als er een alternatieve partij is die wel conform AVG kan leveren, ook als de risico's voor de betrokkenen gering zijn.

- Er is op dit moment aanwezig binnen RIVM t.a.v. contracten met printpartijen:

1. Een raamovereenkomst Rijksbreed voor **standaard mail** met Xerox.

2. Een raamovereenkomst RIVM via Europese aanbesteding **voor transactiemail** met Adcomm, deze loopt af op een onbekend moment.

3. Een raamovereenkomst RIVM via Europese aanbesteding **voor transactiemail** met Impress, deze is ingegaan op 01-10-2020, RIVM (DPV) zit nog in implementatieperiode; in de week van 18 januari 2021 gaat de eerste brief de deur uit).

De mailing die RIVM wil versturen t.b.v. COVID-vaccinatie betreft een standaardmailing en behoort dus bij Xerox. Op het moment dat RIVM een keuze maakt voor Impress of Addcom wordt de opdracht bestempeld als onrechtmatig. Dit betekent dat er een goedkeuring om hiervan af te wijken van de CFO RIVM nodig is, zodat dit verantwoord kan worden naar VWS. Dit risico is

afgewogen – zie onder.

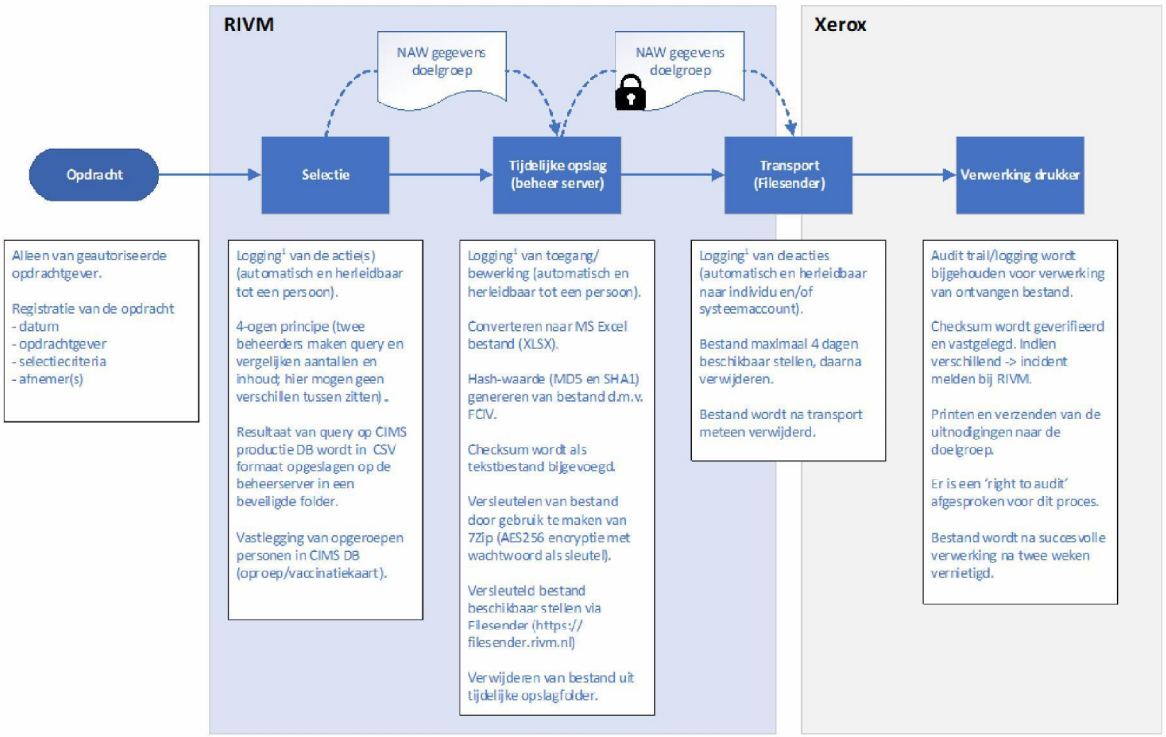
Aanvraagnummer *Geef aan onder welk nummer de aanvraag al in het risk register staat of dat het een nieuwe aanvraag betreft*
Nieuwe aanvraag onder nummer 20210119-01 RACC Xerox

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*
Zie context.

Systeemdecompositie

Systeemdecompositie van het betreffende informatiesyste(e)m(en) [vervang het voorbeeld]

Selecteren en uitnodigen van vaccinatiedoelgroep op basis van leeftijd (tijdelijke oplossing)



Aanvullende informatie

- Bovenstaande afbeelding geeft het oorspronkelijke ontwerp weer voor de tijdelijke oplossing.
- **Transport** van het bestand zal verlopen via een SFTP server die is ondergebracht bij een Nederlandse organisatie (geïnstalleerd op een zgn. Cloud VPS). Filesender zal dus niet gebruikt worden.
- **Aanvullende verklaring (in bezit RIVM) vanuit Xerox**:

  (1) Gegevens die onder het contract worden uitgewisseld maken geen deel uit van het Xerox netwerk. Data wordt uitgewisseld via een secure FTP server; welke gehost wordt bij een Nederlandse Organisatie (Cloud VPS). De e-mail uitwisseling (met b.v. de orderdesk) verloopt via een @xnloverheid account; bij Freedom Internet Hosting Services.

  (2) Bewaren data op server. De data op de server wordt automatisch na 14 dagen verwijderd. De 14 dagen is noodzakelijk voor eventuele analyse; bijvoorbeeld bij fouten.

Risico's	**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*
Ongeautoriseerde inzage van persoonsgegevens.	In dit proces zijn een aantal momenten waar een risico is op mogelijke onrechtmatige inzage van de (persoons)gegevens. Hiervoor zijn de volgende mitigerende maatregelen getroffen: - Toegang tot dataset door databasebeheerders (van Ordina) is beperkt tot twee personen. Logging van activiteiten is actief. - 4-ogen principe hanteren. - Het gegenereerde bestand (na selectie) wordt versleuteld opgeslagen. - Transport naar SFTP-server is versleuteld. Dataset zelf is ook voorzien van

	versleuteling (AES-256). **Update 22-02-2021** In de memo "Risicoanalyse informatiebeveiliging CIMS 2.0 van 14 februari is geconcludeerd dat de IB risico's voor het proces 'selecteren en oproepen' waarvoor nog een risicoacceptatie geldt zijn opgelost en kunnen worden afgesloten.
Verwerking van persoonsgegevens buiten de Europese Economische Ruimte (EER)	Om het risico van mogelijke verwerking van de dataset buiten de EER te mitigeren is door Xerox aangegeven dat er een derde (Nederlandse) partij ingeschakeld die de SFTP-server beschikbaar stelt. De dataset wordt vanaf deze server benaderd en geprint door Xerox. (brief van dhr. A. Vlaander van 18.1.2021 aan dhr. A. Frencken en dhr. W. Bavelaar; mail van A. Vlaander van 18.1.2021, 15:41 uur aan J.L. van Egmond): *"De data zijn ook in geval van back-up of fail-over voor rekening van de Nederlandse organisaties die ik in mijn brief noem. Daar is Xerox niet bij betrokken! In geval van productie voor een mailing bijvoorbeeld, worden de gegevens vanaf de server naar de printer gestuurd en na het afdrukken; wordt de queue gedeelte van de printer. Aangezien we de data niet hebben, het ons eigendom niet is, kunnen we deze ook niet onder de Freedom Act overhandigen. Juist voor dit contract hebben we onze organisatie zodanig ingericht."* Er is expliciet aan Xerox verzocht om de geleverde dataset niet op te slaan op de eigen IT infrastructuur. Deze set mag op geen enkele wijze opgenomen worden in een backup. Dataset wordt na maximaal 14 dagen na verzending oproepbrief verwijderd van de SFTP-server. **Update 22-02-2021** Een extra verwerkersovereenkomst met Xerox is opgesteld tbv het COVID vaccinatie programma om dit risico te mitigeren. 5.1.2e: "Op basis van opzet en bestaan van afspraken, komen we tot de slotsom dat de "Aanvullende informatie aangaande databehandeling en beveiliging t.b.v. de oproepen voor COVID-vaccinatie. Als aanvulling op de afspraken vastgelegd ten behoeve van het contract Grafische Dienstverlening; 502599", een correcte weergave is van de aanvullende eisen die het RIVM aan inrichting en beveiliging stelt voor de verwerking van oproepbrieven COVID – 19. "
Toegang Amerikaanse overheid tot persoonsgegevens	Mail van 5.1.2e van 18.1.2021, 15:41 uur aan 5.1.2e - zie bovenstaand citaat. **Update 22-02-2021** Zie update voorgaande punt. Een extra verwerkersovereenkomst met Xerox is opgesteld tbv het COVID vaccinatie programma om dit risico te mitigeren.
Onrechtmatige inkoop door RIVM	Er is in de periode 15 tot en met 18 januari 2021 in overleg met inkoop RIVM onderzoek gedaan naar het op korte termijn inzetten van de twee reguliere partijen (Impresse en Adcom) die DVP regelmatig inzet voor haar drukwerk. RIVM mag op jaarbasis maar minimaal afwijken van een raamovereenkomst waardoor dit een zeer onwenselijk situatie is. Bij overgaan tot optie 2 en 3 (zie eerder) is het risico dat Xerox bezwaar aantekent, een rechter kan overgaan tot ontbinding van de overeenkomst Impress/Addcom of een schadevergoeding toekennen. De overeenkomst met Impress/Addcom zal een losstaande overeenkomst zijn. Het nemen van dit risico is als onwenselijk bestempeld door de aanwezigen bij de risicoacceptatie op maandag 18 januari om 12u30, w.o. hoofd DVP, afdeling FCC, CIO, CFO, programmamedewerkers. Voor volgende verzendingen dient onderzocht te worden of inzet van deze partijen alsnog mogelijk is, indien het risico rondom Xerox niet afdoende gemitigeerd is gebleken. **Update 22-02-2021** Dit risico is komen te vervallen door voorgaande punten. In aanvulling hierop. Aldus 5.1.2e de strategisch inkoopadviseur van het RIVM schreef in een mail aan 5.1.2e op 22-01-2021:

	Door het ministerie van Justitie en Veiligheid is, als verantwoordelijk ministerie voor de categorie drukwerk en grafische diensten, in 2014 een Europese aanbesteding uitgevoerd, met als resultaat een overeenkomst met Xerox Nederland BV. (hierna voor de eenvoud te noemen 'Xerox') geboekt onder nummer 502599-001. Met het toewijzen van deze overeenkomst aan Xerox geeft de Nederlandse overheid (de participerende eenheden, waaronder VWS en RIVM) hen tot 31-12-2024 het alleenrecht om de eerder beschreven diensten te leveren. Enkel in gevallen dat Xerox niet kan leveren, kan worden afgeweken van deze verplichting, daar dit altijd in goed overleg is tussen het RIVM, minJenV en Xerox. *De wettelijke verplichting om deze diensten af te nemen zijn vastgelegd in de eerder genoemde overeenkomst en de Europese aanbestedingswet 2012, te vinden op https://wetten.overheid.nl/BWBR0032203/2019-04-18. Als summiere samenvatting van deze uitgebreide Europese wetgeving geldt dat (semi) overheidsbedrijven hun diensten of goederen boven een bepaalde waarde (voor de overheid is dit 139.000,00 euro) altijd middels een Europese aanbesteding in concurrentie moeten uitzetten. Omdat de totale waarde van de diensten voor drukwerk en grafische diensten vele malen hoger ligt is deze in 2014 volgens deze wet aanbesteed. Dit houdt in dat we dergelijke diensten niet bij andere bedrijven mogen uitvragen. Zodra het RIVM dit wel doet kan er door de huidige contractpartij (Xerox) een proces worden aangespannen, dat leidt tot een claim die in dit geval kan oplopen tot een enorm bedrag.*

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*
Privacy risico: doeltreffendheid van de mitigerende maatregel om de toepasselijkheid van de Freedom Act te verhinderen is een punt van aandacht.

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*
Op dit moment geen.

Periode *Geef aan voor welke periode de risicoacceptatie moet gaan gelden en wat de einddatum van deze acceptatie is*
De risicoacceptatie geldt voor de eerste brievenbatch met uitnodigingen die via Xerox verstuurd zal worden.

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

De genoemde risico's zullen (doorlopend en tot nader order) worden beoordeeld door de stuurgroep Covid-19 Registratie.

Verzoek op verlenging eerder gemaakte risico-acceptatie (28-01-2021)

- De volgende groep genodigden staat alweer voor de deur – de 80-85 jarigen (~oplagen 450.000). Naar verwachting zal hiervoor de opdracht aanstaande donderdag moeten worden verstrekt om de uitnodigingen op tijd op de mat te krijgen.
- Ondanks dat de acties worden genomen om de IB&P voor data verwerking met Xerox en haar sub-verwerkers spoedig af te ronden, voorzie ik dat dit niet op tijd zal zijn. Om het versturen van de uitnodigingen niet te blokkeren zou ik daarom graag verlenging op de risico-acceptatie van 19-01-2021 ontvangen. De procedure zoals daarin beschreven staat zal ook op deze batch van uitnodigingen van toepassing zijn.

Verzoek op verlenging eerder gemaakte risico-acceptatie (09-02-2021)

- Ondanks de voortgang in het opstellen van de IB&P, het maken van aanvullende afspraken met Xerox aangaande data behandeling en beveiliging voor het COVID vaccinatie programma, het opstellen van het uitnodigingen proces en een DPIA, haalt de realiteit ons in en is de planning voor het versturen van de nieuwe uitnodigingen vervroegd.
- Om het versturen van de uitnodigingen niet te blokkeren vragen we daarom nogmaals om verlenging van de risico-acceptatie van 28-01-2021 (zie bijgevoegd) ontvangen. De procedure zoals daarin beschreven staat zal ook op deze batch van uitnodigingen van toepassing zijn.

Update 22-02-2021
Verzoek op acceptatie van de genoemde mitigerende maatregelen.

Gevraagd besluit:	Verzoek op acceptatie van de genoemde mitigerende maatregelen.		
Partij	***Naam***	***Mening*** *(invullen door Hoofd centrum, IM, CISO, CIO, Privacy, DG, DR etc.)*	***Akkoord***
Hoofd centrum	5.1.2e		
Domein IM	n.v.t. (niet geraadpleegd)	n.v.t.	n.v.t.
CISO *(mandatory voor alle risk levels)*	5.1.2e		
Compliance (Facultatief)	...		n.v.t.
Legal (facultatief)	...		n.v.t.
Privacy (facultatief)	...		n.v.t.
CFO *(mandatory voor medium en hoger risico)*	5.1.2e		
CIO *(mandatory voor medium en hoger risico)*	5.1.2e		
DR *(mandatory voor hoog en zeer hoog risico)*	N.v.t. (niet geraadpleegd)		
Programma Covid-19 vaccinatie Gedelegeerd opdracht gever	5.1.2e		