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]
Aanvrager:	
Telefoonnummer:	
Aanvraagnummer:	
Datum aanvraag:	
Naam verantwoordelijk lijnmanager:	5.1.2e
Naam centrum- of afdelingshoofd:	5.1.2e
Centrum: Naam Informatiemanager:	DVP 5.1.2e
Doel:	
Aan:	
T.b.v. vergadering:	Stuurgroep COVID registratie
Aantal pagina's:	
Notitie toegevoegd:	20210115 concept Versnelde IB en P analyse voorlopige oplossing selecteren en oproepen _.docx & advies privacy officer 15.1.2021 keuze drukker
Versienummer	
Datum laatst gewijzigd	

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 5.1.2e).

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 wordt naar verwachting in de week van 19 januari getekend.

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.

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 ondersteunt.
- 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 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.

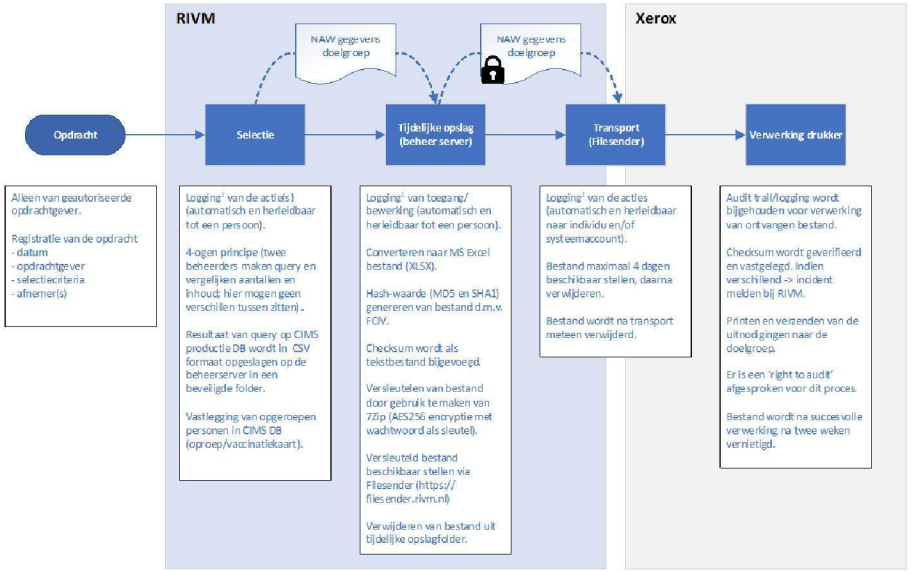
Aanvraagnummer *Geef aan onder welk nummer de aanvraag al in het risk register staat of dat het een nieuwe aanvraag betreft*
Nieuwe aanvraag

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 informatie vanuit Xerox**: "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."

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 - Het gegenereerde bestand (na selectie) wordt versleuteld opgeslagen. - Transport naar SFTP server is versleuteld. Dataset zelf is ook voorzien van versleuteling (AES-256).
Verwerking van persoonsgegevens buiten de Europese Economische Ruimte	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.

(EER)	(brief van 5.1.2e van 18.1.2021 aan 5.1.2e en 5.1.2e ; mail van 5.1.2e van 18.1.2021, 15:41 uur aan 5.1.2e) 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.
Toegang Amerikaanse overheid tot persoonsgegevens	mail van 5.1.2e van 18.1.2021, 15:41 uur aan 5.1.2e "Aangezien we de data niet hebben, het ons eigendom niet is, kunnen we deze ook niet onder de Freedom Act overhandigen."

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*
Niet van toepassing.

Periode *Geef aan voor welke periode de risicoacceptatie moet gaan gelden en wat de einddatum van deze acceptatie is*
Maximaal t/m 3 weken na de verzending van de laatste oproepbrief batch week van 19 januari 2021.

Evaluatie *Geef aan wanneer en op welke wijze evaluatie van het restrisico zal gaan plaatsvinden*
De genoemde risico's zullen worden beoordeeld door de stuurgroep Covid-19 Registratie.

Gevraagd besluit:	In te stemmen met genoemde beschrijving van het bestaan van een restrisico waarvan de kans van optreden wordt verkleind, maar dat continu onder de aandacht moet blijven.		
Partij	***Naam***	***Mening*** *(invullen door Hoofd centrum, IM, CISO, CIO, Privacy, DG, DR etc.)*	***Akkoord***
Hoofd centrum	5.1.2e		Akkoord: ja/nee
Domein IM	5.1.2e		Akkoord: ja/nee
CISO *(mandatory voor alle risk levels)*	5.1.2e		Akkoord: ja/nee
Compliance (Facultatief)	...		Akkoord: ja/nee
Legal (facultatief)	...		Akkoord: ja/nee
Privacy (facultatief)	...		Akkoord: ja/nee
CIO *(mandatory voor medium en hoger risico)*	5.1.2e		Akkoord: ja/nee
DR	5.1.2e /		Akkoord: ja/nee

(mandatory voor hoog en zeer hoog risico)	5.1.2e		