To: 5.1.2e [5.1.2e @rivm.nl]
Cc: 5.1.2e [5.1.2e @rivm.nl]; 5.1.2e [5.1.2e @rivm.nl]
From: 5.1.2e
Sent: Wed 2/10/2021 4:51:21 PM
Subject: FW: Aanvullende eisen RIVM bij verwerkersovereenkomst getekend 502599-003. [Advies over aan Xerox te stellen eisen in verband met verwerken oproepbrieven COVID-19]
Received: Wed 2/10/2021 4:51:21 PM
Data verwerking Xerox tbv oproepen COVID19 vaccinatie signd.pdf

Hallo 5.1.2i Concept

Bij deze mijn aanvullingen op de overige aandachtspunten in 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; 5-02599".*
Zou jij deze aanvullingen met 5.1.2i Concept kunnen delen voor het finaliseren van het document en het laten tekenen door beiden partijen? Zo niet, wie kan dit faciliteren?

Overige aandachtspunten
a) In Art. 8 en 9 van de verwerkers overeenkomst gaat het over Deelnemer. Bedoelt wordt Rijks organisatie die zich aan het contract hebben gecommitteerd. De individuele deelnemer (organisatie) is daarmee afnemer van producten en diensten van leverancier (Xerox).
b) Art. 9 lid 1 en bijlage 3 lijken tegenstrijdig qua timing voor wat betreft de termijn waarbinnen de Leverancier de Koper dient te informeren over een inbreuk in verband met Persoonsgegevens. Art. 9 lid 1 "zonder onredelijke vertraging" en bijlage 3 "onverwijld". De AVG geeft een termijn van melding aan. De voornoemde artikelen geven aan dat de intentie van leverancier is de melding zo kort als mogelijk is aan Deelnemer/ eigenaar van de data, (RIVM) te melden.
c) Bijlage 3 Afspraken betreffende inbreuken in verband met persoonsgegevens. Melding vanuit KVDM~~naar~~ [naam/functie] naar RIVM [naam functie] met medenemen van Xerox CISO ter info. Deze gegevens dienen onverwijld onderling gecommuniceerd worden. Graag verneem ik welke dat voor het RIVM zijn. → 5.1.2i Concept van 5.1.2i Concept begreep ik dat jij hiervoor mogelijk een naam kunt geven?
d) Gelet op de grootschaligheid van de verwerkingen én de~~publicitaire gevoeligheid~~ maatschappelijke gevoeligheid van de verwerking, is het goed nogmaals te stellen dat: - Indien bij verwerking door KVDM een lek wordt geconstateerd dit onverwijld aan RIVM gemeld zal worden (zie boven) RIVM zal melding naar AP moeten verzorgen. Indien er op welke wijze dan ook publiciteit gemoeid is in deze zal daarin ook het RIVM leidend zijn en communicatie vanuit Xerox/KVDM te allen tijde eerst afgestemd worden met RIVM. Wij vernemen graag de naam en contact gegevens van de betreffende dienst/functionaris. → 5.1.2e - 5.1.2e 5.1.2e
e) Bijlage 1, Aan de zijde van het RIVM zal bijlage 1 nog geactualiseerd moeten worden. → Zie hieronder mijn voorstel obv eerdere correspondentie

Het onderwerp/aard en doel van de verwerking	Verwerken van persoonlijke gegevens voor communicatie uitingen en distributie daarvan (zoals mailingen) in het kader van het COVID-19 vaccinatie programma
Het soort persoonsgegevens	Naam, adellijke titel, adres, postcode en woonplaats
Beschrijving categorieën Betrokkenen	Meerderjarige burgers (BRP bestand) die op basis van een opdracht van VWS door RIVM worden opgeroepen
Beschrijving categorieën ontvangers van persoonsgegevens	Medewerkers van sub-verwerker Koninklijke Van der Most
Bewaartermijn	De dataset zal na maximaal twee weken na verzending van de oproepen worden vernietigd

Van 5.1.2e heb ik begrepen dat de gesignaleerde risico's (Ongeautoriseerde inzage van persoonsgegevens) voor informatiebeveiliging met deze oplossing zijn gemitigeerd. Hij zal hierover een korte memo schrijven en de laatste versie van het risico acceptatie formulier hiermee updaten en aanvullen. Hierin zal ook staan dat het CIMS team een procesbeschrijving zal maken van het verwerken van de persoonsgegevens.
Ik ga er nu van uit dat de andere gesignaleerde risico's: Verwerking van persoonsgegevens buiten de Europese Economische Ruimte (EER) en Toegang Amerikaanse overheid tot persoonsgegevens middels de additionele verwerkersovereenkomst met Xerox zijn gemitigeerd gezien jouw ondergenoemde advies: *Dit betreft een correcte*

weergave van de aanvullende eisen die het RIVM aan inrichting en beveiliging stelt voor de verwerking van oproepbrieven COVID – 19. Mocht ik dit verkeerd hebben geïnterpreteerd, hoor ik dit heel graag.

5.1.2e gaf daarnaast ook aan geen problemen te zien de adressen bestanden nu al (nog met de tijdelijke oplossing selecteren en oproepen in CIMS) direct aan Van Der Most aan te leveren omdat de afspraken met VDM gemaakt zijn. Dit zal ik ook aan 5.1.2e communiceren.

Op basis van deze memo en aangevulde risico acceptatie formulier zal ik de groep informeren dat de risico's gemitigeerd zijn. De ondergenoemde beslispunten zal ik dan ook voorleggen aan de stuurgroep. Een additioneel overleg zal hiervoor dan niet meer noodzakelijk zijn, maar kan wel georganiseerd worden indien wenselijk.

Groeten,

...
5.1.2e
06 5.1.2e

From: 5.1.2e < 5.1.2e @rivm.nl>
Sent: woensdag 10 februari 2021 11:21
To: 5.1.2e < 5.1.2e @rivm.nl>
Subject: RE: Aanvullende eisen RIVM bij verwerkersovereenkomst getekend 502599-003. [Advies over aan Xerox te stellen eisen in verband met verwerken oproepbrieven COVID-19]
Sensitivity: Confidential

Ha 5.1.2e

Bij c: bij wie binnen het RIVM een datalek gemeld moet worden weet ik niet, ik denk dat dat niet bij Communicatie moet gebeuren…

Bij d: als het gaat om het afstemmen van de communicatie, daar mag de naam van 5.1.2e (en tel. nr. erbij, is mss handig: +316 5.1.2e) worden ingevuld. Zij is afdelingshoofd Publicaties en Nieuws (en dus ook afdelingshoofd van de persvoorlichters).

Tip van 5.1.2e : maak er bij de niet 'publicitaire gevoeligheid' gevoeligheid van, maar maatschappelijke gevoeligheid. Publiciteit is het probleem namelijk niet, wel de impact op de maatschappij. We zijn immers continu in de publiciteit (dat is geen probleem an sich), maar we willen bovendien ook niet suggereren dat we ons drukker zouden maken om publiciteit dan om het echte probleem/de gevolgen van een datalek voor degenen die het betreft.

Met vriendelijke groet,

5.1.2e
5.1.2e

.....

Stafeenheid Communicatie & Documentaire Informatievoorziening
Rijksinstituut voor Volksgezondheid en Milieu
Antonie van Leeuwenhoeklaan 9 | 3721 MA Bilthoven
Postbus 1 | 3720 BA Bilthoven
.....
T + 31 (0) 5.1.2e
M +31 (0)6 5.1.2e
http://www.rivm.nl

.....

***De zorg voor morgen* begint vandaag**

.....

Van: 5.1.2e <5.1.2e @rivm.nl>
Verzonden: dinsdag 9 februari 2021 16:32
Aan: 5.1.2e <5.1.2e @rivm.nl>; 5.1.2e <5.1.2e @rivm.nl>; 5.1.2e <5.1.2e @rivm.nl>
CC: 5.1.2e <5.1.2e @rivm.nl>; 5.1.2e <5.1.2e @rivm.nl>; 5.1.2e <5.1.2e @rivm.nl>; 5.1.2e <5.1.2e @rivm.nl>
Onderwerp: RE: Aanvullende eisen RIVM bij verwerkersovereenkomst getekend 502599-003. [Advies over aan Xerox te stellen eisen in verband met verwerken oproepbrieven COVID-19]
Gevoeligheid: Vertrouwelijk

Hallo 5.1.2e

Dank voor je terugkoppeling.

Met betrekking tot de "overige aandachtspunten" in de aanvullende dataverwerking met KVDM (zie hieronder en in de bijlagen), moeten er naar mijn inziens de volgende afspraken nog worden gemaakt met Xerox en KVDM:

- De contactpersonen moeten worden doorgegeven vanuit het RIVM (zie geel gemarkeerd hieronder). @5.1.2e 5.1.2e Welke namen kunnen we hiervoor doorgeven?
- Bijlagen 1. De Verwerking van persoonsgegevens moet worden aangevuld voor het vaccinatie programma.

Bijlage 1. De Verwerking van Persoonsgegevens

In deze bijlage moet in ieder geval het volgende worden gespecificeerd:

Het onderwerp/aard en doel van de Verwerking	Verwerken van persoonlijke gegevens voor communicatie uitingen en distributie daarvan (zoals mailingen)
Het soort Persoonsgegevens	NAW-gegevens en bijzondere gegevens voortkomend uit de wettelijke plicht van Koper en of om het gestelde doel van Koper te bereiken
Beschrijving categorieën Persoonsgegevens	NAW- gegevens Bijzonder categorieën conform art. 9 van de Verordening
Beschrijving categorieën Betrokkenen	Natuurlijke personen op wie de persoonsgegevens betrekking hebben
Beschrijving categorieën ontvangers van Persoonsgegevens	Medewerkers Xerox en Sub-verwerkers uit bijlage 4.
Bewaartermijn	Alle persoonsgegevens dienen binnen 90 dagen te worden gewist na afronding opdracht tenzij voor de uitvoering van de overeenkomst een langere bewaartermijn noodzakelijk is en door Koper/Deelnemer aangegeven.

Voor de inhoud van deze bijlage kan onder meer gebruik worden gemaakt van de registratie die de Verwerkingsverantwoordelijke op grond van artikel 30 van de Verordening dient aan te houden.

Zie hieronder mijn voorstel op basis van eerder verkregen input van 5.1.2e en 5.1.2e @5.1.2e heb jij hier nog aanvullingen op?

Het onderwerp/aard en doel van de verwerking	Verwerken van persoonlijke gegevens voor communicatie uitingen en distributie daarvan (zoals mailingen) in het kader van het COVID-19 vaccinatie programma
Het soort persoonsgegevens	Naam, adellijke titel, adres, postcode en woonplaats, leeftijdsgroep

Beschrijving categorieën Betrokkenen	Meerderjarige burgers (BRP bestand) die op basis van een opdracht van VWS door RIVM worden opgeroepen
Beschrijving categorieën ontvangers van persoonsgegevens	Medewerkers van sub-verwerker Koninklijke Van der Most
Bewaartermijn	De dataset zal na maximaal twee weken na verzending van de oproepen worden vernietigd

Groeten,

...
5.1.2e
06 5.1.2e

Overige aandachtspunten
a) In Art. 8 en 9 van de verwerkers overeenkomst gaat het over Deelnemer. Bedoelt wordt Rijks organisatie die zich aan het contract hebben gecommitteerd. De individuele deelnemer (organisatie) is daarmee afnemer van producten en diensten van leverancier (Xerox).
b) Art. 9 lid 1 en bijlage 3 lijken tegenstrijdig qua timing voor wat betreft de termijn waarbinnen de Leverancier de Koper dient te informeren over een inbreuk in verband met Persoonsgegevens. Art. 9 lid 1 "zonder onredelijke vertraging" en bijlage 3 "onverwijld". De AVG geeft een termijn van melding aan. De voornoemde artikelen geven aan dat de intentie van leverancier is de melding zo kort als mogelijk is aan Deelnemer/ eigenaar van de data, (RIVM) te melden.
c) Bijlage 3 Afspraken betreffende inbreuken in verband met persoonsgegevens. Melding vanuit KVDM naar [naam/functie] naar RIVM [naam functie] met medenemen van Xerox CISO ter info. Deze gegevens dienen onverwijld onderling gecommuniceerd worden. Graag verneem ik welke dat voor het RIVM zijn.
d) Gelet op de grootschaligheid van de verwerkingen én de publicitaire gevoeligheid van de verwerking, is het goed nogmaals te stellen dat: - Indien bij verwerking door KVDM een lek wordt geconstateerd dit onverwijld aan RIVM gemeld zal worden (zie boven) RIVM zal melding naar AP moeten verzorgen. Indien er op welke wijze dan ook publiciteit gemoeid is in deze zal daarin ook het RIVM leidend zijn en communicatie vanuit Xerox/KVDM te allen tijde eerst afgestemd worden met RIVM. Wij vernemen graag de naam en contact gegevens van de betreffende dienst/functionaris.
e) Bijlage 1, Aan de zijde van het RIVM zal bijlage 1 nog geactualiseerd moeten worden.

From: 5.1.2e < 5.1.2e @rivm.nl>
Sent: dinsdag 9 februari 2021 16:04
To: 5.1.2e < 5.1.2e @rivm.nl>; 5.1.2e < 5.1.2e @rivm.nl>
Cc: 5.1.2e < 5.1.2e @rivm.nl>; 5.1.2e < 5.1.2e @rivm.nl>; 5.1.2e < 5.1.2e @rivm.nl>; 5.1.2e < 5.1.2e @rivm.nl>
Subject: FW: Aanvullende eisen RIVM bij verwerkersovereenkomst getekend 502599-003. [Advies over aan Xerox te stellen eisen in verband met verwerken oproepbrieven COVID-19]
Sensitivity: Confidential

5.1.2e 5.1.2e

Jouw vraag
Je verzocht FCC/ de privacy officer en de CIO-O / ISO de centraal (JenV) gemaakte afspraken ter zake van drukwerk, te laten toetsen op adequaatheid voor het
verzorgen van de COVID – 19 oproepbrieven.

Uitgaande van een adequaat verlopen inkoopproces, is voor het RIVM de meest relevante vraag over óf de met Xerox ter zake van drukwerk gemaakte afspraken
informatiebeveiligings- en privacy compliance perspectief toereikend (passend beschermingsniveau) zijn voor de verwerking van oproepbrieven COVID -19.

Het antwoord

• De werking van de door Xerox geleverde diensten valt buiten scope van deze beoordeling. Ook de verrichtingen van Xero's sub-verwerkers, anders dan

de weergegeven afspraken, maken geen onderdeel uit van dit advies.

• 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. Mocht de wens zijn om de afspraken ook op werking te (laten) toetsen, dan zal daar een afzonderlijk verzoek over bij de CISO moeten worden ingediend. **[BESLISPUNT** 5.1.2e]

• De in diezelfde brief genoemde punten a t/m e, betreffen geen inrichtings- of beveiligingseisen. Het zijn punten waarop de verwerkersovereenkomst verduidelijking

behoeft en nog afspraken moeten worden gemaakt over uitvoering. **[ACTIE** 5.1.2e]

• Om de juridische houdbaarheid van de afspraak te verifiëren, luidt het advies: laten checken bij de juristen van RIVM Juridisch Advies óf zij vinden dat het RIVM genoegen kan nemen met een schriftelijke vastlegging als aanvullende eis bij een verwerkersovereenkomst van een director public accounts Xerox. [check Kvk]. Dit klemt te meer nu Van der Most B.V. deze afspraken niet heeft meegetekend en uit niets blijkt dat deze tussen RIVM en Xerox gemaakte afspraken, Van der Most B.V. binden (behalve de bewering door dhr. Vlaander, dat Xerox garandeert dat

dat alle door haar in te schakelen sub-verwerkers voldoen aan de door het RIVM aan Leverancier te stellen eisen. **[BESLISPUNT** 5.1.2i Concept **& EVT. ACTIE** 5.1.2i Concept

We vertrouwen jullie hier mee naar behoren te hebben geadviseerd. Tot nadere toelichting zijn wij vanzelfsprekend bereid.

5.1.2e
mede namens 5.1.2e 5.1.2e RIVM)

From: 5.1.2e < 5.1.2e @zorgmail.nl>
Sent: woensdag 3 februari 2021 15:30
To: 5.1.2e < 5.1.2e @rivm.nl>
Subject: Re: Aanvullende eisen RIVM bij verwerkersovereenkomst getekend 502599-003.
Sensitivity: Confidential

Mevrouw 5.1.2e

Helaas net verkeerde versie verstuurd!

Hier de getekende!

Excuses.

5.1.2e

Van: 5.1.2e
Verzonden: vrijdag, 29 januari 2021, 13:48
Aan: 5.1.2e
CC: 5.1.2e ; 5.1.2e ; 5.1.2e ; 5.1.2e
Onderwerp: Aanvullende eisen RIVM bij verwerkersovereenkomst getekend 502599-003.

Geachte heer 5.1.2e ,

Hartelijk dank voor het prettige gesprek van zojuist.

Ter voorbereiding op de door de RIVM (teken) bevoegde te maken afspraken – naar ik verwacht dhr. 5.1.2e stuur ik u de eisen die het RIVM graag

als extra bijlage bij de verwerkersovereenkomst 502599-003 (bijlage) gehecht zou willen zien. Deze eisen hebben betrekking op de specifieke inrichting- en

beveiligingseisen en nog enkele overige aandachtspunten.

Specifieke inrichtings- en beveiligingseisen

1. Er wordt zeker gesteld dat de te verwerken gegevens geen onderdeel worden van een dataset die zich buiten de Europese Economische Ruimte (EER) zou kunnen bevinden (geen doorgifte hoofdstuk 5 AVG). Deze maatregel heeft ook betrekking op de dataset in een back-up bestand of tijdens fail-over situatie.

2. Technische oplossing: gegevens die onder het contract worden uitgewisseld zullen dus ook geen deel uit gaan maken van het Xerox netwerk. Het databestand gaat rechtstreeks naar de (geheel Nederlandse en in Nederland gevestigde) drukker Van der Most B.V. Deze partij voldoet aan de AVG en BIO eisen en garandeert dat de te verwerken gegevens geen onderdeel worden van een dataset die zich buiten de EER zou kunnen bevinden.

3. De te verwerken gegevens worden alleen via een versleuteld communicatiekanaal aangeleverd/opgehaald. Ook het bestand zelf wordt voorzien van encryptie.

4. Het aangeleverde versleutelde bestand wordt pas ontsleuteld bij start van de daadwerkelijke verwerking.

5. Er wordt vóór verwerking vastgesteld of de aangeleverde informatie niet onrechtmatig is aangepast door controleren van de hash-waarde(n) die worden meegeleverd.

6. Het resultaat van de controle in punt 3wordt vastgelegd en kan op verzoek worden aangeleverd bij Opdrachtgever;

7. Het versleutelde bestand zal maximaal twee weken na verzending van de oproepen worden bewaard en worden gebruikt voor opsporing van eventuele fouten.

8. De dataset zal na maximaal twee weken na verzending van de oproepen worden vernietigd; (art. 10 lid 1 niet terugbezorgen, én art. 10. Lid 2 termijn niet van toepassing)

9. Alle verwerkingen (inclusief de vernietiging) worden vastgelegd in een logbestand (conform BIO & AVG richtlijnen);

10. Indien Leverancier verzocht wordt om de van RIVM afkomstige data te ontsluiten in verband met een overheids- of wettelijk verzoek, dan zal Leverancier hierover van tevoren afstemmen met een RIVM directielid.

11. De inhoud van de mails van heer 5.1.2e en 5.1.2e (JenV) en 5.1.2e (Xerox) brief van 18.1.2021 ("dataverwerking Xerox ten behoeve van grafische diensverlening"); mail verklaring samenwerking RIVM-Xerox van 18.1.2021 van dhr. 5.1.2e (Xerox) aan 5.1.2e maken onderdeel uit van de afspraken tussen RIVM en Xerox.

Overige aandachtspunten

12. art. 7 subverwerkers. RIVM geeft (impliciet) toestemming voor de subverwerkers zoals in de verwerkersovereenkomst genoemd. De onderhavige beoordeling strekt zich NIET uit tot de beoordeling van de verwerkingen van de subverwerkers. Graag bepaling toevoegen: *"Leverancier garandeert dat alle door hem in te schakelen sub-verwerkers voldoen aan de door het RIVM aan Leverancier te stellen eisen".*

13. Art. 8 en 9 gaat over Deelnemer. ??? I.c. hebben we het over Leverancier en Koper.

14. Art. 9 lid 1 en bijlage 3 zijn tegenstrijdig qua ***timing*** voor wat betreft de termijn waarbinnen de Leverancier de Koper dient te ***informeren over een inbreuk in verband met Persoonsgegevens***. Art. 9 lid 1 "zonder onredelijke vertraging" en bijlage 3 "onverwijld".

15. Bijlage 3 **Afspraken betreffende inbreuken in verband met persoonsgegevens/ bij wie** : melding van Leverancier aan besteller van Deelnemer (?), contractmanager deelnemer en centrale contractmanager van de rijksoverheid. Niet helder is, welke functies het bij het RIVM betreft. Dient helder te zijn met wie het best/snelst kan worden gecommuniceerd.

16. Gelet op de grootschaligheid van de verwerkingen én de publicitaire gevoeligheid van de verwerking, is het aan te bevelen om ook afspraken te maken over (1) afstemming wanneer Leverancier een datalek aan AP meldt, (2) hoe Leverancier én RIVM publicitair met het datalek om zullen gaan.

17. Bijlage 1, Aan de zijde van het RIVM zal bijlage 1 nog geactualiseerd worden. Onderwerp en doel van de verwerking: het gaat om oproepen in het kader van het Vaccinatieprogramma COVID 19 en NIET om, zoals vermeld in de overeenkomst "verwerken van persoonlijke gegevens voor communicatie uitingen en distributie daarvan (zoals mailingen). "

Hartelijk dank alvast voor de door u aan deze mail te besteden aandacht.

Wij vernemen graag of u met de specifieke inrichtings- en beveiligingseisen zoals onder 1 t/m 11 genoemd instemt.

Voor wat betreft de punten 12 t/m 16 zien wij graag uw tekstvoorstellen tegemoet.

Uw reactie kunt u richten aan 5.1.2e met 5.1.2e, 5.1.2e, 5.1.2e en mijzelf in de cc.

Mocht u vragen hebben over deze mail, aarzelt u niet om contact met 5.1.2e of mij op te nemen.

Hoogachtend,

en met vriendelijke groet,

5.1.2e

mede namens 5.1.2e RIVM)

5.1.2e
5.1.2e RIVM

Rijksinstituut voor Volksgezondheid en Milieu
Stafeenheid Finance, Compliance en Control (FCC)/ AVG-Team
Antonie van Leeuwenhoeklaan 9 | 3721 MA Bilthoven
Postbus 1 | Postvak 5.1.2e | 3720 BA Bilthoven
T: 06-5.1.2e