To: 5.1.2e [5.1.2e @rivm.nl]; 5.1.2e [5.1.2e @rivm.nl]; 5.1.2e 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 [5.1.2e @rivm.nl]; 5.1.2e [5.1.2e @rivm.nl]; 5.1.2e [5.1.2e @rivm.nl]
Sent: Fri 2/12/2021 2:20:04 PM
Subject: RE: [PROCES SELECTEREN EN OPROEPEN] RE: Aanvullende eisen RIVM bij verwerkersovereenkomst getekend 5.1.2h [Advies over aan Xerox te stellen eisen in verband met verwerken oproepbrieven COVID-19]
Received: Fri 2/12/2021 2:20:04 PM

Dag 5.1.2e,

Bedankt voor de update. Mooi dat er zoveel stappen zijn gezet om de risico's te beperken.

Zoals inmiddels meermaals door mij en ook CIO gezegd: ik wil graag een bewuste en gezamenlijke risico-afweging maken op bestuurlijk niveau over de ondernomen acties, het punt waarop we nu gekomen zijn en wat er dan nog resteert. Of de risico's afdoende gemitigeerd zijn is namelijk een afweging van de lijn. Een afspraak is hiervoor nodig, mail volstaat niet. De stuurgroep registratie kan hiervoor gebruikt worden.

Jij bent inderdaad geen business owner/proceseigenaar en draagt zaken binnenkort aan de lijn over, maar als (o.a.) onduidelijk is of de nieuwe partij (VDM) wel of niet een overeenkomst moet tekenen / getekend heeft, dan hoort dat helder krijgen m.i. wel bij voorliggende opdracht.

Voor aansluiting op het reguliere datalekkenproces kan geschakeld worden met de privacy coördinator DVP (5.1.2e 5.1.2e), de informatiemanager DVP (5.1.2e) en team FCC (

Groet,
5.1.2e

Van: 5.1.2e < 5.1.2e @rivm.nl>
Datum: 11 februari 2021 om 22:06:12 CET
Aan: 5.1.2e < 5.1.2e @rivm.nl>, 5.1.2e < 5.1.2e @rivm.nl>, 5.1.2e 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>, 5.1.2e < 5.1.2e @rivm.nl>, 5.1.2e < 5.1.2e @rivm.nl>
Onderwerp: RE: [PROCES SELECTEREN EN OPROEPEN] RE: Aanvullende eisen RIVM bij verwerkersovereenkomst getekend 5.1.2h [Advies over aan Xerox te stellen eisen in verband met verwerken oproepbrieven COVID-19]

Hallo 5.1.2e, 5.1.2e 5.1.2e en 5.1.2e

Bij deze een overzicht van de laatste stand van zaken.

- De gesignaleerde risico's (Ongeautoriseerde inzage van persoonsgegevens) voor informatiebeveiliging zijn gemitigeerd. 5.1.2e 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.
- De gesignaleerde overige risico's: Verwerking van persoonsgegevens buiten de Europese Economische Ruimte (EER) en Toegang Amerikaanse overheid tot persoonsgegevens zijn ook middels de additionele verwerkersovereenkomst met Xerox gemitigeerd. 5.1.2e heeft hierop een positief advies over gegeven. Dit betreft een correcte weergave van de aanvullende eisen die het RIVM aan inrichting en beveiliging stelt voor de verwerking van oproepbrieven COVID – 19

- Voor de punten a t/m e in dezelfde verwerkersovereenkomst is nog wat verduidelijking nodig. Ik heb mijn voorstel hiervoor met 5.1.2e gedeeld (zie bijgevoegd de mail met mijn voorstel voor de punten a t/m e.). Maar ik begrijp uit onderstaande mail dat de 5.1.2e hier verder geen rol in kan spelen. @ 5.1.2e Wie vanuit het RIVM zou dit op kunnen pakken en deze informatie met Dhr. 5.1.2e kunnen delen voor het finaliseren en aan beiden kanten laten tekenen van het document? Ik ben vanuit het programma bureau Covid-19 vaccinatie tijdelijk bij dit proces betrokken om het uitnodigingen proces duidelijkheid te geven, maar ik ben geen business of proceseigenaar. Wie kan voor eventuele datalekken vanuit het RIVM als contact persoon worden ingevuld?
- 5.1.2e gaf 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.
- Op basis van deze memo en aangevulde risico acceptatie formulier zal ik de groep informeren dat de risico's gemitigeerd zijn. Een additioneel overleg zal hiervoor dan niet meer noodzakelijk zijn, maar kan wel georganiseerd worden indien wenselijk.
- Alleen de door 5.1.2e genoemde punten kunnen nog in de stuurgroep worden ingebracht. Ik zal 5.1.2e 5.1.2e vragen dit voor volgende week donderdag op de agenda te zetten.
    - Beslispunt: wil je ook de werking van de IB+P afspraken getoetst hebben, dan zal CIO-O daarvoor moeten worden ingeschakeld
    - Beslispunt: Juridische check ja/nee juridische "zekerheid" over hoe bindend de door 5.1.2e gemaakte afspraken zijn en die zien op door Van der Most B.V. na te komen verplichtingen (nu Van der Most B.V. de aanvullende afspraken niet heeft mee getekend)

Ik hoop het geupdate risico-acceptatie formulier met de gemitigeerde risico's spoedig te kunnen delen en dit af te sluiten.

Groeten,

...

5.1.2e

06 5.1.2e

From: 5.1.2e < 5.1.2e @rivm.nl>
Sent: donderdag 11 februari 2021 19:02
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 < 5.1.2e @rivm.nl>; 5.1.2e < 5.1.2e @rivm.nl>; 5.1.2e < 5.1.2e @rivm.nl>
Subject: RE: [PROCES SELECTEREN EN OPROEPEN] RE: Aanvullende eisen RIVM bij verwerkersovereenkomst getekend 5.1.2h [Advies over aan Xerox te stellen eisen in verband met verwerken oproepbrieven COVID-19]

Sensitivity: Confidential

Hoi 5.1.2e en 5.1.2e

Bedankt voor jullie updates de afgelopen dagen over het proces van uitnodigen voor COVID-19 vaccinaties.

Het klopt dat 5.1.2e en ik enige weken geleden versterking hebben ingevlogen in de vorm van 5.1.2e om het proces van uitnodigen van A tot Z in te regelen, omdat de zittende organisatie bij RIVM overbelast is/was. Dit heeft 5.1.2e vervolgens voortvarend opgepakt, samen met IB&P-collega's.

In mijn antwoord op de meest recente risicoacceptatie die Helen gemaakt heeft heb ik aangegeven dat ik – samen met 5.1.2e en gezien het niveau waarop de risico's geaccepteerd moeten worden ook de CIO en CFO – binnenkort (liefst ruim voor 24/2, zoals deze week door 5.1.2e verzocht) een terugkoppeling krijg in een te plannen overleg over de stand van zaken en de afgehandelde en openstaande punten. Ik ga er vanuit dat 5.1.2e dit plant en dit heeft zij ook aangegeven.

Achtereenvolgens reagerend op jouw punten, 5.1.2e

1. Ik weet niet of ik je helemaal begrijp, eerlijk gezegd. De werking van ingezette IB&P-maatregelen beoordelen is volgens mij wat we beoogden toen we de aanvraag uitzetten een aantal weken geleden. Dus ja, dit moet gebeuren. 5.1.2e kan deze collega's inschakelen, lijkt me.
2. Ik ken de actuele status van punten uit de IB&P niet. Ik ben me er niet van bewust dat de firma Van der Most geen afspraken zou (willen) tekenen. Ik ontvang graag eerst een totale terugkoppeling van opgeloste en openstaande IB&P-punten alvorens ik me goed gepositioneerd voel om te reageren op dit punt. Overigens behoort ook het inzetten van een jurist bij een van de centra van het RIVM tot de mogelijkheden die de projectleider namens de opdrachtgevers (5.1.2e en ik) tot haar beschikking heeft.

Ik ga er vanuit hiermee voor nu even voldoende gereageerd te hebben op onderstaande. Als dat niet zo is, dan hoor ik het graag.

Met vriendelijke groet,

5.1.2e

5.1.2e

Rijksinstituut voor Volksgezondheid en Milieu
Antonie van Leeuwenhoeklaan 9 | Postbus 1 | 3720 BA Bilthoven

T +31(0)30 5.1.2e
M +31(0)6 5.1.2e

5.1.2e @rivm.nl
http://www.rivm.nl

RIVM 5.1.2e

From: 5.1.2e <5.1.2e @rivm.nl>
Sent: donderdag 11 februari 2021 12:03
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>; 5.1.2e 5.1.2e <5.1.2e @rivm.nl>; 5.1.2e <5.1.2e @rivm.nl>
Subject: FW: [PROCES SELECTEREN EN OPROEPEN] RE: Aanvullende eisen RIVM bij verwerkersovereenkomst getekend 5.1.2h . [Advies over aan Xerox te stellen eisen in verband met verwerken oproepbrieven COVID-19]
Importance: High
Sensitivity: Confidential

5.1.2e

Vanochtend heb ik proberen te bellen. Nu dan even per mail.

Het IB+P advies op aanvullende inrichtings- en beveiligingseisen Xerox is gegeven.

Je hebt 5.1.2e en haar collega aangetrokken om het proces oproepen/ Xerox te stroomlijnen.

Als je het mij vraagt zal er nog goed gekeken moeten worden naar m.n. operationele zaken als:

- Aansturing drukker Xerox/ van der Most (in verband met kwaliteit drukwerk e.d.)
- Datalek afhandeling: wie belt wie (nog aan te passen in de verwerkersovereenkomst)

Advies IB+P advies rondom diensten Xerox en subverwerkers:

- Beslispunt 5.1.2e: wil je ook de werking van de IB+P afspraken getoetst hebben, dan zal CIO-O daarvoor moeten worden ingeschakeld
- Beslispunt 5.1.2e: Juridische check ja/nee juridische "zekerheid" over hoe bindend de door 5.1.2e gemaakte afspraken zijn en

die zien op door Van der Most B.V. na te komen verplichtingen (nu Van der Most B.V. de aanvullende afspraken niet heeft mee getekend)

NB. De DPIA selecteren en oproepen is gisteren door 5.1.2e en 5.1.2e uitgevoerd.

Zal vandaag door 5.1.2e en 5.1.2e verder uitgewerkt worden en maandag 15.2 bij de FG moeten liggen.

5.1.2e zal je hier verder over informeren. Zij en ik spraken af dat zij "in de lead" is.

Vr. groet,

5.1.2e

From: 5.1.2e
Sent: donderdag 11 februari 2021 09:21
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>; 5.1.2e < 5.1.2e @rivm.nl>; 5.1.2e < 5.1.2e @rivm.nl>
Subject: [PROCES SELECTEREN EN OPROEPEN] RE: Aanvullende eisen RIVM bij verwerkersovereenkomst getekend 5.1.2h [Advies over aan Xerox te stellen eisen in verband met verwerken oproepbrieven COVID-19]
Importance: High
Sensitivity: Confidential

5.1.2e

Ik ontving enkele mails van jou met verzoeken aan mij gericht. Momenteel moet ik voorrang geven aan andere zaken. In mijn mail van dinsdag 9.2 heb ik

nog enkele beslis/actiepunten geformuleerd. De in groen aangegeven punten zie ik niet terugkomen in de mailtrail met een antwoord, graag alsnog je aandacht hiervoor.

Voor wat betreft de punten at/m e [actie 5.1.2e], is het aan de business/proceseigenaar om hier verdere invulling aan te geven/ met antwoorden te komen. Ik kan hier niets in betekenen.

NB: de DPIA selecteren en oproepen is gisteren, 10.2 uitgevoerd en moet op 15.2 bij de FG liggen. Indien niet voldoende afgehecht en leidend tot een risico, zal dit in de DPIA terug moeten komen.

Vr groet,

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; 5.1.2h *"*, 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. 5.1.2e 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** 5.1.2e **& EVT. ACTIE** 5.1.2e **]**

Vr. groet,

5.1.2e

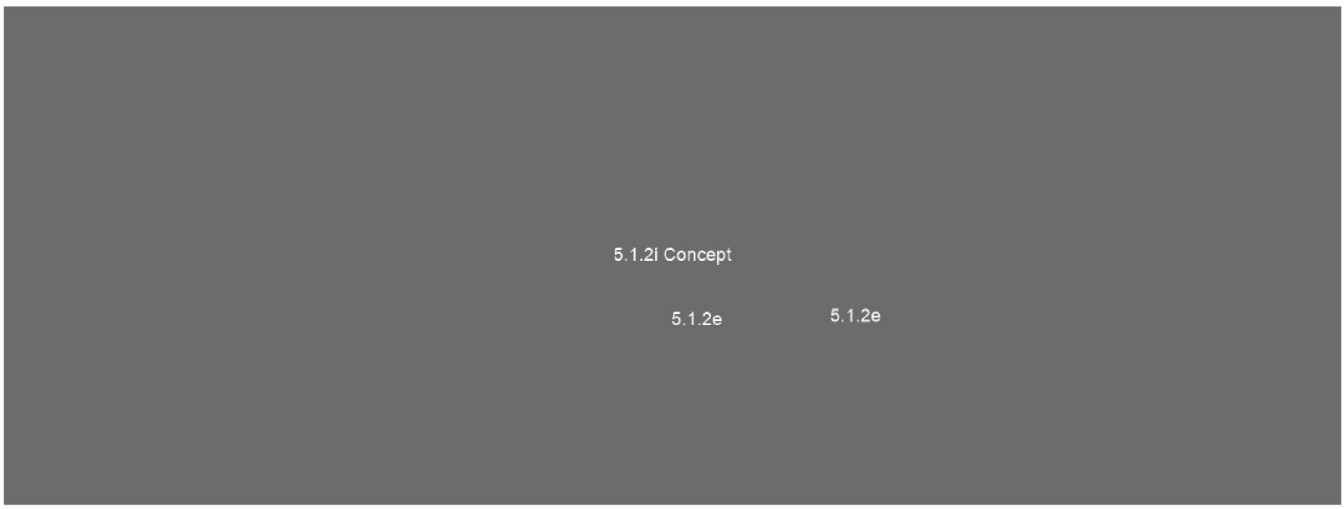
From: 5.1.2e < 5.1.2e @rivm.nl>
Sent: woensdag 10 februari 2021 17:51
To: 5.1.2e < 5.1.2e @rivm.nl>
Cc: 5.1.2e < 5.1.2e @rivm.nl>; 5.1.2e < 5.1.2e @rivm.nl>
Subject: FW: Aanvullende eisen RIVM bij verwerkersovereenkomst getekend 5.1.2h [Advies over aan Xerox te stellen eisen in verband met verwerken oproepbrieven COVID-19]
Sensitivity: Confidential

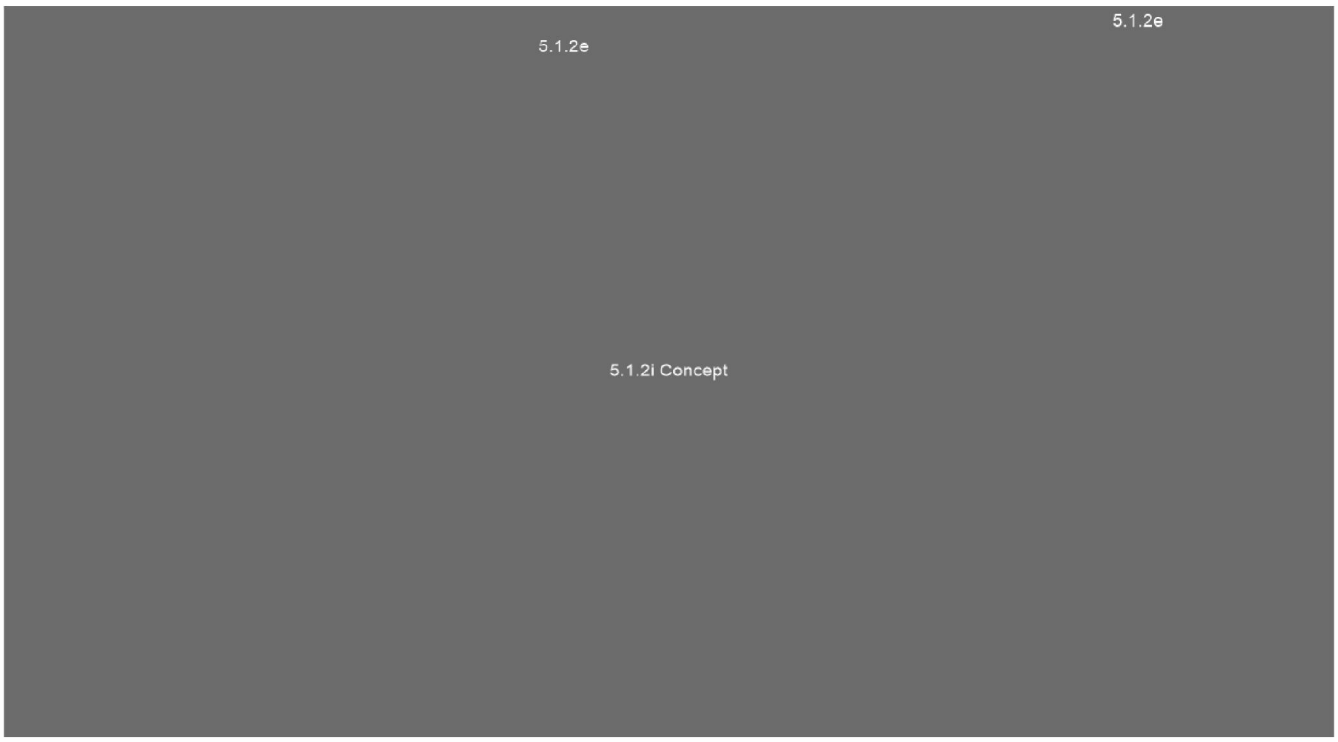
Hallo 5.1.2e

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;* 5.1.2h *".*

Zou jij deze aanvullingen met 5.1.2e kunnen delen voor het finaliseren van het document en het laten tekenen door beiden partijen? Zo niet, wie kan dit faciliteren?

Overige aandachtspunten





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: 5.1.2i Concept 5.1.2i Concept 5.1.2i Concept 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 5.1.2e 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 5.1.2h [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

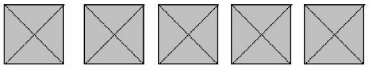
.....

T + 31 (0)30 5.1.2e
M +31 (0)6 5.1.2e
http://www.rivm.nl

.....

5.1.2e

.....



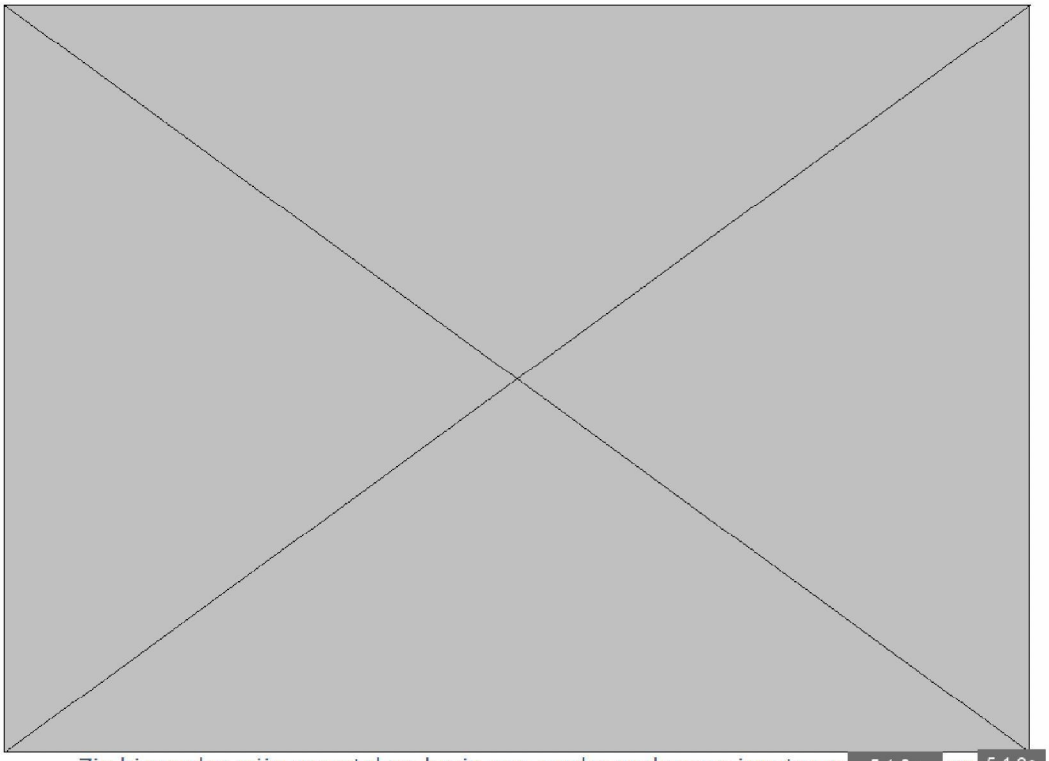
Van: 5.1.2e <5.1.2e @rivm.nl>
Verzonden: dinsdag 9 februari 2021 16:32
Aan: 5.1.2e <5.1.2e @rivm.nl>; 5.1.2e <5.1.2e @rivm.nl>; 5.1.2e <5.1.2e @rivm.nl>
CC: 5.1.2e <5.1.2e @rivm.nl>; 5.1.2e <5.1.2e @rivm.nl>; 5.1.2e <5.1.2e @rivm.nl>; 5.1.2e <5.1.2e @rivm.nl>
Onderwerp: RE: Aanvullende eisen RIVM bij verwerkersovereenkomst getekend 5.1.2h [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.



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

5.1.2i Concept

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 < 5.1.2e @rivm.nl>; 5.1.2e < 5.1.2e @rivm.nl>
Subject: FW: Aanvullende eisen RIVM bij verwerkersovereenkomst getekend 5.1.2h [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; 5.1.2h *"*, 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** 5.1.2e **& EVT. ACTIE** 5.1.2e **]**

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 (Information Security Officer 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 5.1.2h
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 5.1.2h

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 5.1.2h (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 (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

5.1.2e

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

Dit bericht kan informatie bevatten die niet voor u is bestemd. Indien u niet de geadresseerde bent of dit bericht abusievelijk aan u is verzonden, wordt u verzocht dat aan de afzender te melden en het bericht te verwijderen. Het RIVM aanvaardt geen aansprakelijkheid voor schade, van welke aard ook, die verband houdt met risico's verbonden aan het elektronisch verzenden van berichten.
www.rivm.nl 5.1.2e

This message may contain information that is not intended for you. If you are not the addressee or if this message was sent to you by mistake, you are requested to inform the sender and delete the message. RIVM accepts no liability for damage of any kind resulting from the risks inherent in the electronic transmission of messages.
www.rivm.nl/en 5.1.2e