

To: [redacted] [redacted]@rivm.nl
From: [redacted]
Sent: Wed 2/10/2021 12:25:58 PM
Subject: RE: Aanvullende eisen RIVM bij verwerkersovereenkomst getekend [redacted] [Advies over aan Xerox te stellen eisen in verband met verwerken oproepbrieven COVID-19]
Received: Wed 2/10/2021 12:25:58 PM

Hi [redacted]

Bedankt voor je antwoord.

Ik zal het eerste punt wel even met [redacted] checken, hij zou hier vast wel een antwoord op hebben.

Wat betreft het opnemen van deze punten in de extra verwerker overeenkomst met Xerox zal ik met [redacted] en [redacted] opnemen, zij hebben immers het gesprek met [redacted] gevoerd.

Groeten,

...

[redacted]
[redacted]

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

Ha [redacted]

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 [redacted] (en tel. nr. erbij, is mss handig: +316 [redacted]) worden ingevuld. Zij is [redacted] (en dus ook [redacted]).

Tip van [redacted] 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,

[redacted]

[redacted]
[redacted]

.....
Stafeenheden Communicatie & Documentaire Informatievoorziening
Rijksinstituut voor Volksgezondheid en Milieu

Antonie van Leeuwenhoeklaan 9 | 3721 MA Bilthoven
 Postbus 1 | 3720 BA Bilthoven

.....
T + 31 (0)30 [redacted]

M +31 (0)6 [redacted]

<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>; 5.1.2e <5.1.2e@rivm.nl>

Onderwerp: RE: Aanvullende eisen RIVM bij verwerkersovereenkomst getekend 5.1.2e [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
- Welke namen kunnen we hiervoor doorgeven? 5.1.2e
- 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>; 5.1.2e <5.1.2e@rivm.nl>

Subject: FW: Aanvullende eisen RIVM bij verwerkerovereenkomst getekend 5.1.2e [Advies over aan Xerox te stellen eisen in verband met verwerken oproepbrieven COVID-19]

Sensitivity: Confidential

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; 5.1.2e 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 genoeg 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 5.1.2e deze afspraken niet heeft meegetekend en uit niets blijkt dat deze tussen RIVM en Xerox gemaakte afspraken, 5.1.2e binden (behalve de bewering door 5.1.2e 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]

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 (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 5.1.2e

Sensitivity: Confidential

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 5.1.2e

Geachte 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 5.1.2e
stuur ik u de eisen die het RIVM graag

als extra bijlage bij de verwerkersovereenkomst 5.1.2e (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 5.1.2e 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 3 wordt 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 [redacted] 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 [redacted] 5.1.2e (Xerox) aan [redacted] 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 **informer** **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 [redacted 5.1.2e] en mijzelf in de cc.

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

Hoogachtend,

en met vriendelijke groet,

[redacted 5.1.2e]

[redacted 5.1.2e]

RIVM)

[redacted 5.1.2e]

[redacted 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 [redacted 5.1.2e] 3720 BA Bilthoven

T: 06- [redacted 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 *De zorg voor morgen begint vandaag*

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 *Committed to health and sustainability*