Ministerie van Volksgezondheid,
Welzijn en Sport

> Retouradres Postbus 20350 2500 EJ Den Haag

De Voorzitter van de Eerste Kamer
der Staten-Generaal
Postbus 20017
2500 EA DEN HAAG

Bezoekadres:
Parnassusplein 5
2511 VX Den Haag
T 070 340 79 11
F 070 340 78 34
www.rijksoverheid.nl

Ons kenmerk
2369592-1009922-PDC19

Bijlage(n)
-

Uw kenmerk
167290.190u

Correspondentie uitsluitend richten aan het retouradres met vermelding van de datum en het kenmerk van deze brief.

Datum 1 oktober 2021
Betreft Nader schriftelijk overleg in reactie op verslag schriftelijk overleg EK 35.526 / 25.295, AW

Geachte voorzitter,

De leden van de vaste commissies voor Justitie en Veiligheid, voor Volksgezondheid, Welzijn en Sport, voor Binnenlandse Zaken en de Hoge Colleges van Staat / Algemene Zaken en Huis van de Koning, en voor Infrastructuur, Waterstaat en Omgeving hebben een aantal vragen gesteld naar aanleiding van de stand van zakenbrief Covid-19 van 28 mei 2021. Hierbij stuur ik u de antwoorden op uw vragen.

In de breed samengestelde commissievergadering[1] van 18 mei 2021 over de correspondentie m.b.t. de covid-19 wetsvoorstellen en maatregelen is het verslag van een schriftelijk overleg over de stand van zakenbrief COVID-19 van 23 februari 2021[2] aan de orde geweest. De leden van de GroenLinks-fractie hebben kennisgenomen van uw antwoordbrief van 29 april 2021. De leden achten de beantwoording niet op alle punten adequaat. Zij hebben daarom nog enkele vervolgvragen gesteld.

1. In antwoord op de eerste vraag van de GroenLinks-fractie geeft u aan dat zowel de Autoriteit Persoonsgegevens als het College van de Rechten van de Mens betrokken zijn geweest bij het waarborgen van privacy en informatiebeveiliging in de ontwikkeling van de CoronaMelder-app en de CoronaCheck-app. Kunt u meer in detail treden over wat deze betrokkenheid specifiek inhield, en hoe dit is verlopen? Op 17 februari 2021 is de eindrapportage CoronaMelder Evaluatie gepubliceerd. Daarin is te lezen dat bij de evaluatie een vergelijking is gemaakt tussen van gebruikers CoronaMelder en niet-gebruikers CoronaMelder. In hoeverre kunt u garanderen dat bij deze evaluatie of mogelijk andere reeds uitgevoerde of geplande evaluaties over de effectiviteit CoronaMelder onderzoeksdata niet is gekoppeld aan, of verrijkt met, persoonsgegevens uit andere, in uw beheer zijnde of in uw opdracht gerealiseerde applicaties zoals CoronIT of HPZone voor het bestrijden van Covid-19? Oftewel, in hoeverre kunt u de beloofde anonimiteit van CoronaMelder nog steeds garanderen?

Antwoord vraag 1.
Voorafgaand aan de ontwikkeling van CoronaMelder, heb ik mij tijdens de beoordelingen van de marktconsultatie en in de appathon fase voor de niet-functionele eisen van een digitale oplossing, laten adviseren door diverse deskundigen van binnen en buiten de overheid, waaronder het College van de Rechten voor de Mens als ook de Autoriteit Persoonsgegevens (AP). Gedurende het verdere ontwikkeltraject heeft het College meegekeken en mij van advies voorzien vanuit het oogpunt van inclusie en toegankelijkheid. Daarnaast is, zoals op 9 april 2020 door de Tweede Kamer middels de motie Jetten c.s. verzocht, o.a. in het kader van privacy, de Autoriteit Persoonsgegevens ook in de verdere uitwerking van CoronaMelder betrokken geweest. Daarbij heb ik de AP om advies gevraagd ten aanzien van de gegevensverwerking die in het kader van CoronaMelder plaatsvindt. Hierover is advies uitgebracht waarin werd gesteld dat zij explicitering van de bestaande wettelijke grondslag om de gegevens te verwerken in aparte wetgeving noodzakelijk achtten voorafgaand aan landelijke introductie van de app. Hiertoe ben ik een spoedwetprocedure gestart om dit te realiseren. Hier is onder andere de Tijdelijke wet notificatieapplicatie covid-19 uit voortgekomen waar beide partijen advies over hebben gegeven. Ook de Tijdelijke wet coronatoegangsbewijzen covid-19, de wetgeving waarin de inzet van CoronaCheck staat beschreven, is aan de Autoriteit Persoonsgegevens en het college voor de Rechten van de Mens voorgelegd.

De leden van de GroenLinks-fractie vragen in hoeverre de anonimiteit van CoronaMelder nog steeds kan worden gegarandeerd, onder andere in relatie tot onderzoek naar de app. Ik kan de anonimiteit van het gebruik van CoronaMelder nog steeds garanderen. In het kader van de evaluatie CoronaMelder is geanonimiseerd vragenlijstonderzoek gedaan, waarbij middels vraagstelling onderscheid is gemaakt naar gebruikers en niet-gebruikers. De data uit deze en andere vragenlijstonderzoeken van de evaluatie zijn niet gecombineerd of verrijkt met persoonsgegevens in genoemde applicaties CoronIT en HPZone die door de GGD'en gebruikt worden voor het uitvoeren van hun taken in het kader van infectieziektebestrijding en door de GGD-GHOR worden beheerd.

2. De leden begrijpen uit uw reactie dat de GGD'en zelf besluiten welke afwegingskaders ze gebruiken voor hun werkprocessen en systemen, zolang daarmee voldaan wordt aan de AVG. Heeft u er zicht op in hoeverre nationale en internationale adviezen zoals de adviezen van de Gezondheidsraad en de Raad van Europa hierin meegewogen worden? Kunt u het Data Protection Report van de Raad van Europa van oktober jongstleden en een eerdere joint statement van de Raad van Europa onder de aandacht van de GGD'en brengen?

Antwoord vraag 2.
Ik heb geen zicht op, in hoeverre nationale en internationale adviezen zoals de adviezen van de Gezondheidsraad en de Raad van Europa, meegewogen worden bij de GGD's. De toezichthoudende rol is bij de AP belegd. Ik zal de Data Protection Report van oktober jongstleden en een eerdere joint statement van de Raad van Europa bij de GGD's onder de aandacht brengen.

3. U bepaalt tot in groot detail CoronIT en de te gebruiken applicaties die u beschikbaar stelt aan de GGD'en. Ook over wie wanneer welke gegevens aan wie moet verstrekken in het kader van Covid-19. Bent u het eens dat u daarmee feitelijk als verwerkingsverantwoordelijke handelt terwijl de GGD'en dat in naam zijn? Hoe verhoudt dit zich tot de verantwoordelijkheid inzake dataprotectie en dataveiligheid? Volgens AP, EDPB en jurisprudentie is degene die zich feitelijk als verwerkingsverantwoordelijke gedraagt verwerkingsverantwoordelijk. Graag een reactie. In de optiek van de fractie van GroenLinks is het te makkelijk om te

stellen dat de afwegingskaders bij de GGD'en liggen, terwijl zij gelet op diverse protocollen, de website van de GGD, GHOR en persconferenties gehouden zijn te handelen conform de voorschriften vanuit de minister. Graag uw reactie.

Antwoord vraag 3.
De opvatting die de leden van GroenLinks-fractie beschrijven; dat degene die zich als feitelijk verwerkingsverantwoordelijk gedraagt ook verwerkings-verantwoordelijk is, deel ik met de GroenLinks-fractie, de AP, EDPB en is reeds beschreven in jurisprudentie. Belangrijk om te vermelden is dat het daarbij gaat over de feitelijke verwerking van gegevens. Dat is hier niet aan de orde.

De GroenLinks-fractie benoemt specifiek CoronIT. CoronIT wordt door de GGD onder andere gebruikt om testresultaten en gezette vaccinaties in te registreren. De GGD is op grond van de WGBO verplicht dit op te nemen in een medisch dossier. Deze registratie valt onder de verwerkingsverantwoordelijkheid van de arts of instelling die de handeling uitvoert. Degene die deze registratieplicht heeft, is tevens de verwerkingsverantwoordelijke. Ik bepaal als minister niet hoe dat gebeurt, ook niet voor de registratie die de GGD voert in CoronIT.

Daarbij bepaal ik als minister ook niet wie, wanneer welke gegevens aan wie moet verstrekken. Wie welke gegevens moet registreren en wie welke gegevens mag of moet verstrekken is bepaald in de wet. Dat is geen directe beleids- of discretionaire bevoegdheid van de minister.

Het project is gestart zodat GGD GHOR Nederland de 25 regionale GGD'en kan faciliteren en ondersteunen in de taak die zij aan het begin van de crisis hebben geaccepteerd, namelijk het testen voor de bestrijding van het COVID-19-virus.

De minister van VWS is in deze hoedanigheid geen verwerkingsverantwoordelijke voor CoronIT. CoronIT ondersteunt de bedrijfsprocessen van de GGD'en bij testen en vaccineren. GGD GHOR Nederland is, namens de 25 GGD'en, opdrachtgever van de leverancier voor de bouw en de doorontwikkeling van CoronIT.

De GGD'en bepalen daarmee de functionaliteit. GGD GHOR Nederland geeft aan de opbouw van CoronIT grotendeels bepaald te hebben en daarmee ook hoe de persoonsgegevens in deze applicatie verwerkt worden. GGD GHOR Nederland en de 25 GGD'en kwalificeren zich daarom als gezamenlijk verwerkings-verantwoordelijk voor CoronIT. De GGD'en zijn verwerkingsverantwoordelijk voor de persoonsgegevens die zij in hun eigen regio verwerken.

De verantwoordelijkheid voor dataprotectie en dataveiligheid ligt bij de verwerkingsverantwoordelijke. In het genoemde voorbeeld zijn dat de GGD'en in combinatie met GGD GHOR Nederland. De eisen waar de verwerkings-verantwoordelijke aan moet voldoen volgt onder andere uit de AVG, UAVG en in dit geval de NEN-7510 en verder wat een norm betreft voor informatiebeveiliging in de zorg.

4. De leden van de GroenLinks-fractie waarderen de uiteenzetting van de ethische en medische dilemma's ten opzichte van het inzetten van vaccinatiestatus in de kabinetsreactie van 8 maart, en uw specificering dat vaccinatiegegevens enkel bij toestemming vooraf door worden gegeven aan het COVID-vaccinatie Informatie- en Monitoringssysteem van het RIVM. Toch lezen de leden nog geen antwoord op hun vraag om een toezegging te doen m.b.t. function creep. Vandaar nogmaals de vraag: kunt u toezeggen dat het mogelijke vaccinatiebewijssysteem nergens anders voor wordt gebruikt dan voor een van te voren duidelijk omschreven en proportioneel doel? Kunt u garanderen dat deze gegevens niet verrijkt worden met gegevens uit andere systemen in beheer van VWS of RIVM. Welke by design

en by default oplossingen worden gebruikt om de toch verwerkte persoonsgegevens zodanig te minimaliseren en te beschermen dat er de impact zo min mogelijk wordt voor de betrokkenen?

Antwoord vraag 4.
De doelen van de centrale vaccinatieregistratie in CIMS zijn publiek kenbaar gemaakt door het RIVM en is onder meer gestoeld op haar taak in het kader van de Wet publieke gezondheid. In de privacyverklaring wordt ook nader geïnformeerd hoe omgegaan wordt met persoonsgegevens (https://www.rivm.nl/covid-19-vaccinatie/privacy).

CIMS is geen vaccinatiebewijssysteem, maar een registratiesysteem voor het vaccineren en ten uitvoering van de publieke taak zoals genoemd in de Wet publieke gezondheid t.b.v. onderzoek en evaluatie van het vaccinatieprogramma. CIMS is ook een van de bronnen voor uitgifte van een vaccinatiebewijs. Voor epidemiologische evaluatie en onderzoek, kan data uit CIMS worden gebruikt en kan de data gecombineerd worden met andere data. Hierbij staat privacy hoog in het vaandel en er wordt gewerkt volgens de principes van privacy by design en default. Denk bijvoorbeeld aan pseudonimisering.

De verwerking van persoonsgegevens gebeurt altijd binnen de kaders van de privacy wet -en regelgeving. Dat betekent dat persoonsgegevens alleen worden verwerkt voor een vooraf bepaald gerechtvaardigd doel. Hiertoe worden onder meer DPIA's opgesteld voor een zorgvuldige afweging op grond van de AVG. Daarmee wordt tegemoet gekomen – en getoetst aan - aan doelbeschrijving en proportionaliteit.

Hoogachtend,

de minister van Volksgezondheid,
Welzijn en Sport,

Hugo de Jonge