

Vragen gesteld door de leden der Kamer, met de daarop door de regering gegeven antwoorden

2458

Vragen van het lid **Hijink** (SP) aan de Minister voor Medische Zorg over *het bericht «Ook jouw medische data liggen nu bij Google»* (ingezonden 2 april 2019).

Antwoord van Minister **Bruins** (Medische Zorg) (ontvangen 30 april 2019)

Vraag 1

Kent u het bericht «Ook jouw medische data liggen nu bij Google»? Was dit bij u bekend?¹ wat is uw reactie daarop?

Antwoord 1

Ja ik ken dit bericht. Nee, het was mij niet bekend.

Vraag 2

Vindt u het zorgelijk dat de medische gegevens van honderdduizenden Nederlandse ziekenhuisbezoekers door bedrijven worden verwerkt en sinds kort in de cloud van Google bewaard worden? Zo ja, wat gaat u daar aan doen? Zo nee, waarom niet?

Antwoord 2

Ik hecht bij de verwerking van medische gegevens het grootste belang aan informatiebeveiliging en privacybescherming. MRDM heeft mij laten weten een uitgebreide risicoanalyse te hebben uitgevoerd voorafgaand aan het besluit over het plaatsen van de data en juist vanuit de overweging van informatiebeveiliging de keuze gemaakt te hebben voor Google Cloud Platform (GCP).

Zoals ik reeds heb aangekondigd, zal ik onafhankelijk onderzoek laten doen naar de wenselijkheid van het gebruik van niet-Europese Cloud platforms voor het opslaan van zorgdata.

Vraag 3

Zou het volgens u bij de betreffende Nederlanders bekend moeten zijn dat hun persoonlijke gegevens verzameld en verwerkt worden door Medical Research Data Management (MRDM), een van de grootste medische databedrijven van het land? Deelt u de mening van Elektronisch Patiënten-dossier (EPD)-expert Van 't Noordende dat burgers altijd moeten kunnen zien

¹ <https://www.ad.nl/binnenland/ook-jouw-medische-data-liggen-nu-bij-google~abcb3f6a/>

wie de verwerkers van hun data zijn, ook als het gepseudonimiseerde gegevens zijn?

Antwoord 3

Onder de Algemene verordening gegevensbescherming (AVG) bestaat een informatieplicht; elke verwerkingsverantwoordelijke is verplicht betrokkenen waarvan persoonsgegevens worden verwerkt, duidelijk te informeren over wat er met de persoonsgegevens gedaan wordt en waarom. De ziekenhuizen zijn in deze de verwerkingsverantwoordelijken. Aan de informatieplicht wordt doorgaans invulling gegeven middels een (online) privacyverklaring. In de privacyverklaring moet onder andere de (categorieën van) ontvangers van de persoonsgegevens worden opgenomen, dat wil zeggen de verwerkers zoals MRDM. Subverwerkers worden als dusdanig niet expliciet genoemd.

Vraag 4 en 5

Is volgens u het pseudonimiseren van patiëntgegevens voldoende om de privacy te beschermen, ook aangezien veel gegevens weer ontsleuteld kunnen worden en het voor Google technisch gezien een fluitje van een cent schijnt te zijn om de anonieme data naar een persoon te herleiden? Gaan ziekenhuizen en artsen aangaande deze kwestie voldoende secuur met de gevoelige informatie om?

Hoe oordeelt u over het risico dat Google aan de haal gaat met de medische gegevens van de honderdduizenden Nederlanders?

Antwoord 4 en 5

Het pseudonimiseren van patiëntgegevens als enige maatregel is in het onderhavige geval niet afdoende. MRDM heeft mij laten weten dat het pseudonimiseren van persoonsgegevens één van meerdere maatregelen is die zijn genomen om de privacy van de betrokkenen te beschermen. MRDM laat weten de data ook dubbel te versleutelen, dus een versleuteling door Google en een eigen versleuteling, waarmee de gegevens niet toegankelijk zijn voor Google.

MRDM heeft mij laten weten dat de gegevens zijn opgeslagen in het datacentrum van Google in Eemshaven. De gegevens blijven daarmee in Nederland en vallen onder Nederlandse en Europese wet- en regelgeving. Vanuit de contractuele verplichtingen die MRDM met Google heeft gesloten, mag Google niet aan de data komen. Google LCC is gecertificeerd onder het EU-US Privacy Shield. De Europese Commissie heeft met het afsluiten van het EU-US Privacy Shield-framework bedrijven in de EU een mechanisme gebracht voor naleving van de vereisten van de Europese wetten inzake gegevensbescherming.

Vraag 6

Wat is uw reactie op de constatering dat Medical Research Data Management voor de wet als zodanig niet bestaat, aangezien het bedrijf volledig opereert in opdracht van en onder verantwoordelijkheid van de ziekenhuizen en behandelaars? Wat is vervolgens uw reactie op de constatering dat de onderneming als dataverwerker niet verplicht is om toestemming te vragen aan patiënten of om hen te informeren?

Antwoord 6

Het ziekenhuis is in dit geval verwerkingsverantwoordelijke in de zin van de AVG. Een verwerkingsverantwoordelijke kan een verwerker inschakelen om bepaalde verwerkingen te doen, in dit geval het bedrijf MRDM. Dat betekent dat deze verwerker in opdracht van het ziekenhuis opereert. De verwerkingsverantwoordelijke moet waarborgen dat hij met een partij in zee gaat die voldoende garanties biedt ten aanzien van passende technische en organisatorische maatregelen opdat de verwerking aan de AVG voldoet (artikel 28 AVG). Er wordt dan een verwerkingsovereenkomst gesloten waarin onder meer het onderwerp en duur van de verwerking, de aard en het doel, het soort persoonsgegevens en verplichtingen worden vastgelegd.

De verplichting voor het informeren van betrokkenen over gebruik en opslag van data ligt bij de verwerkingsverantwoordelijke, in dit geval de ziekenhuizen.

Vraag 7

Deelt u de mening met Medical Research Data Management dat alles veilig is?

Antwoord 7

Dit oordeel is aan de Autoriteit Persoonsgegevens.

Vraag 8

Bent u van plan de Autoriteit Persoonsgegevens te verzoeken de kwestie te toetsen? Zo nee, waarom niet?

Antwoord 8

De AP heeft mij laten weten een onderzoek te zijn gestart naar de naleving van de verplichtingen die uit de AVG voortkomen bij het betreffende bedrijf. Ik ben daarnaast voornemens een onafhankelijk onderzoek uit te laten voeren naar het gebruik van niet-Europese Cloud platforms voor het opslaan van zorgdata. Ik heb de AP verzocht aan te geven of zij mij hier advies over uit kunnen brengen. De AP heeft mij laten weten dat dit niet binnen de verantwoordelijkheden en bevoegdheden van de AP past. Ik zal hiervoor een geschikte, onafhankelijke partij benaderen.

Vraag 9

Klopt het dat de Amerikaanse inlichtingendiensten op grond van de Cloud Act zichzelf toegang kunnen verschaffen tot data die op servers van Amerikaanse bedrijven staan? Kunt u garanderen dat bij Google deze medische data nooit onderwerp van onderzoek worden van Amerikaanse diensten?²

Antwoord 9

De Cloud Act (Clarifying Lawful Overseas Use of Data Act) bevat geen bevoegdheid voor de Amerikaanse overheid tot het toegang verschaffen tot servers van bedrijven behalve indien die gegevens worden aangemerkt als elektronisch bewijs in strafzaken. Hier is een bevel nodig van een Amerikaanse rechter. In de praktijk is het nog niet voorgekomen dat Europese of Nederlandse wetgeving terzijde is geschoven. De Raad van de EU heeft de Europese Commissie verzocht om voorbereidingen te treffen voor onderhandelingen met de VS over een verdrag naar aanleiding van de Cloud Act. Zodra de Europese Commissie een voorstel zal hebben gedaan voor een onderhandelingsmandaat zal Nederland daarover een standpunt formuleren. (Kamerstuk 32 317, nr. 526)

Vraag 10

Zou het niet veel beter zijn als medische data in beheer worden gebracht bij Nederlandse of Europese organisaties zodat ook de desbetreffende wetgeving en bescherming op de data van kracht is?

Antwoord 10

Ik zal onafhankelijk onderzoek laten doen naar de wenselijkheid van het gebruik van niet-Europese Cloud platforms voor het opslaan van zorgdata.

Vraag 11

Wat is uw (toekomst)visie aangaande de wijze waarop we omgaan met de (steeds groter wordende hoeveelheid) zorgdata?

Antwoord 11

In mijn brief «Data laten werken voor gezondheid» (Kamerstuk 27 529, nr. 164) geef ik u mijn visie op de omgang met zorgdata. In deze brief heb ik op een zestal thema's³ actielijnen geformuleerd die nu nader uitgewerkt en ingevuld worden. Aan het einde van dit jaar zal ik u informeren over de voortgang op elke van deze actielijnen.

² <https://www.securityvandaag.nl/article/item/nieuwe-vs-cloud-act-europese-privacy>

³ De zes thema's: «vertrouwen in de uitkomst van data-analyses», «zeggenschap», «digitale inclusie», «de rol en het vertrouwen van de zorgprofessional», «datasolidariteit» en «interoperabiliteit en data aan de bron»

Toelichting:

Deze vragen dienen ter aanvulling op eerdere vragen terzake van de leden Verhoeven en Raemakers (beiden D66), ingezonden, 2 april 2019 (Aanhangsel Handelingen, vergaderjaar 2018–2019, nr. 2457)