

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

2457

Vragen van de leden **Verhoeven** en **Raemakers** (beiden D66) aan de Ministers voor Rechtsbescherming en voor Medische Zorg en Sport over *het bericht «Medische gegevens duizenden Nederlanders verplaatst naar Google: «Riskant»»* (ingezonden 2 april 2019).

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

Vraag 1

Kent u het artikel «Medische gegevens duizenden Nederlanders verplaatst naar Google: «Riskant»»?¹

Antwoord 1

Ja.

Vraag 2

Bent u van tevoren door de betrokken ziekenhuizen of het bedrijf Medical Research Data Management op de hoogte gesteld van het verplaatsen van medische gegevens van patiënten naar de Google Cloud?

Antwoord 2

Nee, deze verplichting is er ook niet.

Vraag 3, 4 en 5

Wat is uw mening over deze praktijk? Acht u het een veilige manier van opslaan van medische gegevens?

Waarom zijn de patiënten niet op de hoogte gesteld van deze praktijk? Is de privacy van de betrokken patiënten voldoende gewaarborgd? Is de Autoriteit Persoonsgegevens op de hoogte gebracht van deze praktijk?

Klopt het dat Google niet bij de gegevens kan? Is het bekend waar de gegevens precies worden opgeslagen? Is dat in een datacenter in Nederland? Welke wettelijke eisen zijn daarbij van toepassing? Zijn er geen meer privacy-vriendelijke alternatieven die minder risico's met zich meebrengen?

¹ RTL Nieuws, 30 maart 2019, <https://www.rtlnieuws.nl/nieuws/artikel/4660076/medische-gegevens-honderdduizenden-nederlanders-verplaatst-naar-google>

Antwoord 3, 4 en 5

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).

MRDM laat mij tevens 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 met het afsluiten van het EU-US Privacy Shield-framework bedrijven in de EU een adequaat mechanisme gebracht voor naleving van de vereisten van de Europese wetten inzake gegevensbescherming die te maken hebben met de overdracht van persoonlijke gegevens van de Europese Unie naar de Verenigde Staten. MRDM laat daarnaast weten de data dubbel te versleutelen, dus een versleuteling door Google en een eigen versleuteling, waarmee de gegevens niet toegankelijk zijn voor Google. Tenslotte is geregeld dat wanneer beheerders van Google zich vanuit beheerswerkzaamheden toegang verschaffen tot de versleutelde gegevens, MRDM daar melding van krijgt, zodat gecontroleerd kan worden dat Google zich aan wettelijke en contractuele bepalingen houdt.

De verantwoordelijkheid voor het informeren van betrokkenen over de opslag en het gebruik van data ligt bij de betrokken zorginstellingen. Zo ook het in voorkomende gevallen betrekken van de Autoriteit Persoonsgegevens (AP). Na de berichtgeving in de media inzake Medical Research Data Management heb ik contact gezocht met de AP. De AP heeft mij laten weten dat ziekenhuizen onder voorwaarden patiëntgegevens in een cloud mogen opslaan, mits voldaan wordt aan de verplichtingen van de AVG.

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

Vraag 6

Wat zijn onder zorgaanbieders de meest gebruikte praktijken van opslag van medische gegevens van patiënten en welke risico's op het gebied van cyberveiligheid en privacy brengen die verschillende methodes met zich mee?

Antwoord 6

De meest gebruikte praktijk was/is een eigen (in-house) datacentrum/computer. Wij zien nu een versnelde beweging naar de Cloud, met name bij de kleinere zorgaanbieder als huisartsen, tandartsen, fysiotherapiepraktijken, etc. Een belangrijke overweging daarbij is dat deze zorgaanbieders niet de kennis en de middelen hebben om lokale opslag van patiëntgegevens goed te beveiligen. Dataopslag in de cloud komt derhalve relatief vaak voor in de zorg, juist vanwege de gevoeligheid en behoefte aan professionele informatiebeveiligings- en privacywaarborgen.