Ministerie van Binnenlandse Zaken en Koninkrijksrelaties

Aan: de Voorzitter van de Tweede Kamer der Staten-Generaal
Postbus 20018
2500 EA Den Haag

Directoraat-generaal Overheidsorganisatie
Directie Digitale Overheid i.o.

www.rijksoverheid.nl
www.facebook.com/minbzk
www.twitter.com/minbzk

Kenmerk
2019-0000652396

Uw kenmerk

Datum 7 januari 2020

Betreft Kamervragen over het bericht dat de IRMA-app wordt gebruikt in een huisartsenpost

Hierbij bied ik u, mede namens de minister voor Medische Zaken en Sport, de heer Bruins, de antwoorden aan op de schriftelijke vragen die zijn gesteld door het lid Slootweg (CDA) over het bericht dat de IRMA-app wordt gebruikt in een huisartsenpost. Deze vragen werden ingezonden op 12 november 2019 met kenmerk 2019Z21789.

Vanwege de portefeuilleverdeling beantwoordt de minister Medische Zaken en Sport deze vragen en niet de minister van Volksgezondheid, Welzijn en Sport.

De minister van Binnenlandse Zaken en Koninkrijksrelaties,

drs. R.W. Knops

Directoraat-generaal Overheidsorganisatie
Directie Digitale Overheid i.o.

Kenmerk
2019-0000652396

2019Z21789

Vragen van het lid Slootweg (CDA) aan de ministers van Volksgezondheid, Welzijn en Sport en van Binnenlandse Zaken en Koninkrijksrelaties over het bericht dat de IRMA-app wordt gebruikt in een huisartsenpost (ingezonden 12 november 2019)

1. Heeft u kennisgenomen van het bericht 'Medipark Uden gaat live met HiX'? 1)

   Ja.

2. Klopt het bericht dat patiënten van Medipark Uden via het geïntegreerde online Zorgportaal eenvoudig en veilig hun herhaalmedicatie kunnen aanvragen op basis van de actuele medicatie van de patiënt?

   Het klopt dat patiënten van Medipark Uden via het online Zorgportaal hun herhaalmedicatie kunnen aanvragen.

3. Klopt het dat de patiënten van Medipark Uden dit doen door in te loggen via I Reveal My Attributes (IRMA) op het online portaal?

   Ja.

4. Klopt het dat IRMA een applicatie is die patiënten in staat stelt om zelf online aan te geven welke gegevens zij wel en niet willen delen, een methode die de privacy beschermt door 'privacy by design'?

   Volgens de informatie van IRMA houdt het ontwerp van de IRMA app rekening met privacy met een focus op dataminimalisatie, een van de privacybeginselen zoals opgenomen in de Algemene Verordening Gegevensbescherming.

5. Klopt het dat in de meest recente nationale en Europese wetgeving 'privacy by design' wordt vereist voor nieuwe ICT-systemen?

   Ja.

6. Is het juist dat Medipark Uden te horen heeft gekregen dat gebruik van IRMA in strijd is met artikel 87 van de Algemene Verordening Gegevensbescherming (AVG), artikel 46 van de Uitvoeringswet Algemene Verordening Gegevensbescherming (UAVG) en de wet Elektronisch Berichtenverkeer (wet EBV)?

   Nee, er is navraag gedaan bij Medipark Uden en zij heeft aangegeven niet hierover geïnformeerd te zijn.

7. Klopt het dat op basis van de huidige wetgeving patiënten van Medipark Uden eigenlijk alleen via DigiD mogen inloggen?

   Nee. In de zorgsector is het, evenals in andere sectoren, verplicht een inlogniveau van passend betrouwbaarheidsniveau aan te bieden, afhankelijk van de gegevens die worden ontsloten. Bij gegevens die onder het medisch beroepsgeheim vallen is dat niveau "hoog". Bij het gebruik van DigiD zijn nu de niveaus "substantieel" en "hoog" nog niet beschikbaar. De Autoriteit Persoonsgegevens heeft bij brief van 4 oktober 2018 (kenmerk: z2018-17511) gereageerd op vragen hieromtrent van VWS. De AP heeft geantwoord dat authenticatie dient plaats te vinden met ten minste tweefactorauthenticatie, in afwachting van het breder beschikbaar komen van authenticatiemethoden met een passend hoog niveau. Hieraan voldoet onder andere DigiD in combinatie met sms. Andere mogelijkheden worden echter niet uitgesloten.
   Zodra de Wet digitale overheid in werking treedt wordt het mogelijk om private inlogmiddelen toe te laten die een hoog betrouwbaarheidsniveau aanbieden.

8. Klopt het dat wanneer Medipark Uden DigiD zou gebruiken voor elektronische identificatie, zij 14 eurocent zou moeten betalen voor elke succesvolle inlog? 2)

   In 2017 heeft de ministerraad besloten dat vanaf 2018 alle kosten voor beheer en exploitatie van DigiD worden doorbelast aan dienstverleners die zijn aangesloten op DigiD. Deze kosten worden dus niet aan burgers doorbelast.
   Voor 2019 is het bedrag door het ministerie van Binnenlandse Zaken en Koninkrijksrelaties vastgesteld op €0,117 per succesvolle inlog, excl. BTW. Dit bedrag wordt ieder jaar opnieuw vastgesteld voor het daaropvolgende jaar. De prijs is afhankelijk van de kosten voor de doorontwikkeling van DigiD en de onderliggende infrastructuur.
   Overigens is het zo dat de minister van Volksgezondheid, Welzijn en Sport de kosten voor het gebruik van DigiD in de zorg vergoedt. Medipark Uden hoeft daarom niet per succesvolle inlogpoging te betalen.

9. Klopt het dat deze 14 eurocent per inlog gaan naar het bedrijf Logius, dat dan de beheerder is van de gegevens van de burger?

   Ja. Logius brengt het werkelijke gebruik in rekening bij de dienstverlener die gebruikmaakt van DigiD (in dit geval het ministerie van VWS).
   Ik benadruk dat Logius geen bedrijf is, maar een baten-lastendienst die onderdeel is van het ministerie van Binnenlandse Zaken en Koninkrijksrelaties, en onder andere DigiD beheert. Logius verwerkt voor DigiD enkel gegevens van de burger die nodig zijn voor het gebruik van DigiD. Voor een volledig overzicht verwijs ik naar het Besluit verwerking persoonsgegevens digitale infrastructuur en de privacyverklaring van DigiD (zie https://www.digid.nl/wat-is-digid/privacy).

10. Klopt het dat de AVG, de UAVG en de wet EBV alleen toestemming verlenen aan DigiD omdat de firma Logius, als beheerder van de gegevens van de

burger, als enige toestemming heeft om Burger Service Nummers (BSN) van burgers te verwerken?

De verwerking van het BSN vereist een wettelijke basis. Het BSN mag verwerkt worden door overheidsinstanties voor het uitvoeren van hun publiekrechtelijke taak. Organisaties buiten de overheid mogen het BSN verwerken als dat wettelijk is bepaald. Denk in dit geval aan pensioenfondsen en zorgverleners.
In de wet EBV is geregeld dat de minister van BZK persoonsgegevens, waaronder het BSN, verwerkt voor de werking van DigiD.
Op dit moment is het zo dat DigiD het enige publieke elektronische identificatiemiddel is en daarmee ook het enige middel waarbij werking van het BSN is toegestaan. Het wetsvoorstel digitale overheid dat nu in behandeling is, beoogt ook andere (private) inlogmiddelen toe te laten, waarbij – ten behoeve van het inloggen bij de overheid– het BSN wordt verwerkt.

11. Overtreden lokale overheden of - zoals in het geval van Medipark - zorgaanbieders de wet wanneer een burger zich middels de IRMA-app identificeert?

    Op dit moment heeft alleen DigiD een wettelijke basis om het BSN te verwerken. Andere (private) inlogmiddelen kunnen deze wettelijk basis ook krijgen als de Wet digitale overheid van kracht wordt en zij als middel worden toegelaten. In het antwoord op vraag 7 gaf ik aan dat de Autoriteit Persoonsgegevens toeziet op het passend beveiligen van gegevens. De Autoriteit Persoonsgegevens heeft IRMA nog niet uitgesloten.
    Daarnaast geldt dat overheden een eigen verantwoordelijkheid hebben om adequate beveiliging van gegevens in te richten, waaronder de identificatie. Welke mate van beveiliging zij moeten hanteren hangt af van de dienstverlening die wordt aangeboden en de gegevens die daarbij worden ontsloten. Of het gebruik van de IRMA-app rechtmatig is hangt daarom af van de dienstverlening die wordt ontsloten, de gegevens die daarbij worden ontsloten en het betrouwbaarheidsniveau dat IRMA beoogt te bieden.

12. Kunt u uitleggen op welke wijze de stichting achter IRMA het BSN verwerkt?

    Zover mij bekend heeft de stichting dit als volgt ingericht. Het BSN wordt, via de inlog met DigiD, door de gemeente verwerkt bij het ophalen van de gegevens uit de BRP. Vervolgens worden het BSN en de overige gegevens uit de BRP in de IRMA app geplaatst. De gebruiker van de IRMA app kan deze gegevens, waaronder het BSN, onder zijn eigen verantwoordelijkheid verstrekken aan derden.

13. Wat is uw opvatting over attribuut gebaseerde authenticatie als wijze van elektronische identificatie?

    Ik sta in zijn algemeenheid positief tegenover het gebruik van attribuut gebaseerde authenticatie, mits deze voldoet aan de Europese eisen aan privacy (AVG) en inlogmiddelen (eIDAS).

Vooropgesteld merk ik op dat bij (elektronische) identificatie het erom gaat om iemands identiteit vast te stellen. Dit kan via een WID maar langs elektronische weg ook bijvoorbeeld via gezichtsherkenning in combinatie met een ander attribuut. Bij authenticatie wordt gecontroleerd of iemand is wie hij zegt dat hij is. Als we het hebben over authenticatie als wijze van elektronische identificatie, gaat het om de stap nadat een gebruiker zich heeft geïdentificeerd middels een bewijs van identiteit.

Of de authenticatie kan plaats vinden met een attribuut zal afhangen van de vraag of de dienstverlener kan vertrouwen op de juistheid en actualiteit van de attributen en dat deze daadwerkelijk toebehoren aan de betrokken burger. Hoe hoger het vereiste betrouwbaarheidsniveau bij het inloggen, hoe meer eisen aan dit vertrouwen zullen worden gesteld. Ik kijk met interesse uit naar middelen die aan deze eisen voldoen.

14. Kunt u voorbeelden geven van een app die een rechtspersoon of een natuurlijk persoon is?

    Een app is geen van beide. Een app is software die gemaakt wordt en/of geëxploiteerd wordt door een natuurlijke of rechtspersoon en onder diens verantwoordelijkheid valt.

15. Wanneer iemand een BSN intypt op een tekstverwerker en diegene gebruikmaakt van Microsoft, dient Microsoft als verwerker van het BSN dan ook een wettelijke grondslag te hebben?

    Wanneer iemand een natuurlijke persoon is en bij de uitoefening van een zuiver persoonlijke of huishoudelijke activiteit een BSN intypt in een clouddienst, dan is de AVG niet van toepassing. In de overige gevallen waar een BSN wordt ingetypt en opgeslagen in een clouddienst, is degene die de clouddienst aanbiedt verwerker. De clouddienst wordt conform AVG aangemerkt als een verwerker wanneer hij ten behoeve van een verwerkingsverantwoordelijke persoonsgegevens verwerkt. In de meeste gevallen bestaat er bij een clouddienst een dergelijke situatie. Voor de verwerking geldt dan de grondslag voor gegevensverwerking van de verwerkingsverantwoordelijke. In dat geval is een verwerkersovereenkomst verplicht. Deze verwerkersovereenkomst zal dan meestal onderdeel uitmaken van de algemene voorwaarden waaronder de clouddienst wordt aangeboden. Wanneer een BSN wordt ingetypt in een offline softwareapplicatie waarbij het BSN niet op een server wordt opgeslagen, tijdelijk vastgehouden of op een of andere manier via een clouddienst wordt verwerkt, is de aanbieder van de softwareapplicatie geen verwerker. Dit laat overigens de verantwoordelijkheid van de aanbieder van een applicatie om zorg te dragen voor een veilige applicatie onverlet.

16. Waarom zijn volgens u de gegevens van de burger, die nu in handen zijn van het overheidsbedrijf Logius (door het gebruik van DigiD), veiliger en betrouwbaarder belegd dan wanneer ze in handen van de burger zelf blijven, wanneer hij of zij zich elektronisch identificeert via het gebruik van de persoonlijke kluis van IRMA?

Veiligheid hangt af van inrichting en waarborgen die met betrekking tot gegevensverwerking worden getroffen. Daarbij maakt het niet uit of de gegevensverwerking plaatsvindt onder verantwoordelijkheid van de overheid of van een private organisatie. Hierbij moet rekening gehouden worden met alle privacybeginselen uit de AVG, waaronder het helpen van de persoon over wie gegevens worden verwerkt in geval van problemen, bijvoorbeeld als zijn identificatiemiddel is gestolen. Deze mogelijkheid wordt beperkt indien niet te achterhalen is op welk moment tijdens het inloggen wie wat heeft gedaan. Dit is het geval wanneer gegevens enkel in handen van de burger zelf blijven.
De verwerking van gegevens door de minister van BZK/Logius is met specifieke wettelijke waarborgen omkleed (in de Wet EBV en Besluit verwerking persoonsgegevens digitale infrastructuur), die vooralsnog tot inwerkingtreding van de Wet digitale overheid voor private middelen ontbreken.
Een aandachtspunt bij attributendiensten is wel dat het mogelijk maakt dat burgers zo laagdrempelig gegevens kunnen wisselen, ook met instanties die daartoe geen recht hebben, maar waarvan de burger afhankelijk is. In dit kader verwijs ik naar het overheidsbrede programma Regie op Gegevens dat de minister van BZK gestart is en dat beoogt om kaders te stellen voor het digitaal delen van persoonsgegevens die afkomstig zijn uit overheidsregistraties.

17. Heeft u, mede in het licht van de Wet Digitale Overheid, bezwaar tegen het gebruik van IRMA in de zorg, zoals nu bijvoorbeeld gerealiseerd door Medipark Uden? Zo ja, hoe gaat u vormgeven aan uw bezwaar?

    Het is belangrijk dat burgers een adequate beveiliging wordt geboden bij de digitale toegang tot hun medische gegevens. Betrouwbaar inloggen is daarvoor essentieel. Onder de Wet digitale overheid kies ik bewust voor het toelaten van private middelen (op minimaal betrouwbaarheidsniveau substantieel) vanuit het oogpunt van brede dekking en innovatie. De Wet digitale overheid stelt hier regels voor die aansluiten bij de Europese regels (eIDAS) voor inlogmiddelen. Ook IRMA zal hieraan moeten voldoen, om na inwerkingtreding van de Wet digitale overheid als Nederlands middel toegelaten te kunnen worden. Dit is nog niet vastgesteld. Daarnaast geldt dat IRMA ook als Europees middel niet genotificeerd is. In Europa zijn op dit moment enkele tientallen middelen eIDAS-genotificeerd. Voor IRMA geldt dat dit nog niet heeft plaatsgevonden.

1) ICT & health, 3 oktober 2019, 'Medipark Uden gaat live met HiX' (https://www.icthealth.nl/nieuws/medipark-uden-gaat-live-met-hix/).
2) Volkskrant, 24 september 2017, 'DigiD gaat geld vragen aan gebruikers - dat gaat pensioenfondsen 2 miljoen euro extra kosten' (https://www.volkskrant.nl/economie/digid-gaat-geld-vragen-aan-gebruikers-dat-gaat-pensioenfondsen-2-miljoen-euro-extra-kosten~b8528cc3/).