Ministerie van Volksgezondheid,
Welzijn en Sport

> Retouradres Postbus 20350 2500 EJ Den Haag

De Voorzitter van de Tweede Kamer
der Staten-Generaal
Postbus 20018
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
3393294-1032086-DICIO

Bijlagen
1

Uw brief
29 juni 2022

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

Datum 12 september 2022
Betreft Kamervragen

Geachte voorzitter,

Hierbij zend ik u, mede namens de staatssecretaris van Binnenlandse Zaken en Koninkrijksrelaties en de minister van Defensie, de antwoorden op de vragen van de leden Leijten en Hijink (beiden SP) over lekkende zorgdata (2022Z13503, ingezonden op 29 juni 2022).

Hoogachtend,

de minister van Volksgezondheid,
Welzijn en Sport,

Ernst Kuipers

Antwoorden op Kamervragen van de leden Leijten en Hijink (beiden SP) over lekkende zorgdata (2022Z13503, ingezonden op 29 juni 2022).

Vraag 1
Kunt u uitgebreid analyseren hoe het mogelijk is geweest dat een commercieel softwarebedrijf jarenlang de privacy van tienduizenden patiënten en tientallen huisartsen heeft geschonden door medische gegevens niet goed te beschermen? Kunt u uw antwoord toelichten? (1)

Antwoord vraag 1
Medworq verwerkte data in opdracht van huisartsen en heeft haar informatiebeveiliging ingericht conform de geldende normen en is hiervoor ISO27001 en NEN7510 gecertificeerd. Een oud-medewerker heeft in de rol van Information Security Officer (ISO) tijdens zijn interne controlewerkzaamheden data ontvreemd, aldus Medworq. In 2020 bleek volgens Medworq dat de oud-medewerker data had ontvreemd en zijn geheimhoudingsplicht had geschonden. Lopende het strafproces heeft de oud-medewerker de data aan journalistiek platform Follow The Money (FTM) overhandigd. De betreffende data zijn volgens FTM en de oud-medewerker nooit verder verspreid.

In een brief van 6 juli jl. geeft Medworq aan dat in samenwerking met Openbaar Ministerie (OM) is bewerkstelligd dat de ontvreemde data door de ex-medewerker is overhandigd aan een notaris, en dat alle kopieën van de betreffende data zijn gewist. Ook FTM heeft verklaard dat zij alle data die door de oud medewerker aan hen is verstrekt heeft gewist.

Vraag 2
In hoeverre vindt u het wenselijk dat commerciële bedrijven het ontwikkelen van medische apps - waarbij gevoelige medische data wordt verwerkt – sponsoren, terwijl deze bedrijven ook een commercieel belang hebben bij de inhoud van deze data? Kunt u uw antwoord uitbreid motiveren?

Antwoord vraag 2
Voorop staat dat gegevens over de gezondheid van personen tot de meest gevoelige gegevens behoren en dat deze gegevens op uitermate zorgvuldige wijze bewaard moeten worden en dat effectieve maatregelen getroffen moeten worden om te voorkomen dat zij uitlekken. De staatssecretaris van BZK en ik betreuren dat dit heeft plaatsgevonden en zetten ons in om bijzondere persoonsgegevens goed te (blijven) beschermen. Het is primair aan zorgaanbieders zelf om te zorgen dat voldaan wordt aan de wet- en regelgeving en daar goede voorzieningen voor te treffen. Daarnaast is goede controle op de naleving van deze regels noodzakelijk. Wij vinden het echter niet per definitie onwenselijk dat commerciële bedrijven medische apps ontwikkelen. Dit wordt ook al veel gedaan. Gedacht kan worden aan bijvoorbeeld gezondheidsapps (bijvoorbeeld apps die stappen tellen) en draagbare technologie (wearables; zoals horloges waarmee de bloeddruk wordt gemeten). Hierdoor krijgen mensen steeds vaker binnen en buiten de zorgcontext meer gegevens over hun eigen gezondheid. Dit versterkt hun positie en maakt dat zij meer grip krijgen op hun gezondheid. Ook vinden wij het niet per se onwenselijk dat zorgaanbieders gebruik maken van software - zoals een zorginformatiesysteem – die is ontwikkeld en feitelijk beheerd wordt door een softwareleverancier. Immers, ICT-aanbieders hebben de kennis en kunde om ICT te ontwikkelen die aansluit bij de wensen van het veld. Gegevens over de gezondheid vallen onder de bijzondere categorieën persoonsgegevens die onder de AVG extra bescherming genieten. Het uitgangspunt daarbij is dat de verwerking van gezondheidsgegevens verboden is, behalve in een aantal

uitzonderingsgevallen. Een van die uitzonderingen is dat de betrokkene uitdrukkelijk toestemming heeft gegeven voor de verwerking van deze gegevens voor specifieke doelen. Als dit wordt vertaald naar de context van een gezondheidsapp, betekent het vooraf voor de gebruiker van de app duidelijk moet zijn welke gegevens er op welke wijze verwerkt gaan worden en voor welke specifieke doeleinden dit gebeurt. De gebruiker moet hier expliciet toestemming voor geven voordat de gegevensverwerking plaatsvindt. Verder dient de verwerking van de gegevens zorgvuldig te gebeuren, wat onder meer inhoudt dat er niet meer gegevens worden verwerkt dan noodzakelijk en dat passende technische en organisatorische maatregelen worden genomen om de gegevens te beschermen. Dit laatste is in nationale wetgeving nader ingevuld: zorgaanbieders moeten voldoen aan de informatiebeveiligingsnormen NEN 7510, NEN 7512 en NEN 7513.

Daarnaast geldt het medisch beroepsgeheim, dat met zich brengt dat een hulpverlener in beginsel moet zwijgen over alles dat aan hem door de patiënt wordt toevertrouwd. Het belang van het wettelijk beroepsgeheim wordt onderstreept door de strafbaarstelling van schending ervan. Voor degenen die geen medisch beroepsgeheim hebben, maar wel beroepsmatig op de hoogte raken van behandelgegevens van de patiënt, zoal ICT-ers, geldt overigens een afgeleid medisch beroepsgeheim. Dat betekent dat voor hen dezelfde regels gelden als voor hulpverleners.

Deze kaders bieden, mits zij goed worden toegepast, robuuste waarborgen voor de verwerking van gezondheidsgegevens door medische apps. Het is primair aan zorgaanbieders zelf om te zorgen dat voldaan wordt aan de wet- en regelgeving en daar goede voorzieningen voor te treffen.

Wat de AVG betreft, is de Autoriteit Persoonsgegevens verantwoordelijk voor het toezicht op de naleving, ook in het digitale domein. Het verwerken van medische gegevens door apps is een onderwerp dat volop in beweging is en vraagt om een stevige vinger aan de pols. Dit heeft zowel onze aandacht, als de aandacht van de toezichthouder.[1] Verder wordt op verschillende manieren ingezet op bewustwording en verbetering van de naleving. Zo worden zorgaanbieders onder meer ondersteund door de informatie die te vinden is op de AVG-helpdesk (www.avghelpdeskzorg.nl). Daarnaast worden zorgaanbieders ondersteund en gefaciliteerd om de informatiebeveiliging en digitale weerbaarheid te verbeteren. Er wordt gezamenlijk met de zorgkoepels gewerkt aan het Actieplan Informatieveilig gedrag met als doel om het bewustzijn van informatiebeveiliging in de zorg te verhogen. Bij ICT-incidenten kunnen aangesloten zorginstellingen rekenen op hulp van Z-CERT. Deze organisatie helpt zorginstellingen bij het bestrijden van dit soort incidenten. Verder wordt met het project ‘toekomstbestendig maken UZI’ ingezet of verbetering van de manier waarop zorgverleners en zorgaanbieders zich identificeren, authentiseren en autoriseren voor het uitwisselen van medische gegevens. Daarnaast wordt onderzocht of de toezicht- en handhavingsbevoegdheden van de Inspectie Gezondheid en Jeugd (IGJ) van de eerder genoemde informatiebeveiligingsnormen verduidelijking behoeven.

---

1 https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/onderzoek_beveiliging_ggd_corona.pdf, https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/advies_over_concept_tijdelijke_wet_covid-19.pdf

Vraag 3
Waarom zijn de signalen van een medewerker van het betreffende bedrijf niet opgepikt, die dit zowel bij de politie als uw ministerie zou hebben gemeld? Kunt u toelichten wat er volgens u moet gebeuren op uw ministerie zodat dit soort meldingen in de toekomst serieus worden genomen?

Antwoord vraag 3
Het is niet aan de minister van VWS om dit soort meldingen te onderzoeken. Dit laat onverlet dat de melder door mij zeer serieus is genomen. De Beveiligingsautoriteit van VWS heeft o.a. samen met de melder gezocht naar het geschikte loket om deze melding te doen, zoals bij een officier van justitie of het huis voor de klokkenluiders zodat de noodzakelijke data verstrekt kon worden en een onderzoek mogelijk was. De melder heeft echter ervoor gekozen daarvan geen gebruik te maken. De melder heeft aan de BVA van het ministerie van VWS aangegeven zelf de melding bij de AP te hebben gedaan.

Vraag 4
Klopt het dat de Militaire Inlichtingen- en Veiligheidsdienst (MIVD) het datalek heeft gemeld aan het bedrijf in augustus 2020? Zo ja, kunt u aangeven of dit is gebeurd naar aanleiding van (onder andere) de melding van de oud-medewerker?

Vraag 5
Is er op basis van de MIVD-melding actie ondernomen om onderzoek te doen naar het betreffende bedrijf? Zo nee, waarom niet?

Antwoord vraag 4 en 5:
Over werkwijzen en onderzoeken van de AIVD en MIVD worden in het openbaar geen mededelingen gedaan. Wel kunnen wij t.a.v. deze casus meedelen dat bij het Ministerie van Defensie een anonieme melding is binnengekomen van een potentieel datalek van medische gegevens. Deze melding is onderzocht en naar aanleiding daarvan is contact opgenomen met het bedrijf. De onderzoeksresultaten zijn vervolgens overgedragen aan de politie.

Vraag 6
Wat gebeurt er doorgaans indien de Algemene Inlichtingen- en Veiligheidsdienst (AIVD) of MIVD aanwijzingen hebben dat bedrijven kwetsbaar zijn voor datalekken? Kunt u toelichten wat hierbij het gangbare proces is en waarom?

Antwoord vraag 6
Bedrijven zijn zelf verantwoordelijk voor hun eigen informatiebeveiliging. In zijn algemeenheid heeft de AIVD in het kader van de Wet op de inlichtingen- en veiligheidsdiensten 2017 een taak om veiligheidsmaatregelen te bevorderen tegen concrete of voorstelbare dreigingen bij vitale instanties - van overheid tot bedrijfsleven - die van essentieel belang zijn voor het maatschappelijke leven. Indien bij een concrete of voorstelbare dreiging een mogelijk gevolg van deze dreiging datalekken zijn, dan kan de AIVD in samenwerking met andere partners zoals het Nationaal Cybersecurity Centrum betreffende bedrijven benaderen. De MIVD heeft in het kader van de Wiv2017 de taak om veiligheidsmaatregelen te bevorderen tegen concrete of voorstelbare dreigingen bij defensieorderbedrijven.

Vraag 7
Klopt het dat er melding van dit datalek is gedaan bij de Autoriteit Persoonsgegevens? Zo ja, waarom zijn de betreffende huisartsen en patiënten niet geïnformeerd over het datalek?

Antwoord vraag 7
Over individuele meldingen en zaken doet de AP in het kader van eventueel onderzoek in principe geen uitspraken. De AP beoordeelt of er op een juiste wijze invulling is gegeven aan de meldplicht van art. 33 en art. 34 van de AVG.

Vraag 8
Erkent u dat alsnog alle betrokkenen in dit datalek – zowel patiënten als huisartsen – moeten worden ingelicht conform de AVG? Hoe gaat u hierop toezien?

Antwoord vraag 8
Het is aan verwerkingsverantwoordelijken om te beoordelen of een datalek moet worden gemeld aan betrokkenen en de AP. De AP beoordeelt als onafhankelijke toezichthouder of hieraan op een juiste wijze invulling is gegeven.

Vraag 9
Bent u het met mij eens dat medische informatie van mensen zeer gevoelig is of kan zijn en daarom nog beter beschermd dient te worden? Kunt u uw antwoord toelichten?

Antwoord vraag 9
Medische informatie is zeer gevoelige informatie en dient goed beschermd te worden. En dat gebeurt ook: medische informatie wordt beschermd in internationale en nationale regelgeving.

In ons antwoord op vraag 2 zijn wij al op deze regelgeving ervan ingegaan. Deze regelgeving moet goed worden uitgevoerd. Daarnaast zetten wij ons op verschillende manieren in om bewustwording en verbetering van de naleving. In ons antwoord op vraag 2 zijn meerdere voorbeelden genoemd hoe daarop ingezet wordt.

Vraag 10
Bent u in het licht van bovenstaande bereid met aanvullende maatregelen te komen om medische data van mensen beter te beschermen, waarbij commerciële belangen worden uitgesloten? Zo nee, waarom niet?

Antwoord vraag 10
Er is reeds internationale en nationale wetgeving waarin is geborgd dat commercieel gebruik van medische informatie niet zomaar is toegestaan. Deze regelgeving moet goed worden uitgevoerd en gehandhaafd. Daarom zetten wij ons, zoals in het antwoord op vraag 2 toegelicht, op verschillende manieren in om bewustwording van de regelgeving en op het verbeteren van de naleving.

(1) https://www.ftm.nl/artikelen/lekkende-zorgdata?share=NbUZtPVr7fwSYGhmMqEQ6yOPvfrnYk4AJa1H9kZz21Na17ubUL0n5aJKhIUQqnc%3D

(2) https://www.ftm.nl/artikelen/lekkende-zorgdata-farmaceuten-landelijke-database