Tweede Kamer der Staten-Generaal

2

Vergaderjaar 2021–2022

Aanhangsel van de Handelingen

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

3969

Vragen van de leden **Tielen** en **Rajkowski** (beiden VVD) aan de Minister van Volksgezondheid, Welzijn en Sport en de Staatssecretaris van Binnenlandse Zaken en Koninkrijksrelaties over *het bericht over «Commercieel softwarebedrijf schendt jarenlang de privacy van tienduizenden patiënten»* (ingezonden 8 juli 2022).

Antwoord van Minister **Kuipers** (Volksgezondheid, Welzijn en Sport), mede namens de Staatssecretaris van Binnenlandse Zaken en Koninkrijksrelaties (ontvangen 12 september 2022). Zie ook Aanhangsel Handelingen, vergaderjaar 2021–2022, nr. 3614.

Vraag 1
Bent u bekend het met artikel «Commercieel softwarebedrijf schendt jarenlang de privacy van tienduizenden patiënten en het medisch beroepsgeheim van tientallen huisartsen» van 25 juni 2022 door Follow the Money?[1]

Antwoord 1
Ja.

Vraag 2
Is de casus uit dit artikel bekend bij het Ministerie van Volksgezondheid, Welzijn en Sport? Is de casus ook bekend bij de Autoriteit Persoonsgegevens (AP)? Zo ja, sinds wanneer en op welke wijze hebben uw Ministerie en de AP opvolging gegeven jegens de betrokken organisaties en huisartspraktijken?

Antwoord 2
De casus is bekend bij het Ministerie van Volksgezondheid, Welzijn en Sport (VWS), de melder heeft contact opgenomen met het Ministerie. De Beveiligingsambtenaar (BVA) van VWS heeft o.a. samen met de melder gezocht naar het geschikte loket om deze melding te doen, bv. bij een officier van justitie of het huis voor de klokkenluiders. Daarnaast is de informatie die het Ministerie van VWS ontvangen heeft, gedeeld met relevante externe partners, waaronder de Nederlandse Vereniging van Huisartsen.

[1] Follow the Money, 25 juni 2022, «Commercieel softwarebedrijf schendt jarenlang de privacy van tienduizenden patiënten en het medisch beroepsgeheim van tientallen huisartsen» (https://www.ftm.nl/artikelen/lekkende-zorgdata).

ah-tk-20212022-3969
ISSN 0921 - 7398
's-Gravenhage 2022

De melder heeft aan de BVA van het Ministerie van VWS aangegeven zelf de melding bij de AP te hebben gedaan. 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 Algemene verordening gegevensbescherming (AVG).

Vraag 3
Staat deze casus op zichzelf of zijn er andere vergelijkbare situaties waarbij patiëntdossiers voor of na onderzoek ongewenst en onbeveiligd inzichtelijk zijn voor (commerciële) organisaties die daar niets mee van doen hebben?

Antwoord 3
Over individuele meldingen en zaken doet de AP in het kader van eventueel onderzoek in principe geen uitspraken. Van belang om aan te geven is dat organisaties, zoals ziekenhuizen, zelf een verantwoordingsplicht hebben om aan te tonen dat ze aan de AVG voldoen. Dit geldt ook wanneer (commerciële) organisaties (een deel van) de gegevens verwerken.

Dat deze zaak niet op zichzelf staat, kan worden opgemaakt uit de Datalekkenrapportage 2021 van de AP. De rapportage geeft aan dat van de 24.866 datalekmeldingen in 2021, 37% afkomstig was uit de sector gezondheid en welzijn.
Bij iedere melding gaat de AP na of betrokkenen zijn geïnformeerd over het datalek en of er voldoende beveiligingsmaatregelen zijn genomen om het datalek te beëindigen en nieuwe datalekken te voorkomen. Het toezicht op de meldplicht datalekken is risicogestuurd, wat betekent dat de intensiteit van het toezicht toeneemt naarmate het datalek grotere risico's voor de betrokkenen met zich meebrengt. Ook wordt de AP periodiek geïnformeerd door brancheorganisaties NVZ (Nederlandse Vereniging van Ziekenhuizen) en NFU (Nederlandse Federatie van Universitair Medische Centra) over de implementatie, verbetering en naleving van gegevensbescherming en informatiebeveiliging normen van aangesloten ziekenhuizen. Bovendien beoogt de AP via onder andere de jaarlijkse datalekkenrapportage, maar ook de privacyverhalen op de AP website gebaseerd op echte meldingen, het bewustzijn rond de beveiliging van persoonsgegevens te vergroten. Tot slot heeft de Inspectie Gezondheid en Jeugd (IGJ) de bevoegdheid om in het geval van onvoldoende kwaliteit van zorgverlening of wanneer de kans op vermijdbare schade te groot is, door zwakke plekken in het zorgproces, in te grijpen.

Vraag 4
Klopt het dat de in het artikel genoemde activiteiten, zoals het delen en opslaan van dossiers, niet stroken met de huidige wet- en regelgeving en daarmee illegaal zijn? Zo ja, welke vervolgstappen worden er door het Ministerie van Volksgezondheid, Welzijn en Sport en de AP genomen om de data en medische gegevens van servers te halen en ervoor te zorgen dat ongeautoriseerden niet meer bij deze hoog gevoelige data kunnen? Zo nee, welke waarborgen om de privacy van patiënten ontbreken dan in de wet- en regelgeving? Op welke wijze bent u van plan deze te repareren?

Antwoord 4
In internationale en nationale wetgeving staan regels die betrekking hebben op het beschermen van (medische) gegevens, zoals ook het opslaan en delen van medische gegevens. Zo volgt uit de AVG dat er een grondslag moet zijn voor het verwerken van persoonsgegevens en een uitzonderingsgrond op het verbod om bijzondere persoonsgegevens, zoals gegevens over gezondheid, te verwerken. Ook bepaalt de AVG dat er passende technische en organisatorische waarborgen moeten worden getroffen, zodat de gegevens zijn beschermd tegen ongeoorloofde of onrechtmatige verwerking en tegen onopzettelijk verlies, vernietiging of beschadiging. Dit laatste is in nationale wetgeving nader ingevuld: zorgaanbieders moeten voldoen aan de informatiebeveiligingsnormen NEN 7510, NEN 7512 en NEN 7513. De AP houdt toezicht op de naleving van de AVG.

Daarnaast geldt het medisch beroepsgeheim, dat met zich mee brengt dat een hulpverlener in beginsel moet zwijgen over alles dat aan hem door de

patiënt wordt toevertrouwd. 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.
De AP heeft mij laten weten eerst te moeten vaststellen wat er in deze zaak is gebeurd voor ze kan bepalen welke vervolgstappen het meest geschikt zijn. Om deze reden heeft de AP vragen gesteld aan Medworq.
Op basis van de beschikbare informatie gaan wij ervan uit dat Medworq de gegevens enkel feitelijk beheerde voor de zorgaanbieders en niet zelf verwerkingsverantwoordelijk was voor de gegevens. In die situatie blijven de zorgaanbieders verantwoordelijk voor verwerking van de persoonsgegevens en dient in de verwerkingsovereenkomst met de verwerker (in casu de software-leverancier Medworq) afgesproken te worden wat de verwerker wel of niet met de gegevens mag doen.

Vraag 5
Op welke wijze bent u van plan om te voorkomen dat dergelijke praktijken plaatsvinden?

Antwoord 5
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. Daar is goede controle op de naleving van de regels noodzakelijk.

Verder zetten wij ons op verschillende manieren in om bewustwording en verbetering van de naleving. Zo ondersteunen wij zorgaanbieders onder meer door de informatie die te vinden is op de AVG-helpdesk (www.avghelpdesk-zorg.nl). Daarnaast helpen wij zorgaanbiedersom de informatiebeveiliging en digitale weerbaarheid te verbeteren. Gezamenlijk met de zorgkoepels werken wij aan een 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 IGJ van de eerder genoemde informatiebeveiligingsnormen verduidelijking behoeven.

Vraag 6
Bent u bereid om bij de behandeling en implementatie van het wetsvoorstel Gegevensuitwisseling in de zorg (Wegiz) nogmaals nadrukkelijk aandacht te besteden aan alle benodigde waarborgen, waarschuwingen en sancties ter voorkoming en vermindering van privacyschendingen van patiëntgegevens?

Antwoord 6
Het Wetsvoorstel elektronische gegevensuitwisseling in de zorg (Wegiz) gaat uit van en past binnen deze internationale en nationale wetgeving inzake gegevensbescherming. Dat betekent dat bij het uitwisselen van gegevens altijd voldaan moet worden aan de eisen die uit die bestaande kaders volgen. Gegevens worden dus – ook na inwerkingtreding van dit wetsvoorstel – niet uitgewisseld als er geen verwerkingsgrondslag als bedoeld in de AVG is of als er geen doorbrekingsgrond voor het medisch beroepsgeheim is.
En bij de gegevensuitwisseling dient altijd voldaan te worden aan de waarborgen die gelden op grond van die kaders. Die regelgeving moet natuurlijk goed worden toegepast. Daarom zullen wij bij de ontwikkeling van NEN-normen, waar de Wegiz naar verwijst, benadrukken dat de norm moet verzekeren dat cliënten hun rechten onder de AVG kunnen uitoefenen en informatietechnologieproducten- en diensten aan de AVG voldoen.