AUTORITEIT
PERSOONSGEGEVENS

Datum
1-8-2023

Ambtsbericht

Onderwerp

Informatievoorziening voor de beantwoording van de Kamervragen van het lid Van Haga (Groep Van Haga) aan de minister van Volksgezondheid, Welzijn en Sport (VWS) over 'het opslaan van medische gegevens van Nederlanders door externe softwareleveranciers' en de Kamervragen van het lid Bushoff (PvdA) aan de minister van VWS over 'het delen en opslaan van medisch dossiers'

De leden Van Haga (Groep Van Haga) en Bushoff (PvdA) hebben Kamervragen gesteld aan de minister van VWS over 'het opslaan van medische gegevens van Nederlanders door externe softwareleveranciers' en 'het delen en opslaan van medische dossiers'. Dit ambtsbericht dient ter verschaffing van informatie aan het ministerie van VWS voor de beantwoording van de vragen die zien op het werk van de Autoriteit Persoonsgegevens (AP).

Kamervragen lid Van Haga (Groep Van Haga)

Vraag 2

Aangezien de Autoriteit Persoonsgegevens al in 2018 onderzoek deed naar het kopiëren van de medische gegevens van Nederlanders naar een commercieel systeem, kan dan geconcludeerd worden dat u al jaren op de hoogte was van deze grootschalige en mogelijk juridisch oneigenlijke dataverzameling in de Nederlandse zorg? Zo ja, kunt u dan uitleggen waarom hieraan niet eerder ruchtbaarheid is gegeven? Waarom is het Nederlandse volk hierover niet eerder grootschalig ingelicht?

Informatie voor beantwoording van vraag 2:

Op basis van een vooronderzoek heeft de AP in dit geval besloten geen onderzoek te doen. Een vooronderzoek heeft als doel om achtergrondinformatie te verzamelen aan de hand waarvan wordt beoordeeld of nader onderzoek passend is. De beslissing om wel of geen nader onderzoek te doen wil de AP uiteraard zorgvuldig nemen. Daarom is er destijds ook contact geweest met de klager en is er een uitgebreid informatieverzoek uitgegaan voor het opvragen van documenten.

Redenen om het in dit geval niet nader te onderzoeken waren onder meer dat:

- De geëxtraheerde gegevens meteen automatisch worden versleuteld en alleen toegankelijk zijn voor de huisarts, die een sleutel heeft. Zowel de softwareleverancier als ketenzorggroep hebben geen sleutel. Als de huisarts zijn of haar wachtwoord kwijtraakt, zijn de gegevens dus onbruikbaar.
- Medische gegevens niet met externen worden gedeeld voor bijvoorbeeld wetenschappelijk onderzoek of statistiek.

De AP ontvangt veel klachten en tips. In 2022 waren dit er ruim 13.000. Deze resulteren niet allemaal in een onderzoek dat vervolgens tot handhaving in de vorm van bijvoorbeeld een boete leidt. Met haar huidige budget moet de AP bovendien nog strenger dan gewenst prioriteren in de zaken die worden opgepakt. De AP is van oordeel dat het budget van de AP, om onder andere meer te kunnen onderzoeken,

moet groeien naar een structurele financiering van € 100 miljoen euro, vergelijkbaar met andere Nederlandse toezichthouders.

Als de AP geen onderzoek start, wil dat natuurlijk niet zeggen dat de AP een 'stempel van goedkeuring' zet op de werkwijze van een organisatie. De rechtmatigheid van een gegevensverwerking hangt onder meer af van het doel en de noodzaak van een verwerking, en die verschillen van geval tot geval. Daarnaast moet bij verwerkingen altijd rekening worden gehouden met de beginselen uit de Algemene verordening gegevensbescherming (AVG), waaronder transparantie en dataminimalisatie.

Vraag 11
Nu u weet dat de manier waarop medische gegevens worden opgeslagen voor veel huisartsen een (moreel) bezwaar is, bent u dan van plan om toch een vervolgonderzoek te laten doen naar deze dataverzameling?

Informatie voor beantwoording van vraag 11:
De AP is de onafhankelijke Nederlandse toezichthouder op de bescherming van persoonsgegevens. De onafhankelijke status brengt met zich mee dat de AP zelf kan beslissen of zij al dan niet onderzoek doet naar bepaalde verwerkingen. De minister kan hier geen invloed op uitoefenen. Over individuele meldingen en of zaken doet de AP bovendien in het kader van (lopende en beoogde) onderzoeken in principe geen uitspraken.

Vraag 17
Heeft u een risicoanalyse gemaakt met betrekking tot een mogelijk datalek, of een hack? En weet u wat de gevolgen zouden (kunnen) zijn als deze medische gegevens van burgers op straat komen te liggen, of in handen vallen van criminelen?

Informatie voor beantwoording vraag 17:
Om risico's te ondervangen is de organisatie die verantwoordelijk is voor de grootschalige registratie van patiëntengegevens (de verwerkingsverantwoordelijke) verplicht van tevoren een zogenaamde gegevensbeschermingseffectbeoordeling (DPIA) uit te voeren. Hierin moeten de risico's van de gegevensverwerking worden geïdentificeerd, evenals de maatregelen die moeten worden getroffen om die risico's weg te nemen.

Van een datalek is sprake wanneer een inbreuk op de beveiliging leidt tot ongeoorloofde of onbedoelde verstrekking van of toegang tot persoonsgegevens. Maar ook als de inbreuk ertoe leidt dat deze gegevens ongewenst of onrechtmatig zijn vernietigd, verloren of gewijzigd. In Nederland geldt sinds 2016 een meldplicht voor datalekken. Dit houdt in dat organisaties (zowel bedrijven als overheden) direct een melding moeten doen bij de AP zodra zij een ernstig datalek hebben. Wanneer het datalek een hoog risico oplevert, dient de organisatie daarnaast ook de personen wiens data getroffen zijn te informeren. Op basis van de datalekmeldingen controleert de AP of de juiste stappen zijn ondernomen om de gevolgen van een datalek zo goed mogelijk te beperken.

Datalekken kunnen ernstige gevolgen hebben voor slachtoffers. Mensen kunnen financieel getroffen worden, bijvoorbeeld door identiteitsfraude en oplichting. Een ander gevolg van datalekken is dat

slachtoffers reputatieschade kunnen lijden als gegevens uit hun privéleven zijn gelekt. Denk aan privéfoto's, gevoelige informatie over (mentale) gezondheid of problemen in een thuissituatie. Het afgelopen jaar zijn door de drie grootste cyberaanvallen in de zorg naar schatting 900.000 patiënten getroffen. Van hen zijn gevoelige medische gegevens op straat komen te liggen, met alle gevolgen van dien.

Organisaties die getroffen zijn door een datalek kunnen dit melden via het meldformulier datalekken op de website van de AP. In 5 jaar tijd heeft de AP meer dan 114.000 meldingen van datalekken ontvangen. Dat zijn er gemiddeld meer dan 20.000 per jaar. Uit de datalekkenrapportage van de AP van 2022 volgt dat bijna een kwart van de gemelde datalekken over cyberaanvallen in 2022 afkomstig was uit de zorgsector.

Kamervragen lid Bushoff (PvdA)

Vraag 4

Hoe moeten huisartsen omgaan met hun verantwoordelijkheid voor het bewaken van het medisch dossier in deze markt?

Informatie voor beantwoording van vraag 4:

Ook als huisartsen gebruik maken van een IT-leverancier, dan blijven zij zelf verantwoordelijk voor de beveiliging van de persoonsgegevens. Daarnaast zijn huisartsen ook verantwoordelijk voor het melden van een datalek aan de AP én aan de slachtoffers. Het is daarom belangrijk dat huisartsen alleen IT-leveranciers inschakelen die genoeg garanties geven voor passende technische en organisatorische beveiligingsmaatregelen. Huisartsen zijn verplicht om in overeenkomsten met de IT-leveranciers afspraken te maken over de verwerking van persoonsgegevens en de beveiliging daarvan.

IT-leveranciers leveren softwarediensten, digitale werkplekken of opslagruimte aan organisaties. Dat leidt tot een clustering van persoonsgegevens op de servers van deze leveranciers, waardoor zij een gewild doelwit zijn voor cyberaanvallen door criminelen: er valt hier veel te halen. Het is dus van belang dat huisartsen periodiek controleren of de IT-leveranciers de zogeheten verwerkersovereenkomsten naleven. In de datalekkenrapportage van 2021 waarschuwde de AP daarom voor datalekken bij IT-leveranciers.