

Makkelijk scoren voor verder lakse Autoriteit Persoonsgegevens bij Haga- ziekenhuis



Op 16 juli 2019 [maakte de Autoriteit Persoonsgegevens \(AP\) bekend](#) dat ze Het Haga-ziekenhuis in Den Haag een zeer hoge boete van 460.000 euro en een forse last onder dwangsom oplegde. Het besluit dateert van 18 juni 2019. Het gaat om de nasleep van een berucht datalek uit april 2018. Toen raakte bekend [dat 85 ziekenhuismedewerkers](#) onterecht het medische dossier van de “reality ster Barbie” ingezien hadden. Het kwam naar buiten door een tip via de klokkenluiderssite PubLeaks aan de tv-rubriek EenVandaag. Ik schreef er in 2018 drie keer over. ([A](#), [B](#), [C](#)). De AP kwam toen in actie en deed onderzoek bij het Haga-ziekenhuis. Eigenlijk kon de AP het zich niet permitteren om geen onderzoek te doen en geen maatregelen af te kondigen vanwege de forse publiciteit rond deze gebeurtenis. Bij de AP lopen meerdere zaken waarbij sprake is van schending van de privacyrechten van burger in de zorg waar de AP geen beslissing neemt en/of onderzoek op de lange baan schuift.

Geen 85 maar 100

De AP publiceerde heden een [onderzoeksrapport uit maart 2019](#) en een [boetebesluit van 18 juni 2019](#). In dat laatste is te lezen (blz. 4/25) dat van de 197 personen die inzage hadden in dossier van “Barbie” honderd personen dat onrechtmatig deden. In april 2018 had het ziekenhuis nog gemeld dat het om 85 personen ging, die niets met de behandeling te maken hadden, Het gaat dus om een beduidend groter aantal onrechtmatige

daden dan waarvan de AP in het onderzoeksrapport zelf ook nog melding maakt. Geen van de mensen die onrechtmatig inzage hadden is trouwens ontslagen. Ze werden “berispt”.

Toegangscontrole

Uit het rapport blijkt dat het mogelijk was op drie manieren toegang te krijgen tot een dossier. Met twee-factor-authenticatie (personeelspas plus wachtwoord/inlogcode), met één-factor-authenticatie (wachtwoord/inlogcode) en een noodknop-procedure. Dat laatste is een toegang in noodsituaties, waarbij het personeelslid toegang krijgt maar wel op een scherm moet noteren waarvoor die toegang noodzakelijk was. De één-factor-authenticatie beschouwt de AP als verregaand onvoldoende en mag van haar niet blijven bestaan naast de twee-factor-authenticatie. Daarnaast controleerde het ziekenhuis de logging (het vastleggen van de inzage) op een zeer insufficiënte wijze. Van één patiënt per twee maanden, dus zes per jaar controleert men de loggegevens, op een totaal van een paar honderdduizend patiëntdossiers per jaar!! Verregaand insufficiënt noemt de AP dat terecht. In de verste verte lijkt dat op een afdoende, intelligente, consequente controle.

Eerdere melding bij AP

Het is zeker niet de eerste keer dat de AP op de hoogte is gesteld van onterechte inzagen in medische dossiers. Mij is een geval bekend (van vijf jaar terug) van een ex-GGZ-patiënt die aangifte bij de AP en bij de Inspectie Gezondheidszorg en Jeugd (IGJ) deed van het vele malen onterecht inzien van het dossier door nogal wat onbevoegden. De rechtsvoorganger van de AP, het College Bescherming Persoonsgegevens (CBP), liet toen weten er een notitie van gemaakt te hebben, maar deed er vervolgens niets mee. [Men had toen nog niet de mogelijkheid](#) om hoge boetes, zoals nu op te leggen. Wel kon het CBP toen beperkte boetes opleggen bij het verzaken van de meldplicht

van datalekken en een last onder dwangsom of bestuursdwang toepassen. De patiënt meldde het zelf, waardoor gerust gesteld kan worden dat de instelling verzuimd had het datalek te melden. De IGJ draaide zich eruit door te verwijzen naar het “grondige” onderzoek van het instellingsbestuur.

Lastige beslissingen

In diverse zaken neemt de AP geen ferm standpunt in, [traineert beslissingen](#) en poogt ze zelfs als er [rechtszaken komen die eindeloos te vertragen](#) en soms [met beroep op geheimhouding](#) te beïnvloeden. Ik doel daarbij op zaken rond het DBC Informatie Systeem(DIS) en Routine Outcome Monitoring(ROM)-data. Daar spelen hele grote belangen een rol waardoor de AP op eieren loopt om maar geen beslissing te hoeven nemen.

Zieligheids criterium

In de casus met de boete voor het Haga-ziekenhuis is het zieligheids criterium al van stal gehaald door het ziekenhuis. Het Ziekenhuis heeft ter zienswijze-zitting een beroep gedaan op beperkte draagkracht, onderbouwd met de concept jaarrekening 2018(blz. 23/25 boetebesluit). In dat kader voert zij aan dat het Haga-ziekenhuis in 2018 een uitsluitend als “vertrouwelijk” genoemd bedrag heeft overgehouden ten gevolge van incidentele baten. De AP ziet hierin echter geen aanleiding om aan te nemen dat het ziekenhuis gezien haar financiële positie een boete van € 460.000,- niet zou kunnen dragen.

Makkelijk scoren

Uit het voorgaande moge blijken dat de AP bij dit ziekenhuis makkelijk scoren had. En zo daadkracht kon tonen die haar andermaal nogal eens ontbeert. Bovendien was de optie om niets te doen ook geen begaanbare weg. Het zal er waarschijnlijk op neer gaan komen dat het ziekenhuis gaat procederen tegen de boete van de toezichthouder. Zaken bij een andere

toezichthouder, de Autoriteit Consument en Markt, hebben laten zien dat een dergelijke rechtsgang gunstig is voor de instelling.

W.J. Jongejan, 17 juli 2019