

# Datalek melden, anders volgt dikke boete

Het College bescherming persoonsgegevens kan vanaf 1 januari 2016 bestuurlijke boetes uitdelen tot ruim 8 ton, bij overtreden van de vernieuwde Wet bescherming persoonsgegevens. Zeven vragen over deze nieuwe boetes en het verplicht melden van een datalek.



## 1 Wat is er aan de hand?

Cybercrime en digitale spionage zijn de grootste bedreigingen voor de digitale veiligheid in Nederland, zo blijkt uit het Cyber Security Beeld Nederland. Er is daarom een nieuwe Europese wet in aantocht, die de burger beter beschermt tegen aanvallen op zijn persoonlijke gegevens. Nederland is een van de eerste landen die alvast aan de slag is gegaan met betere bescherming van digitale veiligheid. De Eerste Kamer ging in mei dit jaar akkoord met de aanpassing van de Wet bescherming persoonsgegevens; per 1 januari 2016 treedt de vernieuwde wet in werking. Doel is om de gevolgen van een 'datalek' voor de betrokkenen zoveel mogelijk te beperken.

## 2 Wat is een 'datalek'?

Er is sprake van een datalek wanneer persoonsgegevens in handen vallen van mensen die geen toegang mogen hebben, maar ook bij onterechte vernietiging van de gegevens. Een ernstig datalek moet worden gemeld bij de Autoriteit Persoonsgegevens; dat is de nieuwe naam van het College bescherming persoonsgegevens (CBP) vanaf volgend jaar. Het moet ook worden gemeld aan de betrokken mensen als het voor hen ongunstige gevolgen kan hebben. Als er geen melding wordt gemaakt van een datalek, kan dit bestraft worden met een bestuurlijke boete van de Autoriteit Persoonsgegevens. Voorbeelden van datalekken zijn volgens het (nu nog) CBP: een kwijtgeraakte usb-stick met persoonsgegevens, patiëntendossiers die (per ongeluk) op straat terecht komen, een gestolen laptop of een inbraak in een databestand. Het college schrijft richtsnoeren over deze meldplicht datalekken, die op de website te raadplegen zijn.

## 3 Wat betekent dat voor de zorg?

Het CBP schrijft dat organisaties moderne technieken moeten gebruiken om persoonsgegevens te beveiligen. En dat ze niet alleen naar de techniek moeten kijken, maar ook naar hoe ze als organisatie met persoonsgegevens omgaan.

Wie heeft er bijvoorbeeld toegang tot welke gegevens? Verder heeft het CBP op haar website een concept van de beleidsregels gezet over de nieuwe boetes. Daarin is te lezen dat gezondheidsgegevens (artikel 16 van de Wet bescherming persoonsgegevens) met het zwaarste geslacht beschermd zijn. Wie dit artikel overtreedt, riskeert de hoogste boete van 810.000 euro, en dan ook nog de zwaarste categorie 3. Als dat nog niet genoeg pijn doet, bijvoorbeeld voor een bedrijf of instelling met een miljoenenomzet, kan de boete 10 procent van de omzet bedragen. Nu mogen zorginstellingen natuurlijk gezondheidsgegevens opslaan en bewerken (artikel 21). Maar de beveiliging moet goed geregeld zijn (artikel 13) en lekken moeten gemeld worden bij de (straks) Autoriteit Persoonsgegevens (artikel 34a).

**4 Is dat nieuw?** Dat de Autoriteit Persoonsgegevens straks boetes kan uitdelen is geen verrassing, zegt ook een woordvoerder van de Nederlandse Vereniging van Ziekenhuizen. Dit verandert niets aan de werkwijze waarop instellingen hun informatiebeveiliging inrichten en actueel houden. Alleen de meldplicht bij datalekken is echt nieuw. De zorg valt al sinds 2001 onder de Wet bescherming persoonsgegevens, zegt ook Sjaak Nouwt, jurist van de KNMG, dus heel veel verandert er niet voor de zorg. De boete was alleen tot nu toe 4500 euro, en die is nu 810.000 euro. En de meldplicht is inderdaad nieuw. 'Privacybescherming wordt nu *serious business*', vat Nouwt het samen.

**5 Riskeren artsen een boete als ze gegevens overhandigen aan een gemeentebestuur in het kader van de Wmo?** 'Nee', zegt Sjaak Nouwt. 'Niet voor zover dat in overeenstemming is met de Wet maatschappelijke ondersteuning, want die gaat *boven* de Wet bescherming persoonsgegevens.' Artsen mogen ook medische gegevens verstrekken aan zorgverzekeraars voor het declaratieproces; dat is geregeld in de Regeling zorgverzekering

## Wie in overtreding is, riskeert 810.000 euro boete

bij de Zorgverzekeringswet. Zorgverzekeraars mogen op hun beurt gezondheidsgegevens verwerken op grond van artikel 21 van de Wet bescherming persoonsgegevens. Als een leverancier van incontinentiemateriaal om medische gegevens vraagt, zoals een van de lezers schrijft in reactie op een nieuwsbericht over dit onderwerp (website MC, 28 oktober), dan is het oppassen geblazen. Zo'n partij valt niet onder het rijtje in het genoemde artikel 21 van de wet, dat toestaat om gezondheidsgegevens te verwerken. Dat mag alleen als de patiënt daarvoor uitdrukkelijk toestemming heeft gegeven.

**6 Uit een onderzoek van Deloitte bleek dat ziekenhuizen te weinig doen aan bescherming van persoonsgegevens in medische apparatuur. Hoe daarmee om te gaan?**

Innovatieve medische apparatuur wordt steeds vaker met het ziekenhuisnetwerk verbonden. Dit brengt bedreigingen met zich mee, bleek uit een rondgang langs zeventien ziekenhuizen. Tien van hen hadden te maken gehad met een virus op deze apparaten. Ook was het vaak mogelijk voor een bezoeker om met een usb-stick persoonsgegevens uit het apparaat te kopiëren. Slechts vier ziekenhuizen voerden beleid om de persoonsgegevens via de apparaten te beschermen. Er is best wat aan te doen volgens Deloitte; denk aan een versleutelde verbinding met het netwerk. Wie geen eigen ICT-afdeling heeft, doet er goed aan om de gebruikersovereenkomst of bewerkingsovereenkomst van dit soort apparatuur te controleren, adviseert Sjaak Nouwt daarnaast, want daarin kunnen eisen staan over de beveiliging van de persoonsgegevens. Let op, want niet alle overeenkomsten zijn up-to-date. Ze bevatten bijvoorbeeld vaak nog niet de verplichte melding van een datalek die in deze nieuwe wet staat.

Hetzelfde geldt voor de gebruikersovereenkomst voor het epd.

## 7 Hoe kan een arts zich verder voorbereiden op de nieuwe wet?

Artsen die vragen hebben over de nieuwe wet, kunnen die bijvoorbeeld stellen aan de deskundigen van de KNMG Artseninfolijn. Verder heeft de Nederlandse Vereniging van Ziekenhuizen een praktische onlinetest voor veilig gedrag met elektronische patiëntengegevens, te vinden op [zorgzeker.nl](http://zorgzeker.nl). Hierin staat bijvoorbeeld aan welke eisen een veilig wachtwoord voldoet: minstens acht karakters, waaronder een hoofdletter, een leesteken en een cijfer. Het was een van de dingen die misgingen bij het grootschalige datalek in het Groene Hart Ziekenhuis in Gouda drie jaar geleden. Gegevens stonden op een slecht beveiligde server en het wachtwoord van de beheerder was 'groen2000'. Dat was makkelijk te raden, en dat lukte een hacker dan ook. Het wachtwoord gaf toegang tot tientallen dossiers met medische gegevens en persoonsgegevens van het volledige patiëntenbestand met ruim 493 duizend personen. Verder blijkt uit een enquête van de NVZ dat er nog steeds mensen zijn die dossiers open en bloot op het bureau laten liggen, en vergeten uit de loggen als ze even van hun werkplek opstaan. Het CBP raadt ten slotte het volgende aan: richt een goed incidentenbeheer in, beslis wie in de organisatie datalekken gaat beoordelen en melden, denk na over hoe u de betrokkenen gaat informeren bij een datalek, denk na over hoe u wilt omgaan met signalen uit de buitenwereld over mogelijke datalekken en controleer afspraken met uw medewerkers die toestemming hebben om gegevens aan te passen ('bewerkers'). ■

### web

Eerdere MC-artikelen en verwijzingen naar websites met aanvullende informatie vindt u onder dit artikel op [medischcontact.nl/artikelen](http://medischcontact.nl/artikelen).