

Wat betekent dit voor de praktijk?

Meldplicht datalekken

Op 1 januari 2016 is de meldplicht datalekken ingegaan. Deze meldplicht houdt in dat alle organisaties direct een melding moeten doen bij de Autoriteit Persoonsgegevens zodra zij een ernstig datalek hebben. Maar wat is nu datalekken en hoe kun je het beheersen?

Michael Joosen

Bij een datalek gaat het om toegang tot, of vernietiging, wijziging of vrijkomen van persoonsgegevens bij een organisatie, zonder dat dit de bedoeling is. Onder een datalek valt dus niet alleen het vrijkomen (lekken) van gegevens, maar ook onrechtmatige verwerking van gegevens.

We spreken van een datalek als er een inbreuk is op de beveiliging van persoonsgegevens. Zoals bedoeld in artikel 13 van de *Wet Bescherming Persoonsgegevens* (WBP). Bij een datalek zijn de persoonsgegevens blootgesteld aan verlies of onrechtmatige verwerking, dus aan datgene waartegen de beveiligingsmaatregelen bescherming moeten bieden.

Voorbeelden datalekken

Voorbeelden van datalekken zijn: een kwijtgeraakte USB-stick met persoonsgegevens, een gestolen laptop, een inbraak in een databestand door een hacker, maar ook verkeerd adresseren van e-mail en zoekgeraakte papieren dossiers.*

De boete voor het niet melden van een datalek valt in de categorie 'bestuurlijke boetes' en kan maximaal € 810.000,- bedragen, of 10 procent van de jaaromzet. De KNMT heeft echter een verzoek gedaan bij de *Autoriteit Persoonsgegevens* om rekening te houden met de draagkracht van kleine zorgaanbieders. De uitkomst hiervan is nog niet bekend.

Ketenaansprakelijkheid

Een ander nieuw begrip is de zogenaamde 'ketenaansprakelijkheid'. Dit houdt in dat de praktijk die de persoonsgegevens verzamelt, hier altijd voor verantwoordelijk is. Ook als zij deze laten verwerken door dienstverleners als een accountant, salarisverwerker, cloudprovider (online back-up) of softwareleverancier.

Concreet betekent dit dat er afspraken zullen moeten worden gemaakt met deze bewerkers over de bescherming van per-

*Bron: <https://autoriteitpersoonsgegevens.nl/>

soonsgegevens. In de Wet Bescherming Persoonsgegevens (WBP) is al verplicht gesteld dat er tussen partijen een bewerkerovereenkomst moet worden afgesloten. Met de komst van de Meldplicht Datalekken krijgt deze overeenkomst een nieuwe dimensie. De belofte van een bewerker om zorgvuldig met de gegevens om te zullen gaan is niet voldoende. Er dienen schriftelijke afspraken gemaakt te worden over aansprakelijkheden, het melden van datalekken aan de opdrachtgever en er moet een kettingbeding worden opgenomen. Voorbeelden van dit soort 'bewerkerovereenkomsten' zijn eenvoudig op internet te vinden.

Beveiligingstips

Omdat ook diefstal van apparatuur en verlies van mobiele datadragers (USB-stick, externe harde schijf) in de categorie datalekken vallen, is het niet de vraag óf de praktijk te maken krijgt met een datalek, maar wanneer. Onderstaande tips kunnen je helpen:

1. Laat de ICT-omgeving beheren door een professionele partij. Zij zorgen dat alle essentiële software bijgewerkt is naar de laatste en veiligste versie.
2. Zorg voor anti-virus en anti-malware-software en een firewall op je server en werkstations.
3. Controleer de kwaliteit van de wachtwoorden die worden gebruikt. Dit kan op de website van de Nederlandse overheid: <https://veiliginternetten.nl/wachtwoord-check/>. Hier staan nog veel meer tips over veilig gebruik van het internet.
4. Log altijd uit als je je werkplek verlaat.
5. Open nooit koppelingen of bijlagen van onbekende personen.
6. Reageer niet op e-mails die een verandering van jullie wachtwoord eisen en vragen om persoonlijke informatie in te vullen of te corrigeren. Hoe officieel de e-mails er ook uitzien.
7. Gebruik het e-mailadres van de praktijk niet voor het verzenden en ontvangen van persoonlijke e-mails.
8. Gebruik nooit een gratis e-mail-adres voor het versturen van e-mails met patiëntgerelateerde gegevens.

Gaat het toch fout, dan moet je melding maken bij de autoriteit persoonsgegevens: <https://datalekken.autoriteitpersoonsgegevens.nl>



Michael Joosen is directeur van Heertjes en Voorpraktijken. Heertjes (heertjes.nl) ondersteunt praktijken o.a. bij alle inkoop rondom nieuwbouw, verbouw en verhuizingen. Voorpraktijken (voorpraktijken.nl) is een verzameling besparende collectieven, speciaal gericht op (para)medische praktijken. Voorpraktijken organiseert daarnaast ledenvoorstellen als partner van de ANT, de KNMT, de Branchevereniging Tandtechniek en Dierenartsencoöperatie Dactari.