Inbreuk op beveiliging van persoo

De Wet Meldplicht Datalekken is op 19 juni 2015 in het *Staatsblad* gepubliceerd, een aanpassing op de Wet Bescherming Persoonsgegevens (WBP). De wet treedt in zijn geheel in werking op 1 januari 2016. Dit heeft de nodige gevolgen voor eerstelijns zorgaanbieders.

Door de Wet Bescherming Persoonsgegevens (WBP) is een eerstelijns zorgaanbieder een verwerker van persoonsgegevens, omdat deze een database met patiëntgegevens, waaronder de woonplaats en het Burgerservicenummer van patiënten bijhoudt. Verwerkers van persoonsgegevens zijn verplicht om passende organisatorische- en beveiligingsmaatregelen te nemen om verlies of onrechtmatig gebruik van gegevens te voorkomen. De Wet Meldplicht Datalekken die met ingang van 2016 van kracht wordt, borduurt hier op voort.

Inbreuk op de beveiliging

Een inbreuk op de beveiliging van de persoonsgegevens, en de kans dat daardoor nadelige gevolgen ontstaan voor de bescherming daarvan, dient onverwijld aan het College Bescherming Persoonsgegevens (na de inwerkingtreding van de Wet Meldplicht Datalekken wijzigt de naam in Autoriteit Persoonsgegevens) gemeld te worden. Ook moet dit worden gemeld aan de persoon wiens persoonsgegevens het betreft.

Er zijn drie cumulatieve voorwaarden voor het onverwijld melden van het datalek aan de Autoriteit Persoonsgegevens:

1. Er is sprake van een inbreuk op de beveiliging.
2. De inbreuk doet zich voor bij een organisatie in de private of publieke sector.
3. De inbreuk leidt tot een aanmerkelijke kans op nadelige gevolgen voor de bescherming van de persoonsgegevens die door de organisatie worden verwerkt.

De inbreuk op de beveiliging hoeft niet te betekenen dat de beveiliging tekort is geschoten. Het kan bijvoorbeeld ook het resultaat zijn van het hacken van het systeem van de verwerker. Onder tekortschietende beveiliging valt niet slechts het niet hebben van een toereikende firewall tegen hackers, maar ook bijvoorbeeld het aanbieden van papieren dossiers met patiëntgegevens als oud papier, of het kwijtraken van een usb-stick met de betreffende informatie!

Inhoud van de melding

De melding aan de Autoriteit Persoonsgegevens dient in ieder geval de volgende gegevens te omvatten:

- de aard van de inbreuk;
- de instantie(s) waar meer informatie over de inbreuk kan worden verkregen;
- de aanbevolen maatregelen om de negatieve gevolgen van de inbreuk te beperken;
- een beschrijving van de geconstateerde en de vermoedelijke gevolgen van de inbreuk voor de verwerking van de persoonsgegevens;
- de maatregelen die de organisatie heeft genomen of voorstelt te nemen om deze gevolgen te verhelpen.

Een kennisgeving aan de persoon voor wie het lek mogelijk nadelige consequenties heeft, kan achterwege gelaten worden als de persoonsgegevens versleuteld of ontoegankelijk zijn voor degene die geen recht heeft op inzage in deze gegevens.

Verder dient de verantwoordelijke (de organisatie van de zorgaanbieder) een overzicht bij te houden van alle lekken die ernstig genoeg waren om dit aan de toezichthouder te melden. Dit overzicht omvat in ieder geval de feiten en gegevens omtrent het lek, alsmede de kennisgeving aan de betrokkene.

Sancties

Voorheen kon het College Bescherming Persoonsgegevens alleen een boete opleggen bij overtreding van een administratief voorschrift (bijvoorbeeld het niet melden van het verwerken van de persoonsgegevens). De Wet Meldplicht

Foto: Thinkstock

nsgegevens onverwijld melden

Datalekken verruimt de boetebevoegdheid, omdat nu ook boetes opgelegd kunnen worden voor onzorgvuldige verwerking van de persoonsgegevens of onvoldoende beveiliging. De boete kan oplopen tot maximaal 810 euro of, als dat bedrag hoger is, tien procent van de jaaromzet van de organisatie. Het College zal echter in de meeste gevallen (behoudens opzet en bewuste roekeloosheid) eerst overgaan tot het geven van een bindende aanwijzing, omdat het bijvoorbeeld discutabel kan zijn of de genomen beveiligingsmaatregelen als voldoende passend gekwalificeerd dient te worden.
De rechtspersoon is de verantwoordelijke voor de verwerking van de persoonsgegevens. Deze zal dus in de regel door de Autoriteit Persoonsgegevens beboet worden.

Foto: Thinkstock

Een inbreuk op de beveiliging hoeft niet te betekenen dat de beveiliging tekort is geschoten. Denk bijvoorbeeld aan het hacken van het systeem

Naast het beboeten van de rechtspersoon, is het onder de Wet Meldplicht Datalekken tevens mogelijk om bestuurders of feitelijk leidinggevenden te beboeten. Bewezen dient dan echter te worden dat de bestuurder of een andere feitelijk leidinggevende opdracht heeft gegeven tot het verrichten van de verboden gedragingen welke een inbreuk op de persoonsgegevens tot gevolg hebben, óf heeft nagelaten adequate maatregelen te treffen en daarmee de kans te aanvaarden dat de bescherming van de persoonsgegevens in het gedrang zouden komen. Dit bewijs zal in de praktijk erg moeilijk te leveren zijn. Het beboeten van een bestuurder van de rechtspersoon of een andere natuurlijke persoon ligt dan ook niet snel voor de hand.

De boetebevoegdheden van de Autoriteit Persoonsgegevens zijn bovendien niet ongelimiteerd.

Ontoereikende beveiliging

Ten eerste is niet op overtreding van alle wetsbepalingen een boete gesteld. Zo is bijvoorbeeld het uitbesteden van verwerking van de persoonsgegevens zonder deugdelijke bewerkersovereenkomst niet beboetbaar. Dit is enigszins vreemd, aangezien overtreding van deze bepaling vrij ernstige gevolgen voor de persoonsgegevens kan hebben. Ook zijn veel inbreuken op persoonsgegevens strafbaar gesteld in het Wetboek van Strafrecht, zoals bijvoorbeeld het aftappen van gegevens of het verspreiden van wachtwoorden. In dat geval is slechts het Openbaar Ministerie bevoegd op te treden, tenzij het OM daarvan af heeft gezien.
Zorgaanbieders moeten zich dus realiseren dat zij, in geval van een inbreuk op de beveiliging van de verwerkte persoonsgegevens, onafhankelijk van het feit of de inbreuk te wijten is aan een ontoereikende beveiliging, tijdig de Autoriteit Persoonsgegevens te informeren. <<

Ben Schröder, Eldermans|Geerts

ELDERMANS & GEERTS
ADVOCATEN