Verplichting beveiliging persoonsgegevens krijgt ‘tanden’ met datalekkenwet

Ellen Timmer
advocaat
Pellicaan Advocaten
ellen.timmer@pellicaan.nl
www.pellicaan.nl
http://nl.linkedin.com/in/ellentimmer

Iedere organisatie en onderneming die persoonsgegevens in de administratie en andere systemen heeft opgeslagen, is verplicht die gegevens zowel technisch als organisatorisch te beveiligen. Ondernemers die het niet zo nauw namen met beveiliging, hadden daar vaak geen last van. Immers: voordat een benadeelde burger een schadeclaim neerlegt bij een slecht beveiligde onderneming moet er heel wat gebeuren.

Met ingang van 1 januari 2016 wordt dat anders doordat dan een nieuw wet in werking treedt. Officieel heet die wet ‘Wet meldplicht datalekken en uitbreiding bestuurlijke boetebevoegdheid Cbp’. In wandelgangen wordt de wet ‘Datalekkenwet’ genoemd. In dit artikel wordt in het kort aangegeven welke gevolgen deze wet heeft.

Voor wie?

De wet is van toepassing op iedereen die persoonsgegevens onder zich krijgt, ook als er activiteiten aan derden worden uitbesteed (de ‘verantwoordelijke’). Voorbeeld: als u als webwinkel gegevens van consumenten (klanten) in uw administratie opneemt en die administratie wordt uitgevoerd door een cloud-dienstverlener, dan bent u als webwinkel verantwoordelijk voor naleving van de Datalekkenwet en moet u zorgen dat de cloud-dienstverlener zich aan de regels houdt.

Persoonsgegevens

Iedere onderneming moet uiterst voorzichtig zijn met persoonsgegevens en zich bij het gebruik aan de wet houden. Persoonsgegevens omvatten niet alleen naam, adres, postcode, geboortedatum en telefoonnummers. Ook ras, religie, geboorteland en gezondheidsgegevens. Ook andere gegevens, zoals social media accounts, IP-adressen, mac-adressen van gebruikte apparatuur kunnen persoonsgegevens zijn. Het begrip ‘persoonsgegevens’ is zo ruim omdat het volgens de officiële definitie om ‘alle informatie betreffende een geïdentificeerde of identificeerbare natuurlijke persoon’ gaat. Tip: vraag niet meer informatie dan nodig, want wat je niet hebt kan ook niet gestolen worden.

Beveiliging

Op grond van de Europese en Nederlandse regelgeving dient iedereen die persoonsgegevens onder zich heeft afdoende beveiligingsmaatregelen te nemen. In de wet wordt dit omschreven als passende technische en organisatorische maatregelen ter beveiliging tegen verlies of onrechtmatig gebruik. Ook organisatorische maatregelen zijn belangrijk: wie kan er bij de gegevens en hoe wordt dit gemonitord.
Er dient sprake te zijn van een passend beveiligingsniveau gelet op de stand van de techniek en de risico’s verbonden aan verlies of misbruik van de persoonsgegevens. Deze verplichting bestond al.

NIEUW meldplicht datalekken

In Nederland wordt op naleving van deze regelgeving toegezien door het College Bescherming Persoonsgegevens (Cbp). Nieuw is dat de Datalekkenwet extra sancties verbindt aan niet-naleving van de beveiligingsverplichtingen. Op grond van de Datalekkenwet dienen organisaties die verantwoordelijk zijn voor verwerking van persoonsgegevens (‘verantwoordelijken’) alle beveiligingsinbreuken aan het Cbp te melden, als zo’n inbreuk leidt tot een aanzienlijke kans op ernstige nadelige gevolgen dan wel die ernstige nadelige gevolg voor bescherming van persoonsgegevens optreden. Als er risico is voor degenen wiens persoonsgegevens worden verwerkt (‘betrokkenen’) dienen ook zij te worden geïnformeerd.

Sancties

In de Datalekkenwet wordt de mogelijkheid van het Cbp om sancties op te leggen uitgebreid. Het Cbp kan hoge (bestuurlijke) boetes opleggen aan overtreders, die kunnen oplopen tot tien procent van de omzet of 810.000 euro. Voorts kan het Cbp aan ondernemingen een bindende aanwijzing opleggen. Dit laat onverlet dat onder omstandigheden ook strafvervolging van overtreders en hun leidinggevenden kan opleggen.
Het Cbp heeft aangekondigd dat de manier waarop het college omgaat met de nieuwe bevoegdheden zal worden vastgelegd in richtsnoeren. De definitieve versie van die richtsnoeren zal binnenkort bekend worden gemaakt.

Wat nu?

Organisaties die persoonsgegevens verwerken doen er goed aan na te gaan of de beveiliging aan de huidige eisen voldoet. Het is belangrijk om dit technisch te laten toetsen door gespecialiseerde ondernemingen die onafhankelijk zijn van degenen die de technische infrastructuur leveren. Dergelijke onafhankelijke toetsing wordt onder andere uitgevoerd door Mazars Management Consultants , zij voeren zowel ‘privacy audits’ uit inzake bestaande systemen, als ‘privacy impact assessments’ voor in ontwikkeling zijnde nieuwe systemen.
Ook de overeenkomsten die zijn gesloten met derden die direct of indirect betrokken zijn bij de verwerking van persoonsgegevens, dienen te worden getoetst. Voorts is aan te bevelen na te gaan of dergelijke derden ook betrouwbare wederpartijen bij contracten zijn, want papier is geduldig. Ook met een goed contract kan het zijn dat er van alles mis gaat met de beveiliging van persoonsgegevens.

Bij vragen of op uw situatie toegesneden juridisch advies kunt u terecht bij in privacyrecht en IT-beveiliging gespecialiseerde juristen.