DECLERCQ
Advocaten · Notarissen

White paper meldplicht datalekken

Wat verandert er per 1 januari 2016?

Een kort overzicht

In het voorstel voor de Europese Privacyverordening is de verplichting opgenomen voor verantwoordelijken om datalekken te melden. Vooruitlopend op deze verordening is de meldplicht datalekken opgenomen in de Wet bescherming persoonsgegevens. Deze meldplicht wordt op 1 januari 2016 van kracht. Tegelijkertijd wordt per 1 januari 2016 de boete op overtreding van de Wbp verhoogd van maximaal € 4.500,- naar maximaal € 810.000,- of 10% van de jaarlijkse wereldwijde omzet.

Een nieuwe meldplicht

De meldplicht datalekken treedt in werking op 1 januari 2016. Niet voor alle bedrijven is dit een nieuwe verplichting. Sinds 5 juni 2012 geldt immers al een meldplicht datalekken voor aanbieders van 'openbare elektronische communicatienetwerken'. Deze meldplicht is opgenomen in artikel 11.3a van de Telecommunicatiewet.

Wat is een 'datalek'?

Er is sprake van een 'datalek' in de zin van artikel 34a van de Wet bescherming persoonsgegevens ('Wbp') bij een inbreuk op de beveiliging die leidt tot de aanzienlijke kans (of de zekerheid) op ernstige nadelige gevolgen voor de bescherming van persoonsgegevens. Hiervan is bijvoorbeeld sprake wanneer hackers toegang krijgen tot systemen waarin persoonsgegevens zijn opgeslagen. Een datalek hoeft niet digitaal te zijn. Ook wanneer een medewerker een printje van een klantenbestand (met daarin persoonsgegevens) verliest is sprake van een datalek.

Voor wie geldt de meldplicht?

De meldplicht geldt voor de 'verantwoordelijke' in de zin van de Wbp. Dit is de persoon of het bedrijf dat bepaalt met welk doel en met welke middelen de persoonsgegevens worden verwerkt. Dit betekent dat de verplichting om een datalek bij een ingeschakelde (sub)bewerker te melden ligt bij de verantwoordelijke. Er zijn drie situaties waarin de meldplicht niet van toepassing is:

1. er worden geen persoonsgegevens verwerkt;
2. de verantwoordelijke is een financiële onderneming die valt onder de Wet op het financieel toezicht;
3. de verantwoordelijke valt onder de Telecommunicatiewet en heeft al aan de meldplicht uit deze wet voldaan;

Wanneer moet het datalek worden gemeld?

Niet ieder datalek hoeft te worden gemeld. Alleen datalekken met (een aanzienlijke kans op) ernstige negatieve gevolgen voor de privacy moeten worden gemeld. Het CBP werkt aan richtsnoeren aan de hand waarvan beoordeeld kan worden of sprake is van (een aanzienlijke kans op) ernstige nadelige gevolgen voor de bescherming van persoonsgegevens. Wanneer de beveiliging tijdelijk uitgeschakeld is geweest vanwege een stroomstoring en niet aannemelijk is dat er mensen ongeautoriseerde toegang hebben verkregen, hoeft dit niet te worden gemeld. Daarnaast hoeft een datalek niet te worden gemeld wanneer de verantwoordelijke passende technische beschermingsmaatregelen heeft genomen waardoor de persoonsgegevens versleuteld of beveiligd zijn zodat geen sprake kan zijn van ongeautoriseerde toegang.

Een datalek dat niet hoeft te worden gemeld moet wel worden geregistreerd in een logboek door de verantwoordelijke. In ieder geval moet de aard van het datalek worden geregistreerd, de persoon of instantie waar meer informatie over het datalek kan worden opgevraagd en de aanbevolen maatregelen om de negatieve gevolgen van het datalek te beperken. Dit logboek kan vervolgens worden

opgevraagd door het CBP ter controle van de beoordeling door de verantwoordelijke.

Wanneer een datalek wel gemeld moet worden, moet deze melding 'onverwijld' worden gedaan. Naar verwachting zal het CBP op haar website een richtsnoer publiceren met een nadere invulling van dit begrip. In het voorstel voor de Europese Privacyverordening is de termijn gesteld op 24 uur na kennisname van het datalek.

Aan wie moet het datalek worden gemeld?

Een datalek met gevolgen voor de bescherming van persoonsgegevens moet in ieder geval worden gemeld bij het CBP.

Wanneer een datalek (waarschijnlijk) ongunstige gevolgen zal hebben voor de persoonlijke levenssfeer van de betrokkene, dan moet het datalek ook aan deze betrokkene worden gemeld.

Hoe moet het datalek worden gemeld?

Per 1 januari 2016 zal op de website van het CBP een formulier staan waarmee een datalek kan worden gemeld. De melding bevat in ieder geval:

1. de aard van het datalek;
2. de persoon of instantie waar meer informatie over de inbreuk kan worden verkregen;
3. de aanbevolen maatregelen om de negatieve gevolgen van het datalek te beperken;
4. de (vermoedelijke) gevolgen van het datalek voor de verwerking van persoonsgegevens;
5. de voorgenomen maatregelen om deze (vermoedelijke) gevolgen te verhelpen.

Wanneer het datalek ook aan de betrokkene moet worden gemeld, dan is de verantwoordelijke verplicht om de betrokkene te voorzien van behoorlijke en zorgvuldige informatie. Welke informatie hier precies onder valt is afhankelijk van de aard en ernst van het datalek, de (verwachte) gevolgen van het datalek, de kring van betrokkenen en de kosten gemoeid met de melding. Ook hiervoor geldt dat het CBP door middel van een richtsnoer nadere invulling zal geven aan deze vereisten.

Hogere boetes

In het voorstel voor de Euroepese Privacyverordening zijn aanzienlijk hogere boetes opgenomen dan in de Wbp. Vooruitlopend hierop wordt de boetebevoegdheid van het CBP verhoogd naar maximaal € 810.000,- of 10% van de jaarlijkse wereldwijde omzet.

Een boete wordt niet direct opgelegd. Wanneer het CBP een overtreding van de Wbp constateert, moet zij eerst een bindende aanwijzing geven voordat een boete kan worden opgelegd. Deze bindende aanwijzing houdt in dat de persoon of het bedrijf dat de Wbp heeft overtreden, wordt verplicht alsnog aan zijn verplichtingen te voldoen. Pas wanneer ook na de bindende aanwijzing niet wordt voldaan aan de Wbp, kan het CBP overgaan tot het opleggen van een boete. Dit is slechts anders wanneer de overtreding opzettelijk is gepleegd of het gevolg is van ernstig verwijtbare nalatigheid.

Concrete aanbevelingen

Maak afspraken met bewerkers

Wanneer u gebruik maakt van (sub)bewerkers, dan moeten afspraken worden gemaakt met betrekking tot het melden van datalekken. De bewerker moet alle datalekken melden bij de verantwoordelijke, omdat deze ook de datalekken die niet hoeven te worden gemeld bij het CBP of de betrokkene moet opnemen in zijn logboek. Het is van belang dat de bewerker de verantwoordelijke van informatie voorziet over het datalek, welke de verantwoordelijke in de melding moet opnemen. Spoed is geboden bij het melden van het datalek door de bewerker aan de verantwoordelijke, zodat de verantwoordelijke kan voldoen aan zijn verplichtingen.

Ook als u geen verantwoordelijke bent, maar een bewerker, is het raadzaam om afspraken te maken met de verantwoordelijke. U dient immers te voorkomen dat de verantwoordelijke de boetes voor het niet voldoen aan de meldplicht datalekken op u kan afwentelen.

Maak interne afspraken

Het is van groot belang dat intern duidelijk is aan wie datalekken moeten worden gemeld en wie de afweging maakt of het datalek aan het CBP of de betrokkene moet worden gemeld. Gezien de korte periode tussen ontdekking en de verplichting tot het melden (24 uur), kan het direct leiden tot schade wanneer de informatie te lang op een bureau blijft liggen.

Encryptie of beveiliging

Een datalek hoeft niet te worden gemeld wanneer de gegevens ontoegankelijk zijn of onleesbaar. Aangezien niet alle datalekken kunnen worden voorkomen, is het aan te raden bestanden die persoonsgegevens bevatten door middel van encryptie of toegangsbeveiliging te beveiligen. Wanneer de gegevens die zijn getroffen door het datalek voor derden niet te openen zijn of onleesbaar, dan beschermt dit niet alleen de privacy van de betrokkene, maar ook de goede naam van de verantwoordelijke.

Tot slot

Op hoofdlijnen is de meldplicht datalekken duidelijk. In de komende maanden worden de richtsnoeren van het CBP verwacht die de open begrippen uit de meldplicht nadere invulling geven. De meldplicht treedt echter al over ruim drie maanden in werking. Het is daarom zaak dat organisaties zich gaan voorbereiden op de komende veranderingen. De privacy-specialisten van De CLERCQ helpen u daar graag mee.

Leiden/Den Haag, september 2015

Natascha van Duuren (n.vanduuren@declercq.com)
Willem Balfoort (w.balfoort@declercq.com)
Marijn Storm (m.storm@declercq.com)