CONCORDIA DE KEIZER
Riskmanagement & Benefits

Update Invoer Wetgeving Datalekken
Vanaf 1 januari 2016 is het wettelijk verplicht om datalekken te melden. Ieder kwijtraken, diefstal of onbevoegd gebruik van persoonsgegevens zal moeten worden gemeld.
Niet alleen bij de Autoriteit Persoonsgegevens (AP) voorheen het College Bescherming Persoonsgegevens (CBP), maar ook aan de betrokkenen, als dit negatieve gevolgen kan hebben voor hun privacy. Wie dit niet doet conform deze wet kan beboet worden met een maximale boete van Euro 810.000,-- of 10% van de jaaromzet.

Wat verandert er voor uw bedrijf vanaf 1 januari 2016?

1. *Wanneer is er sprake van een datalek?*

   In de wet wordt aangegeven dat er sprake is van een datalek wanneer persoonsgegevens verloren raken of onrechtmatig worden verwerkt. Onder onrechtmatige verwerking valt onder andere het aanpassen en/of veranderen van persoonsgegevens en onbevoegde toegang tot, of afgifte daarvan. Dit is dus niet alleen het geval als een hacker toegang tot persoonsgegevens krijgt. Ook verlies van een USB-stick of het sturen van een mailing met adressen in het CC-veld (in plaats van het BCC-veld) telt al als datalek. En zelfs verlies van gegevens zoals bij een brand in het datacentrum terwijl er geen back up beschikbaar is, ziet de wet als een datalek.

   U dient als bedrijf preventief de juiste beveiligingsmaatregelen te nemen om datalekken te voorkomen. Dit kan bijvoorbeeld door gebruik te maken van encryptietechnieken.

   Lekken waarbij andere gegevens dan persoonsgegevens verloren zijn geraakt of gestolen worden, zijn geen datalekken. Als de broncode van uw nieuwe software wordt ontvreemd, of een lijst met bedrijfsnamen uit uw relatiebeheerpakket wordt gekopieerd, dan valt dat bijvoorbeeld buiten de wet.

2. *Wanneer moet u een datalek melden, wanneer niet en aan wie?*

   Niet elk datalek moet worden gemeld. De wet bepaalt dat ‘ernstige’ datalekken binnen twee werkdagen bij AP gemeld moeten worden. Een lek kan ernstig zijn als het een grote hoeveelheid data betreft (kwantitatief ernstig), maar ook als het om gevoelige gegevens gaat (kwalitatief ernstig). Een paar voorbeelden uit de tweede categorie:

   • inloggegevens;
   • financiële gegevens;
   • kopieën van identiteitsbewijzen;
   • school- of werkprestaties;
   • gegevens die betrekking hebben op levensovertuiging;
   • gegevens die betrekking hebben op gezondheid.

   Indien het datalek waarschijnlijk ongunstige gevolgen heeft voor het privéleven van de personen van wie de gegevens gelekt zijn, dient u - naast de melding aan AP - het lek tevens binnen twee werkdagen te melden aan de personen waarvan de gegevens zijn gelekt. Dit zullen in de meeste gevallen klanten zijn. Ongunstige gevolgen zijn bijvoorbeeld:
   • identiteitsfraude;
   • discriminatie;
   • reputatieschade.
   Wanneer kwantitatief ernstige gegevens (zie vorige vraag) zijn gelekt, is eigenlijk altijd sprake van een ongunstig gevolg. Dit moet dus ook altijd worden gemeld aan de getroffen personen.

Een datalek hoeft echter niet aan de getroffen personen gemeld te worden wanneer de gelekte persoonsgegevens onleesbaar zijn. Hiervan is bijvoorbeeld sprake wanneer de persoonsgegevens versleuteld zijn of wanneer u de gegevens op afstand kunt verwijderen van bijvoorbeeld een gestolen laptop. U moet er dan wel zeker van zijn dat niemand de gegevens heeft kunnen inzien. U draagt hiervoor de bewijslast.

3. *Hoe moet u een datalek melden?*

AP zal hiervoor een standaarddocument beschikbaar stellen welke zal worden bewaard in een besloten register. Echter als er een boete wordt opgelegd dan zal dit wel openbaar worden gemaakt. Een datalek wordt uiteraard al openbaar als de getroffen personen moeten worden ingelicht.

4. *En wat te doen na een datalek?*

Wanneer u een datalek aan AP meldt, dient u een overzicht hiervan in uw administratie te bewaren. Dit overzicht moet de feiten en gegevens van het lek bevatten. Denk hierbij aan de oorzaak van het lek, de soort gegevens die gelekt zijn, het moment dat het lek is ontdekt en op welke wijze het lek gedicht is. Als u het datalek ook aan de getroffen personen heeft gemeld, is het belangrijk de communicatie hierover te bewaren. Voor het bewaren van de voornoemde gegevens dient u uit te gaan van een minimale bewaartermijn van één jaar. Maak hierover ook
afspraken indien u de gegevens heeft uitbesteed.

5. *Waarvoor kan u boetes krijgen?*

De wet kent vanaf 1 januari 2016 de mogelijkheid om boetes op te leggen wanneer niet voldaan wordt aan de wet. Deze boetes kunnen onder meer opgelegd worden voor:

- het niet melden van een datalek terwijl dat wel moet;
- het niet op orde hebben van de beveiliging;
- het verwerken van persoonsgegevens zonder toestemming;
- export van persoonsgegevens naar landen buiten de EU zonder dat goed geregeld te
- hebben.

De boete kan oplopen tot € 810.000,- of 10% van de jaaromzet. Vaak zal er eerst een waarschuwing gegeven worden, maar AP mag besluiten direct een boete op te leggen als u opzettelijk of grof nalatig heeft gehandeld.

6. *Wat als u alles heeft uitbesteed?*

In veel gevallen wordt het verwerken van persoonsgegevens uitbesteed aan een derde partij. Deze derde partij noemt de wet een bewerker. Data kan bijvoorbeeld toegankelijk zijn voor een clouddienstverlener die updates uitvoert op software, opgeslagen staan bij een hostingprovider, of beschikbaar zijn voor het marketing bedrijf dat e-mails in opdracht van klanten verzendt. Een bewerker hoeft een datalek niet te melden bij AP. Wel moet de bewerker er zorg voor dragen dat haar klanten deze melding tijdig bij AP kunnen maken. Er zullen daarom schriftelijke afspraken moeten worden gemaakt waarin wordt vastgelegd op welke wijze de klanten door de bewerker op de hoogte worden gesteld van een datalek. Deze afspraken kunnen worden opgenomen in een bewerkersovereenkomst. Let op: bent u bewerker en zijn bij een datalek ook gegevens met betrekking tot uw eigen klantadministratie gelekt, dan zult u ook zelf een melding van het lek moeten maken. U bent daar dan immers zelf verantwoordelijk voor.

7. *Wat kunt u doen ter voorbereiding?*

Goed voorbereid zijn op de meldplicht datalekken? Onderneem dan de volgende acties:

- inventariseer wie uw gegevens verwerken en of met deze partijen een bewerkersovereenkomst is gesloten;
- update uw bewerkersovereenkomsten met een bepaling omtrent datalekken;
- sluit met iedere partij waarmee u samenwerkt een NDA (Non Disclosure Agreement)waarin u persoonsgegevens benoemt;
- controleer hoe de bedrijven die voor u persoonsgegevens verwerken persoonsgegevens opslaan. Gebeurt dit veilig? Controleer dit uiteraard ook binnen uw eigen bedrijf;
- als bedrijven zeggen gecertificeerd te zijn (bijvoorbeeld ISO 27001), vraag dan naar de scope van deze certificering;
- hanteer intern een procedure voor de omgang met, en melding van, datalekken.
- **regel een verzekering tegen het lekken van persoonsgegevens (een cyberrisico verzekering);**