STICHTING TECHNISCH
INSTALLATIEBEDRIJF BEHEER

Datalekken

De Stichting Technisch Installatiebedrijf Beheer stelt vast dat de meldplicht datalekken alsmede het nemen alle mogelijke acties te voorkoming van, van toepassing is voor:

- Stichting InstallatieWerk Zuid Oost;

- Stichting Flexpool Installatietechniek Zuid Oost;

- Stichting Personeel en Organisatie Technisch Installatiebedrijf.

Vanaf 1 januari 2016 is de Wet Datalek meldplicht van kracht. Bedrijven zijn verplicht om datalekken te melden bij de toezichthouder (College Bescherming Persoonsgegevens) en de consument. Worden datalekken niet gemeld of is het lek veroorzaakt door nalatigheid, dan kunnen er flinke bestuurlijke boetes uitgedeeld worden. Wat wordt er nu bedoeld met een datalek? Moeten getroffen personen altijd op de hoogte gesteld worden? En wat zijn de gevolgen van de wet?

1. Wat is een datalek?

De wettelijke definitie is heel breed. Op het moment dat persoonsgegevens verloren raken of onrechtmatig worden bewerkt spreekt de wet van een inbreuk op de beveiliging van persoonsgegevens en wordt het als een datalek gezien. Dit betekent dat er niet alleen sprake is van een datalek als een hacker toegang heeft verkregen tot de persoonsgegevens, maar ook wanneer er een USB-stick met vertrouwelijke gegevens in een openbare ruimte blijft liggen.

Voor webshops, of andere sites met online inschrijfformulieren, zou er al sprake zijn van een datalek als de formulieren niet via een beveiligde verbinding (SSL) worden verzonden.

2. Wanneer moet men melden?

Niet elk lek hoeft direct gemeld te worden en ook niet elk datalek hoeft aan de getroffen personen gemeld te worden. Bij het melden van een datalek doet het er ook niet toe of het datalek werd veroorzaakt door overmacht of door een fout. Het belangrijkste is dat het gemeld wordt.

3. Toezichthouder (CBP)

Volgens de wet moeten ‘ernstige’ datalekken gemeld worden bij de toezichthouder. Wat precies ernstig is wordt niet helder uitgelegd, wel worden er twee categorieën datalekken onderscheiden:

- Een kwantitatief ernstig lek, waarbij een grote hoeveelheid data is gelekt.
- Een kwalitatief ernstig lek, waarbij gevoelige gegevens openbaar zijn geworden. Het gaat hierbij om bijvoorbeeld; inloggegevens, financiële gegevens, kopieën van identiteitsbewijzen en gegevens die betrekking hebben op de gezondheid.

De ondernemer moet zelf beoordelen of het lek wel of niet gemeld moet worden. Wordt er echter een foute inschatting gemaakt dan kan het gevolg daarvan zijn dat de ondernemer een hoge boete moet betalen of een waarschuwing krijgt.

4. Getroffen persoon

Een datalek hoeft alleen bij de getroffen persoon gemeld te worden als duidelijk is dat het lek negatieve gevolgen heeft op het privéleven van die persoon. Hierbij kan het gaan om reputatieschade of identiteitsfraude.

5. Wie moet het melden?

In principe is de onderneming aan wie de persoonsgegevens verstrekt zijn verantwoordelijk voor wat er met die gegevens gebeurt. Een webshop heeft dus de eindverantwoordelijkheid om lekken te melden. Bewerkers van de persoonsgegevens zoals een derde partij die persoonsgegevens verwerkt hoeven een datalek niet bij de toezichthouder te melden. Deze partij moet er echter wel zorg voor dragen dat de webshop waarvoor hij diensten verleend het lek wel tijdig kan melden.

6. Hoe moet het gemeld worden?

Bij een datalek dient een formulier ingevuld te worden dat door de toezichthouder (CBP) beschikbaar wordt gesteld. Als het formulier ingevuld is, is het niet meer openbaar. Als er wordt besloten om een boete op te leggen dan wordt dat besluit wel openbaar gemaakt.

7. Wat zijn de gevolgen?

De toezichthouder kan boetes opleggen aan bedrijven die niet zorgvuldig omgaan met data. De boetes kunnen oplopen tot €810.000,- of 10% van de jaaromzet. Hoewel er in de praktijk vaak eerst een waarschuwing gegeven zal worden kan er wel direct een boete opgelegd worden als er met opzet nalatig is gehandeld. Er worden onder andere boetes uitgedeeld wanneer:

- een datalek niet gemeld wordt,
- de beveiliging niet op orde is,
- of wanneer de persoonsgegevens zonder toestemming worden verwerkt.

8. Hoe kunnen wij ons voorbereiden?

Om goed voorbereid te zijn op deze meldplicht van datalekken dan kunnen de volgende acties worden ondernomen:

- Controleer of u verzekerd bent tegen het lekken van data, het zogenaamde cyberrisico (dit kunt u checken bij uw verzekering).
- Ga na of u met alle partijen die uw gegevens verwerken bewerkersovereenkomsten hebt gesloten en update deze overeenkomsten met een bepaling omtrent datalekken.
- Zorg dat uw webshop gebruik maakt van SSL verbindingen.

9. Procedure melden datalekken

Onderstaand afloopschema geeft aan of en welke actie genomen moet worden.

STICHTING TECHNISCH INSTALLATIEBEDRIJF BEHEER