EPI
Kenniscentrum

Procedure datalekken

1.Inleiding

Vanaf 1 januari 2016 wordt het wettelijk verplicht om datalekken te melden.
Zowel grootschalige inbraak als ieder kwijtraken, diefstal of onbevoegd gebruik van persoonsgegevens telt als een datalek. Wie data laat lekken of persoonsgegevens verwerkt zonder zich aan de wet te houden, loopt kans op boetes die kunnen oplopen tot € 820.000,-of 10% van de jaaromzet per overtreding.

2.Wat is een datalek?

De wet spreekt van een datalek wanneer persoonsgegevens verloren raken of onrechtmatig worden verwerkt. Er is dus niet alleen sprake van een datalek 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 het verlies van gegevens zoals bij een brand in het datacentrum terwijl er geen back up beschikbaar is, ziet de wet als een datalek.

3.Wanneer moet een datalek gemeld worden aan de toezichthouder?

De toezichthouder is het College Bescherming Persoonsgegevens per 01012016 Autoriteit Persoonsgegevens. De wet bepaalt dat 'ernstige' datalekken binnen 72 uur bij de toezichthouder 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;
- gegevens die betrekking hebben op levensovertuiging;
- gegevens die betrekking hebben op gezondheid.

4.Wanneer moet een datalek gemeld worden aan de getroffen personen?

Indien het datalek ongunstige gevolgen heeft voor het privéleven van de personen van wie de gegevens gelekt zijn, dient het lek binnen 72 uur gemeld te worden aan de getroffen personen. Ongunstige gevolgen zijn bijvoorbeeld:

- identiteitsfraude;
- discriminatie;
- reputatieschade.

5.Wat zijn de gevolgen van de wet?

De wet kent vanaf1 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 € 820.000,-of 10% van de jaaromzet. Vaak zal er eerst een waarschuwing gegeven worden, maar de toezichthouder mag besluiten direct een boete op te leggen als er opzettelijk of grof nalatig gehandeld is.

5. Aanpak EPI-kenniscentrum

a)Datalekken worden binnen 24 uur gemeld bij de functionaris voor de gegevensbescherming (FG). Zodat dit beoordeeld kan worden en tijdig gemeld bij de Autoriteit Persoonsgegevens (AP).
b)Als de functionaris gaat melden stelt ze de directeur daarvan op de hoogte. De directeur beoordeelt per geval of de stuurgroep op de hoogte gebracht moet worden.