Een datalek, wat nu?

PRIVACY OP SCHOOL

Doorloop onderstaande stappen om schade te beperken

Bij een datalek gaat het om ongeoorloofde of onbedoelde toegang tot persoonsgegevens bij een organisatie. Maar ook om het ongewenst vernietigen, verliezen, wijzigen en verstrekken van persoonsgegevens. Of zonder dat dit wettelijk is toegestaan. Hierdoor kunnen de betrokken personen mogelijk schade leiden. Het is dus belangrijk om na te gaan of uw organisatie verplicht is om het datalek te melden. Maar dat is niet het enige. Is er bij uw organisatie sprake van een datalek? Kom dan snel in actie om grotere problemen voor te zijn, informeer uw Functionaris Gegevensbescherming (FG) en doorloop onderstaande stappen.

1

Analyseer de situatie

Wat is er gebeurd, wat is de oorzaak en wat is de omvang? Zijn er gegevens gelekt, vernietigd of gewijzigd? Onderzoek dan wie er (mogelijk) toegang hebben (gehad) tot welke persoonsgegevens.

2

Beperk de schade

Bepaal op basis van stap 1 of er maatregelen zijn die u direct kunt nemen om het datalek te beëindigen en de schade te beperken. Zo ja, neem deze maatregelen onmiddellijk! Bijvoorbeeld door een gestolen laptop op afstand te wissen. Geef het datalek door aan het privacy team, privacy officer en/of FG. Maak vervolgens een inschatting van het (mogelijke) risico dat het datalek oplevert.

3

Moet het lek worden gemeld bij de AP?

De FG adviseert de bestuurder of het datalek moet worden gemeld bij de Autoriteit Persoonsgegevens (AP). Dit moet binnen 72 uur, tenzij het niet waarschijnlijk is dat het datalek een risico oplevert voor de rechten en vrijheden van de betrokken personen. Is bij de eerste melding nog niet alle informatie beschikbaar? Geef dit dan door en doe later een vervolgmelding.

4

Moet het lek worden gemeld bij de betrokkenen?

Een datalek moet aan de betrokken personen worden gemeld, wanneer er sprake is van een hoog risico voor de rechten en vrijheden van de betrokken personen. Is dit het geval? Meld het datalek dan zo snel mogelijk, in overleg met privacy team, privacy officer en/of FG!

5

Registreer en evalueer

U moet het datalek registreren in uw register voor beveiligingsincidenten. Ook wanneer het lek niet aan de AP moet worden gemeld! Stel vervolgens een evaluatie op om herhaling te voorkomen. Wat hebben we (of: wat heeft de organisatie) hiervan geleerd?