Policy inzake datalekken

Zeno Zorg hecht belang aan de bescherming van persoonsgegevens, waaronder alle informatie waarmee een persoon geïdentificeerd kan worden. Datalekken vormen een ernstig risico en moeten waar mogelijk worden vermeden. In deze policy wordt uiteengezet wat je moet doen als er onverhoopt toch sprake is van een datalek bij Zeno Zorg.

Persoonsgegevens

Waar in deze policy gesproken wordt over "**persoonsgegevens**" betekent dit alle informatie waarmee de identiteit van een persoon kan worden vastgesteld. Waar gesproken wordt over "**verwerking**" van persoonsgegevens, gaat het om onder meer verzamelen, gebruiken, opslaan en beveiligen van persoonsgegevens.

Wat is een datalek?

In het algemeen kan een datalek kan worden omschreven als een beveiligingsincident waardoor de vertrouwelijkheid, integriteit of beschikbaarheid van persoonsgegevens wordt of is aangetast. Er is sprake van een datalek als persoonsgegevens verloren zijn gegaan, vernietigd, verminkt of gelekt, als iemand de gegevens onbevoegd inziet of doorgeeft, als gegevens per ongeluk worden gewist of vernietigd of als de gegevens ontoegankelijk worden gemaakt, bijvoorbeeld als ze worden versleuteld door ransomware.

Een aantal specifieke voorbeelden van datalekken zijn:

- Verzending van een e-mail aan een verkeerd adres;
- Het hacken van een computer, mobiele telefoon of software of een malware-aanval daarop;
- Het openen van een 'phishing' e-mail;
- Verlies of diefstal van een mobiele telefoon waarop bedrijfsgegevens zijn opgeslagen;
- Het per ongeluk wissen van een harde schijf dat het enige exemplaar van de gegevens van een persoon bevat, en waarvan geen back-up bestaat;
- Verlies of diefstal van een laptop of USB-stick.

Na ontdekking, dient het (vermoedelijke) datalek intern gemeld te worden

Een vermoedelijk datalek moet onmiddellijk per e-mail worden gemeld aan de functionaris gegevensbescherming, fg@zenozorg.nl.

Daarnaast moet je het vermoede datalek melden aan je leidinggevende en aan elke andere afdeling en/of persoon die daar mogelijk bij betrokken is of door geraakt kan worden. Indien je eventuele herstelacties kunt nemen, moet je dat ook direct doen.

Beoordeling van een datalek en te ondernemen maatregelen

Na melding van het datalek wordt door de functionaris gegevensbescherming vastgesteld of de betrokken gegevensbeschermingsautoriteiten gewaarschuwd moeten worden. Daarnaast moet worden vastgesteld of de betrokkenen van wie de persoonsgegevens door het datalek zijn getroffen, moeten worden geïnformeerd en/of welke (andere) herstelactie(s) genomen moet worden. Daarbij dient het volgende stappenplan gevolgd te worden:

1. Het datalek wordt ontdekt
2. Het datalek wordt intern gemeld
3. Acties die vervolgens tegelijk moeten plaatsvinden:
    a. Neem alle herstelacties die nodig zijn

b. De Functionaris Gegevensbescherming zoekt uit of de impact zodanig is dat melding bij de AP gedaan moet worden (evt. in overleg met advocaat)
    i. *indien wel melding*: binnen 72 uur na ontdekken datalek
    ii. *indien geen melding*: beargumenteer schriftelijk (intern) waarom geen melding noodzakelijk is
c. De Functionaris Gegevensbescherming zoekt uit of de impact zodanig is dat betrokkenen geïnformeerd moeten worden (evt. in overleg met advocaat)
    i. *indien ja*: standaard reactie opstellen voor betrokkenen
    ii. *indien nee*: beargumenteer schriftelijk (intern) waarom geen informatie aan betrokkenen noodzakelijk is

4. Vermeld het datalek en alle ins en outs in het datalekregister (incl. de evt. melding aan de AP en evt. de tekst van de melding aan betrokkenen).

Termijn voor het informeren van de gegevensbeschermingsautoriteiten

Indien het datalek gemeld moet worden aan de gegevensbeschermingsautoriteiten, dient dit binnen 72 uur na ontdekking ervan te geschieden.

Datalekkenregister

Zeno Zorg houdt een datalekkenregister bij, waarin alle datalekken worden omschreven met de daarbij relevante informatie.

Niet naleving van deze policy

Niet-naleving van deze policy inzake datalekken kan leiden tot disciplinaire maatregelen.