evenwijs

Protocol Datalekken

Dit protocol beschrijft de procedure met daarin te nemen maatregelen die genomen worden bij een datalek volgens de meldplicht datalekken van de Wet bescherming persoonsgegevens (Wbp). Er moet sprake zijn van het daadwerkelijk 'lekken van data'. Het lekken heeft een onbedoelde of onwettige vernietiging, verlies of wijziging van, of een niet geautoriseerde toegang tot verwerkte persoonsgegevens tot gevolg.

Datalekken kunnen ontstaan door:
- moedwillig handelen (cybercriminaliteit, hacking, identiteitsfraude, mailware besmetting);
- technisch falen (ICT-storingen);
- menselijk falen (het verstrekken username/wachtwoorden aan collega's en externen);
- calamiteit (brand, wateroverlast);
- verzenden van email met emailadressen van alle geadresseerden.

Een datalek wordt aan de directie medegedeeld. Het incident zal zorgvuldig worden onderzocht.

Hierbij is aandacht voor de volgende aspecten:
a. wat is de aard van het datalek;
b. wat is de oorzaak dat dit incident heeft plaatsgevonden;
c. is er sprake van het niet nakomen van of een tekortkoming in de beveiligingsprocedures;
d. is de organisatie verwijtbaar.

Indien sprake is van een datalek dan zal de directie binnen 2 dagen maar niet later dan 72 uur na ontdekking zorg dragen voor een melding bij de Autoriteit Personengegevens (AP). De organisatie houdt een overzicht bij van alle datalekken. Per datalek wordt aangegeven wat de feiten en gegevens zijn van de aard van de inbreuk. Het overzicht wordt minimaal 1 jaar bewaard.

Mocht er na melding aanleiding zijn om nadere stappen te ondernemen neemt de AP contact op. Hierbij zal met name de herkomst van de melding worden geverifieerd. Wanneer vaststaat dat een datalek bij de AP gemeld moet worden dan dient hierna beoordeeld te worden of een datalek ook aan betrokkene moet worden gemeld. Betrokkenen zijn degenen wiens persoonsgegevens zijn betrokken bij een inbreuk. In het geval van Evenwijs zijn de betrokkenen over het algemeen cursisten of medewerkers. Een betrokkene wordt onverwijld in kennis gesteld van de inbreuk. Indien de inbreuk waarschijnlijk geen ongunstige gevolgen zal hebben voor de persoonlijke levenssfeer van de betrokkene of wanneer de technische beschermingsmaatregelen (bijvoorbeeld encryptie) die zijn genomen voldoende bescherming bieden, kan melding van het datalek aan de betrokkene achterwege blijven.

De directie is verantwoordelijk voor het ondernemen van preventieve, reparatoire en repressieve maatregelen.