WET MELDPLICHT DATALEKKEN

TO DO LIST

Beveiliging en datalek

De meldplicht datalekken ontstaat pas als er tenminste een inbreuk op de beveiliging is en er sprake is van een daadwerkelijk beveiligingsincident. Een to do list ter voorbereiding op de meldplicht datalekken omvat daarom vooral actiepunten rondom de beveiliging van systemen. De beveiligingsverplichting uit de Wbp (art 13) bestaat uit 2 aspecten:

Organisatorische en *technische* beveiligingsmaatregelen om te voorkomen dat de verzameling persoonsgegevens kan worden aangetast, vernietigd of onrechtmatig kan worden gebruikt.

Organisatorisch = maatregelen binnen het bedrijf of de organisatie tegen datalekken van binnenuit.
De meeste datalekken worden veroorzaakt door menselijk gedrag. Het belangrijkste actiepunt is om ervoor te zorgen dat iedereen die betrokken is bij het gebruik van data weet wat de risico's zijn, weet wat de afspraken zijn, zich houdt aan de beveiligingsafspraken en weet wat te doen bij een datalek.

Technisch = maatregelen binnen de systemen tegen datalekken door oorzaken van buitenaf.
Uit de Beleidsregels over datalekken volgen een aantal specifieke technische maatregelen. De AP omschrijft deze als Preventieve, Detectieve, Repressieve en Correctieve maatregelen en Herstelmaatregelen. Deze maatregelen beperken het (boete)risico en worden hierna benoemd.

Acties

INVENTARISEER

- Voer een privacy scan uit en bepaal welke concrete acties nodig zijn;

DOCUMENTEER

- Maak een privacy beleid. Hierin staat hoe binnen de organisatie wordt omgegaan met persoonsgegevens;
- Zorg voor een draaiboek datalekken: aan wie moet intern worden gemeld, wie verzamelt de gegevens over het lek, wie doet de melding, wat is de communicatiestrategie bij een lek;
- Vertaal het beleid en draaiboek in afspraken met medewerkers (protocollen en handboeken);

IMPLEMENTEER

- Zorg dat iedereen op de hoogte is van het beleid en draaiboek. Train de medewerkers hierin;
- Verzorg tenminste jaarlijks een training voor medewerkers om het privacy bewustzijn op niveau te houden;

BEVEILIG

- Stel zo nodig beveiligde hardware (computer met wachtwoorden, encrypted losse harde schijf) ter beschikking. Werk bij voorkeur met private (Europese) cloud oplossingen en beveiligde verbindingen;
- Zorg dat tijdig backups worden gemaakt van bestanden;
- Ken toegangsrechten toe aan medewerkers en zorg voor logging hiervan;
- Zorg voor scheiding van systemen of tenminste de scheiding van databestanden;

- Gebruik encryptietechnologie en controleer deze met regelmaat op actualiteit. Denk na over de wijze waarop de sleutel behorend bij de encryptie wordt bewaard;
- Laat beveiliging van de systemen testen;
- Update tijdig de software die binnen de organisatie wordt gebruikt;

CREEER

- Stel een incidentenregister in. Let op: niet instellen van een incidentenregister is apart beboetbaar;

CONTROLEER

- Controleer de afspraken met bewerkers – de partijen die meewerken bij het gebruik van de persoonsgegevens – op verplichtingen en aansprakelijkheden bij datalekken. Controleer de gehele keten van contracten. Pas zo nodig de overeenkomsten aan (of leg de afspraken alsnog vast);
- Controleer de afspraken met betrokkene – algemene voorwaarden, arbeidsovereenkomsten, privacy verklaringen – op verplichtingen en aansprakelijkheden bij datalekken. Pas zo nodig de overeenkomsten aan;
- Controleer de afspraken over het uitvoeren van up-dates en ook over toegangsrechten, wat dus ook betekent dat er een systeem is waardoor de toegangsrechten van ex-werknemers, oud stagiaires of tijdelijke freelancer daadwerkelijk worden ingetrokken;
- Trek lering uit het incidentenregister. Na een jaar kan het incidentenregister worden opgeschoond, een mooi moment om de “lessons learned” met de organisatie te delen.
- Denk na over de interne aansprakelijkheid, beboetbaarheid, van bestuurders of directeur. Maak hier zo nodig afspraken over of leg bevoegdheden anders vast.