LEGAL UPDATE

In samenwerking met RWV Advocaten houden we u op de hoogte van actueel juridisch nieuws

U constateert een datalek: welke AVG maatregelen moet u als werkgever nemen?

Volg RWV

Als werkgever loopt u het risico op datalekken. Om datalekken en eventuele boetes van de Autoriteit Persoonsgegevens (AP) te voorkomen, moet u voldoen aan verschillende verplichtingen die volgen uit de Algemene verordening gegevensbescherming (AVG). Maar wat als u toch geconfronteerd wordt met een datalek? Welke maatregelen moet u dan nemen? De nieuwe guidelines geven hier meer duidelijkheid over en helpen bij het beoordelen van het risico. Is er sprake van een risico, dan is het belangrijk om het datalek tijdig en juist te melden.

Voorkom een boete voor een datalek van de AP!

Inmiddels is de AVG bijna drie jaar van toepassing en hebben zich bij veel werkgevers de eerste datalekken voorgedaan. Sinds de inwerkingtreding heeft de Autoriteit Persoonsgegevens (de AP) al verschillende sancties voor het niet naleven van de verplichtingen rondom datalekken opgelegd. Onder deze sancties vallen ook zes forse boetes, waaronder een boete voor het te laat melden van een datalek. Het betrof een boete van € 600.000,=.

Om te voorkomen dat u geen boete opgelegd krijgt, is het belangrijk dat u de regels goed naleeft op het moment dat u een datalek constateert!

Wat is het protocol bij het constateren van een datalek?

Als een werknemer zich meldt met een mogelijk datalek, dan dient u de volgende stappen te volgen:

Stap 1: Controleer of er inderdaad sprake is van een datalek;
Stap 2: Is er sprake van een datalek? Registreer het datalek in het register datalekken en neem waar nodig corrigerende en preventieve maatregelen;
Stap 3: Ga na of u het datalek dient te melden aan de AP en/of betrokkene(n) en zorg voor tijdige melding.

Binnen de algemene richtlijnen over datalekken is de hoofdregel dat een datalek binnen 72 uur na de ontdekking van het lek gemeld moet worden aan de AP. Dit hoeft niet als het niet waarschijnlijk is dat er sprake is van een risico. De betrokkene(n) hoeft alleen geïnformeerd te worden als er sprake is van een hoog risico.

Gebleken is dat het niet altijd duidelijk is van welke datalekken er melding gemaakt moet worden aan de AP en/of aan de betrokkene(n). Ook het inschatten van de risico's blijkt moeilijk.

Guidelines datalekmeldingen

Om die reden heeft de European Data Protection Board (EDPB) nieuwe guidelines over datalekmeldingen opgesteld. De guidelines vullen de reeds bestaande algemene richtlijnen over datalekken aan. De nieuwe guidelines zijn overigens nog niet definitief vastgesteld. Dit zal niet lang meer duren, nu de consultatie inmiddels wel is gesloten.

Voorbeelden datalekken moeten helpen bij beoordeling risico

De guidelines moeten helpen bij het beoordelen van deze risico's. Er is voor gekozen om van categorieën datalekken die veel voorkomen, voorbeelden te geven en daarbij aan te geven;

- welke maatregelen een organisatie in dat geval vooraf had moeten nemen;
- welke maatregelen de organisatie na het incident moet nemen;
- hoe de risico's beoordeeld kunnen worden; en

- in welke gevallen de AP en betrokkene(n) op de hoogte gebracht moet worden.

Voorbeelden van datalekken die zijn uitgewerkt in de guidelines zijn onder meer:

- het versturen van een e-mail met gevoelige gegevens aan een verkeerde ontvanger;
- het versturen van een brief met persoonsgegevens naar een verkeerd adres;
- een situatie waarbij door identiteitsfraude een e-mailadres wordt aangepast in het systeem van een bedrijf waardoor de e-mails naar een ander dan de klant verstuurd worden;
- diefstal van documenten met persoonsgegevens.

Advies omtrent AVG en vastlegging datalekken

Wilt u weten hoe u de verplichtingen rondom datalekken goed naleeft? Of wilt u meer weten over de manier waarop u met datalekken dient om te gaan of wilt u hulp bij het opstellen van een beleid, neem gerust contact op met mij of een van de overige specialisten op het gebied van privacyrecht en AVG. Wij adviseren u graag.

Nadine van der Slot

n.vanderslot@rwv.nl
071-750 22 73
06-12 06 07 39