supplier of Independent Risk Solutions

Wat moet u doen om aan de Wet Meldplicht Datalekken te voldoen?

Sinds 1 januari 2016 geldt de Wet Meldplicht Datalekken. Deze wet verplicht organisaties te registreren waar en voor welk doel tot personen te herleiden gegevens worden vastgelegd en, indien deze gegevens worden "gelekt", dit te melden. Hieronder leest u wat u moet doen om aan de Wet Meldplicht Datalekken te voldoen.

De meldplicht datalekken

De Wet Meldplicht Dataleken is in werking getreden als uitbreiding op de Wet bescherming persoonsgegevens (Wbp), welke op termijn door de Algemene Verordening Gegevensbescherming zal worden vervangen. De Wbp heeft betrekking op de verwerking van persoonsgegevens en is bedoeld om datalekken zoveel mogelijk tegen te gaan.

Wat houdt de verwerking van persoonsgegevens in?

Het verwerking van persoonsgegevens betreft elke handeling met betrekking tot gegevens die direct of indirect herleidbaar zijn tot een natuurlijk persoon. Voorbeelden van persoonsgegevens zijn niet alleen een naam, een adres en woonplaats, maar ook een IP-adres en informatie over iemands gezondheid.

Wat is een datalek?

Iedere inbreuk op de persoonsgegevens vormt een datalek. Het gaat hierbij niet alleen om ongeautoriseerde toegang tot persoonsgegevens, zoals bijvoorbeeld bij een hack het geval is, maar ook om het onrechtmatig verspreiden, wijzigen en vernietigen van persoonsgegevens. De omvang van het datalek speelt hierbij geen rol.

Is de Wet Meldplicht Datalekken geldig voor uw organisatie?

U vraagt zich wellicht af of de Wet Meldplicht Datalekken ook voor uw organisatie geldig is. Worden er binnen uw organisatie persoonsgegevens verwerkt? Zo ja, dan is de Wet Meldplicht Datalekken van toepassing op uw organisatie.

Aan wie moet een datalek gemeld worden?

De melding van datalekken is afhankelijk van de aard van het datalek. Afhankelijk van deze aard moet er een melding worden gemaakt aan de *toezichthouder* en aan de *betrokkenen*. De toezichthouder is de Autoriteit Persoonsgegevens, de betrokkene is de natuurlijk persoon op wie de gegevens van het lek betrekking hebben. Laatstgenoemde moeten geïnformeerd worden wanneer het datalek mogelijk nadelig gevolgen voor hen met zich meebrengt.

Welke rollen bestaan er in de verwerking van persoonsgegevens?

De Wet bescherming persoonsgegevens maat onderscheid tussen de *verantwoordelijke* en de *bewerker* of *sub-bewerker* van persoonsgegevens. De verantwoordelijke is de natuurlijk persoon of rechtspersoon die, of het bestuursorgaan dat, het doel van en de middel voor de verwerking van persoonsgegevens vaststelt. De bewerker is diegene die persoonsgegevens verwerkt. De verwerker doet dit in opdracht van de opdrachtgever, conform diens instructies en onder diens (uitdrukkelijke) verantwoordelijkheid. Indien er werk voor uitbesteed, dan gelden er regels voor de sub-bewerker van persoonsgegevens.

supplier of Independent Risk Solutions

Welke maatregelen kunt u nemen om aan de meldplicht te voldoen?

De Wet bescherming persoonsgegevens hanteer inzake maatregelen de open norm van een "passen beveiligingsniveau", rekening houdend met de stand van de techniek en de kosten van de tenuitvoerlegging. De risico's die de verwerking van en de aard van de persoonsgegevens met zich mee brengen spelen hierbij een belangrijke rol. Een aantal maatregelen die u kunt treffen leest u hieronder.

1) Sluit een bewerkersovereenkomst met de partijen die ten behoeve van u gegevens verwerken en zorg ervoor dat hierin afspraken staan omtrent datalekken;
2) Doe aan informatiebeveiliging en neem hiervoor waarborgen op in de bewerkingsovereenkomst;
3) Bepaal in het kader van interne verantwoordelijkheid of er een interne procedure bestaat met betrekking tot de omgang met en de bescherming van persoonsgegevens, het melden van datalekken en wie hiervoor verantwoordelijk is;
4) Registreer alle interne inbreuken op de beveiliging die als datalek kunnen kwalificeren;
5) Verzeker u tegen het lekken van persoonsgegevens.

Heeft u inzicht in de persoonsgegevens binnen uw organisatie?

Veel organisaties hebben geen of onvolledig inzicht in de aanwezige persoonsgegevens binnen de organisatie waardoor zij een verhoogd risico lopen te maken te krijgen met een datalek. Indien een datalek daadwerkelijk heeft plaatsgevonden, dan is een bijkomend probleem dat organisaties niet of onvolledig op de hoogte zijn van welke persoonsgegevens er zijn gelekt.

Hoe kan IR}S u ondersteunen?

De specialisten van IR}S kunnen u helpen om de persoonsgegevens binnen uw organisatie in kaart te brengen. Hierdoor voldoet u aan alle vereisten voor de registratie van deze gegevens en weet u, indien er gegevens worden "gelekt", exact welke gegevens dit zijn.

Meer informatie?

Wilt u meer informatie over de meldplicht datalekken, over de maatregelen die u kunt nemen om aan deze meldplicht te voldoen, of over hoe de specialisten van IR}S u kunnen ondersteunen? Neemt u dan contact met ons op via info@irsnl.com.

Forensic Investigations

De topspecialisten van IRS hebben al meer dan 25 jaar ervaring met het doen van onafhankelijk onderzoek op het gebied van fraude en integriteit. IRS biedt een totaalpakket van 'forensic services' die alle vormen van onderzoek omvatten, waaronder ook forensisch IT-onderzoek. De integrale IRS-aanpak legt de basis voor integriteit, vertrouwen, continuïteit en veiligheid. Proportionaliteit en subsidiariteit zijn bij deze aanpak leidende principes.

Forensic IT Investigations

De omvang en complexiteit van digitale informatie neemt sterk toe en daarmee ook de behoefte aan meer expertise. Met hun ruime en unieke ervaring op het gebied van forensische IT kunnen de specialisten van IRS u bijstaan bij problemen op alle vlakken van hun vakgebied. Daar waar men in traditionele onderzoeken tekortschiet, is IRS in staat het verwijderde weer zichtbaar te maken, veilig te stellen, te doorzoeken en te analyseren.

Integrity Risk Management

De omvang en complexiteit van digitale informatie neemt sterk toe en daarmee ook de behoefte aan meer expertise. Met hun ruime en unieke ervaring op het gebied van forensische IT kunnen de specialisten van IRS u bijstaan bij problemen op alle vlakken van hun vakgebied. Daar waar men in traditionele onderzoeken tekortschiet, is IRS in staat het verwijderde weer zichtbaar te maken, veilig te stellen, te doorzoeken en te analyseren.