

# Meldplicht datalekken

Op 1 januari 2016 is de meldplicht datalekken ingegaan. Deze meldplicht houdt in dat organisaties direct een melding moeten maken bij de Autoriteit Persoonsgegevens zodra zij een ernstig datalek hebben geconstateerd. Daarnaast beschrijft deze meldplicht dat zij de betrokkenen moeten informeren indien het waarschijnlijk ongunstige gevolgen zal hebben voor hun persoonlijke levenssfeer.

- Maar wat is dan een ernstig datalek? En wat zijn ongunstige gevolgen?
- Geldt dit dan ook voor mijn (MKB) organisatie en wat moet ik dan doen?

Om je hier makkelijk en snel inzicht in te geven hebben wij de belangrijkste informatie voor je op een rij gezet en een gratis checklist Meldpunt Datalekken ter beschikking gesteld.

## Wet Meldpunt datalekken in het kort

- Alhoewel het in de volksmond een wet genoemd wordt is het eigenlijk een aanpassing van een aantal wetten waarvan de twee belangrijkste de Wet Bescherming Persoonsgegevens (WBP) en de Telecommunicatiewet zijn. Het gaat er bij deze wetten om dat organisaties de persoonsgegevens die zij verwerken dienen te beveiligen tegen verlies en tegen onrechtmatige verwerking
- Het gaat uit van het melden van inbreuken op de privacy van personen
- Binnen 72 uur moet het datalek gemeld zijn aan de Autoriteit Persoonsgegevens
- Het datalek moet daarnaast ook worden gemeld aan de betrokkenen indien het waarschijnlijk ongunstige gevolgen zal hebben voor diens persoonlijke levenssfeer
- Bij het niet melden, wordt de verantwoordelijke bestraft
- De boete die de Autoriteit Persoonsgegevens kan geven kan oplopen tot maximaal € 820.000,=

## Is er sprake van een datalek?



1. Heeft zich een beveiligingsincident voorgedaan?	
<input type="checkbox"/>	Heeft iemand onterecht toegang gehad tot bedrijfsmiddelen waarop informatie digitaal of analoog informatie is opgeslagen?
<input type="checkbox"/>	Is er een kans dat onbevoegden toegang hebben gehad tot de persoonsgegevens die jouw organisatie verwerkt?
<input type="checkbox"/>	Is iemand zonder toestemming in het kantoorpand of een andere beveiligde ruimte geweest?

2. Is er sprake van een datalek?	
<input type="checkbox"/>	Zijn er persoonsgegevens onbedoeld verloren gegaan of zijn deze gegevens niet meer te lezen of te benaderen?
<input type="checkbox"/>	Is er na onderzoek niet uit te sluiten dat onbevoegde toegang hebben gehad tot de persoonsgegevens die jouw organisatie verwerkt?
<input type="checkbox"/>	Zijn er persoonsgegevens (fysiek of digitaal) onbeheerd achtergelaten zonder dat deze gegevens beveiligd waren via encryptie?

3. Is er sprake van ernstige nadelige gevolgen voor de bescherming van persoonsgegevens?	
<input type="checkbox"/>	Zijn er persoonsgegevens van gevoelige aard gelekt?
<input type="checkbox"/>	Leiden de aard en omvang van de inbreuk tot (een aanzienlijke kans op) ernstige nadelige gevolgen?

4. Kunnen de gevolgen ongunstig zijn voor de persoonlijke levenssfeer van de betrokkene?	
<input type="checkbox"/>	Zal het datalek waarschijnlijk ongunstige gevolgen hebben voor de persoonlijke levenssfeer van de betrokkene?
<input type="checkbox"/>	Heb je als bedrijf geen zwaarwegende redenen om de melding achterwege te laten?