Verbond van Credit Management Bedrijven

De Wet bescherming persoonsgegevens (Wbp)

En wat betekent dit voor u?

Meldplicht datalekken

Whitepaper Datalekken

Augustus 2016

Begin 2016 is de Meldplicht Datalekken ingegaan. Het doel van de meldplicht is om de negatieve gevolgen van een datalek voor de betrokkenen beperken.
Als blijkt dat de gelekte persoonsgegevens onvoldoende beveiligd waren of onrechtmatig werden verwerkt, kunnen bedrijven geconfronteerd worden met een boete van 10 procent van de omzet, met een maximum van 810.000 euro.
Het nalaten van het melden van een datalek bij de toezichthouder kan een boete van €500.000,- opleveren.
Wat is een datalek en wanneer moet u een melding maken?

1. Wat is een datalek?

Een datalek is volgens de wet: iedere inbreuk op de beveiliging van persoonsgegevens. Het kan gaan om het verlies van persoonsgegevens, door bijvoorbeeld het kwijtraken van een laptop met gevoelige informatie. Maar ook het onbedoeld wijzigen of verwijderen van persoonsgegevens is een datalek. En wanneer een onbevoegde toegang krijgt tot persoonsgegevens, bijvoorbeeld door inbreuk op een systeem, is er ook sprake van een lek.

Een datalek is een inbreuk❶ op de beveiliging van de persoonsgegevens, die leidt tot:

- De aanzienlijke kans op ernstige nadelige gevolgen;
- Ernstige nadelige gevolgen heeft;
- Voor de bescherming van persoonsgegevens.

❶ Een inbreuk is een verlies of enige vorm van onrechtmatige verwerking van persoonsgegevens.

2. Beveiliging van persoonsgegevens

Beveiliging bestaat uit maatregelen die een passend beveiligingsniveau garanderen. Deze maatregelen zijn er mede op gericht onnodige verzameling en verdere verwerking van persoonsgegevens te voorkomen.

3. Wanneer is er sprake van een datalek

Indien onderstaande vragen bevestigend worden beantwoord dan is er sprake van een datalek in de zin van de wet:

- Inbreuk : Is er sprake van inbreuk op de getroffen beveiligingsmaatregelen?
- Persoonsgegevens : Kan redelijkerwijs worden aangenomen dat er een aanmerkelijke kans is op nadelige gevolgen voor de bescherming van de persoonsgegevens (verlies, aantasting, toegang door onbevoegden)?
- Aanmerkelijke kans op onrechtmatige verwerking : Kan redelijkerwijs worden aangenomen dat er een aanmerkelijke kans is op nadelige gevolgen voor de bescherming van de persoonsgegevens (verlies, aantasting, toegang door onbevoegden)?

Zijn er persoonsgegevens gelekt, dan moet u hier melding van maken als er sprake is van een datalek. Dit is het geval wanneer het zowel om een grote hoeveelheid data gaat (kwantitatief), maar ook als het om zeer gevoelige data gaat(kwalitatief). Dit gaat dan bijvoorbeeld om wachtwoorden, financiële of medische informatie.

Heeft u te maken met een ernstig datalek dan dient u hier binnen 72 uur melding van te maken.

4. Stappenplan

Zorg voor een update datalek-protocol met weergave van de namen van de juiste aanspreekpersonen.
Zorg dat het protocol bekent is bij al het personeel.

1. Indien er sprake is van vermoeden van een datalek (gerelateerd aan persoonsgegevens) wordt direct na het vooraf afgesproken protocol gehandeld.
2. Informeer direct de Datalek-verantwoordelijke.
3. De Datalek-verantwoordelijke bekijkt of er sprake is van een datalek in de zin van de wet.
4. Als er sprake is van een datalek wordt het Dagelijks Bestuur/Directie hiervan onverwijld op de hoogte gebracht.
5. De Datalek-verantwoordelijke is verantwoordelijk voor het doen van de kennisgeving aan de Autoriteit Persoonsgegevens en aan de betrokkene(n). Indien nodig, worden deze kennisgevingen zonder vertraging gedaan.
6. Het Dagelijks Bestuur/Directie maakt de afweging inzake de publicitaire gevolgen van een datalek. Bij mogelijke publicitaire gevolgen wordt de Communicatie verantwoordelijke ingeschakeld. Bij mogelijke gevolgen voor bepaalde Klanten wordt de Klanten verantwoordelijke ingeschakeld.
7. In overleg met het Dagelijks Bestuur/Directie neemt de Datalek-verantwoordelijke, binnen 24 uur na ontdekking van het datalek, de

benodigde maatregelen op ICT gebied, ter voorkoming van verdere escalatie.

8. In overleg met het Dagelijks Bestuur/Directie verzorgt Communicatie verantwoordelijk de externe communicatie. Indien nodig verlopen de contacten met de pers via de Dagelijks bestuur/Directie/CEO.
9. In overleg met het Dagelijks Bestuur/Directie informeert de Klanten verantwoordelijke de klanten, die mogelijk gevolgen kunnen ondervinden van het datalek. Indien er daadwerkelijk sprake is van kennisname van persoonsgegevens van debiteuren van opdrachtgevers door derden, dan wordt de klant hiervan uiterlijk binnen 24 uur na de ontdekking van het datalek op de hoogte gesteld.
10. De Datalek-verantwoordelijke draagt zorg voor melding van het datalek in het logboek.

5. Kennisgeving aan de Autoriteit Persoonsgegevens

De wet stelt eisen aan de inhoud van de kennisgeving. De kennisgeving dient onverwijld, zonder vertraging te worden gedaan.
In de kennisgeving dient in ieder geval te worden vermeld:

a) De aard van de inbreuk
b) De instanties waar meer informatie over de inbreuk kan worden verkregen.
c) De aanbevolen maatregelen om de negatieve gevolgen van de inbreuk te beperken.
d) Een beschrijving van de geconstateerde en de vermoedelijke gevolgen van de inbreuk voor de verwerking van persoonsgegevens.
e) De maatregelen die de verantwoordelijke heeft getroffen of voorstelt te treffen om deze gevolgen te verhelpen.

De kennisgeving kan worden gedaan met een formulier dat beschikbaar is op de website van de Autoriteit Persoonsgegevens:
https://datalekken.autoriteitpersoonsgegevens.nl/actionpage

6. Kennisgeving aan betrokkene

In sommige gevallen moet het lek ook gemeld worden aan de personen van wie de gegevens gelekt zijn. Het gaat hierbij om situaties waarbij het lek negatieve gevolgen heeft voor de betrokkenen, zoals reputatieschade, identiteitsfraude of discriminatie.

Indien onderstaande vragen eveneens bevestigend worden beantwoord dan dient ook een kennisgeving aan betrokkene te worden gezonden. De Autoriteit Persoonsgegevens heeft richtlijnen ontwikkeld om vraag 1 beter te kunnen beantwoorden.

1. Zijn ongunstige gevolgen voor de persoonlijke levenssfeer van de betrokkene redelijkerwijs te voorzien?

- Is het aannemelijk dat, wanneer de aanmerkelijke kans op verlies of onrechtmatige verwerking zich verwezenlijkt, daaraan ongunstige gevolgen zijn verbonden voor de persoonlijke levenssfeer van de betrokkene.

2. Zijn de gegevens onbeschermd?
   - Indien de gegevens beschermd zijn door versleuteling of doordat ze ontoegankelijk zijn gemaakt, dan is kennisgeving niet voorgeschreven.

De melding waarborgt een behoorlijke en zorgvuldige informatievoorziening. Rekening houdend met de aard van de inbreuk, de geconstateerde en de feitelijke gevolgen daarvan voor de verwerking van persoonsgegevens, de kring van betrokkenen en de kosten van tenuitvoerlegging.

De kennisgeving dient onverwijld, zonder vertraging te worden gedaan.
In de kennisgeving dient in ieder geval te worden vermeld:

a) De aard van de inbreuk;
b) De instanties waar meer informatie over de inbreuk kan worden verkregen ;
c) De aanbevolen maatregelen om de negatieve gevolgen van de inbreuk te beperken.

Indien wordt geoordeeld dat een kennisgeving aan betrokkenen achterwege kan blijven, kan de Autoriteit Persoonsgegevens alsnog besluiten dat een kennisgeving aan betrokkenen moet worden gedaan.

Afhankelijk van het aantal betrokkenen waaraan de kennisgeving dient te worden gedaan, moet gekozen worden voor het te gebruiken medium.

7. Logboek datalekken

De Datalek verantwoordelijk houdt een overzicht bij van datalekken. Het overzicht bevat in ieder geval feiten en gegevens omtrent de aard van de inbreuk, alsmede de tekst van de kennisgeving aan de betrokkene.