Aandachtspunten bij melding maken datalekken

Checklist | Versie 1.1

De meldplicht datalekken verplicht uw organisatie om melding te doen van het lekken van persoonsgegevens. Datalekken kunnen bijvoorbeeld ontstaan doordat een laptop met belangrijke persoonsgegevens wordt gestolen. Een melding hoeft niet in alle gevallen te worden gemaakt, maar in gevallen waarbij een aanzienlijke kans op ernstige nadelige gevolgen is of deze gevolgen heeft voor de bescherming van persoonsgegevens. De Wet bescherming persoonsgegevens (WBP) geeft in artikel 34a toelichting op de meldplicht datalekken. Het artikel vertelt onder andere welke acties moeten worden ondernomen om datalekken te melden. Raadpleeg de details van de meldingsplicht in deze tool.

Deze tool is geschreven vanuit het oogpunt van de verantwoordelijke bij de verwerking van persoonsgegevens. Deze verantwoordelijke stelt de doelen voor verwerking en bepaalt bijvoorbeeld welke middelen voor verwerking moeten worden gebruikt. Is er sprake van datalekken dan moet de verantwoordelijke een aantal acties ondernemen. Een verantwoordelijke kan overigens een natuurlijke, rechtspersoon of ieder ander zijn. Ook kan hij een bestuursorgaan zijn waarin hij alleen of tezamen met anderen over de verwerking van persoonsgegevens beslist.

Onze experts:
De tools en trajecten worden ontwikkeld en onderhouden door een team van ervaren experts. U vindt een overzicht van alle experts op: rendement.nl/tools/experts.

Deze vaktool is mede mogelijk gemaakt door:
Rendement.nl

Voor meer tools en trajecten ga naar:
http://www.rendement.nl/tools

Aandachtspunten bij melding datalekken

✓	Meldplicht datalekken	Opmerkingen
☐	**Verantwoordelijke licht de Autoriteit Persoonsgegevens in** Als er sprake is van datalekken dat een aanzienlijke kans op ernstige nadelige gevolgen kan voortbrengen, dan wel deze gevolgen heeft voor de bescherming van persoonsgegevens, moet er een melding worden gemaakt. Om te beginnen moet de verantwoordelijke dit melden bij de Autoriteit Persoonsgegevens (het voormalige College Bescherming Persoonsgegevens (CBP). Licht de Autoriteit Persoonsgegevens in over de inbreuk op de beveiliging van de persoonsgegevens die u verwerkt of wilt gaan verwerken.	• Per 1 januari 2016 heeft de Autoriteit Persoonsgegevens een formulier beschikbaar gesteld waarmee meldingen kunnen worden gemaakt.
☐	**Verantwoordelijke licht de betrokkene(n) in** Bij inbreuk op de beveiliging van persoonsgegevens moeten de betrokkenen onverwijld op de hoogte worden gesteld. U heeft deze plicht als de inbreuk op de beveiliging waarschijnlijk ongunstige gevolgen heeft op de persoonlijke levenssfeer.	
☐	**Maak een uitzondering bij de inlichtingen** U kunt in bepaalde geval afzien van inlichtingen aan de betrokkene. Dit mag als de betreffende persoonsgegevens zodanig technisch beschermd zijn dat ze voor iedere onbevoegde onleesbaar, ontoegankelijk of onbegrijpelijk zijn. Een expliciete verplichting voor het melden van een inbreuk op de beveiliging van de gegevens (aan betrokkenen) kan worden opgelegd als de Autoriteit Persoonsgegevens daartoe besluit.	
☐	**Neem de volgende elementen in de kennisgeving op** Een kennisgeving moet een aantal vaste elementen bevatten: • aard van de inbreuk; • instanties waar meer informatie over de inbreuk kan worden opgevraagd; • aanbevolen maatregelen om de negatieve gevolgen van de inbreuk te beperken. De kennisgeving naar de Autoriteit Persoonsgegevens moet ook nog de volgende gegevens bevatten: • een beschrijving van het geconstateerde; • de vermoedelijke gevolgen van de inbreuk voor verwerking van de persoonsgegevens; • de maatregelen die de verantwoordelijke heeft getroffen of voorstelt.	

☐	**Houd bij de kennisgeving aan de betrokkene(n) rekening met een aantal zaken** Kennisgeving aan de betrokkene wordt op zodanige wijze gedaan, dat rekening wordt gehouden met: • de aard van de inbreuk; • de geconstateerde feitelijke gevolgen voor de verwerking van persoonsgegevens; • de kring van betrokkenen; • de kosten van de tenuitvoerlegging. Bovendien moet een behoorlijke en zorgvuldige informatievoorziening gewaarborgd zijn.	
☐	**Houd een administratie van datalekken bij** Op het moment dat de meldplicht datalekken ingaat, is er ook een wettelijke plicht om een administratie bij te houden. In de administratie neemt u alle datalekken op die een aanzienlijke kans op ernstige nadelige gevolgen hebben of die voor de bescherming van persoonsgegevens hadden. Noteer per inbreuk op de veiligheid de feiten en gegevens, de aard van de inbreuk en alle andere gegevens die in de kennisgeving naar de betrokkene(n) zijn opgenomen.	

! **Verhouding verantwoordelijke en betrokken**

De verplichtingen vanuit de WBP zijn gericht op de verantwoordelijke voor de persoonsgegevens. Datalekken bij bewerking van de persoonsgegevens door een bewerker hoeft niet te betekenen dat hij vervolgens aansprakelijk is via de WBP. De verantwoordelijkheden en zorgvuldigheid van de bewerker bij het werken met de persoonsgegevens moet privaatrechtelijk tussen de verantwoordelijke en de bewerker worden geregeld.