DE MELDPLICHT DATALEKKEN EN MEER...

WET BESCHERMING PERSOONSGEGEVENS

Nederland kent de Wet bescherming persoonsgegevens (Wbp) waarin regels zijn vastgelegd voor de verwerking van persoonsgegevens. Zo is in de Wbp geregeld dat persoonsgegevens beveiligd moeten zijn tegen verlies en tegen onrechtmatige verwerking. Sinds 1 januari 2016 is daar een artikel bijgekomen waarin het melden van een datalek is beschreven.

DATALEK?

Een datalek dient onverwijld bij de Autoriteit Persoonsgegevens ("AP", voorheen het College bescherming persoonsgegevens, Cbp) gemeld te worden. Maar wat is nu een datalek?

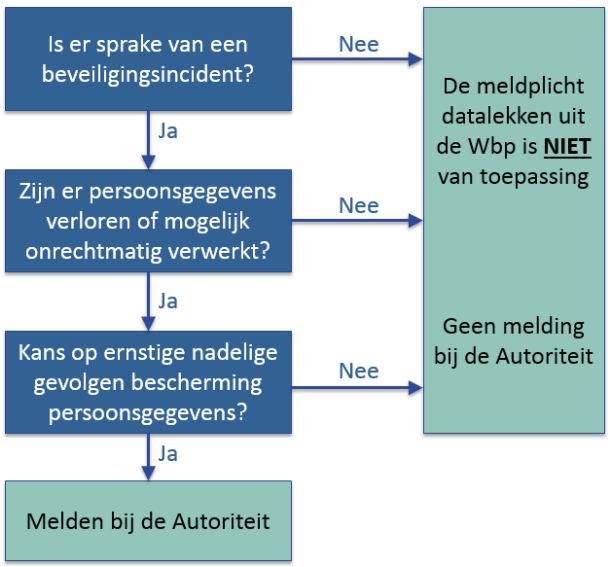
Bij een beveiligingsincident kan er sprake zijn van een datalek of een beveiligingslek. Zijn er persoonsgegevens verloren gegaan of kan onrechtmatige verwerking hiervan niet redelijkerwijs uitgesloten worden, dan is er sprake van een datalek en moet dit binnen 78 uur na de ontdekking van het lek melding gedaan worden bij de Autoriteit Persoonsgegevens. Bij een beveiligingslek hoeft dit niet.

MELDING AAN DE AUTORITEIT

Niet elk datalek hoeft gemeld te worden. Volgens de wet moet een melding gedaan worden als "*het datalek leidt tot een aanzienlijke kans op ernstige nadelige gevolgen voor de bescherming van persoonsgegevens, of als het ernstige nadelige gevolgen heeft voor de bescherming van persoonsgegevens*".

Ook de hoeveelheid en de aard van de persoonsgegevens zijn een factor bij de melding. Bij het lekken van persoonsgegevens van "gevoelige" aard dient er altijd een melding gemaakt te worden. Denk dan aan bijzondere persoonsgegevens zoals godsdienst, levensovertuiging, ras of politieke gezindheid.

Maar ook gegevens over iemands financiële situatie, logingegevens en gegevens die gebruikt kunnen worden voor identiteitsfraude.



DE MELDPLICHT DATALEKKEN

- Voorloper op de Europese privacy verordening;
- Raakt vrijwel iedere organisatie;
- Melden, of niet melden?
- Zorg voor adequate beveiligingsmaatregelen en procedures.

Valid Flight Forum 565, 5657 DR Eindhoven +31 (0)88 - 900 95 00 leon.gubbels@valid.nl www.valid.nl

MELDING AAN DE BETROKKENE

Niet alle meldingen hoeven aan de betrokkene, degene van wie de persoonsgegevens zijn, gemeld te worden. Indien het datalek "*waarschijnlijk ongunstige gevolgen zal hebben voor diens persoonlijke levenssfeer",* dan dient dit ook aan de betrokkene gemeld te worden. Overigens kan de AP dit naar aanleiding van de melding ook van u verlangen.

BOETES

De Autoriteit Persoonsgegevens is per 1 januari 2016 gemachtigd om boetes op te leggen als de beveiliging van persoonsgegevens niet op orde is of als een datalek niet wordt gemeld. Deze boetes kunnen oplopen tot €820.000,-.

De beleidsregels geven echter ook aan dat de AP ook bindende aanwijzingen kunnen opleggen alvorens een boete te geven.

BEWERKER EN VERANTWOORDELIJKE

Degene die de persoonsgegevens verzamelt, vastlegt, bijwerkt of verspreidt is de bewerker. Degene die het doel en de middelen voor verwerking bepaalt, is de verantwoordelijke.

De meldplicht geldt nadrukkelijk voor de verantwoordelijke. Deze draagt de zorgplicht voor de persoonsgegevens, de bescherming daarvan en *ziet ook toe op de bewerker*.

OVEREENKOMST EN BEWIJS

Veel organisaties hebben (een deel van) hun IT uitbesteed. Indien de IT-dienstverlener persoonsgegevens verwerkt, moet er een overeenkomst zijn tussen de verantwoordelijke en de bewerker waarin de bescherming van de persoonsgegevens en ieders verantwoordelijkheden zijn vastgelegd.

Daarnaast moet er bewijs worden vastgelegd. Bij de melding dient onder

andere aan te worden gegeven om welke persoonsgegevens het gaat en de aard van de inbreuk. Deze informatie is nodig om te bepalen of er sprake is van een datalek en om een goede risico-inschatting te maken. Deze informatie zit mogelijk in log-bestanden van verschillende systemen zoals de firewall, de file- en de mail server.

SIEM-systemen die al deze informatie verzamelen en presenteren bieden een goede uitkomst. Andere technische middelen, zoals encryptie van data en Intrusion Prevention Systemen helpen uw organisatie om de data en persoonsgegevens te beschermen.

EN NU?

De impact die deze meldplicht met zich mee brengt is dus niet gering. Maar hoe weet je nou of de getroffen maatregelen voldoende de lading dekken?

Het begint bij een inventarisatie van de huidige omgeving. Denk hierbij aan: waar wordt gebruik gemaakt van persoonsgegevens? Wat is het huidige beschermingsniveau? Zijn er procedures en bewerkersovereenkomsten aanwezig?

Valid werkt samen met een externe specialist in privacywetgeving om een

"IK VRAAG ME AF OF WE HET OP ORDE HEBBEN…"

onafhankelijke Privacy Impact Assessment (PIA) uit te voeren.

Op basis van deze inventarisatie volgt een advies met aanbevelingen en de te volgen stappen, waarin we ook de security architectuur en de technische mogelijkheden mee nemen. Met als resultaat dat de kans op een datalek wordt geminimaliseerd. Mocht het zo ver komen, dan wordt de schade bij een datalek zoveel mogelijk beperkt.

Stap 1 – onafhankelijke PIA;
Stap 2 – technische analyse;
Stap 3 – rapportage met aanbevelingen.

MEER WETEN?

Valid helpt graag. Meer weten over de mogelijkheden? Neem contact op met Leon Gubbels, Security Consultant.

Leon Gubbels (CISSP, CEH, ACE)
+31 (0)88 – 900 9500
Leon.Gubbels@valid.nl