AUTORITEIT PERSOONSGEGEVENS

Het wetsvoorstel Meldplicht datalekken en uitbreiding bestuurlijke boetebevoegdheid Cbp is aangenomen en per 1 januari 2016 in werking getreden. Daarmee is de Wet bescherming persoonsgegevens (Wbp) enkele nieuwe en aangepaste wetsartikelen rijker, die gevolgen hebben voor iedere organisatie die persoonsgegevens verwerkt.

De Autoriteit Persoonsgegevens (voorheen College Bescherming Persoonsgegevens, CBP) heeft haar rol opgepakt, een meldloket geopend en beleid uitgewerkt over de vraag of en wanneer een melding van een datalek noodzakelijk is.

MELDLOKET

Bedrijven, overheden en andere organisaties voor wie de meldplicht datalekken geldt (de 'verantwoordelijke(n)' volgens de Wbp) kunnen terecht bij het meldloket op de site van de Autoriteit Persoonsgegevens, www.autoriteitpersoonsgegevens.nl. Ze moeten zelf een beredeneerde afweging maken of een concreet datalek van persoonsgegevens dat hen ter kennis komt onder het bereik van de wettelijke meldplicht valt. De melding kan niet afgedaan worden met een eenvoudige melding naar een info@emailaccount.nl Er moet een fors vragenformulier ingevuld worden zodra de knop 'Nieuwe melding' wordt aangeklikt. Wel heeft de Autoriteit Persoonsgegevens richtsnoeren uitgewerkt die als hulpmiddel kunnen dienen bij het maken van de afweging of er melding gedaan moet worden van een datalek. Deze zijn te vinden op de site bij het meldloket. De richtsnoeren hebben nog een voorlopig karakter en worden in 2017 definitief vastgesteld.

MELDING AAN BETROKKENEN

Het melden van het datalek aan de betrokkene is verplicht wanneer het gaat om persoonsgegevens. Dat is elk gegeven betreffende een geïdentificeerde of identificeerbare persoon (artikel 1, sub a, Wbp). Een persoon is identificeerbaar indien zijn identiteit redelijkerwijs, zonder onevenredige inspanning, vastgesteld kan worden. Er kan een onderscheid worden gemaakt in *direct* en *indirect* identificerende gegevens. Direct identificerende gegevens zijn gegevens die betrekking hebben op een persoon wiens identiteit zonder veel omwegen eenduidig is vast te stellen, zoals een naam, eventueel in combinatie met het adres en de geboortedatum. Van indirect identificerende gegevens is sprake wanneer gegevens via nadere stappen in verband zijn te brengen met een bepaalde persoon. Een gegeven is geen persoonsgegevens, wanneer doeltreffende technische en organisatorische maatregelen zijn getroffen, waardoor een daadwerkelijke identificatie van individuele natuurlijke personen redelijkerwijs wordt uitgesloten. Dat is van belang omdat in dat geval volgens artikel 34a lid 6 Wbp de melding aan de betrokkene(n) zelf wiens gegevens het betreft, achterwege kan blijven.

ARTIKEL 34A LID 6 WBP

Het tweede lid (over de melding aan betrokkenen, red.) is niet van toepassing indien de verantwoordelijke passende technische beschermingsmaatregelen heeft genomen waardoor de persoonsgegevens die het betreft onbegrijpelijk of ontoegankelijk zijn voor eenieder die geen recht heeft op kennisname van de gegevens.

Die melding aan betrokkenen is volgens de wet (artikel 34a lid 2 Wbp) in alle andere gevallen onverwijld nodig, kijk maar:

ARTIKEL 34A LID 2 WBP

De verantwoordelijke, bedoeld in het eerste lid, stelt de betrokkene onverwijld in kennis van de inbreuk, bedoeld in het eerste lid, indien de inbreuk waarschijnlijk ongunstige gevolgen zal hebben voor diens persoonlijke levenssfeer.

De richtsnoeren van Autoriteit Persoonsgegevens zijn hulpmiddel bij bepalen of datalek gemeld moet worden

VERSLEUTELING GEGEVENS

Op basis van de letterlijk tekst van artikel 34a lid 6 (zie kader) zou men mogelijk verwachten dat als persoonsgegevens adequaat zijn versleuteld, de melding aan de betrokkene(n) achterwege kan blijven. Dat is echter niet het geval volgens de Autoriteit Persoonsgegevens. In de gepubliceerde beleidsregels van de autoriteit over de meldplicht datalekken is onder meer de volgende tekst terug te vinden met bijbehorend voorbeeld:

'Persoonsgegevens die adequaat zijn versleuteld kunnen bij een datalek nog steeds worden vernietigd, en ook aantasting of onbevoegde wijziging is nog steeds mogelijk (bijvoorbeeld door zogenoemde 'cryptoware', die de reeds versleutelde gegevens nogmaals versleutelt met een sleutel die de verantwoordelijke uitsluitend tegen betaling in zijn bezit kan krijgen).'

Een datalek ,waarbij adequaat versleutelde persoonsgegevens niet alleen zijn blootgesteld aan onbevoegde kennisname, maar ook aan verlies of aan andere vormen van onrechtmatige verwerking, kan ongunstige gevolgen hebben voor de persoonlijke levenssfeer van de betrokkene en moet daarom mogelijk aan hem of haar worden gemeld.

Voorbeeld versleuteling gegevens en toch een meldplicht:
De versleutelde laptop van een financieel adviseur is gestolen uit de kofferbak van zijn auto. Op de laptop staan de financiële dossiers – met daarin onder meer details over hypotheken, salarissen en aanvragen van leningen – van 1.000 betrokkenen.

Door de diefstal zijn deze gegevens blootgesteld aan onbevoegde kennisname. De financieel adviseur komt tot de conclusie dat alle gegevens op de harde schijf adequaat versleuteld zijn, en dat het restrisico acceptabel is. In principe zou hij de melding aan de betrokkene dus achterwege kunnen laten.

KLEURT MELDINGSPLICHT IN

Echter: de financieel adviseur beschikt niet over een back-up (reserve-kopie) van de persoonsgegevens op de harde schijf. Dat betekent dat er in dit geval niet alleen sprake is van blootstelling aan onbevoegde kennisname, maar ook van het verlies van de getroffen persoonsgegevens.

Aangezien de financieel adviseur de gegevens niet meer heeft, zal hij ze opnieuw bij de betrokkenen op moeten vragen. De vertraging die hierdoor ontstaat kan ertoe leiden dat deadlines voor de indiening van documenten of aanvragen niet worden gehaald, wat voor de betrokkenen uiteindelijk kan leiden tot boetes, derving van inkomsten of verwachte winst, beëindiging van koopovereenkomsten of andere ingrijpende gevolgen.

In dit geval ligt het, ondanks de genomen technische beschermingsmaatregelen, voor de hand om het datalek te melden aan de betrokkenen. De melding omvat in ieder geval het verzoek om de gegevens opnieuw aan de financieel adviseur te verstrekken en een uitleg van de potentiële consequenties en negatieve gevolgen van de inbreuk.'

Versleuteling beschermt uitsluitend de persoonsgegevens die daadwerkelijk versleuteld zijn op het moment dat er een inbreuk plaatsvindt. Een datalek waarbij (ook) niet-versleutelde persoonsgegevens zijn gelekt moet daarom toch als datalek worden gemeld.

Melding aan betrokkene niet nodig bij passende technische beschermingsmaatregelen die identificatie redelijkerwijs uitsluiten

EUROPESE VERORDENING

De Europese verordening 611/2013 geeft een nadere invulling aan adequate versleuteling. Volgens deze verordening zijn gegevens als onbegrijpelijk te beschouwen als ze:

- op veilige wijze zijn versleuteld met een standaardalgoritme, de sleutel voor decryptie door geen enkele inbreuk gevaar heeft gelopen en de sleutel voor decryptie zodanig werd gegenereerd dat personen zonder geautoriseerde toegang de sleutel met de beschikbare technologische middelen niet kunnen vinden; of
- als ze zijn vervangen door een met een cryptografisch versleutelde hashfunctie berekende hashwaarde, de sleutel die hiervoor werd gebruikt door geen enkele inbreuk gevaar heeft gelopen en deze voor datahashing gebruikte sleutel zodanig is gegenereerd dat personen zonder geautoriseerde toegang de sleutel niet kunnen vinden met de beschikbare technologische middelen.

Een 'hashfunctie' zou je op zijn Nederlands een 'klutsfunctie' kunnen noemen. In de informatica wordt een hashfunctie gebruikt om unieke versleutelingen te berekenen.

REMOTE WIPING

Het op afstand wissen van gegevens (*remote wiping*) op bijvoorbeeld Ipad of mobieltje wordt in de wetsgeschiedenis ook genoemd als technische beschermingsmaatregel, waarmee persoonsgegevens kunnen worden beschermd tegen onbevoegde kennisname. Door de gegevens te wissen worden deze ontoegankelijk voor onbevoegden: na een uitgevoerde *remote wipe* heeft een kwaadwillende nog wel het apparaat in zijn bezit, maar niet meer de gegevens die erop stonden. Voor een succesvolle *remote wipe* zijn er echter wel drie randvoorwaarden:

- Ten eerste moet de *remote wipe* tijdig in gang wordt gezet, zodat een eventuele kwaadwillende nog geen kans heeft gehad om kennis te nemen van de gegevens.
- Ten tweede moet op dat moment het apparaat waar het om gaat nog intact zijn en werken, zodat het in staat is om de *remote wipe* uit te voeren en de gegevens te wissen.
- Tot slot moet de toepassing die voor het wissen van de gegevens wordt gebruikt correct werken, zodat alle gegevens waar het om gaat daadwerkelijk worden verwijderd en er ook geen sporen achterblijven, waaruit de oorspronkelijke gegevens kunnen worden gereconstrueerd.

Als er gebruikgemaakt wordt van *remote wiping*, dan zal, zo stelt de Autoriteit Persoonsgegevens in haar richtsnoer, op basis van de specifieke omstandigheden van het geval vastgesteld moeten worden of er voldaan is aan de strenge norm uit het zesde lid van artikel 34a Wbp.

Ik neem aan dat de adviseur Schadeverzekeringen zakelijk het met mij eens zal zijn dat de genoemde richtsnoeren en de beleidsnota *Meldplicht Datalekken* interessant leesvoer bieden! ●

P.B. (Berrie) van der Heide RMiA
De auteur is registermakelaar in assurantiën, opleider/auteur en tevens lid van de redactieraad van *de Beursbengel*.