holla
advocaten

De nieuwe meldplicht datalekken, een praktische handleiding

1. Inleiding

1.1 Per 1 januari 2016 is, vooruitlopend op de nog niet ingevoerde Europese Privacyverordening, de Nederlandse Wet Bescherming Persoonsgegevens aangevuld met art. 34a waarin een verplichting is opgenomen voor de overheid en voor het bedrijfsleven om het zogenaamde 'datalekken' te melden aan de Autoriteit Persoonsgegevens en/of aan de betrokkenen. Holla Advocaten gaf 31 maart 2016 een seminar over dit actuele onderwerp, waarvan dit document een korte samenvatting is.

1.2 De meest recente cijfers (van 8 maart jl.) laten zien dat er vanaf 1 januari 700 meldingen bij de Autoriteit zijn binnengekomen, waarvan 450 nader zijn bekeken en 40 in behandeling zijn genomen. De boete voor het ten onrechte niet melden van een datalek kan oplopen tot € 820.000,- (of, bij rechtspersonen waarbij deze boete niet toereikend wordt geacht, 10% van de omzet). Het is dus van belang te weten wanneer, aan wie, door wie en wat er precies gemeld moet worden.

2. Wanneer melden?

2.1 Het woord "datalek" staat niet in de wet; art. 34a Wbp bepaalt dat gemeld moet worden 1) een inbreuk op de beveiliging (datalek), van 2) persoonsgegevens die 3) leidt tot (de kans op) ernstige nadelige gevolgen voor de bescherming van deze persoonsgegevens.

2.2 Ad 1: datalek.
Men spreekt van een datalek als persoonsgegevens ofwel onrechtmatig zijn verwerkt (dat wil zeggen: derden hebben toegang gehad terwijl dat niet mocht) ofwel definitief verloren zijn gegaan. Voorbeelden hiervan zijn een zoekgeraakte USB-stick, een gestolen laptop, een inbraak door een hacker, een malware-besmetting of een brand in een datacentrum. Het moet wel gaan om een daadwerkelijk beveiligings*incident*, het enkele feit dat de toegang tot klantgegevens heeft opengestaan waarmee vervolgens niets is gebeurd, is geen inbreuk op de beveiliging.

2.3 Ad 2: persoonsgegevens.
Een persoonsgegeven is elk gegeven dat een persoon identificeert of identificeerbaar maakt (art. 1 onder a Wbp). Een persoon is identificeerbaar wanneer zijn identiteit redelijkerwijs, zonder onevenredige inspanning, vastgesteld kan worden. Er bestaat een onderscheid tussen direct en indirect identificerende gegevens: direct identificerende gegevens zijn gegevens over een persoon waarmee snel duidelijkheid is over zijn identiteit (bijv. de naam in combinatie met een adres en geboortedatum). Van indirect identificeerbare gegevens is sprake als gegevens door middel van vervolgstappen in verband kunnen worden gebracht met een bepaalde persoon.

2.4 Ad 3: ernstige nadelige gevolgen.
Uitgangspunt is dat het lekken van zogenaamde "gevoelige" persoonsgegevens altijd tot ernstige nadelige gevolgen leidt. Onder gevoelige persoonsgegevens wordt verstaan gegevens over iemands godsdienst/levensovertuiging, ras, politieke gezindheid, gezondheid, seksuele leven, lidmaatschap van een vakvereniging, strafrechtelijke gegevens etc., maar ook gegevens over de financiële of economische situatie (salaris, schulden), gegevens die kunnen leiden tot stigmatisering of uitsluiting (bijv. gokverslaving, prestaties op school/werk, relatieproblemen), gebruikersnamen en wachtwoorden en andere inlog-gegevens en gegevens die vallen onder een beroepsgeheim.

Als er geen sprake is van gevoelige gegevens, moet er toch aan de Autoriteit gemeld worden als "de aard en de omvang van de inbreuk" leidt tot een aanzienlijke kans op ernstige nadelige gevolgen, met andere woorden: als er grote hoeveelheden niet-gevoelige data zijn gelekt heeft dit ook een meldplicht tot gevolg.

3. Aan wie melden?

3.1 Als aan de hiervoor onder 2.2-2.4 besproken voorwaarden is voldaan, dient in elk geval gemeld te worden aan de Autoriteit Persoonsgegevens (voorheen: College Bescherming Persoonsgegevens).

3.2 Moet er ook gemeld worden aan de betrokkene? Dit is slechts dan nodig als het lek waarschijnlijk ongunstige gevolgen heeft voor de persoonlijke levenssfeer van de betrokkene. Hiervan is in elk geval sprake als gevoelige gegevens zijn gelekt die niet zijn versleuteld (encryptie). Het lekken van gevoelige gegevens die door encryptie feitelijk ontoegankelijk zijn geworden voor derden hoeft niet aan betrokkene te worden gemeld (wel aan de Autoriteit).

3.3 Er kunnen zwaarwegende redenen zijn om de lek toch niet aan betrokkene te melden, ondanks dat gevoelige, voor derden toegankelijke gegevens zijn gelekt. Dit doet zich bijvoorbeeld voor in het geval een kind een hulpvraag heeft ingediend zonder medeweten van de ouders; een melding zou de ouders ongewenst op de hoogte brengen.

4. Hoe, wat en waarom melden?

4.1 Aan de Autoriteit moet gemeld worden binnen 72 uur middels een webformulier waarop 28 vragen zijn te vinden. Dit formulier vraagt naar gegevens over de instantie, een samenvatting van het incident, hoeveel persoonsgegevens bij de lek zijn betrokken, om welk type persoonsgegevens het gaat, de aard van de inbreuk, etc. Het primaire doel van het melden is het bewerkstelligen van een zorgvuldige omgang met persoonsgegevens. De Autoriteit kan, bij een vermoeden van onzorgvuldige omgang, een nader onderzoek instellen of aanwijzingen geven als zij vermoedt dat de verantwoordelijke onvoldoende maatregelen heeft genomen om het lek te dichten. Het register van de Autoriteit is niet openbaar.

4.2 Aan de betrokkenen moet "onverwijld" gemeld worden. Zo een melding aan betrokkene zal de aard van de inbreuk in moeten houden, de instantie waar de betrokkene meer informatie over de inbreuk kan krijgen en de aan te bevelen maatregelen om de negatieve gevolgen te beperken.

5. Wie moet melden?

5.1 De wet spreekt van de verantwoordelijke. Dit is de drager van alle rechten en plichten onder de Wbp (zie voor de wettelijke definitie art. 1 onder d Wbp). De verantwoordelijke is een andere partij dan de bewerker (dat degene die ten behoeve van de verantwoordelijke de persoonsgegevens verwerkt zonder aan zijn rechtstreeks gezag te zijn onderworpen, bijvoorbeeld een cloud-leverancier, een hosting-partij of een externe salarisadministratie). In de bewerkersovereenkomst zullen afspraken moeten worden gemaakt over de gang van zaken in geval van een datalek. De verantwoordelijke die moet melden moet natuurlijk wel op de hoogte zijn van een eventueel lek bij de bewerker!

6. Tot slot

Wij kunnen u verschillende tips geven om datalekken te voorkomen. Zo is verouderde, niet-onderhouden software een grote risicofactor en is het van belang medewerkers te informeren over de risico's van een rondslingerende USB stick o.i.d. Ook zullen heldere afspraken over dit onderwerp moeten worden gemaakt met de bewerker. Dit document is slechts een korte samenvatting over het onderwerp; voor meer voorbeelden, informatie of op maat gesneden tips, kunt u ons altijd bereiken via onderstaande contactgegevens.

Holla Advocaten
Kim de Bonth
k.debonth@holla.nl
+31 88 4402347

Den Bosch, 14 april 2016