De beleidsregels bij de meldplicht datalekken: een korte beschouwing

mr.drs. T.J.M. de Weerd en mr. J.M. Brölmann[1]

Met ingang van 1 januari 2016 is de meldplicht datalekken opgenomen in de Wet bescherming persoonsgegevens.[2] De Autoriteit Persoonsgegevens heeft beleidsregels gepubliceerd, welke als hulpmiddel kunnen dienen om te bepalen of er sprake is van een datalek dat gemeld dient te worden aan de Autoriteit Persoonsgegevens en mogelijk ook aan de bij het datalek betrokken personen. In deze bijdrage[3] zullen wij de door de Autoriteit Persoonsgegevens opgestelde beleidsregels nader beschouwen, alsmede enige praktische tips meegeven in verband het melden van een datalek.

1. De Meldplicht Datalekken

Per 1 januari 2016 is de regeling omtrent de meldplicht datalekken opgenomen in art. 34a van de Wet bescherming persoonsgegevens (hierna: Wbp). Deze meldplicht houdt in dat verantwoordelijken ernstige datalekken waarbij persoonsgegevens betrokken zijn, moeten melden aan de Autoriteit Persoonsgegevens (hierna: AP) en in bepaalde gevallen ook aan de personen wier persoonsgegevens het datalek betreffen.

Een datalek wordt gedefinieerd als een inbreuk op de beveiliging van persoonsgegevens als bedoeld in art. 13 Wbp, welk artikel bepaalt dat persoonsgegevens beveiligd moeten worden tegen verlies of enige vorm van onrechtmatige verwerking. Onder onrechtmatige verwerking wordt onder meer verstaan onbevoegde kennisname, aantasting, wijziging of verstrekking van persoonsgegevens. Voorbeelden van datalekken zijn het verlies van een USB-stick, diefstal van een laptop, een inbraak door een hacker of een malware-besmetting.

De verplichting om een datalek te melden geldt voor degene die verantwoordelijk is voor de verwerking van de persoonsgegevens (de verantwoordelijke in de zin van de Wbp). Een partij die persoonsgegevens ten behoeve van een verantwoordelijke bewerkt (een bewerker in de zin van de Wbp), zoals een hosting provider of SaaS dienstverlener, heeft geen wettelijke verplichting tot het melden van datalekken, al kan dat wel overeengekomen worden met de verantwoordelijke. Van belang is dat de bewerker en de verantwoordelijke duidelijke afspraken maken zodat de verantwoordelijke tijdig aan de meldplicht kan voldoen.

Niet ieder datalek hoeft te worden gemeld. Uit art. 34a lid 1 Wbp volgt dat een datalek enkel dient te worden gemeld bij de AP indien er sprake is van een inbreuk op de beveiliging die:

> *'leidt tot de aanzienlijke kans op ernstige nadelige gevolgen dan wel ernstige nadelige gevolgen heeft voor de bescherming van persoonsgegevens.'.*

Uit deze in de Wbp opgenomen open norm is lastig concreet af te leiden wanneer er in de praktijk sprake is van een meldplichtig datalek dat leidt tot de aanzienlijke kans op ernstige nadelige gevolgen dan wel ernstige nadelige gevolgen heeft voor de bescherming van persoonsgegevens. De AP heeft ter invulling van deze open norm op 9 december 2015 de beleidsregels[4] voor toepassing van art. 34a van de Wbp (hierna: Beleidsregels) gepubliceerd. De Beleidsregels zijn vastgesteld na een consultatie van derde partijen, op basis van op 21 september 2015 gepubliceerde (concept) richtsnoeren[5] (hierna: Richtsnoeren). Hieronder zal waar relevant worden ingegaan op de verschillen tussen de Richtsnoeren

1. Thomas de Weerd en Jan Brölmann zijn beiden advocaat bij Houthoff Buruma te Amsterdam.
2. *Stb.* 2015, 230 en *Stb.* 2015, 281.
3. In deze bijdrage wordt met name ingegaan op de beleidsregels van de Autoriteit Persoonsgegevens. Zie over de verplichting tot het melden van datalekken ook: E. Thole, C. Gräfin zu Solms-Sonnenwalde en C. Moll, 'De algemene meldplicht datalekken en de cyberverzekering', *Tijdschrift Aansprakelijkheids- en Verzekeringsrecht in de praktijk*, november 2015, nr. 2, p. 21 t/m 26 en J.M. van Essen, 'Een nieuwe meldplicht in privacyland', *P&I* 2013, p. 218-227, en de daarin aangehaalde literatuur.
4. Autoriteit Persoonsgegevens, De meldplicht datalekken in de Wet bescherming persoonsgegevens (hierna: Wbp) – beleidsregels voor toepassing van art. 34a van de Wbp d.d. 8 december 2015.
5. College Bescherming Persoonsgegevens, De meldplicht datalekken in de Wet bescherming persoonsgegevens (hierna: Wbp), Consultatieversie d.d. 21 september 2015.

en de uiteindelijk vastgestelde Beleidsregels, zoals de termijn voor melding van een datalek.
De Beleidsregels geven aan de hand van stroomschema's en een aantal praktijkvoorbeelden een nadere invulling van de in de Wbp opgenomen open norm, aan de hand waarvan een verantwoordelijke kan bepalen of een datalek aan de AP en/of aan betrokkenen dient te worden gemeld. In bepaalde gevallen geven de Beleidsregels echter onvoldoende duidelijkheid, danwel kunnen er enige kanttekeningen worden geplaatst bij de inhoud van de Beleidsregels.

1.1. Termijn voor melding: 72 uur

Uit de Wbp volgt dat een datalek '*onverwijld*' dient te worden gemeld aan de AP. De Beleidsregels bepalen dat een datalek binnen 72 uur na ontdekking van het datalek dient te worden gemeld aan de AP, ongeacht of er sprake is van werk-, weekend-, of feestdagen. Deze termijn komt overeen met de meldingstermijn welke is opgenomen in de tekst van de Europese Algemene Verordening Gegevensbescherming (art. 31). Een op vrijdag ontdekt datalek dient dus uiterlijk binnen 72 uur, te weten op de daaropvolgende zondag, te worden gemeld.
Deze termijn van 72 uur is een aanscherping ten opzichte van de Richtsnoeren, welke bepaalden dat een datalek binnen twee (2) werkdagen na ontdekking van het incident zou moeten worden gemeld bij de AP. Volgens de Richtsnoeren zou een op vrijdag ontdekt datalek, uiterlijk de eerst daaropvolgende dinsdag kunnen worden gemeld.

2. Wanneer is sprake van een datalek?

Om vast te stellen of sprake is van een datalek dienen de volgende omstandigheden te worden beoordeeld[6]: (i) is er sprake van een inbreuk op de beveiliging, (ii) zijn bij de inbreuk persoonsgegevens verloren gegaan en (iii) kan redelijkerwijs worden uitgesloten dat er persoonsgegevens onrechtmatig zijn verwerkt.
Er is sprake van een inbreuk op de beveiliging als zich daadwerkelijk een beveiligingsincident heeft voorgedaan. Een dreigend beveiligingsincident wordt niet als inbreuk op de beveiliging aangemerkt.[7] De Beleidsregels benoemen diverse voorbeelden van beveiligingsincidenten: het kwijtraken van een USB-stick, diefstal van een laptop, een inbraak door een hacker, een malware-besmetting en een calamiteit zoals een brand in een datacentrum.
Indien bij de inbreuk persoonsgegevens zijn vernietigd of op een andere manier verloren zijn gegaan dan is er sprake van een datalek. Van verlies van persoonsgegevens is sprake indien de verantwoordelijke niet beschikt over een complete en actuele reservekopie van de gegevens.[8]
Indien redelijkerwijs kan worden uitgesloten dat er persoonsgegevens onrechtmatig zijn verwerkt, dan hoeft het beveiligingsincident niet als datalek te kwalificeren, en kan worden afgezien van melding bij de AP. Volgens de Beleidsregels zouden logbestanden hiervoor als bewijs kunnen dienen: indien op basis van logbestanden redelijkerwijs kan worden uitgesloten dat er toegang is verkregen tot de gelekte persoonsgegevens, dan is er geen sprake van een datalek. De Beleidsregels vermelden als voorbeeld de situatie dat ten onrechte aan een derde verstrekte inlognaam en wachtwoord, waarbij het wachtwoord wordt gewijzigd voordat de derde toegang heeft verkregen tot het account.
Uit de Beleidsregels blijkt niet duidelijk of een verantwoordelijke enkel op basis van de omstandigheid dat gelekte persoonsgegevens middels encryptie zijn beveiligd zou mogen beargumenteren dat redelijkerwijs kan worden uitgesloten dat er persoonsgegevens onrechtmatig zijn verwerkt. Afhankelijk van de wijze van encryptie en de omstandigheden rondom het datalek zou de omstandigheid dat persoonsgegevens middels encryptie zijn beschermd ons inziens mee moeten wegen in deze beoordeling. De Beleidsregels bepalen wel dat indien sprake is van adequate encryptie het op de hoogte brengen van betrokkenen mogelijk achterwege kan worden gelaten.[9]

2.1. Ernstige nadelige gevolgen voor de bescherming van persoonsgegevens

Indien wordt vastgesteld dat sprake is van een datalek, dan dient vervolgens te worden beoordeeld of er sprake is van een (aanzienlijke kans op) ernstige nadelige gevolgen voor de bescherming van persoonsgegevens. In dat verband dienen de volgende omstandigheden te worden beoordeeld[10]: (i) zijn er persoonsgegevens van gevoelige aard gelekt, (ii) leiden de aard en omvang van de inbreuk tot (een aanzienlijke kans op) ernstige nadelige gevolgen.
Volgens de Beleidsregels dienen datalekken waarbij persoonsgegevens van gevoelige aard betrokkenen zijn, doorgaans gemeld dienen te worden aan de AP. Zo is in de Beleidsregels[11] uitdrukkelijk opgenomen:

> *'Als er persoonsgegevens van gevoelige aard zijn gelekt, dan kunt u er in principe van uit gaan dat u het datalek niet alleen moet melden aan de Autoriteit Persoonsgegevens, maar ook aan de betrokkene.'.*

Onder gevoelige gegevens wordt onder meer verstaan (i) bijzondere persoonsgegevens[12], (ii) gege-

6. Zie het stroomschema in par. 3 van de Beleidsregels.
7. Par. 3.1 Beleidsregels.
8. Par. 3.2 Beleidsregels.
9. Par. 7.2 Beleidsregels.
10. Zie het stroomschema in par. 4.2 van de Beleidsregels.
11. Beleidsregels (p. 7).
12. Gegevens over iemands godsdienst, levensovertuiging, ras, politieke gezindheid, gezondheid, seksuele

vens over de financiële of economische situatie, (iii) (andere) gegevens die kunnen leiden tot stigmatisering of uitsluiting van de betrokkene (gegevens over gokverslaving of relatieproblemen), (iv) gebruikersnamen, wachtwoorden en andere inloggegevens, en (v) gegevens die kunnen worden gebruikt voor (identiteits)fraude.[13]

3. Meldplichtige datalekken

De Beleidsregels noemen onder meer de volgende voorbeelden van datalekken die gemeld dienen te worden aan de AP:

a. Een medewerker verliest een laptop met onversleutelde, financiële klantgegevens;
b. Als gevolg van een hack zijn bij een bedrijf klantgegevens en wachtwoorden ontvreemd;
c. Diefstal van vier laptops bij een gezondheidscentrum voor kinderen, die gevoelige gegevens en andere persoonsgegevens bevatten over de gezondheid en het welzijn van tweeduizend kinderen;
d. Een medewerker van een internetprovider heeft zijn wachtwoord/logingegevens aan een derde gegeven die daardoor nagenoeg onbeperkt bij alle klantgegevens (meer dan honderdduizend) kon komen;
e. Diefstal uit de auto van een versleutelde laptop, waarop financiële gegevens van duizend personen stonden. Hoewel het wachtwoord niet gecompromitteerd is, was er geen backup voorhanden.

Het merendeel van de hierboven genoemde voorbeelden gaat uit van een situatie waarbij persoonsgegevens van een groot aantal betrokkenen is gelekt. Het aantal betrokkenen is echter geen maatstaf voor het bepalen of er wel of geen sprake is van een meldplichtig datalek: ook een datalek dat betrekking heeft op een klein aantal betrokken kan meldplichtig zijn.

Hoewel de hierboven genoemde voorbeelden duidelijk aangeven in welke gevallen de AP van mening is dat sprake is van een meldplichtig datalek, dient er ook bij concrete situaties die grote gelijkenis vertonen met deze voorbeelden rekening te worden gehouden met de concrete omstandigheden van het geval.

Zo is denkbaar dat het verstrekken van een login/wachtwoordcombinatie in het onder d. beschreven voorbeeld bewust gebeurt, bijvoorbeeld aan een tijdelijke kracht die toegang tot een systeem nodig heeft. Hoewel hier vanuit beveiligingsoogpunt uiteraard het nodige op af te dingen valt, zou een dergelijke situatie niet direct als datalek hoeven te kwalificeren, zeker indien de tijdelijke kracht aan een geheimhoudingsverplichting is gebonden.

Het in het onder e. beschreven voorbeeld van diefstal van een laptop lijkt vooral als meldplichtig te worden aangemerkt vanwege de omstandigheid dat er geen backup van de gegevens beschikbaar is, en de betreffende gegevens derhalve als verloren moeten worden beschouwd. Het is niet duidelijk in hoeverre de AP van mening is dat ook zou moeten worden gemeld als er wel een backup beschikbaar zou zijn geweest, bijvoorbeeld vanwege de omstandigheid dat de gegevens op de laptop versleuteld zijn, en kennelijk (bijvoorbeeld via logging) kan worden vastgesteld dat het wachtwoord niet gecompromitteerd is.

4. Niet-meldplichtige datalekken

In de Beleidsregels worden eveneens voorbeelden gegeven van datalekken die niet onder de meldplicht vallen, waaronder (maar niet beperkt tot):

a. Het zoekraken of hacken van de ledenadministratie van een sportvereniging;
b. Een brief met daarin persoonsgegevens wordt naar een foutief adres gestuurd, en wordt ongeopend retour gezonden;
c. Een koffer, voorzien van een deugdelijk slot, met daarin persoonsgegevens wordt achtergelaten in de trein en komt via 'gevonden voorwerpen' ongeopend terug bij de rechtmatige eigenaar.

Bij deze voorbeelden kunnen de nodige kanttekeningen worden geplaatst. Zo kan het zoekraken of hacken van de ledenadministratie van een sportvereniging wel degelijk nadelige gevolgen hebben voor zowel de gegevensbescherming, alsmede de privacy van de bij het datalek betrokken persoon. Uit de Beleidsregels blijkt niet duidelijk waarom een dergelijk datalek niet meldplichtig zou zijn, enkel omdat sprake is van de ledenadministratie van een sportvereniging. Ook persoonsgegevens welke zijn opgenomen in een ledenadministratie kunnen gevoelige gegevens bevatten, zoals loginnamen en wachtwoorden bevatten, en de persoonsgegevens zouden in bepaalde gevallen kunnen worden misbruikt voor identiteitsfraude (zie paragraaf 16).

Omtrent het voorbeeld van de achtergelaten koffer, voorzien van een deugdelijk slot, die via 'gevonden voorwerpen' ongeopend terugkomt bij de rechtmatige eigenaar het volgende. Allereerst gaat dit voorbeeld uit van de premisse dat een koffer ongeopend terugkomt bij de rechtmatige eigenaar. Onduidelijk is echter hoe redelijkerwijs kan worden uitgesloten dat de koffer ongeopend geretourneerd is. Een koffer met een cijferslot kan bijvoorbeeld relatief eenvoudig worden geopend en ogenschijnlijk onaangeroerd worden geretourneerd. Alsdan kan het zijn dat de persoonsgegevens door onbevoegden zijn ingezien of anderszins onrechtmatig zijn verwerkt. Uit dit voorbeeld zou (ten onrechte) kunnen worden afgeleid dat een datalek niet gemeld dient te worden als een drager van persoonsgegevens 'ongeopend' lijkt te zijn. Vertaald naar een digitaal datalek zou dan tevens gesteld kunnen worden dat een in de trein achtergelaten laptop, voorzien van

leven, het lidmaatschap van een vakvereniging en strafrechtelijke persoonsgegevens zoals bedoeld in art. 16 Wbp.

13. Par. 4.2.1 Beleidsregels.

een deugdelijke wachtwoord, die terugkomt bij de rechtmatige eigenaar via 'gevonden voorwerpen' niet onder de meldplicht valt als de laptop 'ongeopend' (zonder dat toegang is verkregen tot de laptop) wordt geretourneerd. Dit terwijl een hacker zich wellicht toegang kan verschaffen tot de laptop zonder digitale sporen achter te laten. Redelijkerwijs uitsluiten dat een fysieke of digitale drager van persoonsgegevens 'ongeopend' is gebleven, zal lastig zijn, waardoor beargumenteerd zou kunnen worden dat er in dergelijk geval wel sprake is van een meldplichtig datalek.

5. Handhaving

In de Beleidsregels is de wettelijke bepaling uitgewerkt dat de Autoriteit Persoonsgegevens direct een boete op kan leggen als er sprake is van een overtreding van de meldplicht datalekken die opzettelijk is gepleegd of het gevolg is van ernstig verwijtbare nalatigheid.[14] Onder ernstig verwijtbare nalatigheid wordt blijkens de Beleidsregels verstaan grof, aanzienlijk onzorgvuldig, onachtzaam dan wel onoordeelkundig handelen.[15] Daarbij kan sneller worden aangenomen dat er sprake is van nalatigheid als eenzelfde soort overtreding meerdere malen plaatsvindt binnen een organisatie.
Is er geen sprake van opzet of ernstig verwijtbare nalatigheid, dan gaat een bindende aanwijzing vooraf aan het opleggen van een bestuurlijke boete. De AP kan de overtreder daarbij een termijn stellen waarbinnen de aanwijzing van de AP dient te worden opgevolgd. Indien de overtreder de bindende aanwijzing niet opvolgt, is de AP op grond van haar boetebeleidsregels gerechtigd om een boete op te leggen.[16] Indien de AP overgaat tot het opleggen van een bestuurlijke boete, wordt blijkens de Beleidsregels rekening gehouden met alle omstandigheden van het geval, zoals de omstandigheid dat de gelekte persoonsgegevens al dan niet door derden zijn ingezien.
Het overtreden van de regels betreffende de meldplicht datalekken kan worden bestraft met een maximale boete van EUR 820.000. In de recent gepubliceerde boetebeleidsregels van de AP is bepaald dat de boete voor het niet melden van een datalek in beginsel binnen een boetebandbreedte van EUR 120.000 en EUR 500.000 zal vallen.[17] Indien het wettelijk maximum van EUR 820.000 naar het oordeel van de AP geen passende bestraffing toelaat, kan de AP een hogere boete opleggen tot maximaal 10% van de omzet van de verantwoordelijke.

14. Zie art. 66 lid 4 Wbp.
15. Beleidsregels, p. 7.
16. Boetebeleidsregels Autoriteit Persoonsgegevens 2016, p. 8.
17. Boetebeleidsregels Autoriteit Persoonsgegevens 2016, par. 2.2 jo Bijlage 1.

6. Conclusie

De Beleidsregels bieden op een behoorlijk aantal punten een verduidelijking van de in art. 34a Wbp opgenomen open normen, onder meer door de grote hoeveelheid concrete voorbeelden. Echter, ook indien sprake is van een concrete situatie die grote gelijkenis vertoont met één met deze voorbeelden, zal rekening moeten worden gehouden met de concrete omstandigheden van het geval.

Enkele praktische tips:

De melding van een datalek dient in beginsel te worden verricht via het meldloket datalekken, een op de website van de AP aangeboden webformulier van de AP. Indien geen gebruik kan worden gemaakt van het webformulier kan ook per fax worden gemeld. De AP biedt een telefonische hulplijn voor vragen over het verrichten van een melding.

Een bij de AP verrichte melding kan op een later moment worden aangevuld. Het is derhalve mogelijk om op basis van de op dat moment (beperkt) beschikbare informatie te melden binnen de termijn van 72 uur. Daarna kan de melding worden aangevuld met nadere informatie. Indien na het verrichten van de melding blijkt dat er toch geen sprake is van een meldplichtig datalek, kan de melding worden ingetrokken.

Het meldingsformulier is ingericht op het verrichten van een melding te verrichten namens één verantwoordelijke. Indien sprake is van een datalek waarbij meerdere verantwoordelijken betrokken zijn, dan voorziet het formulier niet in de mogelijkheid om deze meerdere verantwoordelijken te benoemen (zo kan er bijvoorbeeld maar één Kamer van Koophandel nummer worden ingevuld). Het is wel mogelijk om de extra verantwoordelijken te benoemen in de 'vrije' invulvelden in het webformulier.

In de invulruimte in het meldingsformulier kan een beperkte hoeveelheid tekst worden ingevuld. Zo kunnen maximaal 2.500 tekens worden gebruikt bij invulling van het veld *'gegevens over het datalek*'. Indien het passend zou zijn om een uitgebreidere beschrijving van het datalek in de melding op te nemen, dan zal de melding derhalve per fax dienen te worden verricht.

Er dient altijd een minimum en maximum aantal te worden ingevuld bij het veld omtrent de hoeveelheid personen wiens gegevens betrokken zijn bij het datalek. Het is niet mogelijk om 'onbekend' in te vullen.

De ontvangstbevestiging van de ingediende melding verschijnt enkel op de website van de AP. Er wordt geen bevestiging per e-mail, post of anderszins verstuurd. Het verdient derhalve aanbeveling

om de ontvangstbevestiging te printen, in te scannen of anderszins op te slaan om deze te kunnen documenteren.

De Wbp en de Beleidsregels bevatten geen overgangsrecht in verband met de meldplicht datalekken. Uit de wet en de Beleidsregels is niet af te leiden of datalekken, die hun oorsprong kennen vóór 1 januari 2016, onder de meldplicht vallen. De hulplijn van de AP heeft in dit verband te kennen gegeven dat ook datalekken die hun oorsprong kennen vóór 1 januari 2016, maar op of na voormelde datum zijn ontdekt, gemeld dienen te worden.