Datalekken in de financiële sector

prof. mr. J.M.A. Berkvens[*]

1. Inleiding

Met enige regelmaat komen datalekken boven water, incidenten waarbij persoonsgegevens 'op straat komen te liggen'. Recent zijn incidenten bij Cheaptickets en rondom Diginotar. Datalekken variëren van verloren USB-sticks tot gehackte computersystemen. Zowel binnen de overheid als het bedrijfsleven.[1] De Zurich Insurance case leert dat ook binnen de financiële sector grote incidenten mogelijk zijn.[2] De politiek vraagt om een generieke meldplicht voor datalekken. Ook voor de financiële sector. Eurocommissaris Reding maakte daarover op een bijeenkomst van de British Bankers Association het volgende statement: I intend to introduce a mandatory requirement to notify data security breaches – the same as I did for telecoms and internet access when I was Telecoms Commissioner, but this time for all sectors, including banking and financial services.[3] Binnen de financiële sector bestaat echter al een vorm van meldplicht bij datalekken. Hierna wordt nader op de problematiek van de datalekken ingegaan.

2. Telecommunicatie sector

Hoe een wettelijke regeling met betrekking tot datalekken er uit zou kunnen zien valt te lezen in de Telecommunicatiewet. Momenteel behandelt de Eerste Kamer een voorstel tot aanpassing van de Telecommunicatiewet. Het gaat om een wetsvoorstel dat strekt tot implementatie van Richtlijn 2009/136/EG.[4] Een van de onderdelen van de richtlijn betreft een meldplicht voor datalekken in de openbare telecommunicatie-infrastructuur. Datalekken worden als volgt gedefinieerd:[5]

> Inbreuk in verband met persoonsgegevens: een inbreuk op de beveiliging die resulteert in een onbedoelde of onwettige vernietiging, verlies, wijziging, niet geautoriseerde toegang tot persoonsgegevens die zijn verstuurd, opgeslagen of anderszins verwerkt in verband met de levering van een openbare elektronische communicatiedienst in de Europese Unie.

In art. 11 lid 3a wordt vervolgens uitgewerkt wat de verplichtingen zijn die in geval van een datalek gelden voor de aanbieder van een openbare telecommunicatiedienst:[6]

> 1. De aanbieder van een openbare elektronische communicatiedienst stelt het college (JB: lees OPTA) onverwijld in kennis van een inbreuk op de beveiliging, bedoeld in art. 11.3, die nadelige gevolgen heeft voor de bescherming van persoonsgegevens die zijn verwerkt in verband met de levering van een openbare elektronische communicatiedienst in de Europese Unie.
> 2. De aanbieder, bedoeld in het eerste lid, stelt degene wiens persoonsgegevens het betreft onverwijld in kennis van een inbreuk in verband met persoonsgegevens indien de inbreuk waarschijnlijk ongunstige gevolgen zal hebben voor diens persoonlijke levenssfeer.
> 3. De kennisgeving aan het college en de persoon wiens persoonsgegevens het betreft, omvat in ieder geval de aard van de inbreuk in verband met persoonsgegevens, de instanties waar meer informatie over de inbreuk kan worden verkregen en de aanbevolen maatregelen om de negatieve gevolgen van de inbreuk te beperken. De kennisgeving aan het college omvat tevens de gevolgen van de inbreuk op de persoonsgegevens en de maatregelen die de aanbieder voorstelt of heeft getroffen om de inbreuk aan te pakken.
> 4. Indien de aanbieder van een openbare elektronische communicatiedienst geen kennisgeving als bedoeld in het tweede lid doet, kan het college, indien het van oordeel is dat de inbreuk in verband met persoonsgegevens waarschijnlijk ongunstige gevolgen zal hebben voor de persoonlijke levenssfeer van de persoon wiens persoonsgegevens het betreft, van de aanbieder ver-

---

* Prof. mr. J.M.A. Berkvens is hoogleraar en adjunctdirecteur Recht en Informatica aan de Radboud Universiteit Nijmegen.

1. Voor een overzicht zie https://www.bof.nl/?s=datalekken.
2. De Britse Financial Services Authority legde Zurich UK een forse boete op wegens het lekken van gegevens over 46.000 klanten. Bron: FSA bericht FSA/PN/134/2010 van 24 augustus 2010.
3. BBA (British Bankers' Association) Data Protection and Privacy Conference, London, 20 June 2011. Bron: Press Releases Rapid.
4. Richtlijn 2009/136/EG van het Europees Parlement en de Raad van 25 november 2009 tot wijziging van Richtlijn 2002/22/EG inzake de universele dienst en gebruiksrechten met betrekking tot elektronische communicatienetwerken en –diensten, Richtlijn 2002/58/EG betreffende de verwerking van persoonsgegevens en de bescherming van de persoonlijke levenssfeer in de sector elektronische communicatie en verordening (EG) nr. 2006/2004 betreffende samenwerking tussen de nationale instanties die verantwoordelijk zijn voor handhaving van de wetgeving inzake consumentenbescherming, *PbEU* 2009 L 337/11.
5. *Kamerstukken I* 2010/11, 32 549, nr. A. Zie Art. 11 lid 1 sub j.
6. *Kamerstukken I* 2010/11, 32 549, nr. A. Zie Art. 11 lid 3a.

langen dat hij die persoon alsnog in kennis stelt van de inbreuk.
5. De kennisgeving, bedoeld in het tweede lid, is niet vereist indien de aanbieder naar het oordeel van het college gepaste technische beschermingsmaatregelen heeft genomen waardoor de persoonsgegevens die het betreft, versleuteld of anderszins onbegrijpelijk zijn voor een ieder die geen recht heeft op toegang tot die gegevens.
6. De aanbieder van een openbare elektronische communicatiedienst houdt een overzicht bij van alle inbreuken in verband met persoonsgegevens. Dit overzicht bevat in elk geval de feiten en de in het derde lid bedoelde gegevens.
7. Bij of krachtens algemene maatregel van bestuur kunnen nadere regels worden gegeven met betrekking tot de in dit artikel bedoelde eisen met betrekking tot het verstrekken van informatie en de kennisgeving.

Er is dus sprake van een verplichting om serieuze incidenten te melden bij de OPTA en in een aantal gevallen ook de persoon op wie de gegevens betrekking hebben, in te lichten. De laatstgenoemde verplichting vormt een verzwaring van de uit art. 6 en art. 33 Wet bescherming persoonsgegevens (Wbp) afgeleide verplichting om 'betrokkenen' nadere informatie te verstrekken 'voor zover dat gelet op de aard van de gegevens, de omstandigheden waaronder zij worden verkregen of het gebruik dat ervan wordt gemaakt, nodig is om tegenover de betrokkene een behoorlijke en zorgvuldige verwerking te waarborgen'.

3. Uitbreiding meldplicht naar andere sectoren

3.1 Europa

In de inleiding heb ik reeds melding gemaakt van het voornemen van Eurocommissaris Reding om de meldplicht bij datalekken uit te breiden naar andere sectoren dan de telecommunicatiesector.

3.2 Nederland

Ook in Nederland staat de uitbreiding van de meldplicht bij datalekken naar andere sectoren op de agenda.[7] De problemen bij Diginotar brachten het thema datalekken nog eens extra onder de aandacht.[8] De regering is voornemens om in het komend jaar met voorstellen te komen voor een wettelijke regeling van de meldplicht voor datalekken. Mogelijk wordt dan al geanticipeerd op Europese voorstellen ter zake. VNO-NCW /MKB Nederland heeft zich inmiddels ook in de discussie gemengd. VNO-NCW/MKB Nederland dringt er op aan om niet vooruit te lopen op Europese regels.[9] In het verlengde van een motie van kamerlid Hennis Plasschaert[10] wordt ook gedacht aan een melding bij het Nationaal Cyber Security Centrum (NCSC).[11]

3.3 Wie moet melden?

Bij het invoeren van een meldplicht kan in ieder geval nog veel discussie worden verwacht. Een van de nog niet uitgewerkte vraagstukken betreft degene op wie de meldplicht komt te rusten. Datalekken kunnen optreden binnen de IT-organisatie van een verantwoordelijke. Maar vaak worden processen uitbesteed aan een derde (een bewerker). Als het datalek zich voordoet bij een dergelijke bewerker zou ook overwogen kunnen worden de meldplicht daar neer te leggen. Op de achtergrond speelt dat de grenzen tussen verantwoordelijke en bewerker vervagen zodat een duidelijke allocatie van de meldplicht geen overbodige luxe is.[12]

3.4 Huidige situatie binnen de financiële sector

Op dit moment geldt voor de financiële sector evenals voor andere sectoren al de generieke meldplicht van art. 6 Wbp en art. 33 Wbp richting klant bij relevante incidenten. Die meldplicht kan onder omstandigheden met een beroep op art. 43 van de Wbp worden gemitigeerd.[13] De bank zelf bepaalt in eerste aanleg of een incident relevant is en hoe zij met een incident omgaat.
Daarnaast bestaat er een ruim geformuleerde meldplicht bij incidenten richting financiële toezichthouders (AFM of DNB). Daaronder vallen naar mijn mening ook datalekken. Op grond van de Wft (art. 3:17 en 4:15) zijn banken verplicht de bedrijfsvoering zodanig in te richten dat een beheerste en integere bedrijfsvoering is gewaarborgd.[14] Deze verplichting wordt nader uitgewerkt in het Besluit gedragsregels financiële ondernemingen en het Besluit prudentieel toezicht Wft. In dat kader dient de bank ook te beschikken over procedures en maatregelen die strekken tot analyse van de risico's verbonden aan de bedrijfsvoering. Ook dient de bank bij haar advisering rekening te houden met de risico's die klanten lopen. Art. 3:10 Wft formuleert een meldplicht bij bepaalde incidenten. Daaronder vallen ook veiligheidsincidenten. Art. 4:11 Wft bevat een vergelijkbare tekst voor onder meer beleggingsondernemingen en beleggingsinstellingen. Hieronder wordt de kern van art. 3:10 Wft weergegeven.

1. Een clearinginstelling, kredietinstelling of verzekeraar met zetel in Nederland voert een adequaat beleid dat een integere uitoefening van haar onderscheidenlijk zijn bedrijf waarborgt. Hieronder wordt verstaan dat: (…)
c. wordt tegengegaan dat wegens haar cliënten het vertrouwen in de financiële onderneming of in de financiële markten kan worden geschaad; en d. wordt tegengegaan dat andere handelingen door de financiële onderneming of haar werknemers worden verricht die op een dusdanige wijze ingaan tegen hetgeen volgens het ongeschreven recht in het maatschappelijk verkeer betaamt, dat hierdoor het vertrouwen in de financiële onderneming of in de financiële markten ernstig kan worden geschaad.
2. Bij of krachtens algemene maatregel van bestuur kunnen regels worden gesteld met betrekking tot de

7. Zie o.a. *Kamerstukken II* 2010/11, 32 761 nr. 1 p. 1, *Kamerstukken II* 2010/11, 22 112, nr. 1116, p. 4-5.
8. *Kamerstukken II* 2011/12, 26 643, nr. 214.
9. Brief 7 september 2011 en brief 4 oktober 2011. Bron: privacydossier op www.vno-ncw.nl.
10. *Kamerstukken II* 2011/12, 26 643, nr. 202.
11. *Kamerstukken II* 2011/12, 26 643, nr. 214.
12. Over deze discussie zie J.M.A. Berkvens, 'Naar een wereld zonder controllers en processors', *Privacy en Informatie* 2011/5.
13. Geen melding richting klant indien dat noodzakelijk is voor de bescherming van rechten en vrijheden van de betreffende bank.
14. Vergelijk art. 13 Wbp inzake beveiliging.

> minimumvoorwaarden waaraan het beleid, bedoeld in het eerste lid, moet voldoen.
> 3. Een financiële onderneming als bedoeld in het eerste lid verstrekt aan de Nederlandsche Bank bij algemene maatregel van bestuur te bepalen informatie over incidenten die verband houden met de onderwerpen, bedoeld in het eerste lid.

De invoering van een generieke meldplicht voor datalekken cumuleert voor de financiële sector met de bestaande op de Wft gebaseerde meldplicht. Het feit dat mogelijk sprake zal zijn van overlappende toezichtsdomeinen (DNB, AFM, Cbp) kan ook leiden tot onduidelijkheden en mogelijk ook verschillen van inzicht. Nog afgezien van de eerder genoemde rol van het NCSC.[15] Art. 3:10 Wft biedt de mogelijkheid om de meldplicht voor de financiële sector toe te snijden op de specifieke eisen die deze sector stelt. Er is dan ook iets voor te zeggen om te overwegen de meldplicht voor de financiële sector neer te leggen bij de bestaande toezichthouders binnen die sector.

15. Zie par.3.2.