zaak 245340

VERBOND VAN VERZEKERAARS

Nederlandse Vereniging van Banken

0 BD

Ministerie van Veiligheid en Justitie
Directie Wetgeving
t.a.v. de heer
Postbus 20301
2500 EH DEN HAAG

Onze referentie	Uw referentie	Den Haag
2012/br/7866/AZWAR		22 mei 2012

Betreft
Wijzigingsvoorstel Wbp inzake meldplicht datalekken

Geachte heer

Wij sturen u deze brief naar aanleiding van het Wijzigingsvoorstel Wbp inzake meldplicht datalekken. In het wijzigingsvoorstel is een uitzondering van de Wbp-meldplicht opgenomen voor financiële instellingen die verplicht zijn incidenten te melden op grond van de Wft. Doel van de uitzondering is het voorkomen van een dubbele meldplicht op grond van Wbp en Wft. Verbond en NVB hebben in hun reacties op de consultatie aangegeven zeer positief tegenover de voorgestelde uitzondering voor financiële instellingen te staan. Het ministerie van Financiën en toezichthouders AFM/DNB hebben echter hun twijfel geuit over de haalbaarheid van deze uitzondering. Hierbij willen wij het belang van de voorgestelde uitzondering voor banken en verzekeraars nogmaals onder de aandacht brengen en onderstrepen. Wij vragen het ministerie de uitzondering in het definitieve wetsvoorstel te handhaven.

Het ministerie heeft de uitzondering op de Wbp meldplicht voor Wft instellingen opgenomen omdat deze overlapt met de Wft meldplicht. Verbond en NVB onderschrijven dit standpunt. De meldplicht gebaseerd op de Wft betreft incidenten die een ernstig gevaar vormen voor de integere uitoefening van het bedrijf van de desbetreffende financiële onderneming. De toezichthouder waarbij het incident gemeld wordt is gehouden aan de geheimhoudingsplicht op basis van artikel 1:89 Wft. Doel van de geheimhoudingsplicht is meerledig: (1) bevordering van vrije informatieverstrekking door de onder toezicht staande instellingen en derden, (2) bevordering van effectief toezicht en (3) voorkoming van onherstelbare schade van het vertrouwen in financiële markten. Daarbij is een evenwicht nodig tussen de belangen van alle betrokken partijen. Enerzijds de beschikbaarheid van gedetailleerde (en doorgaans vertrouwelijke) informatie voor effectief toezicht op de financiële markt. Anderzijds het belang van de financiële onderneming of andere betrokkenen bij vertrouwelijke behandeling van die gegevens.

Informatie: Verbond van Verzekeraars, mw. N. Lemmen MSc, 070 - 333 86 59, E-mail n.lemmen@verzekeraars.nl
Nederlandse Vereniging van Banken, mw. L. Jongbloed, (0)20 55 02 820 , E-mail jongbloed@nvb.nl

VERBOND VAN VERZEKERAARS

Nederlandse Vereniging van Banken

Meldplicht op grond van de Wbp betreft datalekken die leiden tot een aanmerkelijk risico op verlies of onrechtmatige verwerking waaraan nadelige gevolgen voor de persoonsgegevens en de persoonlijke levenssfeer van de betrokkene zijn verbonden. Bij een dergelijk datalek dient niet alleen de toezichthouder maar ook de betrokkene te worden geïnformeerd. Daardoor houdt de Wbp melding in principe openbaarmaking in. Als gevolg van openbaarmaking kan het vertrouwen in de financiële markten onherstelbaar geschaad worden. Dit is een zwaarwegend risico waar binnen de Wft incidentenmeldplicht expliciet rekening mee wordt gehouden. De Wbp datalekkenmeldplicht daarentegen houdt hier geen rekening mee.

Uit de geclausuleerde omschrijving van de situaties waarin incident en datalekken gemeld moeten worden, volgt dat het om substantiële incidenten en datalekken moet gaan. Daaruit volgt dat wanneer sprake is van een meldingsplichtig datalek er tevens sprake is van een meldingsplichtig incident, waarbij in de opinie van NVB en Verbond melding aan de financiële toezichthouder in de rede ligt. Dit met name gezien de eerdergenoemde vertrouwelijkheid en geheimhoudingsplicht. De kans dat daarmee geringe datalekken buiten beeld verdwijnen is nauwelijks aanwezig. Deze lekken hoeven namelijk ook op grond van de voorgestelde Wbp meldplicht niet gemeld te worden. Daarnaast is het bezwaar dat de betrokkenen niet geïnformeerd zouden worden bij het melden van datalekken aan DNB/AFM, ongegrond. Wanneer er zich datalekken voordoen die nadelig zijn voor betrokkenen worden zij door de financiële ondernemingen geïnformeerd vanuit de bestaande zorgplicht. Eveneens een verplichting neergelegd in de Wft.

Belangrijk is tevens dat de uitzondering als voorzien leidt tot een meldingsplicht bij de financiële toezichthouders, die de financiële markten door en door kennen en daarmee ook een goede inschatting kunnen maken van de gevolgen van een incident voor deze markten. Bovendien beschikken de financieel toezichthouders over de meest efficiënte instrumenten om indien noodzakelijk te interveniëren. Verbond en NVB zijn er dan ook sterke voorstanders van om alle incidenten/datalekken aan de financieel toezichthouder te melden. DNB heeft specifieke kennis van de financiële markt en kent de inrichting van de beveiligingssystemen van financiële instellingen. Om het CBP toch inzicht te verlenen in de situatie van de financiële sector zou DNB het CBP op geaggregeerd niveau kunnen informeren over eventuele incidenten/datalekken. Art. 1:90 Wft voorziet daartoe in een met waarborgen omgeven procedure.

Er is de financiële sector veel aan gelegen de integriteit waaronder een correcte en veilige omgang met persoonsgegevens te waarborgen. Ook zijn het Verbond en NVB van mening dat de klant recht heeft op tijdige en heldere informatie. Hierbij moet wel een zorgvuldige afweging worden gemaakt over de consequenties voor de gehele sector. Het voorstel van het ministerie biedt daarvoor de juiste handvatten. Verbond en NVB pleiten er dan ook voor dat de voorgestelde uitzondering voor financiële instellingen met een Wft incidentenmeldplicht gehandhaafd blijft. Uiteraard zijn wij bereid een nadere toelichting te geven.

Hoogachtend,

mr. H.L. De Boer
directeur Verbond van Verzekeraars

mr. W.A.J. Mijs
directeur Nederlandse Vereniging van Banken

VERBOND VAN VERZEKERAARS

Nederlandse Vereniging van Banken

[1] Afdeling 1.5.1. Geheimhoudingsplicht en uitzonderingen dienaangaande
Artikel 1:89
1. Het is een ieder die uit hoofde van de toepassing van deze wet of van ingevolge deze wet genomen besluiten enige taak vervult of heeft vervuld, verboden van vertrouwelijke gegevens of inlichtingen die ingevolge deze wet dan wel ingevolge afdeling 5.2 van de Algemene wet bestuursrecht zijn verstrekt of verkregen of van een persoon of instantie als bedoeld in artikel 1:90, eerste lid, onderscheidenlijk 1:91, eerste lid, zijn ontvangen, verder of anders gebruik te maken of daaraan verder of anders
bekendheid te geven dan voor de uitvoering van zijn taak of door deze wet wordt geëist.
2. In afwijking van het eerste lid kan de toezichthouder met gebruikmaking van vertrouwelijke gegevens of inlichtingen verkregen bij de uitvoering van zijn taak op grond van deze wet, mededelingen doen, indien deze niet kunnen worden herleid tot afzonderlijke personen.

DW

VERBOND VAN VERZEKERAARS

Postbus 93450 2509 AL DEN HAAG

Bezoek ook
onze website:

www.verzekeraars.nl

's-Gravenhage post
Port Betaald
Port Payé
Pays-Bas
22.05.12

Postbus 93450
2509 AL

FR 15978
Nederland

05/22/2012 10:32

GOBPP 2500EH301

Kopie

06/06/2013

VERBOND VAN VERZEKERAARS

> Sector Algemene Beleidszaken

Ministerie van Veiligheid en Justitie
Directie Wetgeving
Postbus 20301
2500 EH 'S-GRAVENHAGE

Onze referentie
2012/br/7781/AZWAR

Den Haag
29 februari 2012

Betreft
consultatie Wijziging Wet bescherming persoonsgegevens

Geachte heer, mevrouw,

In reactie op de internetconsultatie voor de wijziging van de Wet bescherming persoonsgegevens sturen wij u deze brief. De sector en Verbond waarderen de consultatie en grijpen deze gelegenheid aan om een bijdrage te leveren.

Aanleiding voor de invoering van de meldplicht zijn een aantal incidenten waarbij door een inbreuk op de beveiliging persoonsgegevens in het publieke domein terecht zijn gekomen. Dit met als doel het vertrouwen te bevestigen of herstellen dat door de markt, publiek, overheid en/of toezichthouder in de desbetreffende instelling wordt gesteld aldus beschreven in de toelichting. Met deze brief reageert het Verbond specifiek op de voorgestelde meldplicht datalekken en doelstelling.

Er is de financiële sector veel aan gelegen de integriteit waaronder een correcte en veilige omgang met persoonsgegevens te waarborgen. Daartoe volgen verzekeraars de voorschriften in de Wet op het financieel toezicht en zelfregulering opgesteld door het Verbond waaronder de Gedragscode Verwerking Persoonsgegevens Financiële Instellingen.

In artikel 34 van het wijzigingsvoorstel wordt de meldplicht beschreven. Onder lid 10 van artikel 34 is bepaald dat verantwoordelijken van financiële instellingen die al een meldplicht hebben op grond van de Wet op financieel toezicht (Wft) uitgezonderd zijn. Het Verbond is zeer positief over het feit dat het Ministerie deze uitzondering heeft opgenomen om zo een dubbele meldplicht voor de financiële instellingen, waaronder verzekeraars, te voorkomen. Op grond van artikel 3:10 derde lid van de Wft zijn verzekeraars verplicht informatie over incidenten inzake integere bedrijfsuitoefening te melden bij de toezichthouder van de financiële sector: De Nederlandsche Bank (DNB). Wij onderschrijven de redeneringen van het Ministerie van harte zoals helder uiteengezet in de toelichting van het wijzigingsvoorstel onder 4.1.9.

Informatie: mw. N. Lemmen MSc.
Doorkiesnummer 070 - 333 86 59 Fax rechtstreeks 070 - 333 86 70 E-mail n.lemmen@verzekeraars.nl
Bordewijklaan 2, 2591 XR Den Haag, Postbus 93450, 2509 AL Den Haag, Internet www.verzekeraars.nl

Op 25 januari heeft de Europese Commissie een voorstel voor een verordening gepubliceerd inzake de bescherming van individuen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens (com (2012)11 final). In de verordening is eveneens een meldplicht datalekken opgenomen in artikel 31. Het huidige commissie voorstel voorziet echter niet in een uitzondering van de meldplicht voor financiële instellingen zoals verzekeraars. Wij dringen er bij het Ministerie op aan dit mee te nemen bij de standpunt bepaling inzake de verordening. Indien er geen uitzondering wordt gemaakt voor de financiële sector zal er in de toekomst alsnog sprake zijn van een dubbele meldplicht. Hetgeen het Ministerie door middel van dit wetsvoorstel juist beoogt te voorkomen. Het Verbond pleit er dan ook voor de opname van een dergelijke uitzondering onder artikel 31 in de verordening.

Uiteraard is het Verbond bereid in een gesprek een nadere toelichting op de reactie te geven.

Met vriendelijke groet,

ir. H.F. Treur
secretaris Algemene Beleidszaken

De Nederlandsche Bank
Eurosysteem

AFM
Autoriteit Financiële Markten

De Staatssecretaris van Veiligheid en Justitie
Mr. F. Teeven
Postbus 20301
2500 EH DEN HAAG

Datum
12 maart 2012

Betreft
Consultatie wetsvoorstel Wet bescherming persoonsgegevens (Wbp)

Geachte heer Teeven,

Bij brief van 19 december 2011 heeft u De Nederlandsche Bank (DNB) en de Autoriteit Financiële markten (AFM) gevraagd om te reageren op de consultatie van het wetsvoorstel tot wijziging van de Wet bescherming persoonsgegevens (Wbp), met het oog op het gebruik van camerabeelden en de meldplicht datalekken. DNB en AFM danken u voor deze mogelijkheid en willen gezamenlijk graag het volgende onder uw aandacht brengen.

Het wetsvoorstel voorziet in onder meer een regeling voor een meldplicht voor datalekken. Deze beoogt te bereiken dat bedrijven en overheid aan het College bescherming persoonsgegevens (Cbp) melden dat zij zijn geconfronteerd met een lek in de beveiliging van hun geautomatiseerde verwerking van persoonsgegevens (een datalek). Voor ondernemingen in de financiële sector wordt een uitzondering op de meldplicht gemaakt. Blijkens het wetsvoorstel is de reden hiervoor het feit dat voor die financiële ondernemingen al een meldplicht op grond van de Wet op het financieel toezicht (Wft) zou bestaan. Het wetsvoorstel bepaalt dat van de meldplicht wordt uitgezonderd 'de verantwoordelijke op wie een verplichting rust tot het verstrekken van informatie op grond van de artikelen 3:10, derde lid, of 4:11, vierde lid, van de Wet op het financieel toezicht.'

In uw brief heeft u gevraagd om een reactie op uw voorstel dat DNB en AFM een convenant sluiten met het College bescherming persoonsgegevens (Cbp) zodat het Cbp op een geaggregeerd niveau op de hoogte kan worden gehouden van het aantal en de aard van de datalekken waarvan

De Nederlandsche Bank
Westeinde 1
Postbus 98
1000 AB Amsterdam

Autoriteit Financiële Markten
Vijzelgracht 50
Postbus 11723
1001 GS Amsterdam

De Nederlandsche Bank
Eurosysteem

AFM
Autoriteit Financiële Markten

De Staatssecretaris van Veiligheid en Justitie
Mr. F. Teeven
Postbus 20301
2500 EH DEN HAAG

Datum
12 maart 2012

DNB en AFM kennis krijgen en de gevolgen die aan die lekken door DNB en AFM worden verbonden.

DNB en AFM stellen voor om het wetsvoorstel in zoverre te wijzigen dat voor de financiële sector geen uitzondering wordt gemaakt op de meldplicht inzake datalekken aan het Cbp die met het wetsvoorstel wordt geïntroduceerd. Dit betekent concreet dat in het voorgestelde artikel 34a van de Wbp het tiende lid wordt geschrapt.

Uiteraard zijn DNB en AFM voorstander om de administratieve lasten daar waar mogelijk voor de financiële sector te beperken en geen dubbele meldplichten te creëren indien dat niet noodzakelijk is. Echter, in dit geval zijn er redenen aanwezig om de voorgestelde uitzondering te schrappen. Voor de goede orde wordt hierbij vermeld dat DNB en AFM geen verandering van de Wft voor ogen staat.

Ter onderbouwing van dit voorstel wijzen DNB en AFM op het volgende. Het met de wijziging van de Wbp beoogde effect is dat de meldplicht aan het Cbp bijdraagt aan een grotere transparantie bij de verwerking van persoonsgegevens, ruimere aandacht voor de noodzaak goed te investeren in beveiligingsmaatregelen, en op den duur toename van het vertrouwen van de samenleving in de geautomatiseerde verwerking van persoonsgegevens. De meldplicht op grond van de Wft dient een ander doel. Dit blijkt uit de definitie van het begrip 'incident' in artikel 1 van het Besluit prudentiële regels Wft respectievelijk het Besluit gedragstoezicht financiële ondernemingen. De meldplicht voor financiële ondernemingen aan DNB en AFM ziet op de verplichting om een incident – zijnde 'een gedraging of gebeurtenis die een ernstig gevaar vormt voor de integere uitoefening van het bedrijf van een financiële onderneming' - te melden aan de toezichthouder. Zulke incidenten kunnen bestaan uit velerlei soorten gebeurtenissen, waartoe in beginsel datalekken, zoals lekken van persoonsgegevens, kunnen worden gerekend. Echter, cruciaal element van de meldplicht aan de toezichthouders DNB en AFM is wel dat slechts die incidenten dienen te worden gemeld die een ernstig gevaar vormen voor de integere bedrijfsuitoefening. Dit leidt er in de praktijk toe dat datalekken van persoonsgegevens als bedoeld in het wetsvoorstel in de regel niet worden gemeld aan DNB en AFM. Immers, niet alle datalekken vormen tevens een ernstig gevaar voor de integere bedrijfsuitoefening. Het is naar het oordeel van DNB en AFM niet zinvol om financiële ondernemingen van de te introduceren meldplicht aan het Cbp uit te zonderen omwille van de *veronderstelling* dat datalekken reeds aan de toezichthouders DNB en AFM moeten worden gemeld. Uit het vorenstaande volgt dat in veel gevallen geen sprake is van een dubbele meldplicht voor financiële ondernemingen (indien die ondernemingen niet zouden worden uitgezonderd van de meldplicht aan het Cbp). Immers, in de regel worden datalekken niet aan de toezichthouders gemeld.

Bij het vorenstaande is nog van belang dat in de memorie van toelichting bij het wetsvoorstel is vermeld dat financiële ondernemingen hun cliënten zo spoedig mogelijk informeren over het

De Nederlandsche Bank
Westeinde 1
Postbus 98
1000 AB Amsterdam

Autoriteit Financiële Markten
Vijzelgracht 50
Postbus 11723
1001 GS Amsterdam

87

De Staatssecretaris van Veiligheid en Justitie
Mr. F. Teeven
Postbus 20301
2500 EH DEN HAAG

Datum
12 maart 2012

incident, wanneer dat gevolgen heeft gehad voor de desbetreffende cliënt. Echter, dit volgt niet uit het Besluit prudentiële regels Wft en het Besluit gedragstoezicht financiële ondernemingen. Daarin is niet bepaald dat financiële ondernemingen hun cliënten moeten informeren over incidenten als hiervoor omschreven. Het wetsvoorstel inzake de Wbp voorziet daarentegen wel in de verplichting de betrokkene van het datalek onverwijld in kennis te stellen. Anders dan in de toelichting van het wetsvoorstel datalekken wordt verondersteld, is er dan ook geen sprake van een tegenhanger van de meldplicht aan betrokkenen als bedoeld in de Wbp in de financiële toezichtswetgeving.

DNB en AFM vragen zich ook af hoe het onderhavige wetsvoorstel zich verhoudt tot het voorstel voor een Verordening betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens (algemene verordening gegevensbescherming) dat recent werd gepubliceerd door de Europese Commissie. In dat voorstel worden financiële ondernemingen niet uitgezonderd van de meldplicht.

In de memorie van toelichting bij het wetsvoorstel wordt vermeld dat openbare kennisgevingen van datalekken in de financiële sector - mede tegen de achtergrond van de financiële crisis - te risicovol zijn om dwingend te worden voorgeschreven. Dit wordt in de memorie van toelichting onderbouwd met het argument dat onvoorspelbaar is of een openbare kennisgeving kan leiden tot het ontstaan van geruchten die niet meer op zakelijke wijze ontzenuwd kunnen worden en die daardoor nodeloos aanleiding kunnen geven tot vermindering van vertrouwen van het publiek of de relevante markt.
Gelet op dit mogelijke gevaar van openbare kennisgevingen wordt voorgesteld dat in het wetsvoorstel er in wordt voorzien dat financiële instellingen kunnen worden vrijgesteld van de verplichting een openbare kennisgeving te doen indien die openbare kennisgeving te risicovol wordt geacht. De verantwoordelijkheid om zich te beroepen op de uitzondering van de verplichting om een openbare kennisgeving te doen kan bij de financiële instellingen worden neergelegd en kan afhankelijk worden gemaakt van de toestemming van de toezichthouder dat inderdaad sprake is van een uitzonderlijke situatie op grond waarvan de openbare kennisgeving achterwege kan worden gelaten.

Ten aanzien van de 'meldplicht' aan de betrokkene stelt de memorie van toelichting bij het wetsvoorstel verder dat de geheimhoudingsplichten van de artikelen 1:89 en 1:90 Wft geen ruimte laten om meldingen van datalekken door de verantwoordelijke aan de betrokkene op dezelfde wijze te doen als in artikel 34a van de Wbp is voorgeschreven. Deze verwijzing naar de geheimhoudingsplicht is in deze context onjuist, aangezien deze artikelen enkel zien op de geheimhoudingsplicht en de uitzonderingen daarop voor DNB en AFM, en die artikelen niet relevant zijn voor de vraag of financiële ondernemingen al dan niet aan het Cbp en/of betrokkene informatie zouden kunnen verstrekken inzake datalekken.

De Nederlandsche Bank
Westeinde 1
Postbus 98
1000 AB Amsterdam

Autoriteit Financiële Markten
Vijzelgracht 50
Postbus 11723
1001 GS Amsterdam

De Nederlandsche Bank
Eurosysteem

AFM
Autoriteit Financiële Markten

De Staatssecretaris van Veiligheid en Justitie
Mr. F. Teeven
Postbus 20301
2500 EH DEN HAAG

Datum
12 maart 2012

Op grond van artikel 1:89, tweede lid, Wft kunnen DNB en AFM aan het Cbp met gebruikmaking van vertrouwelijke gegevens of inlichtingen verkregen bij de uitoefening van zijn taak op grond van de Wft slechts mededelingen doen indien deze niet herleidbaar zijn tot natuurlijke personen. Voor het overige kunnen de toezichthouders geen vertrouwelijke gegevens of inlichtingen aan het Cbp verstrekken.

DNB en AFM stellen naar aanleiding van het voorgaande voor om het wetsvoorstel in die zin te wijzigen dat financiële ondernemingen niet worden uitgezonderd van de meldplicht op grond van de Wbp, en dat financiële ondernemingen in uitzonderlijke omstandigheden kunnen worden uitgezonderd van de meldplicht aan betrokkene. Daarmee is het sluiten van een convenant tussen de toezichthouders en het Cbp niet meer aan de orde. Met de door ons voorgestelde aanpassing van het wetsvoorstel wordt ten slotte bereikt dat datalekken van persoonsgegevens altijd moeten worden gemeld aan het College bescherming persoonsgegevens dat primair voor het toezicht op de Wbp is bestemd.

Wij hopen u hiermee voldoende te hebben geïnformeerd en zijn graag bereid tot het geven van een nadere toelichting.

Hoogachtend,

De Nederlandsche Bank
Dr. J. Sijbrand, Directeur

Autoriteit Financiële Markten
Drs. H.W.O.L.M. Korte, Directeur

2012/150092

De Nederlandsche Bank
Westeinde 1
Postbus 98
1000 AB Amsterdam

Autoriteit Financiële Markten
Vijzelgracht 50
Postbus 11723
1001 GS Amsterdam

Nederlandse
Vereniging van Banken

Ministerie van Veiligheid en Justitie
Postbus 20301
2500 EH 'S-GRAVENHAGE

Datum 29 februari 2012
Referentie BR1587

Betreft: Consultatie wetsvoorstel Wbp (camerabeelden en datalekken)

Geachte heer De Jong,

Hartelijk dank voor het toezenden van bovenstaande consultatie.

Wij zijn verheugd dat banken worden uitgezonderd van de meldplicht datalekken door in artikel 34a lid 10 Wbp een voorziening op te nemen die inhoudt dat de meldplicht niet van toepassing is op ondernemingen voor wie reeds een meldplicht geldt uit hoofde van de Wft.

Voor het overige sluiten wij ons aan bij de opmerkingen van VNO-NCW.

Daarnaast wijzen wij u op bijgevoegde brief van 13 februari 2012 aan het Ministerie van Financiën met betrekking tot overlap toezichtregelgeving in relatie tot het voorstel van de Europese Commissie voor een gegevensbeschermingsverordening.

Met vriendelijke groet,

Mr. E.V. Jongbloed
Adviseur Juridische Zaken

Bijlage
Brief NVB van 13 februari 2012, BR1566

Nederlandse
Vereniging van Banken

Mr. W.A.J. Mijs
Directeur
t + 31 20 55 02 847

Ministerie van Financiën
Directeur Financiële Markten
Mevrouw Drs. G.J. Salden
Postbus 20201
2500 EE DEN HAAG

Datum 13 februari 2012
Referentie BR1566

Betreft Overlap toezichtregelgeving/voorstel voor een gegevensbeschermingsverordening (COM(2012)11 final)

Geachte mevrouw Salden,

Op 25 januari jl. heeft de Europese Commissie een voorstel voor een verordening gepubliceerd betreffende de bescherming van individuen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens (COM(2012)11 final).

De dataprotectieregels uit dit voorstel roepen voor financiële instellingen verplichtingen in het leven die overlappen met reeds bestaande Europese regels en mede daarop gebaseerde regels bij of krachtens de Wet op het financieel toezicht (Wft).
Daarbij lijkt het CBP (College Bescherming Persoonsgegevens) de rol te krijgen van een tweede prudentieel toezichthouder voor de bancaire sector. De overlap kan leiden tot dubbele administratieve lasten, handhavingsconflicten, conflicten tussen privacytoezicht en financieel toezicht en tot afbakeningsproblemen.

Dit probleem is eerder gesignaleerd door het Ministerie van Veiligheid en Justitie, dat op 20 december 2011 een consultatiedocument publiceerde inzake aanpassing van de Wet bescherming persoonsgegevens (Wbp) in verband met een wettelijke meldplicht bij datalekken. Omdat er sprake is van een duidelijke overlap met de reeds bestaande voorschriften in de Wft en met de regeling van toezicht/handhaving ten aanzien van datalekken, wordt de financiële sector in het consultatiedocument expliciet uitgezonderd van het Wbp-regime voor datalekken.

De Nederlandse Vereniging van Banken (NVB) is ter voorkoming van dubbele regelgeving en van dubbel toezicht/handhaving voorstander van het handhaven van de bestaande op de Wft gebaseerde voorschriften en het bestaande prudentieel toezicht.

Naar de mening van de NVB is het gewenst dat de thans in het consultatiedocument voorziene aanpak voor datalekken binnen de financiële wereld onder de verordening wordt gehandhaafd. Ook verdient het de voorkeur dat andere regels bij of krachtens de Wft gesteld betreffende AOIC (Administratie Organisatie Interne Controle) en prudentieel toezicht belegd blijven bij de financiële autoriteiten met uitsluiting van toepasselijkheid van de overlappende bepalingen in de verordening.

Wij willen er daarom bij u op aandringen dat in het kabinetsstandpunt over de ontwerpverordening nog nader in te vullen ruimte wordt gecreëerd voor reeds intensief gereguleerde sectoren zoals de bancaire sector om te voorzien in de mogelijkheid om AOIC en prudentieel toezicht/handhaving exclusief neer te leggen in financieel toezichtsrecht en bij financieel toezichthouders.

Voor een uitgebreide toelichting verwijzen wij u naar de bijlage.

Hoogachtend,

Mr. W.A.J. Mijs
Directeur

Bijlage
Achtergrond bij brief BR1566

Kopie aan
- Ministerie van Financiën: Mw. Mr. H.C.T.M. Borburgh
- Ministerie van Justitie: Mr. Dr. J.P. de Jong
- DNB: Mr. R.F. Luberti

Bijlage behorende bij BR 1566

Achtergrond

Europese regels verplichten financiële instellingen om robuuste AOIC systemen te onderhouden[1]. Deze verplichtingen bestaan al geruime tijd en een recente juridische basis is onder meer te vinden in art. 22 van Richtlijn 2006/48/EG[2] en in de Guidelines van de European Banking Authority[3]. De guidelines zijn voor wat betreft Nederland overgenomen door DNB[4]. Daarnaast is er een veelheid van AOIC-bepalingen in diverse EU deelgebied-richtlijnen en in voorschriften van Europese en nationale bankautoriteiten en standaarden-organisaties.

Bij of krachtens de Wet op het financieel toezicht (Wft) worden op het gebied van AOIC eisen gesteld aan financiële instellingen[5]. Deze eisen hebben betrekking ondermeer op de inrichting van toezicht op naleving van wettelijke regels, het inrichten van administratieve processen, het maken van impact- en risico analyses bij IT-projecten, de uitbesteding van werkzaamheden, de inrichting van klantonderzoek en screening van medewerkers, het documenteren van processen, het documenteren van incidenten en het melden van veiligheidsincidenten (waaronder datalekken).

Tot op heden was slechts in beperkte mate sprake van conflicten/overlap tussen financiële AOIC-regels en AOIC-regels op het gebied van het gegevensbeschermingsrecht. Ook waren er in de praktijk weinig conflicten tussen data protectie autoriteiten en financiële toezichthouders.

Veranderingen

De wetgever gaat in het data protectierecht zoals geformuleerd in de ontwerpverordening betreffende de bescherming van individuen in verband met de verwerking van persoonsgegevens (COM(2012)11 final) echter steeds indringender op de stoel van de ondernemer zitten als het gaat om de AOIC. Daardoor ontstaan binnen de financiële sector dubbele regelsystemen met betrekking tot AOIC en met betrekking tot toezicht en handhaving van deze AOIC-regels. Eén systeem gebaseerd op financieel toezichtsrecht en één gebaseerd op gegevensbeschermingsrecht.

---

[1] AOIC: administratieve organisatie en interne controle.

[2] 22.1. Home Member State competent authorities shall require that every credit institution have robust governance arrangements, which include a clear organisational structure with well defined, transparent and consistent lines of responsibility, effective processes to identify, manage, monitor and report the risks it is or might be exposed to, and adequate internal control mechanisms, including sound administrative and accounting procedures.
22.2. The arrangements, processes and mechanisms referred to in paragraph 1 shall be comprehensive and proportionate to the nature, scale and complexity of the credit institution's activities. The technical criteria laid down in Annex V shall be taken into account.

[3] EBA guidelines on internal governance (GL 44 van 27/9/2011). Zie o.a. punt 28 en verder.

[4] Beleidsregel van De Nederlandsche Bank N.V. van 11 juli 2011 tot toepassing van richtsnoeren van de Europese Bankautoriteit in verband met het prudentieel toezicht bij of krachtens de Wet op het financieel toezicht (Beleidsregel toepassing richtsnoeren EBA Wft), Stcrt. 13104/2011.

[5] Zie bijvoorbeeld hoofdstuk 5en 6 Besluit gedragstoezicht financiële ondernemingen en hoofdstuk 5 en 6 Besluit prudentiële regels Wft.

De dataprotectieregels uit de ontwerpverordening roepen voor financiële instellingen verplichtingen in het leven die overlappen met de regels bij of krachtens de Wft gesteld. Daarbij lijkt het CBP (College Bescherming Persoonsgegevens) een rol te krijgen van tweede prudentieel toezichthouder. De overlap kan leiden tot dubbele administratieve lasten, handhavingsconflicten, conflicten tussen privacytoezicht en financieel toezicht en tot afbakeningsproblemen.[6]

Consultatiedocument Ministerie van Veiligheid en Justitie (V&J) van 20 december 2011

De contouren van het conflict tussen regelsystemen werden op iets kleinere schaal duidelijk zichtbaar toen het Ministerie van V&J een consultatiedocument publiceerde inzake aanpassing van de Wbp met een wettelijke meldplicht bij datalekken[7]. Er was sprake van een duidelijke overlap met de voorschriften en het toezicht/handhaving ten aanzien van financiële instellingen onder de Wft. In het consultatiedocument wordt de financiële wereld daarom uitgezonderd van het Wbp-regime voor datalekken. Er wordt geopteerd voor markttoezicht in plaats van grondrechtentoezicht.
Naar in het consultatiedocument wordt betoogd voldoet de Wft aan de bij datalekken te stellen eisen. De concept memorie van toelichting bevat een gedegen gedocumenteerde onderbouwing van deze stelling.

De ontwerp dataprotectie verordening

De Europese conceptverordening verlaat de oude normatieve benadering van richtlijn 96/46/EG (men moet een state of the art AOIC hebben maar bepaalt zelf hoe dat moet) en gaat nu meer inhoudelijk aangeven hoe de AOIC moet worden ingericht. De nieuwe inhoudelijke AOIC eisen staan hoofdzakelijk in hoofdstuk IV van de conceptverordening betreffen:

Art. 23 Privacy by design
Art. 26 Outsourcing to processor
Art. 27 Outsourcing to processor
Art. 28 Keeping documentation
Art. 30 Security measures
Art. 31 Security breaches
Art. 32 Security breaches
Art. 33 Privacy Impact Assessment.
Art. 34 Prior authorisation from authority
Art. 35-37 Designation of data protection officer.

Positie financiële sector

De NVB is een voorstander van het voorkomen van dubbele regelgeving en van dubbel toezicht/handhaving en opteert voor het handhaven van de bestaande voorschriften en het bestaande prudentieel toezicht.

Naar de mening van de NVB is het gewenst dat de thans in het consultatiedocument voorziene uitzondering bij datalekken voor de financiële wereld blijft bestaan en dat wordt overwogen om ook

[6] Deze redenering ligt ook onder het besluit om de Consumentenautoriteit geen bevoegdheden te geven ten aanzien van financiële dienstverleners. Deze zijn toegekend aan de Autoriteit Financiële Markten.

[7] Internet consultatie 20/11/2011 van Ministerie van Veiligheid en Justitie inzake Wijziging Wbp (gebruik camerabeelden en meldplicht datalekken).

de komende nieuwe regels betreffende AOIC en prudentieel toezicht te beleggen bij de financiële autoriteiten.

Een snelle inventarisatie in de Europese bankenwereld geeft aanleiding te veronderstellen dat deze benadering in Europees verband op steun kan rekenen.

Reden om er op aan te dringen dat in het kabinetsstandpunt over de conceptverordening wordt bedongen om voor intensief gereguleerde sectoren zoals de bancaire sector te voorzien in de mogelijkheid om AOIC en prudentieel toezicht/handhaving exclusief neer te leggen in financieel toezichtsrecht en bij financieel toezichthouders.