Tweede Kamer der Staten-Generaal

2

Vergaderjaar 2012–2013

33 662 Wijziging van de Wet bescherming persoonsgegevens en de Telecommunicatiewet in verband met de invoering van een meldplicht bij de doorbreking van maatregelen voor de beveiliging van persoonsgegevens (meldplicht datalekken)

Nr. 3 HERDRUK[1]

MEMORIE VAN TOELICHTING

ALGEMEEN

1. Strekking van het wetsvoorstel

In dit wetsvoorstel wordt een meldplicht geïntroduceerd in de Wet bescherming persoonsgegevens (hierna: Wbp) voor verantwoordelijken voor de verwerking van persoonsgegevens in geval van gebleken doorbrekingen van de getroffen maatregelen ter beveiliging van persoonsgegevens. De verantwoordelijke moet op grond van het voorgestelde artikel 34a van de Wbp bij een inbreuk waarvan redelijkerwijs kan worden aangenomen dat die leidt tot een aanmerkelijke kans op verlies of onrechtmatige verwerking van persoonsgegevens een melding doen bij de toezichthouder, het College bescherming persoonsgegevens (hierna: Cbp). Daarnaast dient in de meeste gevallen een melding aan de betrokkene te geschieden indien de inbreuk ongunstige gevolgen zal hebben voor diens persoonlijke levenssfeer. De meldplicht rust op alle verantwoordelijken voor de verwerking, zowel in de private als publieke sector. Het nalaten aan deze verplichtingen te voldoen kan worden gesanctioneerd met een bestuurlijke boete, op te leggen door het Cbp. Het doel van de meldplicht is het voorkomen van datalekken ten gevolge van doorbreking van beveiligingsmaatregelen en als deze zich toch voordoen, de gevolgen ervan voor de betrokkenen zoveel mogelijk te beperken. Met de meldplicht wordt bijgedragen aan het behoud en herstel van vertrouwen in de omgang met persoonsgegevens.

2. Beleidsmatige achtergrond

2.1 Aanleiding

Naar aanleiding van een groot aantal incidenten waarbij door een inbreuk op de beveiliging van, onder meer, websites persoonsgegevens vrijkwamen met nadelige gevolgen voor de persoonlijke levenssfeer van de betrokkenen, wordt in dit wetsvoorstel een meldplicht voor dergelijke

[1] I.v.m. een correctie in de titel.

kst-33662-3-n1
ISSN 0921 - 7371
's-Gravenhage 2013

inbreuken ingevoerd. In een aantal gevallen betrof het zeer ernstige schendingen, waarbij de ernst zowel betrekking had op het aantal persoonsgegevens als op de aard van de gegevens. Het is mede daarom dat in het regeerakkoord van het kabinet-Rutte I «Vrijheid en verantwoordelijkheid» van 30 september 2010 is opgenomen dat alle diensten van de informatiemaatschappij, ook als die door de overheid worden aangeboden, zullen worden onderworpen aan een meldplicht voor inbreuken op de beveiliging waarvan redelijkerwijs kan worden aangenomen dat die leidt tot een aanmerkelijke kans op verlies of onrechtmatige verwerking van persoonsgegevens, waaraan nadelige gevolgen voor de persoonlijke levenssfeer van de betrokkene zijn verbonden.
Het toezicht op de naleving en de handhaving van de meldplicht wordt aan het Cbp opgedragen. Het Cbp wordt bevoegd om een bestuurlijke boete op te leggen indien de meldplicht niet wordt nageleefd. De uitbreiding van de boetebevoegdheid is in overeenstemming met het regeerakkoord van het kabinet-Rutte II «Bruggen slaan» van 29 oktober 2012 waarin is opgenomen dat de privacytoezichthouder meer bevoegdheden krijgt, waaronder de bevoegdheid om in meer gevallen bestuurlijke boetes op te leggen.

2.2 Relatie met de Notitie privacybeleid

Bij brief van 29 april 2011 van eerste en tweede ondergetekende aan de voorzitters van de Eerste en de Tweede Kamer der Staten-Generaal (Kamerstukken II 2010/11, 32 761, nr. 1) en de daarbij behorende Notitie privacybeleid is een aantal wetgevingsvoornemens geformuleerd. Een van deze maatregelen betreft de invoering van een meldplicht voor doorbreking van de beveiligingsmaatregelen voor persoonsgegevens, die in dit wetsvoorstel vorm heeft gekregen. Aan de overige in de notitie genoemde maatregelen hechten wij onverminderd groot belang. Echter, een aantal omstandigheden maken nadere keuzes met betrekking tot het moment waarop en het tempo waarin deze maatregelen worden uitgevoerd onvermijdelijk. Beide ondergetekenden hebben dit in een algemeen overleg met de Vaste Commissie voor Veiligheid en Justitie uit de Tweede Kamer der Staten-Generaal op 15 september 2011 toegelicht (Kamerstukken II 2011/12, 32 761, nr. 2). In de brief van de Staatssecretaris van Veiligheid en Justitie van 27 oktober 2011 aan de voorzitter van de Tweede Kamer der Staten-Generaal is dit bevestigd (Kamerstukken II 2011/12, 32 761, nr. 4). Begin 2012 heeft de Europese Commissie voorstellen gepresenteerd die strekken tot herziening van de regels voor de bescherming van persoonsgegevens binnen de Europese Unie (COM (2012)10 en 11 def). Het spreekt vanzelf dat de nationale beleidsruimte voor het privacybeleid sterk wordt beïnvloed door deze voorstellen en de uiteindelijk tot stand te brengen Europese regeling (zie ook de aan de voorzitter van de Tweede Kamer der Staten-Generaal uitgebrachte voorlichting van de Afdeling advisering van de Raad van State van 28 juni 2012, Kamerstukken II 2011/12, 32 761, nr. 32).

2.3 Verhouding met voorstel Algemene verordening gegevensbescherming

Op 25 januari 2012 heeft de Europese Commissie een voorstel gepresenteerd voor een Algemene verordening gegevensbescherming (COM (2012)11 def). Deze verordening zal richtlijn 95/46/EG vervangen en daarmee ook de Wbp (de richtlijn is in Nederland in de Wbp geïmplementeerd). De artikelen 31 en 32 van de ontwerpverordening bevatten een algemene regeling voor een meldplicht van datalekken aan de toezichthouder respectievelijk de betrokkene. Mede naar aanleiding van het advies van Cbp is overwogen of de regeling van dit wetsvoorstel niet volledig moet worden toegesneden op die van de ontwerpverordening.

Ook in de zienswijzen van andere organisaties is daarop aangedrongen, zoals VNO/NCW-MKB Nederland en ICT-Office. Daarvan wordt afgezien. De regeling van de meldplicht in de ontwerpverordening geeft in dit stadium nog te veel aanleiding tot vragen over de reikwijdte van de daarin opgenomen verplichtingen en de invulling van de daarbij in acht te nemen voorwaarden. Het is nog te prematuur om ervan uit te gaan dat de Europese wetgever met een redelijke mate van zekerheid regeling overeenkomstig het voorstel zal vaststellen. Naar verwachting zal het bovendien nog geruime tijd duren voor de ontwerpverordening wordt vastgesteld. Toch is het advies van het Cbp aanleiding geweest het aanvankelijke voorstel voor artikel 34a van de Wbp tekstueel zo nauw mogelijk te laten aansluiten bij artikel 11.3a van de Telecommunicatiewet dat de implementatie vormt van artikel 4, derde lid, van richtlijn 2002/58/EG. Deze bepaling bevat een specifieke meldplicht voor aanbieders van openbare elektronische communicatiediensten met betrekking tot datalekken, die ook ten grondslag ligt aan de artikelen 31 en 32 van de ontwerpverordening. Naar verwachting zal de verordening niet eerder dan in 2016 in werking treden.
Voor de volledigheid zij vermeld dat ook het voorstel van de Europese Commissie voor een richtlijn ter bescherming van personen met betrekking tot de verwerking van persoonsgegevens door de bevoegde autoriteiten ten behoeve van opsporing en vervolging (COM (2012) 10 final) een meldplicht voor datalekken bevat (artikelen 28 en 29 van de ontwerprichtlijn).

2.4 Verhouding tot andere meldplichten die betrekking hebben op de bedrijfsvoering in de private of publieke sector

De meldplicht die in dit wetsvoorstel is opgenomen heeft uitsluitend betrekking op doorbrekingen van de maatregelen voor de beveiliging van persoonsgegevens. De meldplicht ziet dus niet op situaties als die rond DigiNotar waarin fouten werden gemaakt in de beveiliging van certificaten waardoor deze onbetrouwbaar waren, of op andere meldplichten met een min of meer verwant karakter (cybersecurity-incidenten). In dat verband is van belang om op te merken dat ook in Nederland wordt nagedacht en gewerkt aan meer verplichtende meldingen aan de overheid die de risico's van deze incidenten kunnen verminderen dan wel, indien deze zich onverhoopt mochten voordoen, beperken. Zo bereidt de derde ondergetekende een wettelijke meldplicht voor, op grond van de Telecommunicatiewet, voor certificatiedienstverleners ten aanzien van gekwalificeerde certificaten, in het geval er sprake is van een inbreuk op de veiligheid of een verlies van integriteit met aanzienlijke gevolgen voor de betrouwbaarheid van de betreffende certificaten. Verder wordt naar aanleiding van de motie Hennis-Plasschaert c.s. (Kamerstukken II 2011/12, 26 643, nr. 202) door de minister van Veiligheid en Justitie een wettelijke regeling voorbereid die strekt tot invoering van een meldplicht voor de overheid en private bedrijven in randvoorwaardelijke sectoren van cyberincidenten met een potentieel maatschappelijk ontwrichtende werking.
Wat alle meldplichten met betrekking tot datalekken, of andere ernstige incidenten met betrekking tot de bedrijfsvoering, en in het bijzonder de informatiehuishouding, van bedrijven en overheid – ongeacht welke inhoud zij hebben en ongeacht of zij vrijwillig of verplichtend, of privaatrechtelijk of publiekrechtelijk van aard zijn – met elkaar gemeen hebben is dat zij steeds hetzelfde doel dienen. Dat doel is het bevestigen en waar nodig herstellen van het vertrouwen van het publiek, de klanten, de markt, de overheid en de toezichthouders in de desbetreffende instelling of het desbetreffende bedrijf.

Wat de Wbp betreft, geldt dat de wetgever door middel van algemeen-abstract geformuleerde normen, een relatief grote mate van vrijheid, en

dus ook vertrouwen, geeft aan de bedrijven, instellingen en burgers die onder de reikwijdte van de wet vallen. Bij het geven van vertrouwen hoort echter ook het afleggen van een zekere mate van rekenschap aan samenleving en de kringen van betrokkenen. Wanneer er een reëel risico is voor verlies of onrechtmatige verwerking van persoonsgegevens, of wanneer dat risico zich heeft verwezenlijkt, kan dat vertrouwen in meer of minder ernstige mate worden geschaad. Het is in het belang van zowel de verantwoordelijke als de betrokkene dit vertrouwen zo snel mogelijk te herstellen. Transparantie over de aard van het datalek, de vermoedelijke omvang ervan en aard van de mogelijke schade, de inspanningen die gepleegd worden om de schade te herstellen en raadgevingen aan publiek en klanten om zichzelf zo goed mogelijk in staat te stellen de consequenties voor de eigen belangen te overzien zijn noodzakelijke maatregelen voor behoud en herstel van dat vertrouwen.
Dat vertrouwen wordt ondersteund doordat onafhankelijke toezichthouders (Cbp c.q. Autoriteit Consument en Markt) in staat worden gesteld zich een eigen beeld te vormen van de feiten, een oordeel kunnen geven over de genomen maatregelen, onder omstandigheden vertrouwelijk met de verantwoordelijke kunnen overleggen en zonodig kunnen interveniëren.
Als sluitstuk op het geheel wordt het nalaten aan deze verplichting te voldoen gesanctioneerd met een bestuurlijke boete.

Als voorbeelden van bestaande meldplichten die betrekking hebben op datalekken of andere ernstige incidenten met betrekking tot de bedrijfsvoering van bedrijven en overheid kunnen worden genoemd:
– Meldplicht artikel 11.3a Telecommunicatiewet (voor aanbieders van openbare elektronische communicatiediensten van inbreuken op de beveiliging van persoonsgegevens);
– Meldplicht artikel 11a.2 Telecommunicatiewet (voor aanbieders van openbare elektronische netwerken en -diensten van inbreuken op de veiligheid of het verlies van integriteit die leiden tot onderbreking van de continuïteit van het netwerk of de dienst);
– Meldplicht artikel 14.6, tweede lid, Telecommunicatiewet (voor de op grond van dit artikel aangewezen aanbieders van openbare elektronische en -diensten van verstoringen in hun dienstverlening, ter voorbereiding op buitengewone omstandigheden in de telecomsector);
– Meldplicht artikel 3:10, derde lid, en artikel 4:11, vierde lid, Wet op het financieel toezicht, artikel 12, derde lid, Besluit prudentiële regels Wft en artikel 19, derde lid, Besluit gedragstoezicht financiële ondernemingen (voor financiële instellingen, van incidenten in de zin van de Wet op het financieel toezicht, zie hierover paragraaf 4.2 van deze toelichting).

Daarnaast worden in verschillende Europese voorstellen voor regelgeving nieuwe meldplichten voorgesteld:
– Meldplicht artikel 15, tweede lid, van de ontwerpverordening betreffende elektronische identificatie en vertrouwensdiensten voor elektronische transacties in de interne markt (COM (2012) 238 finaal) (inbreuken op de veiligheid of het verlies van integriteit met aanzienlijke gevolgen voor de vertrouwensdienst en voor de persoonsgegevens die daarmee worden beheerd).
– Meldplicht van artikel 14 van de ontwerprichtlijn houdende maatregelen om een hoog gemeenschappelijk niveau van netwerk- en informatiebeveiliging in de Unie te waarborgen (COM (2013) 48 finaal) (incidenten met een aanzienlijke impact op de beveiliging van netwerken en informatiesystemen op de door hen verleende kerndiensten);

Op de verhouding van de in dit wetsvoorstel voorgestelde meldplicht met de meldplicht voor datalekken op grond van artikel 11.3a van de Telecommunicatiewet en de meldplicht op grond van de Wet financieel toezicht met betrekking tot incidenten in de financiële sector wordt in paragrafen 4 en 5 nader ingegaan.

3. Algemene aspecten van de meldplicht

3.1 Inbreuk op beveiligingsmaatregelen

De voorgestelde meldplicht voor datalekken staat in nauw verband met de beveiligingsverplichting van artikel 13 van de Wbp. Die bepaling verplicht de verantwoordelijke om passende technische en organisatorische maatregelen ten uitvoer te leggen om persoonsgegevens te beveiligen tegen verlies of enige vorm van onrechtmatige verwerking. Het Cbp heeft op 19 februari 2013 richtsnoeren gepubliceerd voor de beveiliging van persoonsgegevens (Stcrt. 2013, nr. 5174). Deze richtsnoeren leggen uit hoe het Cbp bij het onderzoeken en beoordelen van beveiliging van persoonsgegevens in individuele gevallen de beveiligingsnormen uit de Wbp toepast. De richtsnoeren vormen de verbindende schakel tussen enerzijds het juridische domein, met daarbinnen de eisen uit de Wbp, en anderzijds het domein van de informatiebeveiliging, waarin de noodzakelijke kennis en kunde aanwezig is om daadwerkelijk aan die eisen te voldoend. Dit betekent dat de richtsnoeren in samenhang moeten worden gebruikt met algemeen geaccepteerde beveiligingsstandaarden binnen de praktijk van informatiebeveiliging, zoals de Code voor Informatiebeveiliging (NEN-ISO/IEC 27002:2007 nl) of de ICT-beveiligingsrichtlijnen voor webapplicaties van het Nationaal Cyber Security Centrum van het Ministerie van Veiligheid en Justitie. Daarnaast voorziet de Wbp in de mogelijkheid dat bij algemene maatregel van bestuur voor een bepaalde sector nadere regels worden gesteld inzake onder andere de beveiliging van persoonsgegevens (artikel 26 Wbp).

Volgens het voorgestelde artikel 34a is pas sprake van een onder de meldplichtbepaling vallend datalek als de technische en organisatorische beveiligingsmaatregelen niet hebben gefunctioneerd en de persoonsgegevens blootgesteld zijn aan een aanmerkelijke kans op verlies of onrechtmatige verwerking. Over het vereiste dat sprake moet zijn van een inbreuk op de beveiliging, bedoeld in artikel 13 Wbp, merken wij op, dat niet noodzakelijkerwijs sprake behoeft te zijn van tekortschietende beveiligingsmaatregelen. Van een inbreuk op de beveiliging kan ook sprake zijn indien de beveiliging van voldoende niveau is, maar de beveiligingsmaatregelen worden teniet gedaan of omzeild. Denk bijvoorbeeld aan een hack van een ICT-systeem dat persoonsgegevens bevat of de diefstal van een laptop of mobiele telefoon uit een afgesloten locker. Er zijn echter ook situaties denkbaar waarin de inbreuk op de beveiligingsmaatregelen het gevolg is van een tekortschietende beveiliging, die de verantwoordelijke zelf kan worden aangerekend. Dit kan variëren van een niet adequate en vakkundig toegepaste beveiliging van de bestanden of de gegevens, tot menselijke fouten van ondergeschikten. Denk bijvoorbeeld aan het slordig omgaan met het beheer van wachtwoorden die toegang geven tot informatiebestanden of aan situaties van het per ongeluk verkeerd adresseren van een brief of e-mail die persoonsgegevens bevat, het als oud papier aanbieden van gevoelige stukken, of het zoekraken van een mobiele telefoon of een geheugenstick. In al deze gevallen wordt het verlies van persoonsgegevens en de blootstelling aan risico's van ongeoorloofde toegang of onrechtmatige verwerking ervan, door een inbreuk op de beveiligingsmaatregelen veroorzaakt.
De meldplicht geldt alleen dan niet wanneer voorzieningen van algemene aard die niet specifiek zijn gericht op de beveiliging van persoonsge-

gevens worden aangetast. Als bijvoorbeeld een blikseminslag tot gevolg heeft dat het gebouw afbrandt, waarbij ook persoonsgegevens verloren gaan, zal niet van een inbreuk op de beveiligingsmaatregelen kunnen worden gesproken.

Bits of Freedom heeft in zijn zienswijze een aanmerkelijk verdergaande reikwijdte van de meldplicht bepleit. Bits of Freedom bepleit elk datalek onder de meldplicht te brengen, wanneer dit in verband kan worden gebracht met elke vorm van ongeoorloofde toegang. Het is zeker zo dat ongeoorloofde toegang kan leiden tot datalekken, die aanleiding behoren te zijn voor het naleven van de meldplicht. Hacken is daarvan het meest aansprekende voorbeeld, maar ook de nalatige omgang met wachtwoorden of vergelijkbare voorzieningen in een werkomgeving. Toch wordt de suggestie van Bits of Freedom niet gevolgd. In de praktijk zal ongeoorloofde toegang moeilijk te onderscheiden zijn van het oneigenlijke gebruik of misbruik maken van gegevens na op zichzelf geoorloofde toegang. Er is dan geen sprake van het inbreuk maken op beveiligingsmaatregelen, maar het misbruik maken van vertrouwen. Hoe schadelijk dit ook kan zijn, dat is niet het onderwerp van dit wetsvoorstel.

3.2 Voorkomen van nodeloze meldingen

3.2.1 Verschillende systemen; systeem Wbp
De effectiviteit van de meldplicht voor datalekken zal snel aan betekenis verliezen wanneer elk denkbaar datalek in aanmerking komt om te worden gemeld. Een meldplicht zonder enige beperking leidt bovendien tot een nodeloze belasting van bedrijfsleven en overheid.
Er zijn twee richtingen denkbaar waarlangs een zinvolle beperking kan worden bereikt. De meldplicht zou beperkt kunnen worden tot bepaalde categorieën gegevens. Daartoe is de Duitse wetgever recent overgegaan. § 42a van het Bundesdatenschutzgesetz beperkt de meldplicht tot bijzondere persoonsgegevens, persoonsgegevens die worden beschermd door een specifiek beroepsgeheim, zoals het medisch of notarieel beroepsgeheim, persoonsgegevens van strafrechtelijke aard en persoonsgegevens met betrekking tot bankrekeningen en kredietkaarten.
Een andere beperking van de meldplicht is het gebruik van een algemene formulering die de meldplicht beperkt tot een algemene categorie van relatief zware gevallen. De Oostenrijkse wetgever heeft die keuze gemaakt in § 24 (2a) van het Datenschutzgesetz 2000.
Het Duitse en Oostenrijkse voorbeeld zijn bij wijze van illustratie gegeven. In dit wetsvoorstel wordt noch voor het ene, noch voor het andere model gekozen, maar voor een regeling die aansluit bij de Wbp en de Tw. De normen van de Wbp zijn algemeen geformuleerd en, behoudens de uitzonderingen op het verbod van de verwerking van bijzondere persoonsgegevens, niet toegesneden op specifieke verwerkingen. Een keuze voor een algemene formulering ter beperking van de meldplicht voor datalekken ligt daarom alleen al uit wetssystematisch oogpunt voor de hand. Een beperking van de meldplicht tot bepaalde categorieën gegevens heeft bovendien als nadeel dat de niet in de wet genoemde categorieën de bescherming door de meldplicht categorisch wordt onthouden, ook wanneer er sprake is van een relatief hoog risico. Zo strekt de hierboven genoemde Duitse regeling zich niet uit tot bedrijfsvertrouwelijke gegevens of gegevens die worden beschermd door het fiscaal geheim. Daar tegenover staat dat een meer algemene formulering leidt tot meer meldingen. Dat kan echter worden ondervangen door een voorziening om nodeloze meldingen tegen te gaan, in combinatie met voorlichtende maatregelen door het Cbp.
Dat lijkt te prefereren boven een meldplicht die beperkt zou zijn voor alleen «zware gevallen», zoals bepleit is door ICT Office.

De voorziening in de Wbp houdt in dat de verantwoordelijke niet elke inbreuk op de beveiliging van persoonsgegevens behoeft te melden, maar alleen die inbreuken waarvan «redelijkerwijs» kan worden aangenomen dat die leiden tot een «aanmerkelijke kans op nadelige gevolgen voor de bescherming van persoonsgegevens» die door hem worden verwerkt. De clausulering geldt zowel de meldplicht van de verantwoordelijke aan het Cbp als aan de betrokkene (zie het voorgestelde artikel 34a, eerste en tweede lid).

3.2.2 Beslismodel meldplicht Wbp

Bij de vraag of aan de meldplicht moet worden voldaan, kan de verantwoordelijke het volgende beslismodel langslopen. Eerst komt de vraag aan de orde of er sprake is van een inbreuk op de getroffen beveiligingsmaatregelen. Is dit het geval, dan komt de vraag aan de orde of de inbreuk tot gevolg heeft gehad dat de verwerkte persoonsgegevens zijn blootgesteld aan een aanmerkelijke kans op nadelige gevolgen voor de persoonsgegevens die door hem worden verwerkt. Die nadelige gevolgen kunnen zich dan vooral voordoen in de vorm van verlies of onrechtmatige verwerking. Tegen die nadelen wil artikel 13 van de Wbp bescherming bieden. Die laatste stap vergt een beoordeling die zo geobjectiveerd mogelijk moet zijn. De aanmerkelijke kans dat persoonsgegevens zijn blootgesteld aan nadelige gevolgen in de vorm van verlies of onrechtmatige verwerking moet redelijkerwijs aanwezig zijn. Dat moet naar feitelijke omstandigheden van het geval worden vastgesteld. Het risico zal zich bij een geslaagde aanval van hackers eerder voordoen dan bij fysieke schade aan het gebouw waar zich de ICT-apparatuur bevindt waarmee de verwerking plaatsvindt.

Vervolgens moet sprake zijn van een aanmerkelijke kans. Niet elk risico rechtvaardigt immers een melding. Of er sprake is van een aanmerkelijke kans is eveneens afhankelijk van de concrete feiten en omstandigheden. De aard van de inbreuk zal doorgaans van belang zijn bij het bepalen van de grootte van het risico. Het is niet goed mogelijk aan te geven of het verlies van een mobiele telefoon, de diefstal van een laptop of het zoekraken van een geheugenstick wel of geen aanleiding geeft een melding te doen. Of die noodzaak aanwezig is, is afhankelijk van de aard van de data die het betreft en het vermoedelijke risico dat de betrokkene en de verantwoordelijke lopen ingeval van zoekraken of onrechtmatige verwerking.

Tenslotte moet ook aannemelijk zijn dat wanneer de aanmerkelijke kans op verlies of onrechtmatige verwerking zich verwezenlijkt, dit redelijkerwijs tot nadelige gevolgen voor de persoonlijke levenssfeer van de betrokkene leidt. Omvang en aard van de verwerking zijn mede bepalend voor de vraag of de verwezenlijking van het risico als nadelig voor de persoonlijke levenssfeer moet worden aangemerkt. Het zoekraken of hacken van de ledenadministratie van een sportvereniging zal doorgaans leiden tot het nodige ongemak voor vereniging en leden, maar zal niet snel aanleiding geven tot een melding bij het Cbp. De gevolgen van een dergelijk datalek blijven doorgaans beperkt en ook van betrokkenen kan worden gevergd dat zij een zekere mate van risico aanvaarden. Dat is nu eenmaal onlosmakelijk verbonden met het normaal vertrouwen in maatschappelijke verhoudingen. Maar een datalek bij, bijvoorbeeld, de Belastingdienst of de Sociale Verzekeringsbank (SVB) of een commerciële bank of verzekeraar is doorgaans van geheel andere orde. Een datalek bij dergelijke instellingen kan leiden tot financieel nadeel bij de betrokkene of tot de compromittering van gegevens die beschermd worden door een geheimhoudingsplicht.

Van deze instellingen mag worden verwacht dat zij de grote hoeveelheden gegevens die zij dagelijks verwerken op een professionele wijze beveiligen en dat die beveiliging ook wordt aangepast aan veranderende omstandigheden. De aard van de door de Belastingdienst verwerkte

gegevens is ook zodanig dat een datalek kan leiden tot een aanmerkelijke inbreuk op de persoonlijke levenssfeer van de betrokkenen, omdat het belastinggeheim kan worden geschonden.

Tenslotte mag van het Cbp worden verwacht dat het richtsnoeren zal vaststellen waarmee het college indirect enig houvast kan geven aan de praktijk. Daarin zal ook kunnen worden ingegaan op de invulling van de voorziening om nodeloze meldingen te voorkomen. Vermoedelijk zal het Cbp ook nog aanvullende voorlichting aan de praktijk geven.
De voorziening voor het voorkomen van nodeloze meldingen is een essentieel onderdeel van dit wetsvoorstel. Om die reden is het advies van het Cbp om deze voorziening in de vorm van een vrijstellingsregeling te delegeren naar het niveau van de algemene maatregel van bestuur en van die delegatiegrondslag pas gebruik te maken nadat enig ervaring met de meldplicht is opgedaan niet overgenomen.

3.3 Verhouding verantwoordelijke voor de verwerking en bewerker

De voorgestelde meldplicht van artikel 34a van de Wbp richt zich tot de verantwoordelijke. De verantwoordelijke is immers krachtens artikel 13 van de Wbp gehouden de nodige beveiligingsmaatregelen te treffen. Ook overigens vloeit uit de systematiek van de Wbp voort dat verplichtingen zijn gericht tot de verantwoordelijke, en niet tot anderen. De verantwoordelijke behoort zich, in het belang van de bescherming van de door hem verwerkte gegevens, aan de betrokkene bekend te maken, zodat deze zo nodig zijn rechten kan uitoefenen. Dat geldt ook in de gevallen waarin een verantwoordelijke zich bedient van een bewerker. Weliswaar zal de bewerker de partij zijn die feitelijk belast is met het ten uitvoer leggen van de passende technische en organisatorische maatregelen in de zin van artikel 13 van de Wbp ter beveiliging van de verwerkte gegevens, maar artikel 14, derde lid, onder b, van de Wbp legt de verantwoordelijke expliciet een zorgplicht op voor het nakomen van deze verplichting. Daaraan kan hij zich niet onttrekken. Artikel 14, vijfde lid, van de Wbp verplicht bovendien tot een schriftelijke (of daarmee als gelijkwaardig aan te merken) vastlegging van, onder meer, de beveiligingsmaatregelen waarop artikel 13 van de Wbp het oog heeft. Deze regels zijn gesteld in het belang van de betrokkene en de verantwoordelijke.
Zodoende is de verhouding tussen verantwoordelijke en bewerker door de wetgever in belangrijke mate ingekleurd door hetgeen de beveiligingsplicht met zich brengt. Dit is zodanig zwaarwegend dat de regeling van de meldplicht ook moet doorwerken in deze rechtsverhouding. Het is bovendien van belang met het oog op de werking van de specifieke aansprakelijkheids- en schadevergoedingsregeling van artikel 49 van de Wbp. Die regeling richt zich primair tot de verantwoordelijke en niet tot de bewerker.
Om een meer evenwichtige regeling te bereiken, wordt voorgesteld dat de zorgplichten van de verantwoordelijke op grond van artikel 14 van de Wbp zich expliciet uitstrekken over datalekken waarvan de bewerker kennis krijgt, onverminderd de eindverantwoordelijkheid van de verantwoordelijke (artikel I, onderdeel A, van het wetsvoorstel).
Dit alles betekent dat de meldplicht zich uitstrekt tot iedere verantwoordelijke in de zin de van de Wbp. Het is niet relevant of de verantwoordelijke een natuurlijke persoon of rechtspersoon is. Evenmin is relevant of de verantwoordelijke deel uitmaakt van de publieke of de private sector. Wel is het zo dat de kring van verantwoordelijken voor wie de meldplicht geldt wordt beperkt door de reikwijdtebepalingen van de Wbp. Het Nederlands Genootschap voor Functionarissen voor de Gegevensbescherming (NGFG) vraagt in zijn zienswijze aandacht voor de noodzaak om de nodige instrumenten beschikbaar te stellen die de verantwoordelijke in staat stellen op de bewerker meer invloed uit te oefenen. Dit is echter geen taak

voor de wetgever. De rechtsbetrekking tussen verantwoordelijke en bewerker is primair van privaatrechtelijke aard. In de bewerkersovereenkomst zullen verantwoordelijke en bewerker daarover afspraken moeten maken.

3.4 Kennisgeving aan betrokkene en verhouding tot het aansprakelijkheidsrecht

Het doen van een kennisgeving van een datalek aan de betrokkene ontheft de verantwoordelijke op zichzelf genomen niet van eventuele burgerrechtelijke aansprakelijkheid voor schade die voortvloeit uit het toerekenbaar niet of niet voldoende naleven van de verplichting neergelegd in artikel 13 van de Wbp. Artikel 49 van de Wbp bevat daarvoor een afzonderlijke voorziening die de aansprakelijkheid en de verplichting tot het betalen van schadevergoeding bij de verantwoordelijke legt. De verantwoordelijk kan eventueel regres nemen op een bewerker. Dat wil niet zeggen dat de kennisgeving uit hoofde van het aansprakelijkheidsrecht geen betekenis heeft. De kennisgeving aan de betrokkene is een uiting van de algemene verplichting tot schadebeperking die deel uitmaakt van het aansprakelijkheidsrecht, met inbegrip van het bijzondere aansprakelijkheidsrecht van de Wbp. Verantwoordelijken doen er daarom goed aan dit bij de afweging om wel of geen kennisgeving aan betrokkenen te doen mee te nemen. Handelt de betrokkene nadat hem een kennisgeving is gedaan niet overeenkomstig de door de verantwoordelijke voorgestelde maatregelen, en vloeit daaruit schade voor de hem voort, dan kan onder omstandigheden sprake zijn van eigen schuld van de betrokkene.
Wanneer het Cbp op grond van artikel 34a, zevende lid, van de Wbp een verantwoordelijke de aanwijzing geeft dat alsnog een melding aan de betrokkenen wordt gedaan, betekent dit niet als vanzelfsprekend dat daardoor bepaalde verantwoordelijkheden en aansprakelijkheden overgaan naar het Cbp, zoals VNO/NCW-MKB Nederland vraagt. De normale regels van de toezichthoudersaansprakelijkheid worden daardoor niet beïnvloed.

4. Verhouding tot andere rechtsgebieden

4.1 Verhouding tot specifieke meldplicht op grond van de Telecommunicatiewet

Een sterk vergelijkbare meldplicht voor inbreuken op de beveiliging van persoonsgegevens is reeds opgenomen in artikel 11.3a van de Telecommunicatiewet (Tw). Dit artikel vormt de implementatie van de in artikel 2, onderdeel 4, van richtlijn 2009/136/EG[1] opgenomen regeling die aanbieders van openbare elektronische communicatiediensten verplicht tot het melden van doorbrekingen van de maatregelen die zijn getroffen om persoonsgegevens te beveiligen. Vanwege de reikwijdte van deze richtlijn geldt de meldplicht op grond van artikel 11.3a van de Tw uitsluitend voor aanbieders van openbare elektronische communicatiediensten. Naar aanleiding van het grote aantal gevallen waarin bij andere

[1] 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 gebruikersrechten 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 L 337). Artikel 2, onderdeel 4, van richtlijn 2009/136/EG bevat een wijziging van artikel 4, derde lid, van richtlijn 2002/58/EG die tot doel heeft een bestaande zeer beperkte meldplicht voor bijzondere risico's voor de gevolgen van inbreuken op de beveiliging van elektronische communicatienetwerken en -diensten voor de persoonlijke levenssfeer uit te breiden.

bedrijven dan de aanbieders van openbare elektronische communicatiediensten sprake was van tekortkomingen in de beveiliging van persoonsgegevens, wordt deze meldplicht met dit wetsvoorstel aangevuld met een meldplicht voor alle verantwoordelijken voor de verwerking van persoonsgegevens, zowel in de private als publieke sector.

Eén toezichthouder voor meldplicht datalekken Wbp/Tw

Aanbieders van openbare elektronische communicatiediensten moeten momenteel op grond van artikel 11.3a van de Tw de melding bij de Autoriteit Consument en Markt (ACM) (voorheen: OPTA) doen. Om redenen van doelmatigheid worden beide meldplichten zoveel als mogelijk is onderling op elkaar afgestemd. Om die redenen wordt ook voorgesteld de melding op grond van artikel 11.3a van de Tw bij het Cbp te beleggen. Hierbij moet worden bedacht dat de beveiligingsplicht die op de aanbieders van openbare elektronische communicatienetwerken en -diensten rust krachtens artikel 11.3 van de Tw zonodig reeds door het Cbp kan worden gehandhaafd. Immers, de bevoegdheid van het Cbp om toezicht op de naleving uit te oefenen strekt zich volgens artikel 51, tweede lid, van de Wbp tot alle vormen van verwerking van persoonsgegevens, waarbij alleen de reikwijdtebepalingen van de Wbp grenzen stellen aan de bevoegdheid. Dit doet er niet aan af dat ACM primair belast blijft met het toezicht op de naleving van artikel 11.3 van de Tw.
In lijn met het overgaan van de toezichtstaken van ACM naar Cbp worden de nodige toezichts- en sanctiebevoegdheden op artikel 11.3a Tw (geregeld in hoofdstuk 15 van de Tw) aan het Cbp verleend. Dat is geregeld in artikel II, onderdelen C tot en met F. De bestuurlijke boete die het Cbp bij overtreding van de artikelen 34a van de Wbp en artikel 11.3a van de Tw zal kunnen opleggen bedraagt € 450.000.

Voor het overige verandert er niets in de verhouding tussen Wbp en Tw. De OPTA gaat er in haar advies dan ook terecht van uit dat dit wetsvoorstel ook geen verandering brengt in de uitleg van artikel 11.3a van de Tw, zoals die is gegeven in de memorie van toelichting die leidde tot dat wetsvoorstel. De OPTA merkt in haar advies ook terecht op dat artikel 11.3a van de Tw alleen een meldplicht oplegt die verband houdt met de levering van openbare elektronische communicatiediensten. Wanneer zich een datalek zou voordoen bij, bijvoorbeeld, de personeelsadministratie van een aanbieder van deze diensten, dan zal gemeld moeten worden overeenkomstig de Wbp, en niet de Tw.

Voor de praktische uitvoering van de meldplicht van de Wbp zal zoveel mogelijk worden aangesloten bij de voorschriften die de Europese Commissie binnenkort zal vaststellen met tot de meldplicht van artikel 11.3a van de Telecommunicatiewet (uitvoeringsverordening van de Europese Commissie op grond van richtlijn 2002/58/EG betreffende privacy en elektronische communicatie (COCOM12–25REV2).

Samenwerking Cbp-ACM

De voorgestelde voorziening heeft consequenties voor de samenwerking tussen Cbp en ACM. De reeds bestaande samenwerking zal geïntensiveerd worden. Er bestaat reeds een samenwerkingsprotocol tussen beide bestuursorganen. Mogelijk moet dit protocol worden herzien. Wellicht willen Cbp en ACM voor wederzijdse informatievoorziening ook enkele organisatorische voorzieningen treffen. Dat blijft aan de ACM en het Cbp om te bepalen. Wel is in artikel I, onderdeel C, van het wetsvoorstel, mede naar aanleiding van het advies van het Cbp, voorzien in een wettelijke grondslag voor deze samenwerkingsrelaties. Voor de ACM bestaat die grondslag al in artikel 18.3 van de Tw.

4.2 Verhouding tot meldplicht incidenten Wet op het financieel toezicht

De voorgestelde meldplicht voor datalekken zal ook van toepassing zijn op de financiële sector, zij het in beperkte vorm. Een financiële onderneming wordt namelijk niet verplicht om datalekken te melden aan betrokkenen. Dit is in lijn met de reeds lang onder de Wet op het financieel (hierna: Wft) bestaande praktijk dat een financiële onderneming incidenten wel moet melden aan de financieel toezichthouder, maar niet aan betrokkene. De overweging is dan ook dezelfde: dergelijke openbare kennisgevingen aan betrokkenen zijn in de financiële sector – mede tegen de achtergrond van de financiële crisis – te risicovol om dwingend te worden voorgeschreven. 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 geven tot vermindering van vertrouwen van het publiek of de relevante markt. De zorgplicht van de financiële onderneming zal echter waarborgen dat zij ook zonder dat dit dwingend wordt voorgeschreven haar verantwoordelijkheid jegens haar cliënten in rechtstreeks contact met die cliënten zal nemen. Dit doet zij nu al met betrekking tot incidenten onder de Wft en dat zal niet anders zijn ten aanzien van datalekken onder dit wetsvoorstel.
Aanvankelijk was in de geconsulteerde versie van het wetsvoorstel een uitzondering op de meldplicht opgenomen voor de financiële sector. Naar aanleiding van de consultatiereactie van De Nederlandsche Bank (DNB) en de Autoriteit Financiële Markten (AFM) is het tiende lid gewijzigd. De uitzondering van financiële ondernemingen als bedoeld in de Wet op het financieel toezicht (Wft) is ingeperkt. De reden voor deze wijziging van het tiende lid is dat de uitzondering van de financiële sector in de consultatieversie te ruim was. In die versie hoefde een financiële onderneming die een incident als bedoeld in de Wft[2] moet melden aan de financieel toezichthouder, geen datalek te melden aan het Cbp en betrokkene. Deze uitzondering is te ruim omdat een incident als bedoeld in de Wft niet altijd een datalek is (een ernstig gevaar voor de integere bedrijfsuitoefening wordt niet altijd veroorzaakt door een datalek); het omgekeerde geldt ook: een datalek is niet altijd een incident (niet alle datalekken vormen een ernstig gevaar voor de integere bedrijfsuitoefening). Door de te ruime uitzondering zouden derhalve de datalekken die niet tevens incident zijn buiten beeld blijven van een toezichthouder.
In het kader van de administratieve lasten voor financiële ondernemingen wordt nog kort iets opgemerkt over eventuele dubbele meldplichten voor de financiële sector. Deze dubbele meldplicht zal alleen bestaan als een datalek eveneens een incident is; alsdan moet zowel aan het Cbp als aan DNB of de AFM worden gemeld. Informatie verkregen van de financiële sector leert echter dat er in de afgelopen twee jaar een tiental incidenten is gemeld. Als we zouden aannemen dat al deze incidenten tevens datalekken zijn, gaat het dus slechts om een vijftal dubbele meldingen per jaar. Daarbij kan nog worden opgemerkt dat deze dubbele meldingen te rechtvaardigen zijn vanuit de verschillende doelen van de betreffende meldplichten. Het doel van de plicht om datalekken te melden aan het Cbp is om een grotere transparantie bij de verwerking van persoonsgegevens te bewerkstelligen, om ruimere aandacht te genereren voor de noodzaak om goed te investeren in beveiligingsmaatregelen en om op den duur toename van het vertrouwen van de samenleving in de geautomatiseerde verwerking van persoonsgegevens te bewerkstelligen. Het doel van de plicht om incidenten te melden aan DNB of de AFM is om de integere uitoefening van het bedrijf van de desbetreffende financiële onderneming

[2] *Incident:* gedraging of gebeurtenis die een ernstig gevaar vormt voor de integere uitoefening van het bedrijf van de desbetreffende financiële onderneming (artikel 1 van het Besluit prudentiële regels Wft en artikel 1 van het Besluit Gedragstoezicht financiële ondernemingen Wft).

te bewaken, waarborgen of herstellen. Het is derhalve belangrijk dat de financiële toezichthouders in kennis worden gesteld van alle incidenten en het Cbp van alle onder de meldplicht vallende datalekken, ook al leidt dat in een enkel geval tot een dubbele meldplicht voor financiële ondernemingen.

4.3 Verhouding tot het strafrecht

In het geval van een datalek kan er een vermoeden zijn van strafbaar handelen. Zo is bijvoorbeeld hacken strafbaar gesteld in artikel 138ab van het Wetboek van Strafrecht. Wanneer er aanwijzingen voor hacken zijn, dan is er ook alle aanleiding om daarvan aangifte te doen bij de politie. Het is niet uitgesloten dat het strafrechtelijk onderzoek aanleiding geeft tot het treffen van opsporingshandelingen als het bewaren van materiaal of het stilleggen van een verwerking. Het belang van het strafrechtelijk onderzoek kan vergen dat een door de verdachte gevolgde unieke werkwijze niet publiekelijk bekend wordt gemaakt, omdat dit het onderzoek zou hinderen.
Ook daarom is in het voorgestelde artikel 34a van de Wbp en in artikel 11.3a van de Tw verzekerd dat de kennisgeving aan het Cbp verschilt van de melding aan de betrokkenen, en dat eerstgenoemde kennisgeving zo nodig ook geheel of gedeeltelijk vertrouwelijk kan worden gedaan. Het initiatief daarvoor ligt primair bij de verantwoordelijke. Het kan noodzakelijk zijn dat het Cbp en het openbaar ministerie overleg plegen over hun reacties.

5. Sanctionering

Het wetsvoorstel voorziet in een stevige bestuurlijke boete voor het nalaten te voldoen aan de meldplicht. Hoewel de voorwaarden waaronder de meldplicht moet worden nagekomen in concreto de nodige beoordeling door het Cbp vergt, blijft het na deze beoordeling een betrekkelijk eenvoudige beoordeling of de meldplicht is nagekomen. In zoverre valt de meldplicht aan te merken als een administratieve verplichting waaraan moet worden voldaan. Het past bij het bestaande stelsel van de Wbp om de overtreding van administratieve verplichtingen en verplichtingen waarvan de handhaving kan plaatsvinden zonder de noodzaak van een gedetailleerde nadere invulling van de onderliggende materiële normen door de toezichthouder, te sanctioneren met een bestuurlijke boete.

Voorgesteld wordt een maximumboete van € 450.000,= (artikel I, onderdeel D en artikel II, onderdeel E). Dit is een hoog bedrag in verhouding tot de huidige boetemaxima in de Wbp. Dit hoge maximum weerspiegelt het belang dat moet worden gehecht aan het geven van transparantie bij de doorbreking van beveiligingsmaatregelen en het verlies aan vertrouwen dat het gevolg kan zijn van het nalaten van het treffen van de nodige maatregelen. Mede naar aanleiding van de adviezen van het Cbp en de OPTA is besloten het boeteniveau zoveel mogelijk in overeenstemming te brengen met het boeteniveau van de Tw. Het voorstel voor een EU-verordening algemene gegevensbescherming kent overigens een aanzienlijk hoger boetemaximum voor hetzelfde vergrijp.
Naast de bevoegdheden die het Cbp heeft op basis van de Wbp zijn in het wetsvoorstel wijzigingen in de Tw opgenomen die de Cbp soortgelijke bevoegdheden verschaffen bij het toezicht op de naleving en de handhaving van artikel 11.3a van de Tw.
Voorgesteld wordt om ook het niet naleven van de medewerkingsplicht van artikel 5:20 van Algemene wet bestuursrecht te bedreigen met eenzelfde boete als in de Tw. Dit betreft dan ook het niet naleven van de medewerkingsplicht in gevallen van onderzoek naar andere overtredingen dan artikel 34a van de Wbp.

In veel ontvangen zienswijzen, met name uit de internetconsultatie, en in de adviezen van het Cbp en het NGFG is erop aangedrongen ook de overtreding van artikel 13 Wbp – de beveiligingsverplichting – te sanctioneren. Dit alternatief is nadrukkelijk overwogen. Het heeft als voordeel dat beveiliging als aspect van de bescherming van persoonsgegevens integraal wordt aanpakt. Daar staat echter tegenover dat artikel 13 van de Wbp een algemeen-abstract geformuleerde norm is. De handhaving van dergelijke normen vraagt afzonderlijke aandacht uit hoofde van artikel 7 van het Europees Verdrag ter bescherming van de rechten van de mens en de fundamentele vrijheden, vooral op het punt van het lex certa beginsel en de kwestie van de voorzienbaarheid van overtredingen. Dit raakt niet alleen artikel 13 van de Wbp, maar feitelijk de hele vraag naar de verbreding van de handhaving van de materiële normen van de Wbp. In dat verband wijzen wij op het in het regeerakkoord van het kabinet-Rutte II van 29 oktober 2012 aangekondigde voornemen om te komen tot uitbreiding van de bevoegdheid van het Cbp om bestuurlijke boetes op te leggen met het oog op de versterking van de handhaving van de normen van de Wbp (vgl. ook de motie van het lid Recourt, Kamerstukken II 2011/12, 32 761, nr. 22). De Staatssecretaris van Veiligheid en Justitie en de Minister van Binnenlandse Zaken zullen bij nota van wijziging op het onderhavige wetsvoorstel voorzien in een regeling die strekt tot uitbreiding van de bestuurlijke bevoegdheden van het Cbp.

6. Rechtsbescherming

De toedeling van de meldplicht op grond van twee wetten aan één bestuursorgaan, het Cbp, heeft ook gevolgen voor de rechtsbescherming tegen de door het Cbp vastgestelde sanctiebesluiten. Immers, tegen besluiten van het Cbp staat op grond van de Wbp beroep op de rechtbank en hoger beroep op de Afdeling bestuursrechtspraak van de Raad van State open. Tegen besluiten die op grond van de handhavingsbevoegdheden van de Tw worden vastgesteld, staat in eerste aanleg beroep open op de rechtbank te Rotterdam, en hoger beroep bij het College van Beroep voor het bedrijfsleven. Waar er sprake is van een meldplicht bij één bestuursorgaan, ligt het voor de hand om ook de rechtsbescherming tegen sanctiebesluiten voortvloeiend uit het niet naleven van de meldplicht te uniformeren, en daarvoor aansluiting te zoeken bij het stelsel van de Wbp. Naast verschillen in de regeling van de rechterlijke bevoegdheid, zijn er ook nog enkele kleine verschillen in regels van procesrechtelijke aard tussen de Wbp en de Tw. Voor wat betreft de regeling van de rechterlijke bevoegdheid is in artikel III van het wetsvoorstel een voorziening getroffen die ertoe strekt dat voor de meldplichtzaken op grond van de Telecommunicatiewet de rechtsgang van de Wbp geldt (rechtbank, Afdeling bestuursrechtspraak van de Raad van State). Naar aanleiding van het advies van de Afdeling advisering van de Raad van State is voor de regels van procesrechtelijke aard meer aansluiting gezocht bij de Telecommunicatiewet. Voorgesteld wordt om artikel 71 van de Wbp te laten aansluiten bij het huidige artikel 15.12 Tw zodat tegen besluiten van het Cbp waarbij een bestuurlijke boete wordt opgelegd ter zake van een meldplicht datalekken (artikel 34a Wbp/artikel 11.3 Tw) niet alleen het maken van bezwaar maar ook het instellen van beroep schorsende werking heeft (artikel I, onderdeel E). Het toekennen van schorsende werking aan het aanhangig maken van een executiegeschil (vgl. artikel 15.14 Tw), wordt niet gevolgd in de Wbp, aangezien dit een afwijking betekent van artikel 4:116 Awb waarvoor wij geen goede reden aanwezig achten.

7. Verhouding tot het geldend Europees recht, notificatie

Richtlijn 95/46/EG bevat geen regeling van de meldplicht voor datalekken. Wel bevat artikel 4, derde lid, van richtlijn 2002/58/EG een meldplicht voor datalekken. Die meldplicht geldt echter alleen voor de aanbieders van openbare elektronische communicatiediensten. Voor een meldplicht voor datalekken die zich richt tot elke verantwoordelijke bestaat geen verplichting. Aangezien het opleggen van een dergelijke verplichting aan een ruimere kring van verantwoordelijken dan die genoemd is in richtlijn 2002/58/EG, betreft het hier een vaststelling van een voorschrift van nationaal recht. Dit voorschrift moet worden aangemerkt als het vaststellen van een regeling met betrekking tot diensten van de informatiemaatschappij in de zin van artikel 1 van *richtlijn 98/34/EG van het Europees Parlement en de Raad van 22 juni 1998 betreffende een informatieprocedure op het gebied van normen en technische voorschriften (PbEG L 204), zoals gewijzigd bij richtlijn 98/48/EG van het Europees Parlement en de Raad van 20 juli 1998 (PbEG L 217)*.
Dit voorschrift is echter gerechtvaardigd. Een regeling voor de meldplicht van datalekken is een dwingende eis van algemeen belang. De Europese Unie erkent de bescherming van persoonsgegevens als een fundamenteel recht. Dat blijkt uit artikel 8 van het Handvest voor de Grondrechten, artikel 16 van het Verdrag betreffende de werking van de Europese Unie, richtlijn 95/46/EG en richtlijn 2002/58/EG. Het voorschrift is vastgesteld met de bedoeling de betrokkene beter te informeren over belangrijke risico's waaraan zijn persoonsgegevens zijn blootgesteld. Het beoogt tevens gegevens die als gevolg van een verwezenlijking van die risico's in strijd met richtlijn 95/46/EG kunnen worden verwerkt tegen te gaan. Het voorschrift dient daarmee tevens de bescherming van de consument. Het voorschrift voldoet aan de eisen van proportionaliteit, aangezien het zoveel mogelijk vormgegeven is conform de eisen die in artikel 4 van de richtlijn 2002/58/EG, het overigens voldoende ruimte laat om meldingen van gering belang achterwege te laten en voorziet in specifiek toezicht van het Cbp. Met een minder vergaande eis kan in dit geval niet worden volstaan, omdat het achterwege laten van een meldplicht het gevaar oplevert dat de belangen van de betrokkene onvoldoende worden behartigd, en een beperking van de meldplicht tot alleen bepaalde typen van verwerkingen mogelijk discriminatoire effecten heeft. Het voorschrift wordt verder wordt zonder onderscheid toegepast op alle verantwoordelijken in de zin van de Wbp.
Overeenkomstig artikel 8 van laatstgenoemde richtlijn is dit wetsvoorstel aan de Europese Commissie genotificeerd.
Afhankelijk van de omstandigheden zal de verantwoordelijke als een dienstverrichter in de zin van artikel 4 van *richtlijn 2006/123/EG van het Europees Parlement en de Raad van 12 december 2006 betreffende diensten op de interne markt (PbEU L 376)* (hierna: Dienstenrichtlijn) kunnen worden aangemerkt. Voor die gevallen geldt dat een meldplicht voor datalekken als een afwijking van het vrij verkeer van diensten kan worden aangemerkt, aangezien de dienstverrichter wordt onderworpen aan een voorschrift van nationale oorsprong dat van invloed is op de wijze van dienstverrichting.
Dit voorschrift is echter gerechtvaardigd in de zin van artikel 16, eerste lid, van de Dienstenrichtlijn. Het voorschrift wordt verder wordt zonder onderscheid toegepast op alle verantwoordelijken in de zin van de Wbp, en zijn ook de uitzonderingen op de verplichting algemeen geformuleerd. Het discriminatieverbod van artikel 16, eerste lid, onder a, van de Dienstenrichtlijn wordt gerespecteerd. Een regeling voor de meldplicht van datalekken is een dwingende eis van algemeen belang die gerechtvaardigd is om redenen van openbare orde. De Europese Unie erkent de bescherming van persoonsgegevens als een fundamenteel recht. Dat blijkt uit artikel 8 van het Handvest voor de Grondrechten, artikel 16 van

het Verdrag betreffende de werking van de Europese Unie, richtlijn 95/46/EG en richtlijn 2002/58/EG. Dat blijkt bovendien uit artikel 17, derde lid, van de Dienstenrichtlijn. Het voorschrift is vastgesteld met de bedoeling de betrokkene beter te informeren over belangrijke risico's waaraan zijn persoonsgegevens zijn blootgesteld. Het beoogt tevens gegevens die als gevolg van een verwezenlijking van die risico's in strijd met richtlijn 95/46/EG kunnen worden verwerkt tegen te gaan. Daarmee wordt de fundamentele waarde van de bescherming van persoonsgegevens gediend. Die fundamentele waarde kan geacht worden deel uit te maken van de openbare orde als bedoeld in artikel 16, eerste lid, onder b, van de Dienstenrichtlijn.
Het voorschrift voldoet aan de eisen van evenredigheid als bedoeld in artikel 16, eerste lid, onder c, van de Dienstenrichtlijn. Het voorstel is zoveel mogelijk vormgegeven conform de eisen die in artikel 4 van de richtlijn 2002/58/EG zijn gesteld, het laat overigens voldoende ruimte om meldingen van gering belang achterwege te laten en voorziet in specifiek toezicht van het Cbp. Met een minder vergaande eis kan in dit geval niet worden volstaan, omdat het achterwege laten van een meldplicht het gevaar oplevert dat de belangen van de betrokkene onvoldoende worden behartigd, en een beperking van de meldplicht tot alleen bepaalde typen van verwerkingen mogelijk discriminatoire effecten heeft.
Overeenkomstig artikel 15, zevende lid, van de Dienstenrichtlijn is dit wetsvoorstel aan de Europese Commissie genotificeerd.

Notificatieprocedure

Het conceptvoorstel is van wet is ingevolge richtlijn 98/34/EG van het Europees Parlement en de Raad van 22 juni 1998 betreffende een informatieprocedure op het gebied van normen en technische voorschriften (PbEG L 204), zoals gewijzigd bij richtlijn 98/48/EG van het Europees Parlement en de Raad van 20 juli 1998 (PbEG L 217) alsmede ingevolge richtlijn 2006/123/EG van het Europees Parlement en de Raad van 12 december 2006 betreffende diensten op de interne markt (PbEU L 376) voorgelegd aan de Europese Commissie. Er zijn geen reacties ontvangen.

8. Administratieve lasten, nalevingskosten, bestuurlijke lasten, effecten voor de rechtspraak en financiële effecten

8.1 Administratieve lasten en nalevingskosten

De meldplicht voor de doorbrekingen van beveiligingsmaatregelen brengt zowel nalevingskosten als administratieve lasten teweeg. Er moet immers zowel aan betrokkenen, als aan de overheid worden gemeld. Het betreft een geheel nieuwe verplichting. Er is dus geen ervaring beschikbaar waarop kan worden teruggegrepen. Gewerkt moet worden met aannames. Die aannames verschillen deels van de aannames die zijn gebruikt bij de wijziging van de Telecommunicatiewet die in paragraaf 4.1 van deze memorie is genoemd. Enerzijds is de kring van verantwoordelijken veel groter dan de kring van bedrijven die bij de ACM zijn ingeschreven. Anderzijds bevat het voorgestelde artikel 34a van de Wbp een voorziening om nodeloze meldingen en bagatelzaken van de meldplicht uit te sluiten.
Aangenomen wordt dat een melding € 16,60 aan nalevingskosten oplevert (een melding aan betrokkenen en het bijhouden van een protocol, elk gewaardeerd op € 8,30), en € 8,30 aan administratieve lasten (melding aan het Cbp). Die bedragen zijn gebaseerd op een uurtarief van € 50,= en een last per geval van 10 minuten. Laatstbedoeld gegeven ligt ten grondslag aan het evenbedoelde wetsvoorstel tot wijziging van de Tw (Kamerstukken II 2010/11, 32 549, nr. 3, blz. 26–27). Deze gegevens kunnen

zonder bezwaar worden geëxtrapoleerd naar de Wbp. De meldplichten verschillen inhoudelijk immers niet.
In een onderzoek van EIM getiteld «Administratieve lasten in het privacydomein, Reductievoorstellen nader bekeken» (Zoetermeer, september 2006) – welk onderzoek mede ten grondslag ligt aan de wet van 26 januari 2012 *wijziging van de Wet bescherming persoonsgegevens in verband met de vermindering van administratieve lasten en nalevingskosten, wijzigingen teneinde wetstechnische gebreken te herstellen en enige andere wijzigingen* (Stb. 33) – is een schatting gemaakt van het aantal bedrijven en overheidsinstellingen dat onder de werking van de Wbp valt. Dat aantal is in het onderzoek vastgesteld op 132.000. Aantekening daarbij verdient dat in Nederland mede als gevolg van een ruimhartig regime voor de vrijstelling van de verplichting om gegevensverwerkingen bij het Cbp aan te melden geen sluitend overzicht bestaat van het aantal bedrijven dat valt onder de reikwijdte van de Wbp. Op dat aantal moet het aantal bedrijven in mindering worden gebracht dat reeds is onderworpen aan de meldplichten op grond van de Tw en de Wft. De meest recente cijfers, gepubliceerd door de ACM, de Autoriteit Financiële Markten en De Nederlandsche Bank over het aantal ondernemingen dat aan het toezicht van deze instellingen is onderworpen geeft het volgende beeld. Bij de ACM staan ongeveer 1000 ondernemingen ingeschreven als aanbieder van een openbaar elektronisch communicatienetwerk of openbare elektronische communicatiedienst. Bij de Autoriteit Financiële Markten staan ongeveer 26.500 ondernemingen in zeer uiteenlopende categorieën ingeschreven. Bij De Nederlandsche Bank gaat het om ongeveer 800 ingeschreven ondernemingen. In totaal betreft het dus 28.300 ondernemingen, zodat de meldplichten op grond dit wetsvoorstel betrekking hebben op ongeveer 131.000 ondernemingen en instellingen waar het de melding aan het Cbp betreft en ongeveer 103.700 ondernemingen en instellingen waar het de meldplicht aan de betrokkenen betreft. Het is onmogelijk om op voorhand volledig betrouwbaar te voorspellen in welke gevallen aan de meldplicht uit dit wetsvoorstel gevolg zal moeten worden gegeven. Het gaat niet om de omvang van bedrijven, maar om de grootte van het risico van elke verwerking. Evenmin valt op voorhand te bezien hoe de bagatelregeling zal uitvallen. Wel bestaat het beeld dat datalekken ook in Nederland regelmatig voorkomen. In dit wetsvoorstel wordt daarom aangenomen wordt dat 50% van het aantal ondernemingen jaarlijks een melding zal moeten doen.
Uitgewerkt voor de administratieve lasten (de melding aan het Cbp) levert dit op dat 50% van 131.500 ondernemingen (namelijk 132.500, verminderd met 1000 ondernemingen die reeds onder de Tw vallen) jaarlijks een melding doet aan het Cbp. Dit levert € 543.650,= jaarlijks aan administratieve lasten op.
Uitgewerkt voor de nalevingskosten, gemoeid met het doen van een melding aan de betrokkene levert dit op dat 50% van 103.700 ondernemingen (namelijk 132.000, verminderd met 1000 ondernemingen die onder de Tw vallen, en 27.300 die onder de Wft vallen) jaarlijks een melding doet. Dit levert € 430.355,= jaarlijks aan nalevingskosten op.
Uitgewerkt voor de nalevingskosten, gemoeid met het bijhouden van een protocol levert dit op dat 50% van 131.500 ondernemingen (namelijk 132.000 verminderd met 1000 ondernemingen die reeds onder de Tw vallen) een protocolbijwerking moet doen. Dit levert € 543.650,= jaarlijks aan nalevingskosten op. De totale jaarlijkse nalevingskosten worden geraamd op € 974.005,=.

Op dit wetsvoorstel is een voorafgaande toets door het Adviescollege toetsing administratieve lasten (Actal) verricht. Actal heeft in zijn advies van 9 februari 2012 (JtH/FvK/2012/05) een aantal aandachtspunten meegegeven. Allereerst vraagt Actal hoe de stijging van de administratieve lasten en nalevingskosten van dit wetsvoorstel wordt gecompen-

seerd. De lastenstijging die uit dit wetsvoorstel voortvloeit zal moeten worden gecompenseerd in het totaal van toe- en afname van lasten waarvoor het ministerie van Veiligheid en Justitie verantwoordelijk is. Op deze plaats kan niet exact worden aangegeven hoe dat gebeurt. Dat zal via de gebruikelijke rapportages plaatsvinden. Actal verzoekt verder de administratieve lasten gemoeid met de protocolplicht in kaart te brengen. VNO/NCW- MKB Nederland, het Cbp en ICT Office dringen daar ook op aan. Die berekening is hierboven weergegeven.
Actal vraagt tenslotte aandacht voor de noodzaak te kiezen voor het voor de sector minst belastende alternatief. Deze keuze heeft nadrukkelijk de aandacht gehad bij de vormgeving van het wetsvoorstel. Het heeft ertoe geleid dat in een wetsvoorstel een voorziening is getroffen die ertoe moet leiden dat inbreuken met een relatief minder belangrijk effect niet hoeven te worden gemeld.

8.2 Bestuurlijke lasten en effecten voor de rechtspraak

Dit wetsvoorstel leidt voor het Cbp tot enkele nieuwe bestuurlijke lasten. De meldplicht bij doorbrekingen van beveiligingsverplichtingen leidt, naar thans wordt geschat tot 66.000 meldingen per jaar. Verwacht mag worden dat het overgrote deel van deze meldingen het Cbp geen enkele aanleiding geeft tot een onderzoek of tot handhavingsmaatregelen. Dat betekent niet dat het Cbp niet meer zal doen dan van de melding kennisnemen en deze gedurende een bepaalde periode zal bewaren. Het Cbp zal deze meldingen moeten beoordelen en een inschatting moeten maken of er aanleiding is een onderzoek in te stellen. Een onderzoek kan leiden tot de oplegging van handhavingsmaatregelen. Het ligt voor de hand dat de handhaving van artikel 13 Wbp daarbij aandacht krijgt. Ook is het evident dat factoren als de omvang van het datalek, de potentiële gevolgen ervan en de aard van de gegevens daarbij betrokken worden. Het Cbp stelt echter de eigen prioriteiten vast. Het valt nog niet te voorzien in hoeveel gevallen de meldingen aanleiding geven tot verdere actie. Aangezien het wetsvoorstel tot wijziging van de Tw naar verwachting veel eerder in werking treedt dan het onderhavige voorstel, zal er eerst een situatie ontstaan waarin de ACM als enig bevoegd bestuursorgaan meldingen in ontvangst neemt, deze beoordeelt en waar nodig interveniëert. Bij inwerkingtreding van dit wetsvoorstel valt deze taak toe aan het Cbp. Hoewel veel praktische gevolgen op informele wijze tussen Cbp en ACM geregeld kunnen worden, bijvoorbeeld in een convenant, is het raadzaam voor eventuele rechtsgeschillen naar aanleiding van opgelegde boetes een overgangsbepaling op te nemen.
De consequenties van het wetsvoorstel voor de organisatie van het Cbp zijn dan ook nog niet goed in kaart te brengen. Zoals volgt uit de meergenoemde brief van de eerste ondergetekende aan de voorzitter van de Tweede Kamer der Staten-Generaal van 27 oktober 2011, zullen de eventuele veranderingen in de werklast van het Cbp als gevolg van de introductie van de meldplicht eerst feitelijk moeten worden vastgesteld, voordat een beslissing kan worden genomen over de gevolgen die aan die vaststelling moet worden verbonden. Zie in dat verband ook de brief van de eerste ondergetekende aan de voorzitter van de Tweede Kamer der Staten-Generaal van 15 april 2013 over de wijze waarop invulling wordt gegeven aan de motie van het lid Schouw inzake de bekostiging van het Cbp nu en in de toekomst (Kamerstukken II 2012/13, 30 400 VI, nrs. 100 en 71).
Het valt uiteraard niet uit te sluiten dat de handhaving van de meldplicht aanleiding geeft tot het opleggen van een sanctie. Een bestuurlijke boete lijkt dan het meest voor de hand liggende middel te zijn. Het Cbp is onafhankelijk, en bepaalt zijn eigen handhavingsbeleid. Niettemin kan ervan worden uitgegaan dat het Cbp na inwerkingtreding van dit wetsvoorstel de praktijk wel enige gelegenheid gunt aan de nieuwe

verplichting te wennen, en dat ook het Cbp zich na inwerkingtreding eerst concentreert op de goede gang van zaken bij de afwikkeling van de meldplicht, het beoordelen van meldingen en het plegen van informele interventies bij verantwoordelijken als daar aanleiding toe is. Verder mag van het Cbp worden verwacht dat het beleidsregels vaststelt omtrent de hoogte en de berekening van de boetes (boetetoemetingsbeleid). Vooralsnog wordt rekening gehouden met tien boetebesluiten per jaar. Een boetebesluit is doorgaans altijd voorwerp van bezwaar en beroep. Er moet dus rekening worden gehouden met een belasting van de rechtspraak met tien zaken per jaar.
De mogelijke aanvullende belasting van de overheid die voortvloeit uit de omstandigheid dat bestuursorganen in hun rol als verantwoordelijke meldingen moeten doen worden niet als bestuurlijke last aangemerkt. Dezelfde lasten rusten in gelijke mate op burgers en bedrijven.

8.3 Positie van rijksoverheid

De Wbp maakt geen onderscheid in verantwoordelijken die tot de publieke sector of de private sector behoren. Op alle verantwoordelijken rusten dezelfde verplichtingen. De rijksoverheid is daarom in beginsel onderworpen aan de meldplicht op grond van het voorgestelde artikel 34a van de Wbp.
Niettemin is er reden afzonderlijk stil te staan bij de positie van de rijksoverheid. Allereerst geldt dat niet de gehele rijksoverheid onderworpen is aan de Wbp. De gegevenshuishouding van de inlichtingen- en veiligheidsdiensten wordt beheerst door een afzonderlijke wettelijke regeling (Wet op de inlichtingen- en veiligheidsdiensten 2002). De gegevenshuishouding van de politie, de Koninklijke marechaussee en de bijzondere opsporingsdiensten wordt beheerst door de Wet politiegegevens. Voor de Justitiële Informatiedienst van het Ministerie van Veiligheid en Justitie en het openbaar ministerie geldt de Wet justitiële en strafvorderlijke gegevens. De meldplicht geldt dus niet voor deze onderdelen van de rijksoverheid. Zoals in paragraaf 2.3 van deze memorie is vermeld, bevat de ontwerprichtlijn voor de bescherming van persoonsgegevens in de sectoren politie en justitie een afzonderlijke meldplicht voor datalekken in die sectoren. Voor de nationale veiligheidssector zal een en ander afhangen van de herziening van het Dataprotectieverdrag van de Raad van Europa. Uitgangspunt bij de onderhandelingen is dat meldplichten voor deze sectoren op geen enkele wijze direct of indirect zouden moeten leiden tot het geven van inzicht in informatie- en kennisniveaus van deze organisaties. Dat is onverenigbaar met de onderzoeksbelangen die de desbetreffende diensten hebben.
De desbetreffende wetten voorzien overigens in een zeer behoorlijk niveau van gegevensbescherming, juist waar het de rechten van betrokkenen aangaat.
Voor zover de rijksoverheid wel onder het wetsvoorstel valt, verdient het de aandacht dat op rijksniveau een relatief groot aantal grote gegevensverwerkingen worden beheerd. Het ligt voor de hand dat de uitvoering van de meldplicht bij het Rijk op gecoördineerde wijze plaatsvindt. De Rijks-CIO (Chief Information Officer) en de CIO's van de ministeries zullen daartoe uitvoeringsbeleid gaan vaststellen.

8.4 Gevolgen voor de rijksbegroting

Het wetsvoorstel heeft geen gevolgen voor de Rijksbegroting. Hoewel de meldplicht datalekken naar schatting zal leiden tot een aanzienlijk aantal meldingen per jaar, mag verwacht worden dat het overgrote deel van deze meldingen het Cbp geen aanleiding geeft tot een onderzoek of tot handhavingsmaatregelen. Van het Cbp mag worden verwacht dat het een risicogestuurde aanpak hanteert, waarbij prioriteit wordt gelegd bij de

aanpak van overtredingen van de Wbp waarbij sprake is van specifieke risico's voor de bescherming van persoonsgegevens. Het Cbp is onafhankelijk en beslist uiteraard zelf welke zaken het oppakt. Na inwerkingtreding van het wetsvoorstel zullen de veranderingen in de werklast voor het Cbp die de meldplicht datalekken met zich meebrengt worden gemonitord. Er kan dan op basis van objectieve cijfers een verantwoorde beslissing worden genomen over eventuele gevolgen voor de formatie en begroting van het Cbp. Indien geconstateerd wordt dat extra financiering nodig is, zal hier voor binnen de begroting van het Ministerie van Veiligheid en Justitie dekking worden gevonden.

9. Advies en consultatie[3]

Het wetsvoorstel zoals dat voor advies is voorgelegd en in internetconsultatie is geweest bestond oorspronkelijk uit twee hoofdonderdelen. Het ene onderdeel zag op de verruiming van de mogelijkheid van het gebruik van camerabeelden van strafbare feiten ten behoeve van de ondersteuning van de rechtshandhaving, het andere onderdeel op de invoering van de meldplicht datalekken. Mede op advies van de Afdeling advisering van de Raad van State is het wetsvoorstel gesplitst en bevat het huidige voorstel alleen de invoering van de meldplicht datalekken.
Het wetsvoorstel is in zijn oorspronkelijke vorm voor advies voorgelegd aan het Cbp. Daarnaast zijn in een consultatie de volgende organisaties in de gelegenheid gesteld een zienswijze te geven: de Raad voor de rechtspraak, de Nederlandse Vereniging voor Rechtspraak, het College van procureurs-generaal, de Nederlandse Orde van Advocaten, de OPTA, het Agentschap Telecom, DNB, de AFM, VNO/NCW-MKB Nederland, ICT Office, de Nederlandse Vereniging van Banken, het Nederlands Genootschap van Functionarissen voor de Gegevensbescherming, Bits of Freedom en de FNV. Behoudens van de Raad voor de rechtspraak is van al deze instanties een reactie ontvangen. Van het Verbond van Verzekeraars is een spontane reactie ontvangen.

9.1 Reacties op ontvangen zienswijzen en adviezen

In de ingewonnen adviezen en zienswijzen, met name die van VNO/NCW-MKB Nederland, ICT Office en Bits of Fredholm is gevraagd naar mogelijke meer concreet omschreven doelen van de meldplicht. Die zijn er ook. De meldingen dienen ook ter bescherming van de concrete belangen van betrokkenen. Wanneer er duidelijke aanwijzingen bestaan dat er persoonsgegevens gelekt zijn met behulp waarvan het mogelijk is identiteitsfraude te plegen, kan de verantwoordelijke in zijn melding aan betrokkenen aangeven wat de betrokkene daar zelf tegen kan ondernemen, en welke maatregelen de verantwoordelijke heeft getroffen om dat risico te beheersen. Zijn er creditcardgegevens gelekt, dan ligt het voor de hand dat de betrokkene attent wordt gemaakt op de mogelijkheid zijn creditcard te laten blokkeren door de uitgevende instantie. Na een hack bij een provider voor e-mailservices kan in de melding aan de betrokkene wordt geadviseerd het wachtwoord te wijzigen.
Tegelijk moet met VNO/NCW-MKB Nederland en ICT Office worden erkend dat een 100% veilige informatiemaatschappij niet bestaat, en dat het wetsvoorstel daarin geen verandering brengt. Dat is echter geen reden de voorgestelde maatregelen dan maar achterwege te laten. Wanneer de wetgever redelijke maatregelen kan treffen om de veiligheid van de informatiemaatschappij te verhogen, moet dit niet worden nagelaten. Het is inderdaad zo dat de voorgestelde maatregelen leiden tot een verzwaring van de lasten van verantwoordelijken. Die lasten liggen zeker

[3] De ontvangen adviezen en reacties zijn ter inzage gelegd bij het Centraal Informatiepunt Tweede Kamer

niet alleen bij het bedrijfsleven. Ook de overheid beschikt over een groot aantal zeer omvangrijke en gevoelige verwerkingen van persoonsgegevens. Te denken valt aan die van de Belastingdienst, de uitvoeringsorganen van de sociale zekerheid en de gemeentelijke basisadministratie persoonsgegevens. Beveiligingslekken in deze verwerkingen kunnen zeer grote gevolgen hebben voor betrokkenen.
VNO/NCW-MKB Nederland en ICT Office hebben met het oog op de beheersbaarheid van de lasten voor het bedrijfsleven die aan de meldplicht verbonden zijn aandacht gevraagd voor de ontwikkeling van positieve prikkels voor bedrijven. In hun visie is het effectiever wanneer de wetgever bedrijven die meer inspanningen leveren hun informatiebeveiliging op orde te brengen, beloont, bijvoorbeeld door middel van vrijstellingen of ontheffingen van meldplichten, in plaats van het confronteren van het complete bedrijfsleven met een mogelijk vergaande verplichting. In het wetsvoorstel is erin voorzien dat de verantwoordelijke die technische beschermingsmaatregelen, zoals cryptografie, treft om persoonsgegevens te beveiligen in elk geval is vrijgesteld van de melding aan de betrokkenen. Aan een algehele vrijstelling van de meldplicht zou gedacht kunnen worden wanneer er sprake zou zijn van een algemeen aanvaarde beveiligingsstandaard waarvan het gebruik een zo grote mate van zekerheid biedt voor de beveiliging van persoonsgegevens dat inbreuken of datalekken vrijwel uitgesloten zouden zijn. Dergelijke standaarden bestaan echter niet.
Verwerkingen die zijn onderworpen aan specifieke wetgeving, zoals de Wet politiegegevens of de Wet justitiële en strafvorderlijke gegevens vallen niet onder de meldplicht. Naar aanleiding van de zienswijze van de NOvA kunnen wij aangeven dat mede in het licht van de in voorbereiding zijnde richtlijn zal worden beoordeeld of ook in die wetten een meldplicht voor datalekken moet worden opgenomen.
De overige reacties en opmerkingen worden om doelmatigheidsredenen besproken bij de desbetreffende onderdelen van deze memorie.
Verder is dit wetsvoorstel voorwerp van een internetconsultatie geweest. De internetconsultatie heeft 43 reacties opgeleverd. Die vallen in een aantal categorieën te onderscheiden. In de eerste plaats hebben 9 individuele burgers zelfstandig hun mening over het wetsvoorstel met de overheid gedeeld. Het gaat daarbij om zeer uiteenlopende reacties. Het betreft zowel voorstanders als tegenstanders van beide hoofdonderdelen van het wetsvoorstel. In de tweede plaats hebben 8 burgers gereageerd met een ondersteuning van de zienswijze van Bits of Freedom. In de derde plaats hebben 11 bedrijven, combinaties van bedrijven en adviseurs en advocaten op individuele basis hun zienswijze aan de overheid uitgebracht. Het betreft hier vrijwel uitsluitend reacties op de voorgestelde meldplicht datalekken. Op www.internetconsultatie.nl is het verslag van de consultatie geplaatst.

ARTIKELSGEWIJS

Artikel I, onderdeel A (wijziging artikel 14 Wbp)

Deze wijzigingen zijn in paragraaf 3.3 van het algemeen deel van deze memorie toegelicht.

Artikel I, onderdeel B (artikel 34a)

Eerste en tweede lid (melding aan Cbp en aan betrokkene)

In overeenstemming met het nieuwe artikel 11.3a van de Tw is ervoor gekozen om de verantwoordelijke te verplichten de melding zowel aan het Cbp als aan de betrokkene te doen. In het voorgestelde artikel 34a, eerste en tweede lid, van de Wbp is dat geregeld.

Met de meldplicht aan het Cbp wordt beoogd het toezicht op potentieel ernstige datalekken te ondersteunen. Het Cbp moet door de verantwoordelijke worden geïnformeerd opdat het Cbp kan beoordelen of een onderzoek of het geven van aanwijzingen noodzakelijk is. Het is geen gegeven dat het Cbp iedere melding laat volgen door een onderzoek of andere maatregelen. Of een onderzoek en verdere maatregelen volgen, is afhankelijk van de omstandigheden. Het Cbp zal de ingekomen meldingen moeten bezien en daarop reageren in overeenstemming met de door het college zelf gestelde prioriteiten. Verder geldt dat een verantwoordelijke die handelt op de manier die van hem mag worden verwacht zelf zo spoedig mogelijk de nodige maatregelen treft om het datalek te dichten en herhaling van het voorval tegen te gaan. De verantwoordelijke zal ook bekend maken wat hij onderneemt. Een melding bij het Cbp zal in die gevallen veelal zonder enige reactie blijven. Het ligt overigens in de rede dat het Cbp deze meldingen zelf wel opslaat, mede om daarover, bijvoorbeeld in het jaarverslag, verantwoording over af te leggen. Het NGFG wijst er in zijn zienswijze terecht op dat het voor de hand ligt dat een melding aan het Cbp vergezeld gaat van een melding aan de functionaris voor de gegevensbescherming, indien deze is aangesteld.

Met de meldplicht aan de betrokkene wordt beoogd de betrokkene op de hoogte te stellen van de feitelijke situatie en de consequenties die dat voor zijn belangen heeft. De betrokkene heeft aldus de mogelijkheid nadere informatie te vragen of te beslissen of hij van zijn rechten op inzage, correctie of afscherming gebruik wil maken. Artikel 11.3a, tweede lid, van de Tw bevat bij de meldplicht aan de betrokkene de voorwaarde «indien de inbreuk waarschijnlijk ongunstige gevolgen zal hebben voor diens persoonlijke levenssfeer». Die voorwaarde is ook opgenomen in het voorgestelde artikel 34a, tweede lid, van de Wbp. Uit artikel 34a, eerste lid, van de Wbp volgt voldoende duidelijk onder welke beperkende omstandigheden er een meldplicht bestaat. Door de in artikel 34a, tweede lid, van de Wbp opgenomen verwijzing naar het eerste lid is voldoende duidelijk dat de beperkende omstandigheden uit het eerste lid ook gelden voor de meldplicht uit het tweede lid.
Voor organisaties die een functionaris voor de gegevensbescherming hebben aangesteld, ligt het voor de hand dat de functionaris degene is die belast is met de feitelijke uitvoering van de melding namens de verantwoordelijke. Het ligt evenzeer voor de hand dat het Cbp in de gevallen waarin nader contact met de verantwoordelijke nodig is, zich met de functionaris in verbinding stelt.
De suggestie van Bits of Freedom om elk datalek onder alle omstandigheden ook aan de betrokkene te melden wordt niet gevolgd. Stellig zou dat leiden tot maximale transparantie, maar dat belang moet worden afgewogen tegen het belang van het beheersen van de lasten van de verantwoordelijke. Dat heeft geleid tot bovenvermelde belangenafweging.

Derde lid (inhoud van de melding)

De kennisgeving aan het Cbp en betrokkene omvat in het voorgestelde artikel 34a, derde lid, Wbp een aantal gemeenschappelijke elementen. In elk geval worden steeds de aard van de inbreuk, de instanties waar meer informatie kan worden verkregen en aanbevolen maatregelen om de negatieve gevolgen van de inbreuk te beperken gemeld. Bij vermelding van de aard van de inbreuk zal doorgaans met een algemene omschrijving kunnen worden volstaan. Wanneer de betrokkene wil weten waar hij persoonlijk aan toe is, kan hij contact opnemen met de verantwoordelijke. Die moet daartoe in de kennisgeving contactgegevens opnemen. Organisaties die een functionaris voor de gegevensbescherming hebben aangesteld kunnen overwegen dat contact via de functionaris te laten verlopen, al doet dat niets af aan de verantwoorde-

lijkheid van de verantwoordelijke, zoals het NGFG terecht in haar zienswijze stelt. Verder dient de verantwoordelijke, ter beperking van de schade die door het mogelijke verlies of de onrechtmatige verwerking kan ontstaan, maatregelen bekend te maken die de betrokkene zelf kan of moet nemen. Gedacht kan worden aan het veranderen van gebruikersnamen en wachtwoorden wanneer deze door de inbreuk mogelijk gecompromitteerd zijn. Het staat de verantwoordelijke vrij om meer toe te voegen aan de kennisgeving, maar verplicht is dat niet.
De kennisgeving aan het Cbp omvat meer elementen. In het voorgestelde artikel 34a, vierde lid, van de Wbp moeten aan het Cbp meer gegevens, vooral van technische aard, worden gemeld. Dat stelt het Cbp in staat effectief toezicht uit te oefenen. De aanvullende kennisgeving is echter ook in het belang van de verantwoordelijke. Het kan zijn dat bij de kennisgeving melding moet worden gemaakt van technische details die van vertrouwelijke aard zijn. Van het ongecontroleerd prijsgeven van details over de beveiliging van persoonsgegevens kunnen kwaadwillenden immers profiteren. Bedrijven kunnen deze gegevens desgewenst expliciet als bedrijfsvertrouwelijk in de zin van artikel 10, eerste lid, onder c, van de Wet openbaarheid van bestuur aanmerken. Er is dan sprake van een behoorlijk niveau van bescherming van die informatie. Er is dan ook geen noodzaak over te gaan tot een wettelijke voorziening die deze meldingen principieel steeds als vertrouwelijk aanmerkt, zoals VNO/NCW-MKB Nederland en ICT Office hebben bepleit. Anders dan het Agentschap Telecom adviseert, wordt niet voorzien in een verplichting tot een nadere melding wanneer de oorzaak van het incident is achterhaald en de gebreken zijn verholpen. Of een dergelijke mededeling opportuun is, is aan de betrokken instelling of bedrijf overgelaten.

Vijfde lid (wijze van melden)

Ter beperking van de administratieve lasten en nalevingskosten is bewust gekozen voor een zo eenvoudig mogelijke melding. Wel zijn er enkele minimumeisen opgenomen met betrekking tot de inhoud van de melding. Het voorgestelde artikel 34a, vijfde lid, van de Wbp geeft een in het systeem van de Wbp passende afwegingsplicht mee. De verantwoordelijke moet rekening houden met de aard van de inbreuk en de gevolgen ervan. Daarnaast mag hij rekening houden met de omvang van de kring van de betrokkenen en de kosten van de tenuitvoerlegging. Wanneer de inbreuk zich zou beperken tot een verhoudingsgewijs klein aantal betrokkenen, kan de verantwoordelijke ervoor kiezen hen persoonlijk en gericht te benaderen. Wanneer de inbreuk een groot aantal betrokkene treft, ligt naast de gebruikelijke bekendmaking op een website een advertentie in de dagbladen meer in de rede.
Zonodig kunnen nadere regels worden gesteld voor gebruikmaking van een formulier, of een ander format, bij algemene maatregel van bestuur op grond van artikel 34a, elfde lid, van de Wbp worden voorgeschreven, zoals het Cbp suggereert. Dit formulier zal dan alleen gebruikt worden voor de melding aan het Cbp, niet voor de melding aan de betrokkenen. Het advies van Cbp en de zienswijze van VNO/NCW-MKB Nederland, ICT Office en het NGFG om voor het tijdstip van de melding een gefixeerde tijdslimiet te hanteren wordt niet gevolgd. De maatstaf onverwijld wordt gehandhaafd om de aansluiting bij de Tw te handhaven. Bovendien geeft het de verantwoordelijke enige gelegenheid om onderzoek te doen naar de inbreuk, te overwegen welke maatregelen hij aanbeveelt en de manier waarop hij communiceert met Cbp en betrokkenen.

Zesde lid (uitzonderingen op de meldplicht)

Wanneer de verantwoordelijke de moeite heeft genomen de door hem verwerkte persoonsgegevens zodanig te beveiligen dat het redelijkerwijs

is uitgesloten dat een datalek kan leiden tot kennisname van persoonsgegevens door onbevoegden, kan de kennisgeving aan de betrokkene achterwege worden gelaten. Het voorgestelde artikel 34a, zesde lid, van de Wbp verwijst naar het gebruik van encryptie, maar laat de mogelijkheid open dat andere technieken die een vergelijkbaar beschermingsniveau bieden ook in aanmerking komen. Naar aanleiding van een suggestie van Bits of Freedom merken wij op dat het wetsvoorstel geen maatstaven bevat waaraan de encryptie moet voldoen. Dat past bij het techniekneutrale karakter van de Wbp. Naar aanleiding van het advies van het Cbp en de zienswijzen van VNO/NCW-MKB Nederland en het NGFG is een voorafgaand oordeel van het Cbp over de kwaliteit van de encryptie geschrapt. Zodoende blijft de verantwoordelijke in staat zelf het beveiligingsniveau vorm te geven.
De verantwoordelijke kan zelf in zijn kennisgeving aan het Cbp aangeven dat hij van oordeel is, dat een kennisgeving aan de betrokkene achterwege kan blijven. Echter, bij de beoordelingsruimte die het Cbp krijgt toegekend, past dat het Cbp zonodig expliciet kan verlangen dat de verantwoordelijke toch een kennisgeving aan de betrokkene doet. Deze voorziening is opgenomen in het voorgestelde artikel 34a, zevende lid, van de Wbp.
De meldplicht krachtens het voorgestelde artikel 34a geldt niet, indien de verantwoordelijke in zijn hoedanigheid van aanbieder van een openbare elektronische communicatiedienst op grond van artikel 11.3a, eerste en tweede lid, van de Tw al een kennisgeving heeft gedaan. Deze uitzondering op de meldplicht van artikel 34a van de Wbp geldt niet in situaties waarin de verantwoordelijke een ander is dan de aanbieder van de openbare elektronische communicatiedienst bedoeld in artikel 11.3a van de Tw. In een dergelijk geval is een inbreuk gemaakt op zowel de beveiligingsmaatregelen die de verantwoordelijke moet nemen ter uitvoering van artikel 13 Wbp als op de maatregelen die de aanbieder op grond van artikel 11.3 Tw moet nemen. Dan moeten beide partijen een melding doen op grond van artikel 34a Wbp, respectievelijk 11.3a Tw.

Achtste lid (protocolplicht verantwoordelijke)

Op grond van het voorgestelde artikel 34a, achtste lid, van de Wbp moet de verantwoordelijke een overzicht bijhouden van alle inbreuken. Dat betreft ook de inbreuken die wel zijn geconstateerd, maar niet zijn gemeld, omdat zij naar het oordeel van de verantwoordelijke niet waren aan te merken als meldingsplichtige inbreuken. Het is voor de verantwoordelijke van belang dit protocol goed bij te houden. Mocht de toezichthouder achteraf vragen hebben aan de verantwoordelijke, dan kan de laatste aan de hand van zijn protocol aantonen wat hij heeft geconstateerd en welke maatregelen hij heeft genomen. Verder dienen de gegevens die aan het Cbp zijn verstrekt te worden geregistreerd, alsmede de tekst van de kennisgeving die de verantwoordelijke aan de betrokkene doet. Deze protocolplicht is uitsluitend bedoeld voor de ondersteuning het interne en externe toezicht op de gegevensverwerking. Zo kan bijvoorbeeld achteraf aan de hand van het protocol door de toezichthouder worden beoordeeld of een geconstateerde, maar niet gemelde inbreuk toch had moeten worden gemeld. Het protocol heeft niet de functie van een openbaar register. Het belang bij het vertrouwelijk blijven van details met betrekking tot de beveiliging van de gegevensverwerking en de daarmee gemoeide investeringen staat daaraan in de weg. De aanbeveling van Bits of Freedom om dit protocol juist wel openbaar te maken wordt dan ook niet gevolgd.

Negende lid (samenloopvoorziening Wbp-Tw)

Indien in een inbreukgeval zowel artikel 11.3a van de Tw als artikel 34a van de Wbp in beginsel van toepassing zijn, en de verantwoordelijke dezelfde persoon is als de aanbieder van de elektronische communicatiedienst, hoeft deze uitsluitend op grond van artikel 11.3a van de Tw een melding te doen. In dat geval hoeft hij in zijn hoedanigheid als verantwoordelijke geen melding meer te doen op grond van artikel 34a van de Wbp. Artikel 34a, negende lid, van de Wbp bevat daarvoor een voorziening. Is de verantwoordelijke die op grond van artikel 34a van de Wbp meldingsplichtig is, een ander dan de aanbieder van de elektronische communicatiedienst die op grond van artikel 11.3a van de Tw meldingsplichtig is, bijvoorbeeld omdat die aanbieder de bewerker in de zin van de Wbp is, dan moeten beide partijen voldoen aan hun meldplicht.

Elfde lid (delegatiebepaling)

In het voorgestelde artikel 34a, elfde lid, van de Wbp is de grondslag opgenomen voor een algemene maatregel van bestuur. In die maatregel kunnen nadere regels worden opgenomen met betrekking tot de inhoud en de wijze van kennisgeving. De meldplicht voor datalekken is een nieuwe regeling waarmee nog weinig ervaring bestaat. Wanneer meer ervaring is opgedaan met de nieuwe regeling kan blijken dat er behoefte bestaat aan aanvullende regels over de kennisgeving. Zekerheid bestaat daarover niet, zodat volstaan kan worden met een bevoegdheid tot het stellen van nadere regels. Een vergelijkbare bepaling is opgenomen in artikel 11.3a, zevende lid, van de Tw. Het ligt in de rede dat wanneer de noodzaak tot het vaststellen van deze nadere regels zich aandient, die regels in één algemene maatregel van bestuur worden opgenomen die zijn grondslag vindt in zowel de Wbp als de Tw.

Artikel I, onderdeel C (artikel 51a Wbp)

Het Cbp heeft in de afgelopen jaren samenwerkingsrelaties van uiteenlopende aard ontwikkeld met andere toezichthouders op gebieden waar sprake is van aan elkaar grenzende verantwoordelijkheden. Het toezicht op de naleving op de verwerking van persoonsgegevens speelt immers op velerlei terreinen een rol. Ook op terreinen waarop sectorspecifiek toezicht is ingesteld. Op drie specifieke terreinen heeft dit inmiddels geleid tot het vaststellen van samenwerkingsprotocollen. Het eerste betreft het terrein van de telecommunicatie. Het Cbp heeft samenwerkingsprotocollen met de ACM en met het Agentschap Telecom (AT) van het Ministerie van Economische Zaken, Landbouw en Innovatie. De ACM draagt (mede) zorg voor het toezicht op de naleving van de hoofdstukken 11 en 13 van de Telecommunicatiewet. In die hoofdstukken vinden belangrijke gedeelten van het gegevensbeschermingsrecht voor de telecommunicatiesector regeling. Het AT draagt specifiek zorg voor het toezicht op de naleving van de bepalingen uit de Telecommunicatiewet met betrekking tot de dataretentie. Het tweede terrein betreft de zorg. Het Cbp beschikt ook over samenwerkingsprotocollen met de Nederlandse zorgautoriteit (Nza) en met de Inspectie voor de gezondheidszorg (IGZ). De Nza houdt toezicht op de naleving van de Zorgverzekeringswet en heeft uit den hoofde ook bemoeienis met de verwerking van persoonsgegevens door de zorgverzekeraars. De IGZ houdt toezicht op de naleving van een groot aantal wetten op het gebied van de zorg en komt daar in aanraking met de verwerking van persoonsgegevens door zorgaanbieders. Een derde terrein is het gebied van inkomen en sociale zekerheid. De Inspectie SZW houdt toezicht op de uitvoering van de sociale zekerheidswetgeving en komt daar in aanraking met de verwerking van persoonsgegevens door de uitvoeringsinstanties. Het is zonder meer

voorstelbaar dat in andere sectoren deze samenwerkingsrelaties ook worden ontwikkeld.
Onverminderd de eigen verantwoordelijkheid van elk van de in aanmerking komende toezichthouders is het voor een efficiënt en effectief toezicht op de naleving van belang dat het Cbp en de andere daarvoor in aanmerking komende toezichthouders elkaar zonodig over en weer toezichtgegevens kunnen verstrekken. In de praktijk blijkt dat zich van tijd tot tijd de noodzaak voordoet dat daarbij ook persoonsgegevens moeten worden verstrekt. Daarvoor is in verband met toepassing van de artikelen 7 en 9 van de Wbp een behoorlijke wettelijke grondslag vereist.
In artikel I, onderdeel E, van het wetsvoorstel is daartoe een voorziening getroffen, mede naar aanleiding van het advies van het Cbp. Het nieuwe artikel 51a van de Wbp is gebaseerd op een van de modellen opgenomen in het bij brief van de Minister van Justitie van 29 oktober 2008 aan de Voorzitter van de Tweede Kamer der Staten-Generaal (Kamerstukken II 2008/09, 31 700 VI, nr. 70) gezonden rapport van de Werkgroep herijking toezichtsregelgeving. In verband met de door artikel 28 van de richtlijn gegarandeerde onafhankelijke positie van het Cbp moeten wel enige bijzondere voorzieningen worden getroffen. Er kan geen sprake zijn van een *eenzijdig* op te leggen verplichting – hetzij door de wetgever, hetzij anderszins – tot deze gegevensoverdracht. Dat behoort een zaak van consensus te zijn. Daarom staat in het voorgestelde artikel 51a van de Wbp voorop dat het Cbp bevoegd – dus niet verplicht – is met andere toezichthouders samenwerkingsprotocollen te sluiten. Eerst wanneer aan die voorwaarde is voldaan, kan er sprake zijn van een niet vrijblijvende wederzijdse gegevensverstrekking. Verder ligt het niet voor de hand dat het Cbp dergelijke samenwerkingsprotocollen sluit met bestuursorganen die niet tevens de hoedanigheid hebben van toezichthouder. Dat zou kunnen leiden tot onevenwichtigheden. Het ligt in de bedoeling de gegevensuitwisseling tussen het Cbp en andere instellingen na verloop van tijd – in samenwerking met het Cbp – te bezien om te beoordelen of de samenwerkingsbepaling aan zijn doel beantwoordt.

Artikel II, onderdelen A en B (wijzigingen Telecommunicatiewet)

Met deze wijzigingen in hoofdstuk 11 van de Tw wordt beoogd de verantwoordelijkheid voor het in ontvangst nemen van meldingen op grond van artikel 11.3a Tw bij het Cbp te beleggen.

Artikel II, onderdelen C tot en met F (wijzigingen Telecommunicatiewet)

Het Cbp wordt volgens de systematiek van de Tw belast met het toezicht op de naleving van de bepalingen met betrekking tot de beveiligingsplichten en de meldplicht. Daartoe strekt de wijziging van artikel 15.1 Tw. Daarnaast krijgt het Cbp de bevoegdheid tot oplegging van een last onder bestuursdwang. Dat wordt geregeld in het nieuwe artikel 15.2, vierde lid, Tw. Deze bevoegdheid brengt in het systeem van de Algemene wet bestuursrecht (Awb) van rechtswege de bevoegdheid tot het opleggen van een last onder dwangsom met zich mee. In het nieuwe artikel 15.4, vierde lid, Tw is voorzien in de bevoegdheid van het Cbp tot oplegging van een bestuurlijke boete bij het niet naleven van de meldplicht.
Opmerking verdient dat de Tw een van de Wbp afwijkende reikwijdtebepaling kent. Bepalend voor de bevoegdheid van de Cbp is niet de regeling van artikel 4 van de Wbp, die uitgaat van de vestigingsplaats van de verantwoordelijke, maar het feit of de desbetreffende aanbieder van een openbare elektronische communicatiedienst overeenkomstig de Tw is geregistreerd bij de ACM.

Artikel III (wijziging bijlage 2 van de Awb)

Deze wijzigingen van de bevoegdheidsregeling bestuursrechtspraak (bijlage 2 Awb) strekken ertoe de rechtsbescherming tegen sanctiebesluiten van het Cbp op grond van de artikelen 15.2, vierde lid, en 15.4, vierde lid, van de Tw op te dragen aan de rechtbank en de Afdeling bestuursrechtspraak van de Raad van State.

Artikel IV (overgangsrecht)

Aangezien de Telecommunicatiewet een ander rechtsbeschermingsregime kent dan de Wbp is het noodzakelijk overgangsrecht vast te stellen voor recht om bezwaar te maken of beroep of hoger beroep in te stellen tegen sanctiebesluiten van de ACM terzake van het nalaten te voldoen aan de meldplicht, alsmede voor het procesrecht dat van toepassing is op de behandeling van de geschillen. Artikel IV bevat daarvoor een voorziening.

Deze memorie is opgesteld onder medeverantwoordelijkheid van de Ministers van Binnenlandse Zaken en Koninkrijksrelaties en van Economische Zaken.

De Staatssecretaris van Veiligheid en Justitie,
F. Teeven