Tweede Kamer der Staten-Generaal

2

Vergaderjaar 2013–2014

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. 6

NOTA NAAR AANLEIDING VAN HET VERSLAG

Ontvangen 16 april 2014

1. Strekking van het wetsvoorstel

Ik dank de leden van de fracties van de VVD, PvdA, SP, CDA, PVV en ChristenUnie voor hun reactie op het wetsvoorstel. Het verheugt mij dat de leden van de fracties van de VVD, PvdA, SP, CDA en D66 het belang van het wetsvoorstel onderschrijven. Tegelijkertijd constateer ik dat er over algemene aspecten van de meldplicht (relatie met de beveiligingsplicht, formulering van de meldplicht, voorkomen van nodeloze meldingen) belangrijke vragen bestaan. Alvorens op de in het verslag gestelde vragen in te gaan, hecht ik eraan om op te merken dat ik in het verslag aanleiding heb gezien om de regeling van de meldplicht te verduidelijken en te vereenvoudigen. Deze nota naar aanleiding van het verslag gaat daarom vergezeld van een nota van wijziging, zoals door mij ook is aangekondigd in het Algemeen Overleg over privacy in de digitale samenleving op 12 februari j.l. Beide nota's worden ingediend mede namens de Minister van Binnenlandse Zaken en Koninkrijksrelaties en van Economische Zaken.

Voors hecht ik eraan om enige opmerkingen te maken over de voorgeschiedenis van dit wetsvoorstel, de verhouding tot de bestaande («smalle») meldplicht in de Telecommunicatiewet (hierna: Tw) voor inbreuken in verband met de bescherming van persoonsgegevens die in verband met de levering van openbare elektronische communicatiediensten worden verwerkt, en de EU-verordening algemene bescherming persoonsgegevens waarover in Brussel wordt onderhandeld.

In het regeerakkoord van het kabinet-Rutte I van 30 september 2010 kondigde het kabinet een voorstel aan voor een meldplicht voor alle aanbieders van diensten van de informatiemaatschappij, waaronder de overheid, in geval van verlies, diefstal of misbruik van persoonsgegevens waarbij alle datalekken worden gemeld aan de nationale toezichthouder die boetes kan opleggen indien de meldplicht niet wordt nageleefd. Kort daarna werd het wetsvoorstel ingediend dat leidde tot de invoering van een specifieke meldplicht voor datalekken in de Telecommunicatiewet

kst-33662-6
ISSN 0921 - 7371
's-Gravenhage 2014

voor aanbieders van openbare elektronische communicatiediensten in de Europese Unie (wet tot wijziging van de Telecommunicatiewet ter implementatie van de herziene telecommunicatierichtlijnen, waaronder de e-privacy richtlijn uit 2002, Stb. 2012, 235). Het gaat hierom om persoonsgegevens die in verband met de levering van openbare elekronische communicatiediensten worden verwerkt. Alle inbreuken op de beveiliging met nadelige gevolgen voor de bescherming van de persoonsgegevens, moeten worden gemeld bij de toezichthouder (Autoriteit Consument en Markt). In de gevallen waarin het waarschijnlijk is dat de inbreuk ongunstige gevolgen zal hebben voor de persoonlijke levenssfeer van degene wiens persoonsgegevens zijn blootgesteld aan verlies of onrechtmatige verwerking, dient de inbreuk ook te worden gemeld aan de getroffen abonnee of andere betrokkene[1].Deze meldplicht, die zich tot ongeveer 1000 bij de Autoriteit Consument en Markt geregistreerde aanbieders richt, geldt sinds 5 juni 2012.

Ter uitvoering van het eerdergenoemde regeerakkoord is naast de specifieke meldplicht voor inbreuken op de bescherming van persoonsgegevens op grond van de Telecommunicatiewet, het voorliggende wetsvoorstel ontwikkeld (internetconsultatie eind 2011). De Wbp-meldplicht richt zich tot alle verantwoordelijken voor de verwerking van persoonsgegevens in de private en publieke sector (naar schatting 132.000 bedrijven en overheidsorganisaties). Gelet op de ruime werkingssfeer van de Wbp heeft de regering van meet af aan een clausulering van de meldplicht beoogd. Voorkomen moet worden dat ieder denkbaar datalek aan de toezichthouder (College bescherming persoonsgegevens) en in voorkomend geval ook aan de betrokkene(n) moet worden gemeld. Enerzijds omdat de effectiviteit van de melding daarmee aan betekenis verliest, anderzijds om een nodeloze belasting van bedrijfsleven en overheid te voorkomen. Daar komt bij dat het niet of niet volledig naleven van de meldplicht door het Cbp met een bestuurlijke boete kan worden bestraft. In verband hiermee dient de formulering van de wettelijke verplichting voldoende duidelijk, voorzienbaar en kenbaar te zijn (lex certa-beginsel). Ook daarom is het voor bedrijven en overheden van belang om aan de hand van feiten en omstandigheden van het concrete geval te kunnen beoordelen of een datalek binnen het bereik van de meldingsplicht valt. Het Cbp kan daar middels richtsnoeren een nadere verduidelijking over geven.

In Brussel wordt sinds januari 2012 onderhandeld over een algemene verordening die de huidige EU-privacyrichtlijn uit 1995 zal vervangen. Met de algemene verordening wordt een meer uniform Europees stelsel geschapen van bescherming, toezicht en handhaving op het terrein van de verzameling en verwerking van persoonsgegevens. De meldplicht voor datalekken in de conceptverordening is vergelijkbaar met die in de e-privacyrichtlijn (alle datalekken, hoe gering ook, moeten aan de toezichthouder worden gemeld en daarnaast ook aan de betrokkene(n) indien het datalek waarschijnlijk ongunstige gevolgen heeft voor de persoonlijke levenssfeer van de betrokkene). De algemene verordening zal naar verwachting in 2015 tot stand komen en in werking treden. De conceptverordening kent een implementatietermijn van twee jaar, alvorens deze van toepassing wordt (artikel 91 commissievoorstel). Ter uitvoering van de verordening zal uitvoerings- en aanpassingswetgeving nodig zijn. Tot die tijd (2017) geldt de Wbp. Met de invoering van nationale meldplicht voor datalekken wordt beoogd toe te groeien naar de EU-verordening. Hoe de uiteindelijke verordening eruit zal zien is nog onduidelijk.

[1] Kamerstukken II 2010/11, 32 549, nrs. 3 en 7 (resp. memorie van toelichting en nota n.a.v. verslag).

De leden van de PvdA-fractie menen dat naast het vergroten van vertrouwen in digitale gegevensverwerking, het ook belangrijk is dat er zoveel mogelijk lessen worden getrokken uit opgetreden datalekken. Daarvoor is het belangrijk dat de informatie van het College bescherming persoonsgegevens (Cbp) gedeeld wordt met bijvoorbeeld het Nationaal Cyber Security Centrum en de toezichthouders De Nederlandsche Bank, de Autoriteit Financiële Markten en de Autoriteit Consument en Markt (ACM). Voornoemde leden willen graag meer uitleg van de regering over de wijze waarop de aangemelde datalekken gebruikt worden om lessen te trekken en onveiligheden te bestrijden.
De voorgestelde meldplicht, aan het Cbp als toezichthouder en in voorkomend geval ook aan de betrokkene wiens persoonsgegevens het betreft, draagt bij aan een betere bescherming van persoonsgegevens. Ik onderschrijf dat het belangrijk is om lessen te trekken uit opgetreden datalekken. Immers, indien zich bij een bedrijf of overheidsorganisatie een datalek voordoet, is er iets mis gegaan bij de bescherming van de persoonsgegevens die in het kader van de activiteiten van de betreffende organisatie worden verwerkt. De meldplicht aan het Cbp is ondersteunend aan het toezicht door het Cbp, met name op de beveiligingsplicht van artikel 13 Wbp. Daarnaast zal de melding aan het Cbp ervoor zorgen dat het Cbp meer zicht krijgt op datalekken, op de aard en het ontstaan ervan en het nemen van herstelmaatregelen door verantwoordelijken. De melding aan de betrokkene wiens persoonsgegevens zijn gelekt zal zijn positie versterken omdat het hem een handelingsperspectief biedt. Het Cbp zal de opgedane kennis en ervaringen met het publiek en met andere belanghebbenden kunnen delen, bijv. via jaarverslag of andere publicaties op de website, hetgeen nieuwe datalekken kan voorkomen. Uiteraard kunnen meldingen of signalen over niet gemelde datalekken voor het Cbp aanleiding zijn om handhavingsbevoegdheden jegens verantwoordelijken in te zetten, bijvoorbeeld als blijkt dat het beveiligingsniveau van een bedrijf of overheidsorganisatie ernstig tekort schiet.

Het Cbp kan informatie delen met andere toezichthouders voorzover dat in het belang is van een efficiënt en effectief toezicht op de verwerking van persoonsgegevens. De genoemde toezichthouders houden toezicht op een groot aantal wetten in specifieke sectoren en komen daarbij ook in aanraking met verwerking van persoonsgegevens door bedrijven en instellingen. Het Cbp is bevoegd om toezicht uit te oefenen op de verwerking van persoonsgegevens overeenkomstig het bij of krachtens «de wet» bepaalde (artikel 51, eerste lid, Wbp). Dit impliceert dat het toezicht van het Cbp zich uitstrekt tot alle vormen van verwerking van persoonsgegevens, voor zover de reikwijdtebepalingen van hoofdstuk 1 van de Wbp deze bevoegdheid niet begrenzen. Omdat bevoegdheden en verantwoordelijkheden van toezichthouders op basis van verschillende wetten elkaar onderling kunnen raken, bevatten veel wetten tegenwoordig een grondslag voor samenwerkingsafspraken. Zo wordt met dit wetsvoorstel ook voor het Cbp een bevoegdheid in de Wbp opgenomen om samenwerkingsprotocollen met andere toezichthouders vast te stellen (artikel 51a). Voor de Autoriteit Consument en Markt geldt een wettelijke verplichting om samenwerkingsafspraken met het Cbp te maken (art. 18.3 Tw). Beide organisaties hebben daartoe een samenwerkingsprotocol vastgesteld (zie hierover par. 4.1). Verder heeft de Minister van Economische Zaken op grond van artikel 21 van de Kaderwet zelfstandige bestuursorganen de bevoegdheid om beleidsregels vast te stellen met betrekking tot de taakuitoefening van de ACM. Daarnaast is de informatieverstrekking van de ACM aan het Cbp geregeld in de Regeling gegevensverstrekking ACM van de Minister van Economische Zaken.
Het op structurele basis delen van informatie over datalekken met het Nationaal Cyber Security Centrum, dat een onderdeel is van het Ministerie van Veiligheid en Justitie, ligt niet voor de hand. Het Nationaal Cyber

Security Centrum is geen toezichthouder en heeft binnen de overheid geen specifieke verantwoordelijkheid voor de bescherming van persoonsgegevens.
Of structurele samenwerkingsafspraken met DNB of de AFM van belang zijn is in verband met het toezicht op de verwerking van persoonsgegevens door het Cbp, laat ik graag ter beoordeling aan het Cbp en de andere toezichthouders.

Vooraleerst willen de leden van de fractie van D66 graag weten waarom is gekozen voor de titel «meldplicht datalekken». Deze titel wordt ook in de memorie van toelichting en aanverwante stukken veelvuldig gebruikt, maar de wet gaat eigenlijk over lekken veroorzaakt door doorbroken beveiliging.
De regering deelt de analyse van deze leden. Het gaat om een inbreuk op de beveiliging van de persoonsgegevens tegen verlies of onrechtmatige verwerking. Dit komt ook duidelijk tot uitdrukking in het opschrift van het wetsvoorstel. De aanduiding «meldplicht datalekken» staat tussen haakjes in het opschrift vermeld en betreft niet meer dan een verkorte, enigszins huiselijke aanduiding. Het wetsvoorstel heeft geen officiële citeertitel meegekregen. Een inbreuk op de beveiliging van persoonsgegevens moet ruim worden geduid. Dit betreft alle beveiligingsincidenten waardoor de bescherming van persoonsgegevens op enig moment is doorbroken waardoor de persoonsgegevens zijn blootgesteld aan verlies of onrechtmatige verwerking van persoonsgegevens. Het is daarbij niet van belang of de verantwoordelijke passende technische of organisatorische beschermingsmaatregelen had getroffen of niet. Een datalek kan zich in beide situaties voordoen. Het volstaat dat de verantwoordelijke op de hoogte is geraakt van een incident inzake de beveiliging van persoonsgegevens in zijn organisatie.

Voorts vragen zij waarom er een lange periode zat tussen het advies van de Raad van State bij het wetsvoorstel en de toezending van het wetsvoorstel naar de Kamer.

De periode die is verstreken tussen het uitbrengen van het advies van de Raad van State (14 september 2012) en het indienen van het wetsvoorstel bij de Tweede Kamer (21 juni 2013) laat zich verklaren door de heroverweging die heeft plaatsgehad aan de zijde van de regering, naar aanleiding van het kritische advies van de Afdeling advisering. Deze heroverweging heeft erin geresulteerd dat het wetsvoorstel zoals dat aan de Raad van State is voorgelegd in twee aparte wetsvoorstellen is gesplitst. Het onderhavige wetsvoorstel behelst de meldplicht datalekken. Het tweede wetsvoorstel, dat ziet op een verruiming van het gebruik van private camerabeelden ten behoeve van de opsporing van strafbare feiten, wordt momenteel opnieuw vormgegeven en daarna in internetconsultatie gebracht.
Verder is van invloed dat op 30 september 2012 het regeerakkoord-Rutte II aankondigde dat het Cbp meer bevoegdheden krijgt, waaronder een uitbreiding van de bevoegdheid om bestuurlijke boetes op te leggen bij overtreding van de Wbp. De uitbreiding van de bevoegdheid van het Cbp om overtreding van de Wbp bestuurlijk te beboeten, wordt bij nota van wijziging aan het onderhavige wetsvoorstel toegevoegd. Deze nota van wijziging is aan de Afdeling advisering van de Raad van State voorgelegd. Het advies is op 19 februari 2014 uitgebracht. Mijn streven is de nota van wijziging voor de zomer bij de Tweede Kamer in te dienen.

2. Beleidsmatige achtergrond

2.1 Aanleiding

De leden van de PVV-fractie vragen of het voorgestelde systeem in het wetsvoorstel het meest effectief is om datalekken te voorkomen en de gevolgen voor betrokkenen te beperken.
Het voorgestelde systeem is in belangrijke mate geënt op het systeem dat sedert 5 juni 2012 geldt op grond van artikel 11.3a van de Telecommunicatiewet voor aanbieders van elektronische communicatiediensten. Artikel 11.3a Tw is de Nederlandse omzetting van een richtlijnlijnverplichting (richtlijn 2009/136/EG tot wijziging van richtlijn 2002/58/EG, ook wel: e-privacy richtlijn). Eenzelfde systeem is opgenomen in de conceptverordening algemene gegevensbescherming. Uitgangspunt van die systemen is dat ieder datalek door de verantwoordelijke wordt gedocumenteerd en aan de toezichthouder wordt gemeld, maar dat het niet in alle gevallen nodig is om het datalek te melden aan de betrokkene wiens persoonsgegevens het betreft. De melding aan de betrokkene is bedoeld om deze te informeren over maatregelen die de betrokkene zelf kan nemen om de voor hem of haar mogelijk nadelige gevolgen van de beveiligingsinbreuk te beperken. Aan de Wbp-meldplicht ligt een meer risicogerichte benadering ten grondslag: zij geldt niet voor alle datalekken, maar alleen voor inbreuken met ernstige nadelige gevolgen voor de bescherming van persoonsgegevens.
Verwacht wordt dat een meldplicht voor datalekken stimulerend zal werken op de op de verantwoordelijke rustende verplichting om zorg te dragen voor adequate beveiliging van de door hem verwerkte persoonsgegevens (krachtens artikel 13 Wbp). Daarmee zal deze bijdragen aan een betere bescherming van persoonsgegevens in het algemeen en een versterking van de positie van de burger in het bijzonder.
Tevens regelt het wetsvoorstel dat de zorgplichten van de verantwoordelijke zich expliciet uitstrekken over datalekken waarvan een bewerker kennis krijgt (artikel 14 Wbp). Een bewerker is een derde partij die ten behoeve van de verantwoordelijke persoonsgegevens verwerkt uit hoofde van een privaatrechtelijke overeenkomst. Een datalek bij een bewerker kan de persoonsgegevens van verschillende verantwoordelijke betreffen. De bewerker zal de verantwoordelijke in staat moeten stellen om zijn meldplicht na te komen. Hierover zullen afspraken moeten worden gemaakt in de bewerkersovereenkomst.
Het wetsvoorstel legt geen wettelijke verplichting aan de bewerker op om inbreuken met ernstige nadelige gevolgen voor de bescherming van persoonsgegevens aan de verantwoordelijke te melden. De conceptverordening algemene gegevensbescherming bevat wel een dergelijke verplichting (artikel 31, tweede lid, commissievoorstel). Deze verplichting sluit aan op de uitbreiding van de beveiligingsverplichting; de bewerker krijgt een zelfstandige beveiligingsplicht (artikel 30 commissievoorstel).

De leden van de D66-fractie lezen dat de basis van onderhavig wetsvoorstel mede ligt in het regeerakkoord van het kabinet-Rutte I. Zij wijzen de regering erop dat hier sprake is van verkeerd dan wel selectief citeren. In de memorie wordt aangehaald dat het ging om een meldplicht voor inbreuken op de beveiliging, terwijl in voornoemd regeerakkoord duidelijk wordt gesteld dat alle datalekken worden gemeld. Deze leden vragen de regering in te gaan op dit duidelijke verschil.
Inderdaad wordt in het regeerakkoord uit 2010 gesproken over «alle datalekken». In de opvatting van de regering wordt hieronder echter hetzelfde verstaan als «datalekken die een gevolg zijn van een inbreuk op de beveiliging». Ik meen dat het zuiver is om bij de bepaling van de reikwijdte van de meldplicht een relatie te leggen met de beveiligingsplicht die op de verantwoordelijke rust. Dit is ook de benadering in de

Telecommunicatiewet (implementatie van de e-privacyrichtlijn) en in de conceptverordening algemene gegevensbescherming. In paragraaf 1 van deze nota is reeds aangegeven dat de regering, gelet op de ruime werkingssfeer van de Wbp, van meet af aan een geclausuleerde meldplicht heeft beoogd, waardoor niet alle datalekken, hoe gering ook, behoeven te worden gemeld.

2.2 Verhouding met voorstel Algemene verordening gegevensbescherming

De leden van de VVD-fractie merken op dat de huidige Wbp is gebaseerd op de Richtlijn 95/46/EG van het Europees Parlement en de Raad van 24 oktober 1995 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens (hierna: Europese richtlijn 95/46/EG). Momenteel is een verordening in de maak die deze richtlijn grotendeels zal vervangen. De verordening zal volgens de regering naar verwachting niet eerder dan in 2016 in werking treden. Deze leden hebben begrepen dat de verordening de huidige Wbp zal vervangen. Toch heeft de regering ervoor gekozen nu al de Wbp aan te passen voor wat betreft de meldplicht, mede omdat nog niet duidelijk is op welke wijze de meldplicht in de verordening zal komen te staan.
Begrijpen deze leden goed dat de regelgeving rondom de meldplicht voor datalekken na inwerkingtreding van de verordening dus opnieuw zal worden gewijzigd? Betekent dit dat burgers en bedrijven zich weer aan andere regels moeten houden? Is dit bevorderlijk voor de rechtszekerheid? Graag horen de leden van de VVD-fractie de mening van de regering op dit punt.
De conceptverordening bevat in de artikelen 31 en 32 een regeling van een algemene meldplicht voor inbreuken op de bescherming van persoonsgegevens. Over de preciese reikwijdte van deze meldplicht wordt nog onderhandeld. De inzet in de onderhandelingen is tweeërlei. Ten eerste om de verplichting in de verordening zo te formuleren dat niet alle datalekken, hoe gering ook, aan de toezichthouder en aan betrokkenen behoeven te worden gemeld, maar alleen potentieel ernstige datalekken en ten tweede om de verplichting om een openbare kennisgeving aan de betrokkene te doen niet te laten drukken op verantwoordelijken in gevallen waarin een dergelijke openbare kennisgeving aan betrokkenen ongewenste effecten zou hebben in verband met zwaarwegende algemene belangen, zoals de belangen van bijvoorbeeld de financiële sector. In paragraaf 4.2 van de memorie van toelichting is de opvatting van de regering over de risico's van ongewenste effecten in de financiële sector uiteengezet. Ook is aangegeven dat de zorgplicht van de financiële onderneming zal waarborgen dat zij ook zonder dat dit dwingend wordt voorgeschreven haar verantwoordelijkheid jegens haar cliënten, ook ten aanzien van datalekken, in rechtstreeks contact met die cliënten zal nemen (zie artikel 4:24a Wet financieel toezich).
Naar het zich laat aanzien zullen de effecten van de overgang van een nationale meldplicht voor datalekken naar een Europese meldplicht voor het bedrijfsleven (grote bedrijven, midden- en kleinbedrijf en zelfstandigen zonder personeel) meevallen. Hierbij moet worden bedacht dat de Wbp-meldplicht is beperkt tot inbreuken met ernstige nadelige gevolgen voor de bescherming van persoonsgegevens. Dit betekent dat inbreuken met geringe nadelige gevolgen voor de bescherming van de persoonsgegevens niet behoeven te worden gemeld. De verantwoordelijke is niet verplicht om alle inbreuken te documenteren. Het niet naleven van de meldingsverplichtingen kan voor het Cbp aanleiding zijn om handhavende maatregelen te treffen, zoals het opleggen van een bestuurlijke boete.

De leden van de PvdA-fractie onderschrijven het standpunt van de regering dat het onverstandig zou zijn om te wachten op de databeschermingsverordening, terwijl een meldplicht nu al de veiligheid kan vergroten. Uiteindelijk is het na de komst van een meldplicht op basis van een Europese verordening van belang dat er geharmoniseerd wordt. Deze leden horen graag van de regering wat de meest recente ontwikkelingen zijn ten aanzien een Europese meldplicht voor datalekken.
In de tweede kwartaalrapportage over 2013 is verslag gedaan over dit onderwerp (Kamerstukken 2012/13, 32 761, nr. 51). Op 29 en 30 april 2013 heeft de Raadswerkgroep de bepalingen die op beveiligingsplicht en de meldplicht zien (artikel 30, 31 en 32 van de verordening) voor een tweede keer behandeld, op basis van een door het voorzitterschap opgestelde nieuwe tekst. Nederland is voorstander van enige verbeteringen die het voorzitterschap aanbracht in artikel 30 (beveiligingsplicht). Nederland ziet in de nieuwe redactie van de artikelen 31 en 32 (meldplicht datalekken) sterke verbeteringen. De aangepaste teksten voorzien niet langer in een algehele meldplicht voor elk datalek, en de termijn waarbinnen gemeld moet worden is aanzienlijk verruimd. Toch blijven er nog vragen over die beantwoording behoeven. De verhouding tussen de meldplicht van de verordening en elders in het EU-recht gereguleerde sectoren (zoals de financiële sector) moet nog nader worden bepaald. Verder zal de overheid in beginsel ook onder de werking van de meldplicht moeten worden gebracht, zij het dat voor bepaalde gevoelige sectoren bij de wet afzonderlijke regels zouden moeten worden vastgesteld. In de loop van dit jaar zal de meldplicht waarschijnlijk opnieuw worden besproken in de Raadswerkgroep.

De leden van de ChristenUnie-fractie vragen op welke termijn de regering verwacht dat de Europese verordening gegevensbescherming van kracht wordt en hoe voorkomen wordt dat organisaties de processen binnen een korte periode meerdere malen moeten aanpassen.
Naar verwachting komt de EU-verordening in 2015 tot stand. Zij treedt in werking 20 dagen na de plaatsing ervan in het EU-Publicatieblad. De verordening kent een implementatietermijn van 2 jaar voordat zij van toepassing wordt (artikel 91). Omdat de nationale meldplicht in belangrijke mate is geënt op het Europese systeem, zal de overgang op de verordening geen grote aanpassingen vergen. De invoering van een -geclausuleerde- nationale meldplicht zal het toegroeien naar de invoering van een algemene Europese meldplicht kunnen vergemakkelijken. Het gaat in beide gevallen om een inbreuk op de beveiliging van persoonsgegevens en de mogelijk ongunstige gevolgen ervan voor de betrokkene.

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

De leden van de D66-fractie zijn geïnteresseerd in de andere meldplichten die in ontwikkeling zijn. Zij vragen of het niet wenselijker is om te kiezen voor een algemene meldplicht voor cyberinbraken in plaats van allerlei meldplichten voor deelonderwerpen. Binnen de algemene meldplicht kan dan gedifferentieerd worden voor «datalek» of «ontwrichting». Graag ontvangen deze leden een reactie op dit voorstel.
De bestaande meldplichten dienen wettelijk bepaalde doelen en zijn ingebed in bestaande wetgeving op verschillende terreinen waar gespecialiseerde sectorale toezichthouders zijn belast met de behandeling van de meldingen (Telecommunicatiewet, Wet financieel toezicht, Wbp). Dit is een overzichtelijk en hanteerbaar systeem, met goed afgebakende verantwoordelijkheden.
Bij de in ontwikkeling zijnde meldplicht voor inbreuken op elektronische informatiesystemen ligt dit anders. Het gaat hier om de ontwikkeling van een nieuwe wet waarin een meldplicht wordt geregeld voor aanbieders

van voor de Nederlandse samenleving vitale producten en diensten. Deze aanbieders moeten ICT-inbreuken met potentieel ernstige maatschappelijke gevolgen onverwijld melden aan de Minister van Veiligheid en Justitie. Het Nationaal Cyber Security Centrum (NCSC), een onderdeel van het Ministerie, is belast met de behandeling van de meldingen en de acties ter opvolging daarvan. Het NCSC is anders dan het Cbp, de ACM, het Agentschap Telecom, of de Autoriteit Financiële Markten, geen toezichthouder. Het NCSC is er primair om vitale aanbieders te helpen om inbreuken te voorkomen of zo snel mogelijk te verhelpen, en daardoor ernstige maatschappelijke ontwrichting, die zou optreden bij het wegvallen van vitale producten of diensten, te voorkomen of te beperken. Hoe een algemene meldplicht voor cyberinbraken met deze meldplichten te rijmen zou zijn laat zich moeilijk doorgronden. Het voorstel van de leden van de D66-fractie roept o.a. de vraag op waarom de verplichting alleen zou gelden voor cyberinbraken, bij welk overheidsorgaan een dergelijke melding zou moeten plaatsvinden, en hoe en onder wiens verantwoordelijkheid vervolgens een uitsplitsing gemaakt zou moeten worden met het oog op het «doorzetten» van de melding. Ook nu reeds geldt dat indien sprake is van een digitale (of fysieke) inbraak, aangifte kan worden gedaan bij de politie. Het wetsvoorstel computercriminaliteit III, dat in de eerste helft van 2014 bij de Tweede Kamer wordt ingediend, beoogt onder andere de strafrechtelijke bescherming van gegevens die door middel van een geautomatiseerd werk zijn opgeslagen te verbeteren.

Voorts lezen de leden van de D66-fractie dat wetgeving voor het melden van ontwrichtende cyberincidenten nog altijd onderweg is. Zij vragen de regering hoe lang dit nog moet duren en waarom dit zo lang duurt. Is het gebruikelijk dat wetgeving op het terrein van een onderwerp dat zo dynamisch is als de informatietechnologie enkele jaren op zich laat wachten?
Het onderwerp technologie en veiligheid is inderdaad dynamisch. Eind oktober heeft het kabinet de Nationale Cybersecurity Strategie 2 aan de Tweede Kamer aangeboden[2]. Ook in internationaal verband zijn er belangrijke ontwikkelingen. Vorig jaar is de Europese Cyber Security Strategie gepubliceerd alsmede het ontwerp van een Netwerk- en Informatiebeveiligingsrichtlijn (kortweg: NIB-richtlijn).[3] De ontwerprichtlijn zet in op het toegenomen belang van samenwerking binnen de Europese Unie op het terrein van informatiebeveiliging en ziet op het opbouwen van nationale capaciteiten en de coördinatie bij grensoverschrijdende inbreuken. Beoogd wordt dat het om de uiteindelijke NIB-richtlijn zo goed mogelijk te laten aansluiten op het Nederlandse stelsel. In juli 2013 is een wetsvoorstel voor een Wet melding inbreuken elektronische informatiesystemen in consultatie gebracht. Daarop zijn adviezen en internetreacties binnengekomen. Zoals de Minister van Veiligheid en Justitie in zijn brief van 12 december 2013 heeft aangegeven, zal het wetsvoorstel worden uitgebreid met het oog op het versterken van de positie van het Nationaal Cyber Security Centrum (Kamerstukken II 2013/14, 26 643, nr. 297). In verband daarmee wordt in een aanvullende consultatie voorzien. Het streven is om het wetsvoorstel tegen de zomer in consultatie te doen, zodat het eind 2014 bij de Tweede Kamer kan worden ingediend.
De leden van de ChristenUnie-fractie merken op dat er verschillende meldplichten zijn, wat onduidelijkheid kan geven waar en onder welke condities gemeld dient te worden. Zij vragen hoe de regering de eenduidigheid gaat bevorderen.
De verschillende (deels in voorbereiding zijnde) meldplichten dienen verschillende doelen. Vanuit de rijksoverheid zal via websites van de

[2] Kamerstukken II 2013/14, 26 643, nr. 291.
[3] Kamerstukken II 2012/13, 22 112, nr. 1588 en 33 602, nr. 1.

verantwoordelijke toezichthouders en van het Nationaal Cyber Security Centrum voldoende bekendheid worden gegeven aan de specifieke meldingsverplichtingen. Waar dat de duidelijkheid ten goede komt zullen de betrokken overheidsdiensten zoveel mogelijk samenwerken. Een voorbeeld hiervan is de inrichting van een gezamenlijk meldloket door het Agentschap Telecom en de Autoriteit Consument en Markt, dat is ingericht voor aanbieders van openbare elektronische communicatiediensten en -netwerken (www.meldplichttelecomwet.nl). Via een webformulier kan de melding «continuïteitsverstoringen» (artikel 11a.2 van de Tw) aan het Agentschap Telecom worden gedaan en de melding «inbreuk bescherming persoonsgegevens» (artikel 11.3a van de Tw) aan de Autoriteit Consument en Markt. Op grond van het voorliggende wetsvoorstel moet de melding op grond van artikel 11.3a Tw, na inwerkingtreding van dit wetsvoorstel, aan het Cbp worden gedaan (zie daarover paragraaf 4.1).

De leden van de Christen-Uniefractie vragen voorts of de regering kan schetsen hoe deze meldplicht zich verhoudt ten opzichte van andere meldplichten zoals die gelden in de telecomsector en de meldplicht security breaches? Deze leden vragen of de ervaringen met al bestaande meldplichten betrokken zijn bij de totstandkoming van dit wetsvoorstel en zien dat graag nader toegelicht.
De Wbp-meldplicht is een algemene meldplicht voor datalekken die voor alle verantwoordelijken in de private en publieke sector geldt. Het doel ervan is een betere bescherming van persoonsgegevens en herstel van het vertrouwen in de verwerking ervan. De meldplicht van artikel 11.3a van de Telecommunicatiewet heeft eenzelfde doel, maar geldt alleen in de sector elektronische communicatie, voor aanbieders van openbare elektronische communicatiediensten die persoonsgegevens verwerken in verband met de levering van deze diensten. De Wbp-meldplicht bevat daarom een uitzondering voor inbreuken op de bescherming van persoonsgegevens die reeds op grond van artikel 11.3a Tw bij de Autoriteit Consument en Markt moeten worden gemeld (artikel 34a, achtste lid nieuw).
De overige meldplichten dienen andere doelen en hebben elk een daarop afgestemd eigen bereik.
De meldplicht op grond van artikel 11a.2 van de Telecommunicatiewet geldt voor aanbieders van openbare elektronische communicatiediensten en/of -netwerken bij inbreuken op de veiligheid of het verlies van integriteit die leiden tot onderbreking van de continuïteit van de dienst of het netwerkt.
De meldplicht van artikel 14.6, tweede lid, van de Telecommunicatiewet geldt voor aangewezen aanbieders van openbare elektronische diensten en netwerken en van verstoringen in hun dienstverlening, ter voorbereiding op buitengewone omstandigheden in de telecomsector.
De meldplicht op grond van artikel 18.15, eerste lid, van de Telecommunicatiewet geldt voor certificatiedienstverleners ten aanzien van gekwalificeerde certificaten. Deze meldplicht is op 1 november 2013 in werking getreden (Stb. 2013, 362).
Hierboven ben ik reeds ingegaan op de in voorbereiding zijnde meldplicht voor «security breaches» in de vitale infrastructuur door de Minister van Veiligheid en Justitie. Ik verwijs de leden van de fractie van de ChristenUnie kortheidshalve naar mijn eerdere antwoord.

3. Algemene aspecten van de meldplicht

3.1 Inbreuk op beveiligingsmaatregelen

De leden van de PVV-fractie lezen in het advies van de Raad van State dat de meldplicht niet geldt wanneer er in het geheel geen maatregelen als bedoeld in artikel 13 Wbp zijn genomen. De regering geeft daarop aan dat dit geen probleem zou vormen, nu dit een in hoge mate hypothetische situatie betreft. Kan de regering aangeven hoe deze opmerking zich verhoudt tot de berichtgeving rond «Lektober»?
Zoals hiervoor reeds aan de orde kwam geldt de in dit wetsvoorstel voorgestelde meldplicht indien er sprake is van een inbreuk op de beveiliging van persoonsgegevens. Artikel 13 Wbp verplicht de verantwoordelijke tot het nemen van passende technische en organisatorische maatregelen teneinde persoonsgegevens te beveiligen tegen verlies of tegen enige vorm van onrechtmatige verwerking. Een inbreuk op de beveiliging moet ruim worden opgevat (zie paragraaf 3.1 van de memorie van toelichting). Hiervan kan sprake zijn bij technisch of organisatorisch falen (waaronder menselijke fouten) of bewust menselijk gedrag (digitale of fysieke inbraak, diefstal). Een inbreuk op de beveiliging betekent niet noodzakelijkerwijs dat de beveiliging te kort schiet, maar sluit dat ook niet uit. Het maakt voor het bestaan van de meldplicht niet uit of er passende beveiligingsmaatregelen zijn getroffen of niet. Ook als de beveiliging adequaat is, kan een datalek zich voordoen.
Dat een professionele verwerker van persoonsgegevens (verantwoordelijke) in het geheel geen beveiliging zou toepassen en er om die reden dus ook nooit sprake zou kunnen zijn van een meldingsplichtige inbreuk acht ik hypothetisch. Iets anders is, waar ook de berichtgeving rond Lektober op zag, dat het met de beveiliging van persoonsgegevens niet altijd even goed gesteld is.
In 2011 riep de ICT-nieuwssite Webwereld de maand oktober uit tot «Lektober». Elke dag plaatste de ICT-nieuwssite een privacylek in een website van een bijvoorbeeld een overheidsdienst. Webwereld wilde daarmee de aandacht vestigen op de slechte beveiliging van veel websites. De betrokken sites of instanties werden wel van tevoren ingelicht, zodat zij het «lek» konden dichten voor publicatie. De Vereniging Nederlandse Gemeenten heeft naar aanleiding van Lektober een e-mail gestuurd naar alle gemeenten met het advies om de beveiliging van hun websites kritisch te onderzoeken en snel maatregelen te nemen als deze tekort schoot.
Afgezien van bedoelde berichtgeving, vragen de leden van de PVV-fractie of de regering het verkoopbaar vindt aan de burger dat bedrijven en instellingen die in het geheel niet voldoen aan de beveiligingsplicht van artikel 13 Wbp onder deze regeling «vrijuit» gaan?
Het moge duidelijk zijn, op grond van het voorgaande, dat bedrijven en instellingen die onvoldoende invulling geven aan hun beveiligingsplicht niet vrijuit gaan onder deze regeling. Artikel 13 van de Wbp verplicht de verantwoordelijke tot het ten uitvoer leggen van passende technische en organisatorische maatregelen om persoonsgegevens te beveiligen tegen verlies of tegen enige vorm van onrechtmatige verwerking. In het begrip «passend» ligt besloten dat de beveiliging in overeenstemming is met de stand van de techniek en voorts dat de beveiligingsmaatregelen proportioneel zijn in relatie tot de te beschermen persoonsgegevens. Naarmate de gegevens een gevoeliger karakter hebben, of de context waarin deze worden gebruikt een grotere bedreiging voor de persoonlijke levenssfeer betekenen, worden zwaardere eisen gesteld aan de beveiliging van de gegevens. De verantwoordelijke zal bij het voldoen aan de beveiligingsplicht een afweging moeten maken, gelet op de risico's van de specifieke verwerking, de stand van de techniek en de kosten van de beveiligings-

maatregelen. Een onvoldoende beveiliging zal uiteraard de kans op datalekken doen toenemen.

De leden van de SP-fractie constateren dat de voorgestelde meldplicht pas van toepassing is zodra er sprake is van een inbreuk op de beveiliging. Hoewel dit volgens de toelichting ruim dient te worden opgevat, zodat ook slordige omgang met USB-sticks of laptops, een hack van een ICT-systeem of tekortschietende beveiligingsmaatregelen hier onder vallen, vragen deze leden toch of dit vereiste niet onnodig beperkend is en of de meldplicht hierdoor wel een voldoende ruim bereik heeft. Als er in het geheel geen beveiliging is, zou letterlijke lezing van artikel 34a met zich meebrengen dat er niet gemeld hoeft te worden. Dit geeft de Raad van State ook aan in het advies bij het wetsvoorstel. Hoewel deze situatie wellicht hypothetisch is, vragen deze leden of het toch niet beter is deze situatie door het artikel te laten dekken?
Zoals hiervoor, in reactie op vragen van de leden van de fracties van D66 en PVV, is uiteengezet, is het niet realistisch om te veronderstellen dat een verantwoordelijke die persoonsgegevens verwerkt deze op geen enkele manier beveiligt. Hoe dan ook zal elke verantwoordelijke wel enige vorm van beveiliging toepassen. Deze leden merken terecht op dat een inbreuk op de beveiliging ruim opgevat dient te worden. Van een inbreuk op de beveiliging kan sprake zijn bij technisch of organisatorisch falen (waaronder menselijke fouten) of bewust menselijk gedrag (digitale of fysieke inbraak, diefstal). In deze ruime opvatting wordt geen enkel datalek uitgesloten. Ik zie dan ook geen meerwaarde in de gedachte dat het wetsvoorstel ook deze (hypothetische) situatie zou moeten dekken. Verder raad ik het schrappen van de verwijzing naar de beveiligingsplicht in artikel 34a af, omdat de relatie met de beveiligingsplicht ook in artikel 11.3a van de Telecommunicatiewet (implementatie e-privacy richtlijn) en de conceptverordening algemene gegevensbescherming wordt gelegd (artikel 4).

De leden van de SP-fractie vragen voorts aandacht voor de suggestie van Bits of Freedom om de meldplicht te laten gelden voor iedere vorm van ongeoorloofde toegang. Het is deze leden nog niet geheel duidelijk welk fundamenteel bezwaar de regering heeft tegen een dergelijke verruiming van de reikwijdte van de meldplicht. Wat is er onredelijk aan als het aan de betrokkene gemeld dient te worden indien en zodra er ongeoorloofde toegang is verschaft tot de persoonsgegevens van de betrokkene, zoals in de voorbeelden die Bits of Freedom noemt?
Wat is de reactie van de regering op de voordelen aan dit andere uitgangspunt die door Bits of Freedom worden genoemd, namelijk het voorstel om ook vermoedens van ongeoorloofde toegang te melden en het voorstel dat ieder lek gemeld moet worden, ongeacht de (door de verantwoordelijke in te schatten) gevolgen voor de betrokkene?
In het advies van Bits of Freedom van 29 februari 2012 worden tal van voorbeelden genoemd waarbij verschillende problemen spelen, zoals schending van (beroeps)integriteitsregels, schending van een beroepsgeheim of strafbare gedragingen. Hoewel alle voorbeelden samenhangen met verwerking van persoonsgegevens, is het criterium onbevoegde toegang als aanknopingspunt voor de meldplicht te abstract omdat dit ook naar geheel andere problemen kan verwijzen (zoals gebrek aan integriteitsbesef bij medewerkers in de organisatie of criminele activiteiten). Het voorstel van Bits of Freedom om alle gevallen van onbevoegde toegang tot persoonsgegevens en zelfs ook vermoedens van onbevoegde toegang meldingsplichtig te maken gaat daarmee het wettelijk kader van bescherming van persoonsgegevens te buiten.

De leden van de SP-fractie vragen of het exacte verschil en de consequenties van dit verschil tussen het eerste en tweede lid van artikel 34a

duidelijker kan worden toegelicht. Niet alle meldingen die aan het Cbp moeten worden gedaan, moeten ook aan de betrokkene zelf worden gemeld. Waarom is hier voor gekozen?
Zoals aan het begin van deze nota al is opgemerkt is bij de vormgeving van de meldplicht van artikel 34a Wbp aangesloten bij de meldplicht voor inbreuken op de beveiliging van persoonsgegevens in artikel 11.3a van de Telecommunicatiewet. In dat systeem worden alle inbreuken met nadelige gevolgen voor de bescherming van de persoonsgegevens bij de toezichthouder (Autoriteit Consument en Markt) gemeld, en worden de inbreuken die waarschijnlijk ongunstige gevolgen voor de persoonlijke levenssfeer van de betrokkene hebben daarnaast ook aan de betrokkene gemeld. In verband met de veel ruimere werkingssfeer van de Wbp, is ervoor gekozen om de melding aan het Cbp te clausuleren. Omdat de bewoordingen van artikel 34a, eerste lid, vragen oproepen, wordt bij nota van wijziging voorgesteld het eerste lid te herformuleren. In de gewijzigde tekst komt het verschil met de Telecommunicatiewet duidelijker tot uitdrukking. Anders dan in de Telecommunicatiewet behoeven niet alle inbreuken te worden gemeld aan de toezichthouder (Cbp) maar alleen de inbreuken met ernstige nadelige gevolgen voor de bescherming van de verwerkte persoonsgegevens. Net als in de Telecommunicatiewet geldt vervolgens dat van de aan de toezichthouder gemelde inbreuken, alleen die inbreuken waarvan het waarschijnlijk is dat deze ongunstige gevolgen voor de persoonlijke levenssfeer hebben van degene wiens persoonsgegevens het betreft, aan de betrokkene behoeven te worden gemeld (getrapt systeem). Voor dit systeem is gekozen omdat de meldplicht aan de toezichthouder ondersteunend is aan het toezicht op de naleving van de beveiligingsplicht door verantwoordelijken. Voor de personen wier persoonsgegevens zijn gelekt geldt dat zij door de melding op de hoogte zijn van de beveiligingsinbreuk, dat zij daarover nadere informatie kunnen inwinnen en dat de verantwoordelijke aangeeft welke maatregelen de betrokkene zelf kan treffen om ongunstige gevolgen voor de persoonlijke levenssfeer te voorkomen of te beperken.
In het negende (oud: tiende) lid is bepaald dat financiële instellingen als bedoel in de Wet op het financieel toezicht niet verplicht zijn om een kennisgeving aan de betrokkene te doen. De relatie met de afnemers van hun diensten valt onder de wettelijke zorgplicht van de financiële instellingen.

De aan het woord zijnde leden ontvangen graag een reactie op de suggestie van het Cbp om de meldingen van datalekken bij de toezichthouder niet te onderwerpen aan beperkingen, omdat ook de ontwerpverordening verplicht tot het melden van ieder datalek en het argument van het Cbp dat juist omdat er vaak sprake is van een combinatie van gegevens, er op voorhand geen soorten datalekken kunnen worden uitgesloten van de meldplicht.
Zoals hiervoor al is opgemerkt, is het uitgangspunt bij de Wbp-meldplicht dat niet alle inbreuken op de beveiliging van persoonsgegevens meldingsplichtig zijn, maar alleen de inbreuken die ernstige nadelige gevolgen hebben voor de bescherming van de verwerkte persoonsgegevens. De redenen hiervoor zijn ten eerste dat de effectiviteit van de meldplicht snel aan betekenis zal verliezen wanneer elk denkbaar datalek, hoe gering ook, in aanmerking komt om te worden gemeld. Ten tweede zou een meldplicht zonder enige beperking tot een nodeloze belasting van bedrijfsleven en overheid leiden. De Nederlandse inzet in de onderhandelingen over de verordening is er eveneens op gericht de meldplicht te clausuleren.

Ten slotte vragen voornoemde leden op dit punt of de uitzondering van artikel 34a, zesde lid, wel wenselijk is, omdat het soms niet ingewikkeld blijkt voor kwaadwillenden om de versleutelde gegevens te ontsleutelen.

Het huidige zesde lid bepaalt dat de melding aan de betrokkene achterwege kan blijven indien de verantwoordelijke gepaste technische beschermingsmaatregelen heeft genomen waardoor de persoonsgegevens die het betreft versleuteld zijn of anderszins onbegrijpelijk zijn gemaakt voor eenieder die geen recht heeft op kennisname van de gegevens. De reden is dat in dat geval ongunstige gevolgen voor de persoonlijke levenssfeer van de getroffen persoon niet waarschijnlijk zijn. Het is bij nadere beschouwing niet logisch dat deze uitzondering alleen wordt gemaakt voor de melding aan de betrokkene en niet voor de melding aan het Cbp. Indien persoonsgegevens op passende wijze zijn versleuteld, zullen immers ook geen (ernstige) nadelige gevolgen voor de bescherming van deze gegevens te duchten zijn. In verband hiermee wordt bij nota van wijziging het zesde lid gewijzigd en wordt daarin bepaald dat de meldingsverplichtingen van het eerste en tweede lid niet gelden indien passende technische beschermingsmaatregelen zijn genomen waardoor de persoonsgegevens die het betreft onbegrijpelijk of ontoegankelijk zijn voor eenieder die geen recht heeft op kennisname van de gegevens.
De verantwoordelijkheid voor de beoordeling of aan het criterium van het zesde lid is voldaan ligt bij de verantwoordelijke. De verantwoordelijke doet er bij twijfel over de kwaliteit van de technische beschermingsmaatregelen verstandig aan om wel een melding te doen bij het Cbp als gelet op de feiten en omstandigheden van het geval ernstige nadelige gevolgen voor de bescherming van de persoonsgegevens niet uit te sluiten zijn. Het Cbp kan dan de kwaliteit van de versleuteling beoordelen en zo nodig een kennisgeving aan de betrokkene afdwingen als het Cbp van mening is dat waarschijnlijk ongunstige gevolgen voor diens persoonlijke levenssfeer te duchten zijn (artikel 34a, zevende lid).

De leden van de CDA-fractie hebben kennisgenomen van het feit dat de regering het voorstel van Bits of Freedom niet heeft gevolgd om elk datalek onder de meldplicht te brengen als dit in verband kan worden gebracht met elke vorm van ongeoorloofde toegang (zoals hacken). De regering volgt deze suggestie niet, omdat in de praktijk ongeoorloofde toegang moeilijk te onderscheiden zal 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, zo wordt gesteld. Deze leden vragen of de regering voornemens is om omwille van deze problematiek op andere wijze in regelgeving te voorzien. De leden van de D66-fractie begrijpen ook niet wat de regering bedoelt met haar reactie op het voorstel van Bits of Freedom om elk datalek te laten melden. Deze leden zijn van mening dat het moet gaan om de consequenties voor consumenten en het vertrouwen in de informatiemaatschappij. Ook verwijzen ze naar de eerder in dit verslag genoemde aanleiding in de memorie inclusief verwijzing naar het regeerakkoord van het kabinet-Rutte I waar het juist gaat om alle datalekken. Voornoemde leden vragen daarom in ieder geval om een betere uitleg op dit punt, maar liever nog zien zij een nota van wijziging tegemoet.

Zoals ook hiervoor in antwoord op vragen van de leden van SP-fractie is aangegeven kunnen de onderliggende problemen waarvan sprake kan zijn bij «ongeoorloofde toegang» ook bestaan in schending van (beroeps)integriteitsregels, een geheimhoudingsplicht of strafbare gedragingen. Daarvoor wordt reeds op andere wijze in de wetgeving voorzien. De regering heeft voor een andere opzet van de meldplicht gekozen. Deze is deze enerzijds ruim genoeg (inbreuk op de beveiliging van persoonsgegevens met ernstige nadelige gevolgen voor de bescherming van de verwerkte gegevens) en anderzijds voldoende geclausuleerd om een

evenwicht te creëren tussen de belangen die met de bescherming van persoonsgegevens zijn gemoeid (voorkomen van nadelige consequenties voor consumenten, herstel van vertrouwen in de informatiemaatschappij) en de uitvoerbaarheid van de meldplicht voor alle betrokkenen (bestuurlijke lasten, administratieve lasten en nalevingskosten).

De leden van de D66-fractie maken zich zorgen over de definitie die de regering hanteert voor de meldplicht. Zij zijn van mening dat een datalek centraal zou moeten staan en niet de beveiliging. Zij stellen voor om datalekken met mogelijk ongunstige gevolgen voor de persoonlijke levenssfeer allemaal te laten melden en dit los te trekken van de mate van beveiliging. Het vertrouwen in de informatiemaatschappij is van groot belang voor onze economie. Om de vruchten te kunnen plukken van het internet moet voorkomen worden dat het vertrouwen van mensen geschaad wordt doordat enkele bedrijven of overheidsinstellingen hun verantwoordelijkheid niet helemaal pakken. Graag ontvangen zij van de regering een reactie op dit voorstel die verder gaat dan wat al in de memorie van toelichting genoemd is. Verder merkt de regering op dat een inbreuk op de beveiliging ruim geduid moet worden. Deze leden vragen wat dan de waarde nog is van deze definitiekeuze. Zij verzoeken de regering dit dan ook aan te passen conform bovenstaande suggestie.

Zoals hierboven in antwoord op vragen van de SP-fractie is opgemerkt ben ik er geen voorstander van om de relatie met de beveiligingsplicht los te laten. Beveiligingsinbreuken kunnen de bescherming van persoonsgegevens in gevaar brengen. Van een inbreuk op de beveiliging kan sprake zijn bij technisch of organisatorisch falen (waaronder menselijke fouten) of bewust menselijk gedrag (digitale of fysieke inbraak, diefstal). In deze ruime opvatting wordt geen enkel datalek uitgesloten. De relatie met de beveiliging wordt ook gelegd in artikel 11.3a van de Telecommunicatiewet (implementatie e-privacy richtlijn) en de conceptverordening algemene gegevensbescherming gelegd (artikel 4). Ik zie kortom geen meerwaarde in het aanpassen van de redactie van artikel 34a, eerste lid, op dit punt. De meldplicht voor datalekken moet worden gezien als een nevenverplichting in relatie tot de algemene beveiligingsplicht van artikel 13 Wbp. De meldplicht ondersteunt het toezicht door het Cbp en versterkt de positie van de burger.

De leden van de ChristenUnie-fractie merken op dat het niet duidelijk is in welke gevallen aan de Nederlandse toezichthouder gemeld moet worden indien een datalek een grensoverschrijdend karakter heeft. Zij vragen bovendien hoe een cumulatie van meldplichten in een dergelijke situatie vermeden wordt.
Artikel 4 van de Wbp bepaalt dat de Wbp van toepassing is op de verwerking van persoonsgegevens in het kader van activiteiten van een vestiging van een verantwoordelijke in Nederland, of wanneer door een verantwoordelijke die buiten de EU is gevestigd gebruik wordt gemaakt van al dan niet geautomatiseerde middelen die zich in Nederland bevinden, tenzij deze middelen slechts worden gebruikt voor doorvoer van gegevens. Wanneer zich bij verwerkingen – waarop de Wbp van toepassing is – als gevolg van een beveiligingsinbreuk een datalek voordoet, zal de in Nederland gevestigde verantwoordelijke of de Nederlandse vertegenwoordiger van een buiten de EU gevestigde verantwoordelijke het datalek aan de Nederlandse toezichthouder moeten melden.
Gesteld dus dat een datalek zich voordoet bij verwerking van persoonsgegevens van een in Nederland gevestigde verantwoordelijke in een andere EU-lidstaat of buiten de Unie, dan dient het datalek aan de Nederlandse toezichthouder te worden gemeld.

Doet het datalek zich evenwel voor bij een gegevensverwerking die in Nederland plaatsvindt door een verantwoordelijke die in een andere EU-lidstaat is gevestigd, dan is de Wbp niet van toepassing en zal het datalek niet bij de Nederlandse toezichthouder behoeven te worden gemeld. Het zal dan afhangen van de nationale wetgeving van de desbetreffende lidstaat van de Europese Unie of er een verplichting bestaat om het datalek aan een buitenlandse toezichthouder te melden. Van Duitsland en Oostenrijk is bekend dat zij dergelijke verplichtingen in de nationale algemene gegevensbeschermingswetgeving hebben opgenomen; de reikwijdte van de meldplichten is echter verschillend. In aanloop naar de nieuwe Europese algemene gegevensbeschermingswetgeving ontstaan binnen de EU verschillende regimes. Voor een cumulatie van meldplichten zal een binnen de EU gevestigde verantwoordelijke niet snel behoeven te vrezen. Op zijn gegevensverwerking is immers het eigen nationale recht van toepassing. Van een cumulatie van meldplichten kan wel sprake zijn bij buiten de EU gevestigde verantwoordelijken, die in lidstaten waar een meldplicht voor datalekken geldt, met gebruikmaking van al dan niet geautomatiseerde middelen die zich aldaar bevinden, persoonsgegevens verwerken. Voorzover de middelen zich in Nederland bevinden, dient een datalek, door de Nederlandse vertegenwoordiger bij het Cbp te worden gemeld.

3.2 Voorkomen van nodeloze meldingen

De leden van de PvdA-fractie hebben vragen over de invulling van de norm, om te bepalen welke inbreuken gemeld moeten worden en welke niet. Veel partijen zien problemen in de open clausulering van de meldplicht, omdat deze te weinig houvast zou bieden bij de beslissing of er wel of geen melding gemaakt moet worden. De regering heeft een beslismodel opgesteld die de volgorde aangeeft waarin de impliciete vragen, besloten in de norm, beantwoord moeten worden.
Deze leden vragen de regering om in te gaan op de risico's van overmelding, door de angst voor een hoge boete. In dat kader zouden deze leden ook graag meer horen over de ervaringen die er al zijn met de meldplicht in de Telecommunicatiewet.
In de telecomsector geldt een wettelijke meldplicht voor datalekken sinds 5 juni 2012 (artikel 11.3a Tw); bij de OPTA kwamen in 2012 in totaal 143 meldingen van inbreuken op de beveiliging van persoonsgegevens binnen. Hier zaten veel kleine incidenten bij die weinig gevolgen hadden voor de klant. Bijvoorbeeld omdat het alleen ging om een telefoonnummer dat iemand te weten kwam. Of om een rekening die verstuurd werd naar een verkeerd adres.

– bij 60 procent van de meldingen heeft het incident helemaal geen gevolg gehad voor de privacy van de klanten. Het ging bijvoorbeeld om een gestolen laptop, waarbij de informatie over klanten zo opgeslagen was dat deze niet te lezen was;
– bij 39 meldingen heeft het bedrijf de klanten ingelicht
– bij 7 meldingen was er sprake van een computervirus of van een hacker die toegang had gekregen tot computers van het bedrijf.

In 2013 heeft de ACM in totaal 211 meldingen ontvangen. In 16% van de gevallen (34) bleek geen sprake te zijn van een inbreuk. Bij 38% van de inbreuken (67) heeft het bedrijf de klanten ingelicht. Bij 45% van de inbreuken (79) betrof het persoonsgegevens die waren versleuteld.

Ook zijn de leden van de PvdA-fractie benieuwd naar de verantwoordelijkheidsverdeling bij een datalek waarbij partijen uit meerdere landen met verschillende rollen betrokken zijn. Graag krijgen zij daarover nadere duiding.
De Wbp is duidelijk over de verantwoordelijkheidsverdeling bij de verwerking van persoonsgegevens. Verantwoordelijk voor de verwerking

van persoonsgegevens is de natuurlijke persoon, rechtspersoon of ieder ander die of het bestuursorgaan dat, alleen of tezamen met anderen, het doel van en de middelen voor de verwerking van persoonsgegevens vaststelt (artikel 1 onder d). In de praktijk bedient de verantwoordelijke zich vaak van een bewerker. Een bewerker is degene die ten behoeve van de verantwoordelijke persoonsgegevens verwerkt, zonder aan zijn rechtstreeks gezag te zijn onderworpen (artikel 1 onder e). Bewerkers (dienstverleners) treden op hun beurt vaak voor (veel) verschillende verantwoordelijken op, bijvoorbeeld in het kader van personeelsbeheer of onderdelen van de administratie.
Gesteld dat een in Nederland gevestigde verantwoordelijke zich in het kader van zijn bedrijfsactiviteiten bedient van een bewerker in Frankrijk, die aldaar de door hem verwerkte persoonsgegevens op de server van een computer opslaat. Zou zich een datalek bij de Franse bewerker voordoen, dan is de verantwoordelijke verplicht om van het datalek melding te doen bij de Nederlandse toezichthouder. Om aan deze verplichting te kunnen voldoen wordt in dit wetsvoorstel voorgesteld om de zorgplicht van de verantwoordelijke jegens de bewerker (artikel 14) zich expliciet te laten uitstrekken tot datalekken waarvan de bewerker kennis krijgt. Zij zullen daar in de bewerkersovereenkomst afspraken over moeten maken.

De leden van de SP-fractie merken op dat de bepaling die voorschrijft wanneer gemeld moet worden (artikel 34a Wbp) onderdelen bevat die niet heel concreet zijn. Zo moeten het Cbp en de betrokkene «onverwijld» in kennis worden gesteld. Waarom is er niet gekozen voor een concrete termijn? Hoe moet beoordeeld worden of er wel of niet onverwijld is gemeld? Ook de leden van de CDA-fractie vragen aan welk tijdsbestek moet worden gedacht bij de maatstaf «onverwijld».
In de memorie van toelichting is opgemerkt dat deze maatstaf de voorkeur heeft boven een gefixeerde tijdslimiet, en dat deze de verantwoordelijke enige gelegenheid geeft om onderzoek te doen naar de inbreuk, te overwegen welke maatregelen hij aanbeveelt en de manier waarop hij communiceert met Cbp en betrokkenen. De maatstaf «onverwijld» komt overeen met die in de meldplicht van artikel 11.3a Telecommunicatiewet. Wat in een concreet geval als «onverwijld» moet worden aangemerkt zal afhangen van de omstandigheden van het geval. Het is aan het Cbp om deze begrippen, waar nodig, in richtsnoeren te verduidelijken met het oog op zijn toezichthoudende en handhavende bevoegdheden.
In de uitvoeringsverordening die de Europese Commissie op 24 juni 2013[4] heeft vastgesteld voor de meldingen op grond van artikel 11.3a van de Telecommunicatiewet wordt het doen van de melding aan de toezichthouder geconcretiseerd tot «waar mogelijk uiterlijk 24 uur» na opsporing van de inbreuk in verband met persoonsgegevens (artikel 2, tweede lid). Ook kent de uitvoeringsverordening een mogelijkheid van een voorlopige kennisgeving aan de toezichthouder, waarbij een deel van de informatie wordt verstrekt, gevolgd door een tweede kennisgeving uiterlijk drie dagen na de voorlopige kennisgeving, waarbij de overige informatie wordt verstrekt (artikel 2, derde lid, eerste alinea). De uitvoeringsverordening bepaalt voorts dat wanneer de aanbieder, ondanks zijn onderzoek, niet binnen drie dagen na de voorlopige kennisgeving alle informatie kan verstrekken, hij moet toelichten waarom de overige informatie laattijdig wordt verstrekt. De aanbieder is verplicht de overige informatie zo spoedig mogelijk te verstrekken en de informatie waar nodig bij te werken (artikel 2, derde lid, tweede alinea). De kennisgeving aan de abonnee of de andere persoon dient «zonder onnodige vertraging»(artikel 3, derde lid)

[4] Verordening (EU) nr. 611/2013 van de Commissie van 24 juni 2013, PBEU L173/2; inwerkingtreding op 25 augustus 2013.

na opsporing van de inbreuk in verband met persoonsgegevens te worden gedaan.

De leden van SP-fractie merken op dat ook de begrippen «redelijkerwijs», «aanmerkelijke kans op nadelige gevolgen» en «waarschijnlijk ongunstige gevolgen», niet heel concreet zijn. Het is wellicht deels onvermijdelijk om te werken met enigszins vage bepalingen, maar zijn de mogelijkheden bekeken om dit objectiever en duidelijker in de wet vast te leggen?

De vragen van deze leden hebben mede geleid tot de bijgaande nota van wijziging. Daarin wordt het eerste lid geherformuleerd en worden de begrippen «redelijkerwijs» en «aanmerkelijke kans» geschrapt. Het moet gaan om een inbreuk die ernstige nadelige gevolgen heeft voor de bescherming van de verwerkte persoonsgegevens. Dit betekent dat de ernstige gevolgen voor de bescherming van de persoonsgegevens zich moeten hebben voorgedaan, hetgeen objectiever en duidelijker door de verantwoordelijke vast te stellen is. Het gaat er niet om dat zich al daadwerkelijk misbruik van de persoonsgegevens heeft voorgedaan door derden. Voor de terminologie van het tweede lid («waarschijnlijk ongunstige gevolgen») geldt dat deze is ontleend aan artikel 11.3a van de Telecommunicatiewet dat de omzetting vormt van artikel 4 van de e-privacy richtlijn.

Voorts hebben de leden van de CDA-fractie geconstateerd dat met het oog op het voorkomen van nodeloze meldingen ervoor is gekozen dat niet elke inbreuk op de beveiliging van persoonsgegevens behoeft te worden gemeld, 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 de organisatie in kwestie worden verwerkt. Deze leden kunnen zich daarin in beginsel vinden. Deze leden vragen zich echter wel af, of de invulling in de praktijk van de begrippen «redelijkerwijs» en «aanmerkelijke kans op» interpretatieproblemen kan geven en of de vast te stellen richtsnoeren van het Cbp voldoende (in plaats van het gestelde «enig») houvast zullen bieden aan de praktijk en nodeloze meldingen voorkomen. Dit temeer daar het hier slechts een verwachting ten aanzien van het Cbp betreft. Deze leden vragen de regering om een nadere toelichting op dit punt. Ook de leden van de SP-fractie vragen hoe er voor wordt gezorgd dat er in de praktijk geen onduidelijkheid komt te bestaan wanneer de meldplicht wel en niet geldt.

Het verheugt mij dat de leden van de CDA-fractie zich in beginsel kunnen vinden in de clausulering van de meldplicht aan het Cbp. Zoals ik hiervoor heb aangegeven, hebben de vragen over de enigszins vage bewoordingen geleid tot de nota van wijziging waarin de meldplicht aan het Cbp wordt geherformuleerd.
In de memorie van toelichting wordt de verwachting uitgesproken dat het Cbp door middel van richtsnoeren nader houvast zal bieden aan de praktijk. Van het Cbp is vernomen dat het Cbp inderdaad het voornemen heeft om met betrekking tot het onderwerp van de meldplicht datalekken richtsnoeren te publiceren. Dit past in het beleid van het Cbp om richtsnoeren te publiceren om de verantwoordelijke helderheid te bieden over de wijze waarop de toezichthouder uitleg geeft aan de algemene normen van de Wet bescherming persoonsgegevens. Dergelijke richtsnoeren geven verantwoordelijken en burgers behalve houvast ook rechtszekerheid. Het Cbp brengt dergelijke richtsnoeren overigens eerst in brede consultatie alvorens tot vaststelling over te gaan. Ik meen dat op deze wijze voor de praktijk vrij snel duidelijkheid zal ontstaan over de toepassing van de meldplicht in concrete gevallen.

De leden van de D66-fractie zien dat de regering in het wetsvoorstel gebruik maakt van open normen zoals «redelijkerwijs». Dergelijke open normen in wetgeving worden vaak geconcretiseerd middels jurisprudentie. Deze leden hebben het idee dat dit bij privacywetgeving niet veel gebeurt. Zij vragen de regering daarom welke recente rechtszaken hebben geleid tot nadere invulling van de open normen in de Wbp en wat dit betekent voor de voorgestelde wetgeving.
De Wbp bestaat voor een belangrijk deel uit algemeen-abstracte normen. Dit vloeit onvermijdelijk voort uit de formulering van de EU-richtlijn. Verheldering van de normen vindt op verschillende niveaus plaats. Op Europees niveau geeft de «Artikel 29»-werkgroep, waarin de Europese toezichthouders zijn verenigd, gezaghebbende opinies uit over uitleg van de normen van de EU-richtlijn. Deze opinies worden o.a. op de website van het Cbp gepubliceerd. Daarnaast is er rechtspraak van het Hof van Justitie van de Europese Unie en van het Europees Hof voor de Rechten van de Mens. Op nationaal niveau stelt het Cbp richtsnoeren vast die helderheid en rechtszekerheid bieten over de wijze waarop de toezichthouder uitleg geeft aan de normen in het toezichts- en handhavingsbeleid. Een voorbeeld hiervan zijn de richtsnoeren beveiliging van persoonsgegevens (2013). Deze geven invulling aan de beveiligingsplicht van artikel 13 Wbp. Mij zijn geen recente rechterlijke uitspraken bekend over de Wbp die relevant zijn voor dit wetsvoorstel.

De aan het woord zijnde leden vinden de term «beslisboom» een te groot woord voor de tekstuele opsomming in paragraaf 3.2.2 in de memorie van toelichting. Zij vragen daarom de regering om een grafische weergave. Ook willen zij weten of elk datalek dat volgt uit een hack zou moeten leiden tot een melding.
In paragraaf 3.2.2 van de memorie van toelichting wordt niet van een beslisboom, maar van een beslismodel gesproken. Daarmee wordt een stapsgewijze analyse bedoeld om te komen tot een antwoord op de vraag of een opgetreden datalek aan de toezichthouder en daarnaast ook aan de betrokkene moet worden gemeld. Met inachtneming van de nota van wijziging zijn de volgende stappen te onderscheiden:

Stap 1 – Is er een beveiligingsinbreuk? (art. 34a lid 1)

Eerst komt de vraag aan de orde of er sprake is van een inbreuk op de beveiliging waardoor persoonsgegevens zijn blootgesteld aan verlies of onrechtmatige verwerking. Daarbij is niet van belang of de verantwoordelijke passende beveiligingsmaatregelen had getroffen of niet. Een datalek kan zich in beide situaties voordoen. Het volstaat dat de verantwoordelijke op de hoogte is geraakt van een beveiligingsincident in zijn organisatie, door constateringen of signalen van binnen of buiten de organisatie (bijv. een melding door een door hem ingeschakelde bewerker).
De aandacht van de verantwoordelijke zal in deze fase, naast herstelmaatregelen om de inbreuk te verhelpen en de gevolgen ervan te beperken, vooral uitgaan naar de oorzaak en aard en omvang van de inbreuk:
– hebben de beveiligingsmaatregelen gefaald, is er sprake van een menselijke fout, of van bewust menselijk gedrag (zoals een hack).
– Voor welke systemen of verwerkingen heeft de inbreuk gevolgen? Welke persoonsgegevens betreft het precies?

Stap 2 – Is het datalek uitgezonderd van de meldingsplicht? (art. 34 lid 6)

De meldingsverplichtingen zijn niet van toepassing indien de verantwoordelijke passende technische beschermingsmaatregelen heeft genomen waardoor de persoonsgegevens die het betreft onbegrijpelijk of ontoegankelijk zijn voor eenieder die geen recht heeft op kennisname van de gegevens.

– De verantwoordelijke moet er dan wel zeker van zijn dat de technische beschermingsmaatregelen adequaat zijn;
– Bij twijfel over de kwaliteit van de technische beschermingsmaatregelen, moet melding aan het Cbp worden overwogen (zie stap 3);

Stap 3 – Melding aan Cbp vereist? (art. 34 lid 1)

Is het datalek niet uitgezonderd, dan komt de vraag aan de orde of de inbreuk ernstige nadelige gevolgen heeft voor de bescherming van de verwerkte persoonsgegevens. De verantwoordelijke zal daarbij in elk geval moeten betrekken:
– de aard en omvang van de inbreuk;
– de aard van de getroffen gegevens: is sprake van bijzondere persoonsgegevens of anderszins gevoelige persoonsgegevens?
– in welke mate worden de persoonsgegevens door technische maatregelen beschermd?

Bij een datalek als gevolg van een hack (ar. 138ab van het Wetboek van Strafrecht), is van belang wat de aard van de gelekte persoonsgegevens is, en wat de risico's van misbruik van deze persoonsgegevens voor de betrokkene zijn. Bij een hack zal melding al snel gepast zijn gelet op de risico's van misbruik van persoonsgegevens. Bij een hack ligt ook aangifte bij de politie in de rede in verband met opsporing van de daders.

Stap 4 – Is daarnaast ook melding aan betrokkene vereist? (art. 34 lid 2)

Of het datalek ook aan de betrokkene moet worden gemeld hangt af van de vraag of waarschijnlijk ongunstige gevolgen zijn te duchten voor de persoonlijke levenssfeer van betrokkene. Het gaat dan om de gevolgen van het lekken van de persoonsgegevens voor de persoonlijke levenssfeer van de getroffen personen. Burgers kunnen door het verlies, onrechtmatig gebruik of misbruik van persoonsgegevens in hun belangen worden geschaad. De schade kan van materiële of immateriële aard zijn (zoals bijvoorbeeld onrechtmatige publicatie, aantasting in eer en goede naam, identiteitsfraude, discriminatie). De verantwoordelijke moet daarom ook aanbevelingen aan de betrokkene doen om deze ongunstige gevolgen te beperken (lid 3).

Tot slot op dit punt vragen de leden van de D66-fractie wat de exacte rol van het Cbp is. Volgens de memorie dient het Cbp met richtsnoeren te komen om daarmee wetgeving te verduidelijken. Deze leden vragen zich af of dit wenselijk is. Wordt het Cbp op deze manier geen medewetgever? Het komt hen logischer voor om concretiseringen van deze wet in lagere wetgeving uit te werken, zoals ook het Cbp heeft voorgesteld.
Het Cbp voert als zelfstandig bestuursorgaan, in volledige onafhankelijkheid, de hem bij wet en ingevolge verdrag opgedragen taken, uit (artikel 52, tweede lid Wbp en artikel 28 richtlijn 95/46).[5] Het Cbp heeft geen regelgevende bevoegdheid en kan reeds om die reden niet als medewetgever worden aangeduid. In het advies van het Cbp van 15 maart 2012 over het conceptwetsvoorstel heeft het Cbp een model bepleit waarin een algemene meldplicht, zonder een voorziening die bagatelzaken uitsluit, tot stand zou worden gebracht en na verloop van tijd, aan de hand van de praktijkervaring via een AMvB of ministeriële regeling te voorzien in uitzonderingen op de algemene meldplicht. Dit model is niet gevolgd. De regering is van meet af aan voorstander geweest van een geclausuleerde meldplicht die zodanig is geformuleerd dat elke verant-

[5] Vgl. ook de Wet van 6 november 2013 tot aanpassing van enige wetten op het terrein van het Ministerie van Veiligheid en Justitie teneinde een aantal zelfstandige bestuursorganen onder de werking van de Kaderwet zelfstandige bestuursorganen te brengen (Stb. 2013, 450) (Kamerstukken 33 554).

woordelijke zelf een beredeneerde afweging kan maken of een concreet datalek onder de wettelijke meldplicht valt. Het Cbp zal deze afweging met richtsnoeren kunnen ondersteunen.

De leden van de ChristenUnie-fractie wijzen op het risico van een omgekeerd effect die deze meldplicht met zich mee kan brengen, namelijk dat bedrijven die secuur werken en daardoor vaker melding maken, publicitair meer schade ondervinden dan bedrijven die door onzorgvuldiger opereren een datalek zelf niet opmerken en dus niet melden. Deze leden vragen wat de regering doet om dit ongewenste effect te voorkomen.
De vraag is of dit ongewenste effect zich inderdaad zou voordoen. Een door een bedrijf of overheidsinstantie onopgemerkt datalek, dat niet wordt gemeld, kan ook op andere manieren in de publiciteit komen. Betrokkenen kunnen immers nadelige gevolgen ondervinden en aan de bel trekken. Komt het datalek dan alsnog aan het licht, dan komt ook het onterechte niet-melden aan het licht. De publicitaire gevolgen kunnen dan groter zijn dan wanneer een datalek tijdig wordt gemeld en betrokkenen worden geïnformeerd over de maatregelen die worden getroffen en die zij zelf kunnen treffen om nadelige gevolgen zoveel mogelijk te voorkomen of te beperken.

3.3 Verhouding verantwoordelijke voor de verwerking en bewerker

De leden van de VVD-fractie merken op dat de meldplicht voor datalekken zal gelden voor alle verantwoordelijken in de zin van artikel 1, sub d, Wbp. Hoe verhoudt de meldplicht voor alle verantwoordelijken zich tot het onderscheid dat in de conceptverordening wordt gemaakt tussen verschillende groepen en sectoren in het kader van de bescherming van persoonsgegevens? Begrijpen de aan het woord zijnde leden goed dat er in het wetsvoorstel geen verschil wordt gemaakt tussen bedrijven met meer of minder dan 250 werknemers, terwijl dat wel gebeurt in de conceptverordening? Wat zijn de gevolgen voor dit wetsvoorstel als over enkele jaren de conceptverordening in werking treedt?

In de conceptverordening wordt bij de regeling van de meldplicht, die is opgenomen in de artikelen 31 en 32, geen onderscheid gemaakt tussen verschillende groepen of sectoren. Dat onderscheid wordt ten aanzien van enkele andere verplichtingen in de conceptverordening wel gemaakt. Voor bedrijven met minder dan 250 werknemers zijn uitzonderingen voorzien op de verplichting voor een niet in de EU gevestigde verantwoordelijke om een vertegenwoordiger in de EU aan te wijzen (artikel 25), de documentatieplicht (artikel 28) en de verplichting om een functionaris voor de gegevensbescherming aan te wijzen (artikel 35). Voorts is in de bepaling over administratieve sancties opgenomen dat bij een eerste en niet-opzettelijke niet-naleving van de verordening met een waarschuwing kan worden volstaan wanneer het een onderneming of organisatie betreft met minder dan 250 werknemers die persoonsgegevens slechts als nevenactiviteit verricht (artikel 79, lid 3).

4. Verhouding tot andere rechtsgebieden

4.1 Verhouding tot specifieke meldplicht op grond van de Telecommunicatiewet

De leden van de CDA-fractie vragen of het gestalte geven aan de samenwerkingsrelatie tussen Cbp en ACM geheel aan beide organisaties zelf wordt overgelaten.
Samenwerking tussen toezichthouders is eerst en vooral een zaak van de toezichthouders zelf. De beide toezichthouders hebben hun samenwer-

kingsrelatie bij het toezicht op de naleving van de bepalingen van de Wbp en de Telecommunicatiewet vorm gegeven in een protocol dat dateert van 12 juli 2005. Dit protocol is met name zinvol omdat bij de bepalingen van de Wbp en de Tw op onderdelen sprake is van samenloop van bevoegdheden van ACM en Cbp. Hiervoor bevatten met name de artikelen 2 tot en met 7 van het protocol nadere regels, over primaire aandachtsgebieden van elk van de toezichthouders, over samenwerking in concrete zaken, over taakverdeling ten aanzien van enkele specifieke onderwerpen en over gemeenschappelijke behandeling. Met het in dit wetsvoorstel voorgestelde artikel 51 wordt in de Wbp, net als in de Instellingswet ACM is gebeurd, een expliciete wettelijke basis onder dit samenwerkingsprotocol gelegd, ter onderstreping van het belang van deze samenwerking. Overigens is de Minister van Economische Zaken op grond van artikel 21 Kaderwet zelfstandige bestuursorganen bevoegd om beleidsregels aangaande de taakuitoefening van de ACM te stellen; ten aanzien van het Cbp zijn ministeriële beleidsregels niet mogelijk in verband met de onafhankelijkheid van het Cbp.

In het kader van dit wetsvoorstel is besloten, om redenen van eenduidigheid en efficiëncy, om één toezichthouder, te weten het Cbp, te belasten met het in ontvangst nemen en behandelen van meldingen in verband met inbreuken op de bescherming van persoonsgegevens. Het wetsvoorstel regelt dat aanbieders van openbare elektronische communicatiediensten de melding op grond van de specifieke meldplicht datalekken van artikel 11.3a Tw, bij het Cbp moeten doen in plaats van de Autoriteit Consument en Markt. Daarnaast regelt het wetsvoorstel dat ook de toezichts- en sanctiebevoegdheden ten aanzien van de Tw-meldplicht verschuiven van de ACM naar het Cbp (artikel II). De toezichthouders zullen dan ook, in gezamenlijk overleg met het Agentschap Telecom, bezien hoe zij de melding praktisch inrichten. De ACM en het Agentschap Telecom hebben nu een gezamenlijk meldpunt via de website www.meldplichttelecomwet.nl .
In de memorie van toelichting (blz. 10) is aangegeven dat ACM primair belast blijft met het toezicht en de handhaving van de bepalingen van de beveiligingsplicht van artikel 11.3 van de Tw. Datzelfde verwachting kan gelden voor de overige bepalingen van hoofdstuk 11, hoewel ook het Cbp bevoegd is voor wat betreft de verwerking van persoonsgegevens binnen de elektronische communicatiesector (zie artikel 2 van het samenwerkingsprotocol).

4.2 Verhouding tot meldplicht incidenten Wet op het financieel toezicht

Door de fracties van de PvdA, SP en D66 zijn vragen gesteld over de positie van de financiële instellingen. Het valt de leden van de PvdA-fractie op dat financiële instellingen een andere informatieplicht ten opzichte van hun cliënten kennen bij datalekken dan andere organisaties en bedrijven. Deze leden begrijpen van de regering dat instellingen vanuit hun zorgplicht ook informatie moeten verschaffen. Graag horen zij echter eerst meer over de ervaringen die er zijn met meldingen door financiële instellingen bij een datalek. Ook vernemen zij graag of de zorgplicht minstens even veel meldingen teweeg zou moeten brengen als de informatieplicht uit dit wetsvoorstel.

Navraag bij de Nederlandse Vereniging van Banken en de Nederlandsche Bank leert het volgende:
Er is wat datalekken betreft een duidelijk onderscheid tussen:
1. Datalekken in de bancaire omgeving
   Dit betreft voorbeelden zoals het stelen van USB-sticks, laptops, papieren prints, etc. met persoonlijke gegevens, die in het bezit waren van bankmedewerkers. Het aantal gevallen van datalekken is klein (een

tiental/mogelijk enige tientallen) en zeer divers (van verlies van apparatuur tot onnadenkendheid van personeel). Banken zijn zeer beveiligingsbewust en monitoren intensief op misbruik. De casussen worden individueel beoordeeld op mogelijke gevolgschade en mitigerende maatregelen worden toegepast.
2. Datalekken buiten de bancaire omgeving waarbij wel gegevens van bankklanten worden gestolen
   Dit betreft bijvoorbeeld skimming, maar ook phishing en malware.

Over de handelwijze ten aanzien van deze datalekken wordt het volgende opgemerkt:
1. Banken informeren in het algemeen elke klant over misbruik van producten op het moment dat de bank dat constateert. Banken nemen in het algemeen ook direct mitigerende maatregelen om daadwerkelijke misbruik te voorkomen, en
2. Banken voorkomen ook misbruik als gevolg van datalekken door gegevens daarover in het monitoring systeem op te nemen.

Het verplicht informeren van cliënten bij datalekken brengt risico's van misbruik van persoonsgegevens met zich. Als een bank of een andere financiële instelling meldingen zou doen, komt dat immers niet alleen terecht bij de goedwillende klanten, maar ook bij klanten die misbruik willen maken van de situatie. Dit geldt bij grootschalige incidenten, waar bijvoorbeeld veel credit card gegevens zijn gestolen en banken besluiten om middels extra monitoring zich voldoende te beschermen. Een wettelijke meldplicht aan het publiek is daarom te risicovol. Daarnaast is het niet denkbeeldig dat een datalek bij een financiële onderneming tot een drastisch dalend vertrouwen zou kunnen leiden bij de klanten van de onderneming, en dat een daling in het vertrouwen in het uiterste geval de stabiliteit van de financiële onderneming of van het financiële stelsel in gevaar kan brengen. Daarbij wordt met name gedacht aan de mogelijkheden voor klanten van banken om (spaar)tegoeden (oftewel deposito's) langs elektronische weg snel op te kunnen vragen.
De betrokken bank of andere financiële onderneming kan in verband met zijn wettelijke zorgplicht jegens de cliënten te allen tijde in overleg treden met de betrokken toezichthouder over het wel of niet informeren van de betrokken klanten over een datalek.

Als de leden van de SP-fractie het goed begrijpen dan zijn financiële ondernemingen niet verplicht datalekken te melden aan betrokkenen, maar wél aan het Cbp. Waarom is in artikel 34a, lid 10, ook lid 7 van het betreffende artikel uitgezonderd? Zou het niet goed zijn het Cbp de bevoegdheid te geven te bepalen dat betrokkenen alsnog in kennis moeten worden gesteld? Hoe zijn de belangen van de betrokkenen en belanghebbenden verzekerd als een financiële onderneming een datalek geheim mag en kan houden?
Het negende (oud: tiende) lid van artikel 34a bevat een uitzondering voor financiële instellingen op de verplichting om een melding aan de betrokkene te doen van een datalek. De overweging hierbij is dat dergelijke openbare kennisgevingen aan betrokkenen in de financiële sector – mede tegen de achtergrond van de financiële crisis – te risicovol om dwingend te worden voorgeschreven. Het tiende lid verklaart het tweede en het zevende lid niet van toepassing op financiële ondernemingen als bedoeld in de Wet financieel toezicht. Zoals hierboven is aangegeven kan en financiele onderneming te allen tijde in overleg treden met de betrokken toezichthouder over het wel of niet informeren van de betrokken klanten over een datalek. Desgewenst kan ook het Cbp worden geraadpleegd.

De leden van de D66-fractie lezen dat er in de meldplicht datalekken een uitzondering zal worden gemaakt voor financiële instellingen. Financiële instellingen moeten een doorbraak van de beveiliging van persoonsgegevens wel melden bij het Cbp, maar niet aan de slachtoffers. De redenering die hierbij wordt gevolgd is dat een openbare kennisgeving te risicovol zou zijn in verband met verminderd vertrouwen. Deze leden zetten hun vraagtekens bij deze redenering voor wat betreft persoonsgegevens. Allereerst zijn zij van mening dat juist bankgegevens persoonsgegevens zijn die personen kwetsbaar maken voor fraude. Daarbij zijn zij niet overtuigd dat een dergelijke openbare kennisgeving grotere consequenties zou hebben voor een bank dan nodig. De leden zien grote waarde in transparantie en vinden dat consumenten zouden moeten weten hoe goed banken hun beveiliging van persoonsgegevens op orde hebben. Dit zou immers een argument kunnen zijn om al dan niet voor een bepaalde bank te kiezen. Daarom vragen zij de regering dit punt aan te passen.
Als gezegd acht ik dergelijke openbare kennisgevingen in de financiële sector te risicovol. 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. Een meldplicht op grond van de Wbp is in die zin overbodig. Ik voeg hier nog aan toe dat per 1 januari 2014 in de Wet financieel toezicht een algemene zorgplicht voor financiëledienstverleners is opgenomen (artikel 4:24a) (Stb 2013, 487 en 552). Deze algemene zorgplicht is bedoeld als vangnet voor situaties waarin bestaande (specifieke) zorgplichten en voorschriften voor financiëledienstverleners ontbreken. Artikel 4:24a Wft kan door de toezichthouder (Autoriteit Financiële Markten) worden gehandhaafd.

5. Sanctionering

De leden van de VVD-fractie merken op dat het wetsvoorstel voorziet in een stevige bestuurlijke boete van maximaal 450.000 euro bij overtreding van de meldplicht. Deze leden erkennen dat dit een fiks bedrag is, zeker vergeleken met de hoogte van de boetes die het Cbp tot nu toe kan opleggen. In de conceptverordening over gegevensbescherming staat echter een hoger boetemaximum. Deze leden gaan er dus van uit dat als de huidige conceptverordening in werking treedt, het Cbp de bevoegdheid krijgt nog hogere boetes op te leggen. Hoe liggen de boetemaxima momenteel in de ons omringende Europese landen? Is 450.000 euro ook hoog vergeleken met de boetes die in die landen kunnen worden opgelegd?

Bijgaand overzicht van wettelijke boetemaxima, waarbij ook de huidige Wbp is meegenomen, is op basis van openbare bronnen samengesteld.

Naam toezichthouder	Maximale boete	Opmerkingen
College bescherming persoonsgegevens	Bestuurlijke boete: € 4.500 (artikel 66 Wbp) Strafrechtelijke boete: € 8.100 of € 20.250 (opzettelijk begaan) (artikel 77 Wbp)	

Naam toezichthouder	Maximale boete	Opmerkingen
Belgische Commissie voor de Bescherming van de Persoonlijke Levenssfeer (CBPL)	Strafrechtelijke boete: € 100.000	De CBPL kan zelf geen boetes opleggen, hiervoor kunnen belanghebbenden naar een Rechtbank.
Commission National de l'informatique en des libertés (CNIL)	Bestuurlijke boete: € 300.000 Strafrechtelijke boete: € 300.000 natuurlijk persoon € 1.5 miljoen rechtspersoon	De maximale boetehoogte is normaliter € 150.000, maar in geval van recidive € 300.000 of 5% van de omzet. Een boete kan worden opgelegd ten aanzien van elke overtreding van de nationale privacy wetgeving.
Duitse Federale DPA's	Bestuurlijk boete: € 150.000 in geval van verzuimovertredingen € 300.000 in geval van opzettelijke overtredingen	In beginsel is € 300.000 de maximale boete maar een verhoging is in bijzondere gevallen mogelijk. Een boete kan worden opgelegd ten aanzien van elke overtreding van de nationale privacy wetgeving.
Italiaanse DPA	Bestuurlijke boete € 500.000	€ 6.000 tot € 36.000 i.g.v. overtreding van informatieplicht; € 10.000 tot € 120.000 i.g.v. verwerken van persoonsgegevens door private ondernemingen of publieke instellingen met winstoogmerk zonder schriftelijke toestemming; € 10.000 tot € 120.000 i.g.v. onvoldoende beveiligingsmaatregelen; € 10.000 tot € 120.000 i.g.v. niet treffen van maatregelen n.a.v. een voorafgaand onderzoek door de DPA i.v.m. specifieke risico's voor personen (bijv. biometrische gegevens); € 20.000 tot € 120.000 i.g.v. niet melden van risicovolle gegevensverwerking door verwerker bij de DPA; € 500.000 i.g.v. spam
Spaanse DPA	Bestuurlijke boete € 600.000	De maximale boete is afhankelijk van de zwaarte van de overtreding. Er worden drie categorieën gehanteerd: 1) € 9.000 tot € 40.000 2) € 40.000 tot € 300.000 3) € 300.000 tot € 600.000 Een boete kan worden opgelegd ten aanzien van elke overtreding van de nationale privacy wetgeving.
UK Commissioners Office (ICO)	Bestuurlijke boete £ 500.000	Deze boete kan worden opgelegd ten aanzien van elke overtreding van de nationale privacy wetgeving.

Er bestaat geen overzicht van maximale (bestuurlijke of strafrechtelijke) boetes die op basis van de telecommunicatierichtlijnen (meldplicht artikel 11.3a Tw) door buitenlandse toezichthouders kunnen worden opgelegd. Vermeldenswaard is dat de Minister van Economische Zaken onlangs een onderzoek heeft laten verrichten naar de haalbaarheid van een aanscherping van het boetebeleid (juridisch en economisch) van de Autoriteit Consument en Markt. In zijn brieven van 27 augustus 2013 en 11 februari 2014 aan de Tweede Kamer heeft de Minister zijn voornemens dienaangaande uiteengezet. Een van de voornemens betreft een verhoging van het absolute (bestuurlijke) boetemaxium van € 450.000 tot € 900.000 (Kamerstukken II 2012/13, 33 662, nr. 9 en 19).

De leden van de PvdA-fractie lezen in de memorie van toelichting een aankondiging van een omvangrijke nota van wijziging om de boetebevoegdheid van het Cbp te vergroten. Deze leden steunen dit doel, maar hopen ook op een snelle invoering van de nu voorliggende meldplicht. Daarom krijgen zij graag een realistische tijdsplanning voor deze nota van wijziging. Ook de leden van de SP-fractie vragen wanneer zij de aangekondigde nota van wijziging tegemoet kunnen zien.
De nota is in december 2013 voor advies aan de Afdeling advisering van de Raad van State voorgelegd; de Afdeling heeft op 19 februari jl advies uitgebracht. Mijn streven is de nota van wijziging voor de zomer bij de Tweede Kamer in te dienen.

De leden van de PVV-fractie lezen in de memorie van toelichting dat er van is afgezien om een boetebevoegdheid in het leven te roepen voor wat betreft de beveiligingsverplichting van artikel 13 Wbp nu het hier een algemeen-abstracte normstelling betreft en een dergelijke boetebe-

voegdheid daarmee in strijd zou komen met het lex certa beginsel. Niettemin behelst de boetebevoegdheid van artikel 34a uit het onderhavige wetsvoorstel eenzelfde algemeen-abstracte norm. Deze leden vragen de regering te onderbouwen of de bepaling van het voorgestelde artikel 34a voor de burger wel voldoende houvast biedt om te voorzien welke concrete handelingen in een voorkomend geval tot bestraffing kunnen leiden, terwijl ten aanzien van een soortgelijke algemeen-abstracte normstelling wordt verdedigd dat dit niet het geval is.
In de memorie van toelichting is vermeld dat de regering nadrukkelijk heeft overwogen om ook, naar aanleiding van de ontvangen zienswijzen en adviezen, overtreding van artikel 13 Wbp – de beveiligingsverplichting – te sanctioneren. Daarvan is in dit wetsvoorstel afgezien, aangezien inmiddels in het regeerakkoord van het kabinet-Rutte II is opgenomen dat bij wet zal worden voorzien in een algehele uitbreiding van de bevoegdheid van het Cbp om overtredingen van de Wbp met bestuurlijke boetes te sanctioneren. De uitbreiding van de bestuurlijke boetebevoegdheid is vervat in een nota van wijziging op dit wetsvoorstel die aan de Raad van State is voorgelegd. Anders dan deze leden menen is de handhaving van een algemeen-abstracte norm door middel van een bestuurlijke boete of door middel van het strafrecht niet a priori in strijd met het lex certa beginsel. In de memorie van toelichting wordt niet gesproken over een onmogelijkheid. Wel heb ik opgemerkt dat uit het lex certa beginsel voortvloeit dat een wettelijk voorschrift dat door een bestraffende sanctie wordt gehandhaafd voor de burger voldoende duidelijk en precies geformuleerd moet zijn, zodat voor de burger voorzienbaar en kenbaar is op welke gedragingen een bestraffende sanctie kan volgen. Datzelfde geldt in het Nederlandse recht overigens voor voorschriften die met bestuurlijke herstelsancties worden gehandhaafd (zie artikel 5:4 Awb jo. artikel 89 van de Grondwet).

De aan het woord zijnde leden vragen of het inderdaad zo is dat als de kleine ondernemer met de te «bagatelliseren risico's» die hij loopt weinig te vrezen heeft van de voorgestelde regeling en het meer de grote spelers zijn die op hun hoede moeten gaan zijn, het maximumbedrag van de voorgestelde boete dan niet te laag is om deze tot melding te bewegen? Het gaat bij het verwerken van persoonsgegevens om de risico's van de specifieke verwerking; deze risico's niet per definitie kleiner als het een kleine ondernemer betreft. Ook een kleine ondernemer kan, al dan niet in opdracht van andere bedrijven, grote aantallen gevoelige persoonsgegevens verwerken, terwijl het anderzijds zo kan zijn dat een grote onderneming gelet op de aard van de bedrijfsactiviteiten relatief weinig persoonsgegevens verwerkt. Vanuit dit perspectief bezien is het onderscheid tussen grote en kleine bedrijven bij de handhaving van de normen van de Wbp minder gemakkelijk te maken dan bijvoorbeeld in het economisch ordeningsrecht.

De leden van de SP-fractie vinden het goed dat het maximale boetebedrag dat door het Cbp kan worden opgelegd wordt verhoogd naar 450.000 euro. Deze leden hebben eerder al aangedrongen op hogere boetes. In de voorgestelde EU-verordening bescherming persoonsgegevens komen boetemaxima die hoger liggen dan thans voor de Wbp wordt voorgesteld. Ook de leden van de CDA-fractie merken op dat het wetsvoorstel in een stevige bestuurlijke boete van maximaal 450.000 euro voorziet, maar dat de conceptverordening een aanzienlijk hoger boetemaximum voor hetzelfde vergrijp kent. De leden van de SP-fractie en de CDA-fractie vragen waarom niet is gekozen voor het hogere boetemaximum uit de verordening.
Het maximale boetebedrag van 450.000 euro is gelijk aan de bestuurlijke boete die nu ten hoogste door de ACM kan worden opgelegd bij overtreding van de specifieke meldplicht in de elektronische communica-

tiesector (art. 11.3a Tw). Het leek de regering passend om hierbij aan te sluiten. In de conceptverordening (commissievoorstel) is het maximale boetebedrag dat door de nationale toezichthouder kan worden opgelegd 1 miljoen voor particulieren en voor ondernemingen 2% van de wereldwijde jaaromzet. Hoewel de regering de forse boetebedragen in de conceptverordening steunt, moet worden afgewacht wat de uiteindelijke inhoud van de verordening is. Het ligt om die reden niet voor de hand nu al bij deze bedragen aan te sluiten.

De leden van de D66-fractie merken op dat de regering stelt dat het een betrekkelijk eenvoudige beoordeling is om na te gaan of de meldplicht is nagekomen. Voornoemde leden zetten hier hun vraagtekens bij. Zij horen graag van de regering hoe het Cbp erachter kan komen dat een lek van persoonsgegevens niet is gemeld. Consumenten kunnen immers getroffen worden door negatieve consequenties als gevolg van een fraude door een lek, zonder dat valt te achterhalen waar de bron van de informatie ligt.
De opmerking in de memorie van toelichting waarop deze leden doelen had niet zozeer betrekking op de «pakkans» bij het niet melden, maar op de beoordeling door het Cbp of een gedane melding ook tijdig is gedaan en of de verstrekte informatie juist en volledig is. Van die beoordeling wordt gezegd dat deze betrekkelijk eenvoudig is. De wijze waarop het Cbp op de hoogte kan komen van het feit dat zich een datalek heeft voorgedaan, dat niet gemeld is, verschilt niet van de wijze waarop het Cbp op de hoogte raakt van andere overtredingen van de Wbp. Bij datalekken zullen dit vooral signalen zijn van consumenten, andere toezichthouders, of berichten in de media.

Voorts vragen de leden van de D66-fractie of de boete van 450.000 euro nu echt zo hoog is in vergelijking met de reputatieschade die optreedt bij een openbare kennisgeving van een datalek. Hoe groot schat de regering de kans in dat gegeven het voorgaande partijen geen melding zullen doen, gezien de overzichtelijke boete, kleine pakkans en grote reputatieschade? Hoe verhoudt zich dit tot het feit dat de regering gezien de potentieel enorme reputatieschade financiële instellingen uitzondert van de verplichting tot openbare kennisgeving? Dit suggereert immers dat de reputatieschade immens groot is.
Om redenen die hiervoor zijn aangegeven acht ik wettelijk verplichte openbare kennisgevingen van datalekken (in bijvoorbeeld als gevolg van skimming, phishing etc) in de financiële sector te risicovol omdat deze in het uiterste geval de stabiliteit van de financiële onderneming of van het financiële stelsel in gevaar zou kunnen brengen. Wat de overweging van mogelijke reputatieschade als gevolg van de melding van een datalek betreft, breng ik graag naar voren dat de gedachte achter de meldplicht veeleer is dat deze zal bijdragen aan het vergroten van het vertrouwen in de zorgvuldige omvang met persoonsgegevens door een verantwoordelijke. De melding aan het Cbp, en in voorkomend geval aan de betrokkene, gaat immers altijd minimaal vergezeld van een beschrijving van de aard van de inbreuk, de instanties waar meer informatie over de inbreuk kan worden verkregen en de aanbevolen maatregelen om de negatieve gevolgen van de inbreuk te verhelpen (artikel 34a lid 3). In dat opzicht lijkt het niet melden, waar dat wel had gemoeten, ook nadelig te kunnen uitpakken voor de reputatie van een verantwoordelijke. Daar kan ook nog het financiële nadeel van een hoge boete bijkomen. Wat de pakkans betreft: deze zal mede afhankelijk zijn van de wijze waarop het Cbp invulling geeft aan niet-naleving van de meldplicht in zijn toezichts- en handhavingsbeleid.

De aan het woord zijnde leden snappen de voorstellen in de adviezen van het Cbp en het Nederlands genootschap Functionarissen Gegevensbe-

scherming (NGFG) om ook overtredingen van artikel 13 Wbp te sanctioneren. Zij begrijpen echter niet dat de regering dit verwerpt op basis van het argument dat de Raad van State aanhaalt in haar kritiek op de open normen in het wetsvoorstel. Daarbij lijkt dit dan weer geen probleem in de aangekondigde nota van wijziging om alsnog een boetemogelijkheid te regelen. Kan de regering hier wellicht helderheid scheppen?
Zoals hiervoor in reactie op de vragen van de leden van de PVV-fractie is aangegeven, wordt overeenkomstig het regeerakkoord gewerkt aan een nota van wijziging waarin wordt voorzien in een algehele uitbreiding van de bevoegdheid van het Cbp om overtredingen van de Wbp ook bestuurlijk te kunnen beboeten. Daarmee wordt het sanctie-instrumentarium van het Cbp versterkt. Onder de huidige wet ligt de nadruk bij het sanctioneren van overtredingen van de Wbp op bestuurlijke herstelsancties (met name de last onder dwangsom); slechts ten aanzien van enkele overtredingen is een bestuurlijke boete mogelijk.

6. Verhouding tot het geldend Europees recht, notificatie

De leden van de CDA-fractie lezen in de memorie van toelichting dat het wetsvoorstel is genotificeerd aan de Europese Commissie. Laatstgenoemde heeft echter geen reactie gestuurd. Betekent dit dat er sprake is van stilzwijgende goedkeuring door de Europese Commissie?

Er is voor de Europese Commissie gedurende een standstillperiode gelegenheid geweest om opmerkingen te maken over eventuele handelsbelemmerende effecten. Uit het feit dat de Europese Commissie geen opmerkingen heeft gemaakt, mag worden afgeleid dat zij van mening is dat daarvan geen sprake is. Formeel is geen sprake van een goedkeuringsprocedure (zie aanwijzing 261a over notificatie uit hoofde van EU-verplichtingen).

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

7.1 Administratieve lasten en nalevingskosten

De leden van de PvdA-fractie merken op dat een meldplicht uiteraard uitvoeringskosten met zich meebrengt, zoals de regering ook aangeeft en inschat. De toezichthouder heeft echter ook ideeën om die kosten te beperken door het proces zo ver mogelijk te standaardiseren. In het wetsvoorstel is de melding van een datalek nog vormvrij, met de mogelijkheid dit bij algemene maatregel van bestuur in te vullen. Deze leden willen graag weten of zij ook mogelijkheden ziet om de uitvoeringskosten te drukken, onder andere door vormvereisten aan de melding. Ook horen zij graag of en hoe de regering haar bevoegdheden in het kader van de algemene maatregel van bestuur wil gebruiken.

In het voorgestelde artikel 34a, tiende (oud: elfde) lid, van de Wbp is een facultatieve grondslag opgenomen voor een algemene maatregel van bestuur waarin regels kunnen worden opgenomen met betrekking tot de inhoud en de wijze van kennisgeving. Dit betekent dat nog zal worden bezien worden of er behoefte is aan aanvullende regels, bijvoorbeeld over het verplicht gebruik van een webformulier voor het doen van de melding aan het Cbp. Het spreekt vanzelf dat ik graag de ideeën van de toezichthouder over de uitvoeringsaspecten zal betrekken.

De leden van de D66-fractie vragen de regering om naast de administratieve lasten ook de voordelen van de meldplicht te becijferen. Het positieve effect van de afschrikwekkende werking zou immers betere

beveiliging, minder incidenten en minder fraude tot gevolg moeten hebben.
De voordelen van de meldplicht laten zich helaas niet becijferen. Daarvoor zijn geen modellen voorhanden. In een kwalitatieve benadering kunnen de positieve effecten die deze leden schetsen zich in meer of mindere mate verwezenlijken. In hoeverre dat daadwerkelijk het geval zal zijn zal niet gemakkelijk vast te stellen zijn. Het effect op de beveiliging van persoonsgegevens zou in onderzoek nog aantoonbaar vast te stellen zijn, maar een daling van fraudegevallen is een wel erg verwijderd effect.

Daarnaast willen deze leden graag weten of de regering de analyse deelt dat de administratieve- en nalevingslasten niet «normaal verdeeld» zullen worden over de verschillende bedrijven. De verwachting van voornoemde leden is dat bedrijven die hun systemen op orde hebben minder vaak slachtoffer zullen zijn van braak en daarom ook minder vaak melding moeten doen. Het effect is dan dat de lasten enkel neerslaan bij hen voor wie deze wet bedoeld is.
In zijn algemeenheid kan ik de redenering van deze leden onderschrijven. Het wetsvoorstel (gewijzigde artikel 34a, zesde lid) voorziet in een uitzondering op de meldingsverplichtingen voor de verantwoordelijke die passende technische beschermingsmaatregelen, zoals cryptografie, treft om persoonsgegevens te beveiligen. Immers, mochten deze persoonsgegevens door een beveiligingsinbreuk worden getroffen, dan zijn er geen risico's voor de bescherming van de desbetreffende persoonsgegevens of voor de persoonlijke levenssfeer van de betrokkene. Melding kan in zulke gevallen achterwege blijven. Daarnaast zullen bedrijven en instellingen die in een goede beveiliging investeren en zich bijvoorbeeld aan algemeen aanvaarde beveiligingsstandaarden houden, de risico's op een datalek kunnen verkleinen (zie richtsnoeren beveiliging Cbp uit 2012). Geheel uit te sluiten vallen beveiligingsinbreuken echter nooit, hoe goed de beveiliging ook is. Of de aanname van de leden van de fractie van D66 dat het effect van de meldplicht zal zijn dat de administratieve lasten vooral zullen drukken op bedrijven die de bescherming van persoonsgegevens niet op orde hebben, juist is, valt op voorhand moeilijk te voorspellen.

7.2 Bestuurlijke lasten en effecten voor de rechtspraak

De leden van de fracties van PvdA en D66 hebben vragen over een mogelijke verzwaring van de uitvoeringlasten voor het Cbp als gevolg van de nieuwe taak, mede in relatie tot het budget van het Cbp. De leden van de PvdA-fractie merken terecht op dat deze kosten niet alleen bestaan uit het registreren van de meldingen, maar ook uit de kosten voor toezicht en extra onderzoek als er twijfel is of een bedrijf alle relevante datalekken meldt. De leden van de PvdA zijn van mening dat de meldplicht vanaf het begin goed moet lopen. Daarom vragen zij de regering of zij bereid is om vóór het begin, in samenspraak met het Cbp, een reële schatting van de meerkosten te maken door deze regeling en het Cbp daarvoor te compenseren.
De leden van de D66-fractie merken op dat de regering niet voornemens is om die gevolgen vooraf al in kaart te brengen. Deze leden vragen op welke wijze er dan in zal worden voorzien dat het Cbp straks afdoende op haar taak is toegerust en de inrichting van de benodigde processen en geautomatiseerde systemen tijdig plaatsvindt? De aan het woord zijnde leden zijn van mening dat het Cbp straks wel in staat moet zijn om de meldplicht datalekken ook feitelijk te handhaven en haar bevoegdheden dienaangaande te kunnen inzetten. Het kan niet zo zijn dat de meldplicht straks door overbelasting van het Cbp een papieren werkelijkheid dreigt te worden. De leden van de D66-fractie willen zodoende weten op welke

wijze bij inwerkingtreding van de meldplicht en in de opstartfase van handhaving zal worden voorzien in voldoende capaciteit bij het Cbp.

De behandeling van de meldingen (registratie etc.) zal een plaats moeten krijgen in de werkprocessen van het Cbp. Het Cbp zal de ingekomen melden moeten bezien en daarop reageren in overeenstemming met de door het College in zijn toezichtsstrategie gestelde prioriteiten. Het ligt voor de hand dat het Cbp in het toezichts- en handhavingsbeleid stil zal staan bij de nieuwe taak die het Cbp ingevolge dit wetsvoorstel krijgt en duidelijk maakt hoe hij de nieuwe taak inpast in het bestaande takenpakket. Voor de toezichthouder is de meldplicht ondersteunend aan het toezicht op de Wbp. De verantwoordelijke zal in een aantal gevallen een separate melding doen aan de getroffen burgers/consumenten. Daarbij zal hij ook vermelden bij welke instanties nadere informatie kan worden verkregen en welke maatregelen de getroffene zelf kan nemen om de negatieve gevolgen van de inbreuk te beperken.
De kosten die met de uitvoering van de meldplicht zijn gemoeid zijn verdisconteerd in het budget van het Cbp. Ik verwacht dat de meeste meldingen geen aanleiding zullen geven tot verdere actie van het Cbp. Voorts wijs ik erop dat vorig jaar aan het Cbp extra financiële middelen zijn toegekend (Kamerstukken II 2012/13, 30 400 VI, nrs. 100 en 71). Hiermee is een houdbaar financieel kader geschapen. Na inwerkingtreding van het wetsvoorstel zullen de gevolgen van de nieuwe taken voor de werklast van het Cbp nauwlettend worden gemonitord.

De leden van de D66-fractie vragen ook of de regering kijkt naar de ervaringen die de ACM heeft met de meldplicht zoals is vastgelegd in artikel 11.3a van de Telecommunicatiewet en naar de ervaringen van buitenlandse toezichthouders? Deelt de regering de mening dat deze ervaringen van waarde zijn voor het zicht op de beheersaspecten van de onderhavige meldplicht?
Ik deel de mening dat de ervaringen van de ACM en van buitenlandse toezichthouders met de «smalle» meldplicht van belang zijn. Op basis van de eerste ervaringen (anderhalf jaar) kan worden geconcludeerd dat het aantal meldingen bij de ACM achterblijft bij de aannames die eerder werden gedaan (in 2013 heeft de ACM 211 meldingen ontvangen, terwijl de prognose ten aanzien van dit wetsvoorstel was 2430 meldingen per jaar). De ervaringen van buitenlandse toezichthouder laten geen ander beeld zien. Als deze ervaringen een voorspellende waarde hebben is de schatting van 66000 meldingen op jaarbasis bij het Cbp (5500 per maand) wellicht aan de hoge kant.

De leden van de ChristenUnie-fractie vragen welke analyse en opvolging wordt verbonden aan de jaarlijkse meldingen die het Cbp ontvangt en wijzen op de mogelijkheid van samenwerking met het Nationaal Cyber Security Centrum.
Op een eventuele samenwerking met het NCSC is hierboven in reactie op vragen van de leden van de D66-fractie ingegaan. Zoals hierboven is aangegeven is de meldplicht datalekken ondersteunend aan het toezicht op de beveiliging van persoonsgegevens en wordt het aan het Cbp overgelaten om te bepalen welke opvolging wordt gegeven aan concrete meldingen.

7.3 Positie van rijksoverheid en decentrale overheden

De leden van de SP-fractie constateren dat de meldplicht datalekken in beginsel ook voor de overheidsinstellingen geldt, maar dat deze meldplicht niet geldt voor inlichtingen- en veiligheidsdiensten, politie, Koninklijke Marechaussee, bijzondere opsporingsdiensten, de Justitiële Informatiedienst van het Ministerie van Veiligheid en Justitie en het

Openbaar Ministerie. Voor de gegevenshuishouding van deze diensten gelden andere wetten. Vindt de regering ten principale dat datalekken ook door de overheid gemeld zouden moeten worden? Zo ja, is dat al geregeld in genoemde wetten? Of kan de Kamer hiertoe nog voorstellen verwachten?

De meldplicht die hier is opgenomen geldt voor alle overheidsverwerkingen van persoonsgegevens die onder de Wbp vallen; deze raakt derhalve ook de positie van de decentrale overheden. Voor een aantal specifieke verwerkingen in het kader van belangrijke overheidstaken in het kader van de veiligheid gelden – van oudsher – andere wetten. In die wetten wordt ook in de bescherming van persoonsgegevens voorzien; zij bevatten een regeling van verplichtingen van de verantwoordelijken en van de rechten van de betrokkene. Ook wordt in die regelingen in onafhankelijk toezicht voorzien. Het doel ervan is een betere bescherming van persoonsgegevens en herstel van het vertrouwen in de verwerking ervan.

Zoals in paragraaf 2.3 van de memorie van toelichting is vermeld, bevat de ontwerprichtlijn voor de bescherming van persoonsgegevens in de sectoren politie en justitie een afzonderlijke meldplicht voor datalekken in die sectoren. De ontwerprichtlijn gaat uit van een melding zowel aan de toezichthouder als aan de betrokkene (artikel 28 en 29 ontwerprichtlijn). De verplichting tot melding aan de betrokkene onder de richtlijn is evenwel niet absoluut; ter waarborging van zwaarwegende algemene belangen zijn uitzonderingen mogelijk (artikel 29 vierde lid jo. artikel 11, vierde lid). Ook het voorstel voor herziening van het Dataprotectieverdrag, dat een zeer brede reikwijdte heeft, breder zelfs dan de Wbp, en alle overheidsverwerkingen van persoonsgegevens omvat, bevat een meldplicht voor datalekken, maar dan uitsluitend aan de onafhankelijke toezichthouder, niet aan de betrokkene.

Uitgangspunt bij de onderhandelingen over deze rechtsinstrumenten is dat meldplichten voor gevoelige 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 overheidsdiensten hebben. In het licht van de Europese ontwikkelingen en toenemende grensoverschrijdende samenwerkingen zijn is de regering terughoudend met het vooruitlopend daarop invoeren van separate meldplichten.

7.4 Gevolgen voor de rijksbegroting

De leden van de SP-fractie vragen, naar aanleiding van de schatting dat 66.000 meldingen per jaar worden verwacht, naar de gevolgen voor het Cbp. Wat verwacht de regering dat het Cbp met deze meldingen zal doen en wat is precies het doel van deze meldingen aan het Cbp? Hoeveel tijd zal het Cbp naar verwachting kwijt zijn aan het ontvangen van deze meldingen, het eerste onderzoek of de melding al dan niet tot grondig onderzoek moet leiden, eventueel daaropvolgend onderzoek en eventuele sanctioneringsbesluiten? Welke werklast brengt dit voor het Cbp met zich mee? Wordt het Cbp uitgebreid en krijgt het extra middelen om dit extra werk goed te doen? Waarom wordt deze beslissing vooruit geschoven? Zoals hiervoor in paragraaf 7.2 in antwoord op vragen van de leden van de fracties van de PvdA en D66 is vermeld, zal het merendeel deel van de meldingen geen aanleiding geven tot verdere actie. De meldplicht aan het Cbp is ondersteunend aan de toezichtstaak. Als onafhankelijke toezichthouder bepaalt het Cbp in het kader van het toezicht op de Wbp en de handhaving ervan zijn eigen prioriteiten. Het Cbp zal in het toezichts- en handhavingsbeleid ingaan op de meldplicht. Het zwaartepunt bij de

meldplicht ligt in de visie van de regering bij de verantwoordelijke zelf. Deze is immers verplicht om persoonsgegevens op zorgvuldige wijze te verwerken en daarover transparantie te betrachten ten opzichte van de personen wier persoonsgegevens het betreft. Wanneer persoonsgegevens «op straat komen te liggen» als gevolg van een datalek, is primair de verantwoordelijke aan zet.

ARTIKELSGEWIJZE TOELICHTING

Artikel I

Artikel 34a, vijfde lid, Wbp

De leden van de SP-fractie vragen een reactie op de wens van het Cbp dat de wijze van melden niet vormvrij dient te zijn maar dat hiervoor altijd een (web)formulier gebruikt zou moeten worden. Dit voorkomt administratieve lasten voor verantwoordelijke en toezichthouder. De leden van de D66-fractie merken op dat is gekozen voor een vormvrije melding. Dit betekent dat niet al tijdens het melden een controle van juistheid en volledigheid van gegevens mogelijk is waardoor achteraf aanvullingen en correcties nodig zijn. Daarnaast zullen meldingen administratie verwerkt moeten worden in een automatiseringssysteem. Dit brengt administratieve lasten met zich mee voor de toezichthouder. Deze leden vragen of die extra werklast niet overbodig is in het huidige technologische tijdperk. Heeft de navolging van een melding niet juist baat bij een formulier waarmee gerichter naar informatie gevraagd wordt en er ook op beveiligde en betrouwbare wijze gemeld kan worden? Zij vragen de regering in te gaan op de Europese ontwikkelingen op dit vlak en aan te geven waarom hier niet voor gekozen is.

Hierboven is in paragrafen 2.3 en 7.1 reeds aangegeven dat een webformulier in beginsel een goede vorm lijkt voor het doen van een melding aan de toezichthouder. De Europese uitvoeringsverordening die op grond van artikel 4, vijfde lid, van de e-privacyrichtlijn is vastgesteld en op 25 augustus 2013 in werking is getreden, verplicht de nationale toezichthouders om alle in de desbetreffende lidstaat gevestigde aanbieders van openbare elektronische communicatiediensten beveiligde elektronische middelen ter beschikking te stellen voor het doen van een melding.

Artikel 34a, zesde lid, Wbp

De leden van de D66-fractie lezen dat wanneer cryptografie gebruikt wordt, men is vrijgesteld van melding aan betrokkenen. Dit verbaast deze leden. Deelt de regering de mening dat niet elke vorm van versleuteling voldoende is, maar dat het erom gaat dat het gebruikte algoritme sterk genoeg moet zijn en dat niet ook de sleutel gelekt mag zijn om aan deze bepaling te voldoen? Voorts vragen voornoemde leden of het tweede lid van artikel 34a het zesde lid niet overbodig maakt. Op het moment dat de encryptie voldoende was, volgt uit het tweede lid dat er geen melding aan de betrokkene nodig is. Wat is dan de toegevoegde waarde van het zesde lid dat een en ander enkel ingewikkelder maakt?

Het zesde lid is bij nota van wijziging geherformuleerd. Bij nader inzien is geoordeeld dat meldingsverplichtingen niet nodig zijn in situaties waarin een datalek geen nadelige gevolgen heeft voor de desbetreffende persoonsgegevens. Ik erken dat niet elke vorm van versleuteling voldoende is, gelet op de specifieke risico's van een verwerking en de voortschrijdende techniek. De veiligheid van de versleuteling is uiteraard een aandachtspunt. Het is in eerste instantie aan de verantwoordelijke zelf om te beoordelen of de versleuteling sterk genoeg is, en op juiste wijze

wordt uitgevoerd, waardoor een melding aan het Cbp en in voorkomend geval aan de betrokkene(n) achterwege kan blijven. Overigens wordt in de Europese uitvoeringsverordening voor de telecomsector nader uitgewerkt wanneer persoonsgegevens door technologische maatregelen als onbegrijpelijk worden beschouwd. Dat is volgens deze verordening het geval wanneer de persoonsgegevens: a. op veilige wijze zijn versleuteld met een standaardalgoritme, de sleutel voor decryptie door geen enkele inbreuk gevaar heeft gelopen en de sleutel voor decryptie zodanig werd gegenereerd dat personen zonder geautoriseerde toegang de sleutel met de beschikbare technologische middelen niet kunnen vinden; of b. zijn vervangen door een met een cryptografisch versleutelde hashfunctie berekende hashwaarde, de sleutel die hiervoor werd gebruikt door geen enkele inbreuk gevaar heeft gelopen en deze voor datahashing gebruikte sleutel zodanig is gegenereerd dat personen zonder geautoriseerde toegang de sleutel niet kunnen vinden met de beschikbare technologische middelen (artikel 4 lid 2).

Artikel 34a, achtste lid, Wbp

De leden van de fracties van PvdA en D66 hebben vragen gesteld over het achtste lid. In bijgaande nota van wijziging wordt voorgesteld om het achtste lid te schrappen. Hieraan ligt de nadere afweging ten grondslag dat het opleggen van een zelfstandige (met een bestuurlijke boete te sanctioneren) verplichting om intern binnen de organisatie een overzicht («register») bij te houden van alle inbreuken (de ernstige en de niet ernstige), minder wenselijk is, gelet op de lasten die een dergelijke verplichte registratie met zich brengt.
Verder vloeit uit de algemene beveiligingsverplichting van artikel 13 Wbp reeds voort dat de verantwoordelijke interne procedures heeft voor het tijdig en doeltreffend behandelen van beveiligingsincidenten en de ervaringen met afgehandelde incidenten gebruikt om de beveiliging van persoonsgegevens waar mogelijk structureel te verbeteren.
Handhaving van de meldplicht van artikel 34a door het Cbp kan op de gebruikelijke wijze lopen, via signalen van gedupeerde burgers, belangenorganisaties, of berichten in de media. De interne registratieplicht is daarvoor niet nodig; het Cbp kan altijd informatie over vermoedelijke datalekken bij een verantwoordelijke opvragen (artikel 61 Awb jo. artikelen 5:16 en 5:17 Awb).

De leden van de PvdA-fractie merken op dat er een duidelijk twistpunt bestaat als het gaat om de mate van openbaarheid van het register van meldingen. Hierbij speelt de vraag wat het meeste bijdraagt aan een betere beveiliging van informatie en een groter vertrouwen in gegevensverwerkingen. Maximale transparantie kan helpen om kwetsbaarheden te voorkomen en onduidelijkheid over inbreuken weg te nemen. Tegelijk kan het bedrijven huiveriger maken om een melding te doen als alle details daarover openbaar worden. Graag zouden deze leden aan de regering willen vragen of het wetsvoorstel op dit moment maximale openbaarheid bevat. Ook zouden deze leden willen weten of het Cbp de ruimte heeft om in de toekomst, binnen de wet, de openbaarheid over datalekken te vergroten.
In reactie op deze vragen merk ik op dat de regering nooit een openbare registratie van beveiligingsinbreuken heeft beoogd (vgl. ook het overzicht van artikel 10.3a, zesde lid Tw, dat evenmin openbaar is). Het belang bij het vertrouwelijk blijven van gegevens over de beveiliging van de gegevensverwerking of over gelekte persoonsgegevens staat daaraan in de weg. Het Cbp zou ook nimmer gegevens uit een interne registratie openbaar maken (artikel 10, eerste lid, onder c en d, van de Wet openbaarheid van bestuur). Het staat het Cbp vrij om op basis van de aan het Cbp gedane meldingen en de openbare kennisgevingen aan betrok-

kenen in het jaarverslag of in een andere publicatie aandacht te besteden aan datalekken. Het Cbp heeft in dit opzicht alle ruimte.

De leden van de D66-fractie lezen dat het protocol met niet gemelde inbraken geen openbaar register dient te zijn, omdat dit het vertrouwelijk blijven van details met betrekking tot de beveiliging van de gegevensverwerking en de daarmee gemoeide investeringen in de weg staan. Deze redenering kunnen zij niet volgen. Allereerst lezen zij nergens in de registratieplicht dat bij het noemen van een inbreuk er iets dient te worden opgegeven over dergelijke details die volgens de regering vertrouwelijk zouden moeten blijven. Ten tweede denken deze leden juist dat een inzicht in het aantal inbraken bij een partij relevante informatie is voor een consument om al dan niet gebruik te maken van de diensten van een bepaalde partij. Deelt de regering de mening dat de redenering onvolledig is en ziet zij ook de toegevoegde waarde voor consumenten om te kunnen kiezen voor een partij die haar zaken op orde heeft? Is het juist niet zo dat transparantie en openheid bijdraagt aan het vertrouwen, terwijl geheimzinnigheid en de suggestie dat de burger zaken niet mag weten enkel bijdraagt aan wantrouwen?
Zoals in reactie op de voorgaande vraag is aangegeven, is aannemelijk dat een interne registratie van ernstige (aan het Cbp gemelde) en niet ernstige inbreuken op de beveiliging van persoonsgegevens bedrijfsvertrouwelijke gegevens en informatie over gelekte persoonsgegevens bevat. Deze belangen wegen mijns inziens zwaarder dan het belang van de consument om inzage te hebben in de interne registratie van beveiligingsinbreuken van een organisatie. Het is de meldplicht zelf, aan Cbp in voorkomend geval ook aan betrokkenen, die bijdraagt aan grotere transparantie en daarmee aan het vertrouwen van de burger in de verwerking van zijn persoonsgegevens.

Artikel V

De leden van de VVD-fractie willen graag voorkomen dat de oude Wbp niet is ingetrokken op het moment dat de verordening in werking treedt. Dit zou namelijk de te vaak ontstane onduidelijke situatie scheppen dat men niet weet welke wettelijke regeling geldt, namelijk die van de Wbp of die van de verordening. Kunnen deze leden ervan uitgaan dat de regering, vóór inwerkingtreding van de verordening, een nieuw wetsvoorstel zal indienen om de inhoud van de Wbp te vervangen door die van de verordening?
Deze leden kunnen er van op aan, dat er tijdig uitvoerings- en aanpassingswetgeving naar aanleiding van de verordening in procedure zal worden gebracht, zodat de met de verordening strijdige wetgeving op het moment dat de verordening van toepassing wordt komt te vervallen. Naar het zich laat aanzien zal de huidige Wbp grotendeels komen te vervallen.

De Staatssecretaris van Veiligheid en Justitie,
F. Teeven