33662 **Wijziging van de Wet bescherming persoonsgegevens en enige andere wetten in verband met de invoering van een meldplicht bij de doorbreking van maatregelen voor de beveiliging van persoonsgegevens alsmede uitbreiding van de bevoegdheid van het College bescherming persoonsgegevens om bij overtreding van het bepaalde bij of krachtens de Wet bescherming persoonsgegevens een bestuurlijke boete op te leggen (meldplicht datalekken en uitbreiding bestuurlijke boetebevoegdheid Cbp)**

Nr. 11 Herdruk[1] **NOTA NAAR AANLEIDING VAN HET NADER VERSLAG**
Ontvangen 2 december 2014

1. Strekking van het wetsvoorstel

Ik dank de leden van de fracties van de VVD, PvdA, SP, CDA, PVV en ChristenUnie voor hun nadere reactie op het wetsvoorstel en de daarop ingediende nota van wijziging van 16 april jl. (hierna ook: de eerste nota van wijziging).
Graag ga ik hieronder in op de bij de verschillende fracties levende vragen en de opmerkingen waarop men de reactie van de regering wenst te vernemen. Met deze nadere schriftelijke ronde beoog ik meer duidelijkheid te scheppen over de reikwijdte van de voorgestelde meldplicht voor datalekken in de Wet bescherming persoonsgegevens, het doel ervan, en de Europese en internationale ontwikkelingen inzake de totstandkoming van meldplichten voor datalek-incidenten, als onderdeel van een verderstrekkende modernisering van gegevensbeschermingsstandaarden zoals de herziening van de OESO-richtlijnen[2], of de onderhandelingen over de modernisering van het Europees Dataprotectieverdrag[3] en de EU-privacyrichtlijn[4]. Deze ontwikkelingen vormen de achtergrond van de Nederlandse wetgevingsinspanningen.
Deze nota wordt ingediend mede namens de Minister van Binnenlandse Zaken en Koninkrijksrelaties en de Minister van Economische Zaken.

Ik dank de leden van de VVD-fractie voor hun positieve grondhouding ten aanzien van dit wetsvoorstel en het feit dat zij zich grotendeels in de eerste nota van wijziging kunnen vinden.
De leden van de VVD-fractie pleiten ervoor om de uitwerking en invulling van de in artikel 34a gehanteerde criteria bij algemene maatregel van bestuur te doen plaatsvinden en niet door het College bescherming persoonsgegevens (Cbp) door middel van richtsnoeren. Een uitwerking van

---

[1] I.v.m. een correctie in het opschrift

[2] Herziening van de OESO-richtlijnen over bescherming van persoonsgegevens en grensoverschrijdende gegevensdoorgifte van 11 juli 2013 (C(80)58/FINAL). In artikel 15 worden de verplichtingen van de verantwoordelijke opgesomd. Artikel 15 onderdeel c bepaalt: Provide notice, as appropriate, to privacy enforcement authorities or other relevant authorities where there has been a significant security breach affecting personal data. Where the breach is likely to adversely affect data subjects, a data controller should notify affected data subjects.

[3] In 2013 is een ad hoc comité ingesteld dat zich buigt over de herziening van het Verdrag tot bescherming van personen met betrekking tot geautomatiseerde verwerking van persoonsgegevens (Conventie 108). Artikel 7 lid 2 van het meest recente voorstel luidt: Each Party shall provide that the controller shall notify, without delay, at least the supervisory authorities within the meaning of Article 12 bis of this Convention of those data breaches which may seriously interfere with the rights and fundamental freedoms of data subjects.

[4] Zie paragraaf 2.1 van deze nota voor ontwikkelingen op EU-niveau inzake herziening van EU-regelgeving inzake bescherming van persoonsgegevens. De Kamer ontvangt hierover elk kwartaal een rapportage.

deze criteria door de regering kan in de visie van deze leden een aanknopingspunt vormen voor het uitoefenen van democratische controle. Voorts wijzen zij erop dat het Cbp eerder ook heeft geadviseerd om uitwerking bij algemene maatregel van bestuur te doen plaatsvinden. Deze leden noemen met name de criteria van artikel 34a, eerste en tweede lid.

Zoals ik in paragraaf 3.2 van de nota naar aanleiding van het verslag heb opgemerkt heeft het Cbp in zijn advies van 15 maart 2012 over het conceptwetsvoorstel 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 algemene maatregel van bestuur of ministeriële regeling te voorzien in uitzonderingen op de algemene meldplicht. De regering heeft niet voor dit model gekozen. De regering is van meet af aan voorstander geweest van een geclausuleerde meldplicht die zodanig is geformuleerd dat elke verantwoordelijke zelf een beredeneerde afweging kan maken of een concreet datalek dat hem ter kennis komt onder het bereik van de wettelijke meldplicht valt. Het Cbp zal deze afweging met richtsnoeren (beleidsregels) kunnen ondersteunen. Voor het vaststellen van richtsnoeren volgt het Cbp een procedure met brede consultatie van maatschappelijke groeperingen en andere belanghebbenden in de private en publieke sector. In de kort geleden aan de Tweede Kamer verzonden tweede nota van wijziging wordt voorgesteld om in de Wbp (artikel 67) te bepalen dat zulke beleidsregels van het Cbp, waarin uitleg wordt gegeven aan de open geformuleerde normen waarvan overtreding met een bestuurlijke boete kan worden bestraft (zoals artikel 34a), de goedkeuring behoeven van de voor de Wbp verantwoordelijke ministers.

Kijkend naar de in artikel 34a geformuleerde meldplicht, dan valt daarin op dat met name het eerste, tweede en zesde lid gebruik maken van algemeen geformuleerde criteria die nadere uitwerking en invulling door het Cbp behoeven.

Artikel 34a, zesde lid (adequate technische beschermingsmaatregelen)
In het zesde lid is bepaald dat er geen wettelijke meldplicht bestaat als gelekte persoonsgegevens op een passende technische wijze zijn beschermd waardoor de persoonsgegevens die het betreft onbegrijpelijk of ontoegankelijk zijn voor eenieder die geen recht heeft op kennisname van de gegevens. Dit is een strenge norm die van geval tot geval door de verantwoordelijke moet worden toegepast, naar de actuele stand van de techniek[5]. Als het beveiligingsniveau van de gelekte gegevens aan deze norm voldoet valt het datalek niet onder de wettelijke meldplicht. Ook hier past echter de kanttekening dat 100 procent veilig niet bestaat en dat in geen enkel geval de garantie bestaat dat de gelekte persoonsgegevens niet toch, op enig moment in de toekomst, onrechtmatig worden verwerkt.

Artikel 34a, eerste lid (meldplicht aan Cbp)
In het eerste lid is de meldplicht van de verantwoordelijke aan de wettelijke toezichthouder op de verwerking van persoonsgegevens, het Cbp, geformuleerd. Deze meldplicht bestaat als er sprake is van:

- een inbreuk op de beveiliging van persoonsgegevens[6], én deze inbreuk
- ernstige nadelige gevolgen heeft voor de bescherming van de verwerkte persoonsgegevens.

Deze formulering is in belangrijke mate geënt op de (Europese) meldplicht in artikel 11.3a van de Telecommunicatiewet (hierna: Tw). Het inhoudelijke verschil is dat artikel 11.3a Tw niet spreekt over

[5] Zie voor de telecomsector een uitwerking hiervan in Verordening (EU) nr. 611/2013 van de Commissie van 24 juni 2013, PBEU L173/2; in werking getreden op 25 augustus 2013.
[6] De verwijzing naar artikel 13 Wbp verwijst naar de algemene verplichting om persoonsgegevens op een passende manier te beveiligen. Voor de meldplicht datalekken is evenwel niet van belang of de beveiliging van de gelekte gegevens passend was, een inbreuk op de beveiliging met ernstige nadelige gevolgen voor de bescherming van de verwerkte persoonsgegevens volstaat.

"*ernstige*" nadelige gevolgen" voor de bescherming van de verwerkte persoonsgegevens, maar over "nadelige gevolgen".
Een ander, meer wetstechnisch verschil is dat de Telecommunicatiewet een aparte definitie bevat van het begrip datalek en het onderhavige wetsvoorstel niet.
In artikel 11.1, onder j, Tw wordt onder een "inbreuk in verband met persoonsgegevens" verstaan:
een inbreuk op de beveiliging die resulteert in een onbedoelde of onwettige vernietiging, verlies of wijziging van, of een niet geautoriseerde toegang tot persoonsgegevens die zijn verstuurd, opgeslagen of anderszins verwerkt in verband met de levering van een openbare elektronische communicatiedienst in de Europese Unie[7]*.*
In artikel 11.3a, eerste lid, Tw is de meldplicht voor de aanbieder van openbare elektronische communicatiediensten aan de wettelijke toezichthouder als volgt gedefinieerd:
De aanbieder van een openbare elektronische communicatiedienst stelt het college onverwijld in kennis van een inbreuk op de beveiliging, bedoeld in artikel 11.3, die nadelige gevolgen heeft voor de bescherming van persoonsgegevens die zijn verwerkt in verband met de levering van een openbare elektronische communicatiedienst in de Europese Unie.

Uit deze teksten en uit de nadere bestudering van de wetsgeschiedenis van de implementatie van richtlijn 2009/136/EG (richtlijn burgerrechten) in de Telecommunicatiewet kan worden afgeleid dat deze specifieke meldplicht aan de toezichthouder een ruime strekking heeft. De aanbieder van een openbare elektronische communicatiedienst moet iedere inbreuk op de beveiliging die nadelige gevolgen heeft voor de bescherming van de persoonsgegevens die door de inbreuk zijn geraakt melden. Deze ruime meldplicht gaat echter niet zo ver dat elke tekortkoming in de beveiliging – die nadelige gevolgen voor de bescherming van de verwerkte persoonsgegeven zou kunnen hebben – moet worden gemeld aan de toezichthouder. In de nota naar aanleiding van het verslag van 24 februari 2011 op het desbetreffende wetsvoorstel tot wijziging van de Telecommunicatiewet ter implementatie van de herziene telecommunicatierichtlijnen is een voorbeeld gegeven dat bij nader inzien tot een te ruime uitleg van de meldplicht kan leiden[8]. Op blz. 23 wordt, in reactie op een vraag van de leden van de PvdA-fractie, vermeld dat het mogelijk is dat er sprake is geweest van een inbreuk op de beveiliging waardoor bijvoorbeeld onbevoegden persoonsgegevens "hadden kunnen inzien", maar waarbij is vastgesteld (bijvoorbeeld aan de hand van de logbestanden van de server) dat geen enkele onbevoegde gebruik heeft gemaakt van die mogelijkheid. Uit het vervolg van de passage kan worden opgemaakt dat een dergelijke inbreuk wel aan de toezichthouder dient te worden gemeld. Een zo vergaande uitleg is bij nadere beoordeling niet in overeenstemming met de tekst van artikel 11.1, onder j, jo. 11.3a van de Telecommunicatiewet. Er moet wel sprake zijn van een gegevensstroom ("lekken van data"); een enkele tekortschietende beveiliging is niet voldoende**.** Als niet met zekerheid vastgesteld kan worden dat geen enkele onbevoegde van de beveiligingsinbreuk gebruik heeft gemaakt, is het wel meldingsplichtig.

---

[7] Artikel 2, onder i, van richtlijn 2002/58/EG omschrijft "een inbreuk in verband met persoonsgegevens" als volgt: een inbreuk op de beveiliging die resulteert in een accidentele of onwettige vernietiging, wijziging, niet-geautoriseerde vrijgave van of toegang tot persoonsgegevens die zijn verstuurd, opgeslagen of anderszins verwerkt in verband met de levering van een openbare elektronische communicatiedienst in de Gemeenschap. De "niet geautoriseerde vrijgave van persoonsgegevens" is in de definitiebepaling van de Telecommunicatiewet niet apart vermeld. Artikel 4, derde lid, onder 3, van richtlijn 2002/58/EG omschrijft de meldplicht voor de aanbieder van openbare elektronische communicatiediensten aan de wettelijke toezichthouder als volgt:
In geval van een inbreuk in verband met persoonsgegevens stelt de aanbieder van openbare elektronische communicatiediensten de bevoegde nationale instantie zonder onnodige vertraging in kennis van de inbreuk in verband met persoonsgegevens. In de Telecommunicatiewet is de verwijzing naar de algemene beveiligingsverplichting van artikel 11.3 toegevoegd aan de meldplicht.
[8] Kamerstukken II 2010/11, 32549, nr. 7.

Ook voor de meldplicht in dit wetsvoorstel geldt dat er sprake moet zijn van het "lekken van data" en dat het lekken een onbedoelde of onwettige vernietiging, verlies of wijziging van, of een niet geautoriseerde toegang tot verwerkte persoonsgegevens tot gevolg heeft. Het is dus niet zo dat een enkele tekortkoming of kwetsbaarheid in de beveiliging tot een melding aan de toezichthouder moet leiden. Als niet redelijkerwijs kan worden uitgesloten dat een inbreuk op de beveiliging tot een onrechtmatige verwerking heeft geleid, moet de verantwoordelijke een melding aan de toezichthouder (Cbp) doen.

Zoals in de nota naar aanleiding van het verslag is uiteengezet is een verschil tussen beide meldplichten dat de meldplicht in de Wbp is geclausuleerd (beperkt tot: ernstige datalekken). Hier liggen inhoudelijke redenen aan ten grondslag en redenen die zijn gelegen in het beperken van administratieve en bestuurlijke lasten. Gelet op de diversiteit van de normadressaten van de Wbp (van een zzp'er tot een multinational) en de diversiteit van de door hen verwerkte persoonsgegevens past een meer risicogerichte benadering. Met de toevoeging van het criterium dat sprake moet zijn van "*ernstige*" nadelige gevolgen voor de bescherming van de verwerkte persoonsgegevens wordt een afbakening aangebracht tussen ernstige datalekken waarvan de toezichthouder (onverwijld) op de hoogte moet worden gebracht en gevallen waarin dat niet noodzakelijk is. Hierbij zijn aard en omvang van de inbreuk en de aard van de gelekte persoonsgegevens doorslaggevend. De verantwoordelijke zal een dergelijke beoordeling voor de door hem verwerkte persoonsgegevens zelf moeten maken.
Het Cbp zal deze afweging door de verantwoordelijke door middel van richtsnoeren (beleidsregels) kunnen ondersteunen. In de beleidsregels kan een verdere uitwerking en invulling worden gegeven aan datalekken die zodanig ernstig zijn dat zij aan Cbp gemeld moeten worden en incidenten waarbij dat niet het geval is. Het is gewenst dat het Cbp deze duidelijkheid verschaft aangezien het ten onrechte niet melden van een datalek bestuurlijk kan worden beboet door het Cbp. In de kort geleden ingediende tweede nota van wijziging wordt voorgesteld om in de Wbp (artikel 67) te bepalen dat beleidsregels van het Cbp waarin uitleg wordt gegeven aan de open geformuleerde normen waarvan overtreding met een bestuurlijke boete kan worden bestraft (zoals artikel 34a), de goedkeuring behoeven van de voor de Wbp verantwoordelijke ministers.

Artikel 34a, tweede lid (meldplicht aan personen van wie de gegevens zijn gelekt)
In lid 2 van artikel 34a is de meldplicht geformuleerd voor het doen van een melding aan personen van wie de persoonsgegevens zijn blootgesteld aan verlies of onrechtmatige verwerking. Hiervoor geldt het criterium dat de inbreuk:

- Is gemeld aan de toezichthouder in verband met ernstige nadelige gevolgen voor de bescherming van de verwerkte persoonsgegevens ; én
- Waarschijnlijk ongunstige gevolgen zal hebben voor de persoonlijke levenssfeer van de betrokken personen.

Deze criteria zijn identiek aan de meldplicht aan de getroffen personen in artikel 11.3a Tw. Met name het tweede criterium vergt uitwerking en invulling door de bevoegde toezichthouder. Dit is onder de huidige Telecommunicatiewet de Autoriteit Consument en Markt, maar op grond van dit wetsvoorstel zal het Cbp voor beide meldplichten datalekken de bevoegde toezichthouder zijn. Het gaat bij dit criterium om een beoordeling van de 'waarschijnlijke' gevolgen van onrechtmatige verwerking en misbruik van de gelekte persoonsgegevens voor de persoonlijke levenssfeer van betrokken personen. Hier valt met name te denken aan vormen van fraude (financiële fraude, identiteitsfraude) en aantasting van goede naam en reputatie. Het Cbp kan hier door middel van beleidsregels (bijvoorbeeld aan de hand van voorbeelden) nadere duiding aan geven.

Ik heb er kennis van genomen dat de leden van de PvdA-fractie de eerste nota van wijziging bij het oorspronkelijke wetsvoorstel met enige reserve hebben ontvangen. Deze leden vinden het belangrijk dat er een effectieve meldplicht komt voor datalekken, nu de afhankelijkheid van digitale

communicatiemiddelen steeds groter wordt. Zij zijn bang dat met deze nota van wijziging het aantal meldingen zodanig sterk teruggedrongen wordt dat aan een effectieve meldplicht afbreuk gedaan wordt.
Ik deel de zorgen van deze leden niet, zoals ook uit de beantwoording van deze vragen zal blijken. Het is ook mijn bedoeling een effectieve meldplicht in te voeren, tegelijkertijd is een meldplicht geen doel op zich, en zal de meerwaarde ervan voor alle deelnemers aan onze digitale samenleving goed doordacht moeten zijn. De nota van wijziging beoogt niet het aantal meldingen terug te dringen, maar meer eenduidige criteria te formuleren waarlangs tot een beoordeling moet worden gekomen over de toepasselijkheid van de meldplicht. Dit is temeer van belang omdat het ten onrechte niet melden van een datalek, een bestuurlijk beboetbaar feit oplevert.

De leden van de SP-fractie zijn teleurgesteld over de voorgestelde wijzigingen. Zoals in het verslag gemeld, zijn zij groot voorstander van een meldplicht. Voor betrokkenen van wie persoonsgegevens worden gelekt, is het van groot belang hiervan op de hoogte te worden gesteld, zodat zij ook zelf maatregelen kunnen nemen om zich te beschermen tegen inbreuken op hun privacy, openbaarmaking van persoonsgegevens of identiteitsfraude.
Hoewel ik het belang van het informeren van burgers onderschrijf voor situaties waarin hun persoonsgegevens onbedoeld zijn blootgesteld aan onrechtmatige verwerking , meen ik dat er ook voor moet worden gewaakt dat er verplichte meldingen moeten worden gedaan van voorvallen waarin de risico's op nadelige effecten voor de persoonlijke levenssfeer van burgers niet noemenswaardig zijn. Mijn streven is om de meldplicht toe te snijden op situaties waarin er voor de burger daadwerkelijk ongunstige gevolgen voor diens persoonlijke levenssfeer te duchten zijn zodat de burger, na een kennisgeving te hebben ontvangen, alert is op de mogelijke gevolgen en zich, voor zover dat mogelijk is, daartegen kan wapenen door bijvoorbeeld extra voorzorgsmaatregelen te treffen (bijvoorbeeld vervanging van een wachtwoord) of door diensten of producten van een andere marktpartij af te nemen. Deze kern van het wetsvoorstel is door de eerste nota van wijziging niet veranderd.

Het verheugt mij dat de leden van de CDA-fractie een afdoende antwoord op hun vragen hebben gekregen in de nota naar aanleiding van het verslag en dat zij zich in de voorgestelde wijzigingen in de eerste nota van wijziging kunnen vinden. In antwoord op hun vraag of aan de introductie van de meldplicht een publiekscampagne vooraf zal gaan, merk ik op dat mijn ministerie de invoering van de meldplicht op gepaste wijze zal begeleiden. Daarbij kan geprofiteerd worden van de ervaring die met de meldplicht voor inbreuken in verband met persoonsgegevens in de Telecommunicatiewet is opgedaan. Deze meldplicht is nu twee jaar van kracht. Invoering ervan is vrij geruisloos verlopen. Van de meldplicht kan zeker een prikkel uitgaan voor bedrijven en organisaties om de beveiliging van persoonsgegevens te verbeteren. Ik zal nog bezien in hoeverre het nodig is om burgers met een publiekscampagne voor te bereiden op meldingen die zij in de toekomst kunnen ontvangen, zoals deze leden opmerken. Het wetsvoorstel voorziet er immers in dat burgers op een zorgvuldige en behoorlijke wijze informatie ontvangen in het geval zich een concrete inbreuk op hun persoonsgegevens voordoet. Zij ontvangen in een dergelijk geval o.a. informatie over maatregelen die ze zelf kunnen treffen om de negatieve gevolgen te beperken en over een contactpunt waar bij terecht kunnen voor nadere informatie (artikel 34a, lid 3 en 5).

De leden van de PVV-fractie hebben naar aanleiding van het gewijzigde wetsvoorstel nog enkele vragen. Zij willen graag van de regering weten wat haar visie is op de beveiliging van persoonsgegevens, en welke rol zij voor zichzelf weggelegd ziet op dit gebied. Voor de visie van de regering op beveiliging van ICT-systemen, netwerken en diensten en daarin opgeslagen informatie , waaronder persoonsgegevens, verwijs ik naar de notitie Vrijheid en veiligheid in de digitale samenleving (Kamerstukken II 2013/14, 26 643, nr. 298), de daar op genomen actiepunten, de Nationale Cybersecurity Strategie II (Kamerstukken II 2013/14, 26642, nr. 291) en de kabinetsvisie op

e-privacy (Kamerstukken II 2013/14, 32 761, nr. 49). De Kamer wordt door middel van voortgangsrapportages van de uitvoering van de aangekondigde maatregelen op de hoogte gehouden.
Verder vragen deze leden hoe de regering ervoor zorgt dat bedrijven serieuze datalekken daadwerkelijk bij de overheid melden, zonder dat de overheid misbruik zal maken van hun gegevens. Zoals hiervoor al is aangegeven, zal de invoering van de meldplicht vanuit mijn ministerie op zodanige wijze worden begeleid dat de doelgroepen op de hoogte zijn van hun verplichtingen. Zoals in de memorie van toelichting al is aangegeven zal het Cbp de meldingen vertrouwelijk behandelen en deze niet openbaar maken. De vrees voor misbruik van gegevens over datalekmeldingen door de overheid is naar mijn mening dan ook niet gegrond.

Ik constateer dat de leden van de D66-fractie met verbazing hebben kennisgenomen van de eerste nota van wijziging inzake de meldplicht. Ik hoop deze leden met de beantwoording van hun vragen meer duidelijkheid te verschaffen.

2. Beleidsmatige achtergrond

2.1 Verhouding met voorstel Algemene verordening gegevensbescherming

De leden van de CDA-fractie vragen ten aanzien van de voorgestelde Algemene verordening gegevensbescherming (COM (2012)11 def) of de inbreng van de regering in Europa gericht zal zijn op de realisering van de geclausuleerde meldplicht zoals die nu in onderhavig wetsvoorstel wordt gecreëerd. Ook de leden van de D66-fractie merken op dat in Europa wordt gewerkt aan een meldplicht voor datalekken. Zij constateren dat de regering er met het onderhavige wetsvoorstel voor kiest om de bescherming van persoonsgegevens af te zwakken. Zij vragen hoe de voorgestelde inperking van de meldplicht zich verhoudt tot het de voorstellen van de Europese Commissie en de onderhandelingen in de Raad. De leden van de ChristenUnie-fractie geven aan te hebben kennisgenomen van de voorgestelde wijziging van het oorspronkelijke wetsvoorstel. Zij lezen dat beoogd is te verduidelijken dat alleen datalekken met ernstige nadelige gevolgen voor de bescherming van de verwerkte persoonsgegevens aan het Cbp dienen te worden gemeld. Zij vragen hoe deze wijziging zich verhoudt tot de voorgestelde tekst in de Europese Algemene verordening gegevensbescherming, die naar alle waarschijnlijkheid volgend jaar van kracht wordt.

De meldplicht voor datalekken in het Commissievoorstel voor een algemene verordening is vergelijkbaar met de ruim geformuleerde Europese meldplicht in de telecommunicatiesector. Ook bevat het Commissievoorstel een vergelijkbare definitie van het begrip datalek.
In artikel 4 lid 9 van het Commissievoorstel wordt onder “inbreuk in verband met persoonsgegevens” verstaan:
een inbreuk op de beveiliging met de vernietiging, het verlies, de wijziging of de ongeoorloofde verstrekking van of de ongeoorloofde toegang tot de doorgezonden, opgeslagen of anderszins verwerkte gegevens, hetzij per ongeluk hetzij onrechtmatig, tot gevolg;
In artikel 31 lid 1 van het Commissievoorstel wordt de meldplicht aan de toezichthoudende autoriteit, voor zover hier van belang, als volgt geformuleerd:
In geval van een inbreuk in verband met persoonsgegevens meldt de voor de verwerking verantwoordelijke de toezichthoudende autoriteit deze inbreuk zonder onnodige vertraging en zo mogelijk niet later dan 24 uur nadat hij ervan kennis heeft gekregen.
In artikel 32 lid 1 van het Commissievoorstel wordt de meldplicht aan degene van wie de persoonsgegevens zijn gelekt, voor zover hier van belang, als volgt geformuleerd:
Wanneer de inbreuk in verband met persoonsgegevens waarschijnlijk negatieve gevolgen voor de bescherming van de persoonsgegevens of de privacy van de betrokkene heeft, deelt de voor de verwerking verantwoordelijke na de in artikel 31

bedoelde melding, de betrokkene de inbreuk in verband met persoonsgegevens zonder onnodige vertraging mee.

De inzet in de onderhandelingen van de Nederlandse regering in Raadskader 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. Onze Brusselse inzet sluit aan bij de benadering in dit wetsvoorstel. Beide zijn gericht op het bereiken van een evenwichtige belangenafweging, tussen verhoging van het beschermingsniveau (dat doen we met het invoeren van de wettelijke meldplicht voor datalekken) en het beheersen van de administratieve lasten en de nalevingskosten. Nederland is juist zeer bezorgd over het voorstel van de Europese Commissie, omdat dat niet alleen tot een hoge belasting van bedrijven en toezichthouders leidt, maar de meldplicht ook uitholt. De balans is zoek in het Commissievoorstel. Het argument van de Commissie is dat een algemene meldplicht voor alle datalekken al tot het acquis behoort; zo'n meldplicht is immers reeds opgenomen in de e-privacyrichtlijn (richtlijn EG/2002/58, zoals gewijzigd bij richtlijn 2009/36/EG). Dat argument gaat volgens Nederland niet op, omdat de verordening kan worden aangemerkt als "acquis in wording". Een ander argument van de Commissie is dat aanbieders onder de e-privacyrichtlijn niet ongelijk behandeld mogen worden ten opzichte van andere sectoren. De reactie van Nederland daarop is dat het risico van de gevolgen van onrechtmatig gebruik als gevolg van een beveiligingsinbreuk in deze sector hoog te noemen is, hetgeen een daarop afgestemde (zware) verplichting rechtvaardigt. Bij de Wbp moet ook rekening worden gehouden met verwerkingen waarbij de gevolgen van een doorbreking van de beveiliging minder hoge of slechts geringe risico's met zich brengt.
Van belang is voorts dat Nederland in deze meer risicogerichte benadering niet alleen staat. De uiteindelijke verwoording van deze inzet in een gemeenschappelijke positie van de Raad is echter een zaak van 28 lidstaten.
Tijdens de Raad voor Justitie en Binnenlandse Zaken op 9-10 oktober 2014 heeft de Raad een gedeeltelijke algemene benadering bereikt over hoofdstuk IV van de ontwerpverordening (verantwoordelijke en bewerker), waaronder de artikelen 31 en 32 over de meldplicht datalekken.[9] Ik wil er daarbij wel op wijzen dat de artikelen 31 en 32 van de verordening niet helemaal op zichzelf kunnen worden gezien. De meldplicht datalekken maakt deel uit van een breder concept, de risico-georiënteerde benadering als geheel. Het ontwerp van Hoofdstuk IV gaat uit van een regime met drie lagen. De eerste laag is een algemeen artikel waarin een algemene verplichting voor alle verantwoordelijken is neergelegd om maatregelen te nemen ter bescherming van de rechten van betrokkenen, rekening houdend met het risico van de verwerking. Daarover moet hij ook verantwoording kunnen afleggen. De tweede laag bestaat uit twee specifieke verplichtingen die voor alle verantwoordelijken gelden. Ten eerste de verplichting tot het toepassen van privacy by design. Er moet altijd worden gestreefd naar de minst zware inbreuk op de rechten van betrokkene in de verwerking. Ten tweede geldt altijd een beveiligingsplicht. Bij de uitvoering mag de verantwoordelijke daarbij wel rekening houden met de aard van de verwerking, maar de verplichting geldt altijd. Het derde niveau betreft alle andere verplichtingen, zoals de documentatieplicht, de meldplicht datalekken, de verplichting een privacy impact assessment te houden en de verplichting tot voorafgaand overleg met de toezichthouder. Deze verplichtingen zijn niet onvoorwaardelijk. Als er sprake is van een hoog risico voor de betrokkene in termen van het soort gegevens (bijvoorbeeld medische gegevens, creditcardnummers) dan gelden die verplichtingen bovenop de andere verplichtingen. Met dit model kan Nederland akkoord gaan.[10]

---

[9] Vgl. document 13772/2014 (bron: www.consilium.europa.eu).
[10] Kamerstukken II 2014/15, 32761, nr. 75 (rapportage derde kwartaal 2014).

3. Algemene aspecten van de meldplicht

3.1 Inbreuk op beveiligingsmaatregelen

De leden van de PvdA-fractie zijn bang dat de nieuwe formulering van de meldplicht in de nota van wijziging ervoor zorgt dat het tijdstip van een melding naar achteren verplaatst wordt, doordat niet meteen bij het ontdekken van een datalek duidelijk is of er daadwerkelijk nadelige gevolgen zijn. Zij vragen bezorgd of de regering deze mogelijkheid ook ziet. Deelt zij de mening dat hiermee de preventieve werking van de meldplicht afgezwakt wordt? Ook maken deze leden zich zorgen over de hogere drempel bij de meldingen, omdat mogelijk voor de betrokken organisatie niet altijd in te schatten is hoe groot het risico voor de bescherming van persoonsgegevens daadwerkelijk is.
Hoewel ik begrijp dat de tekst van artikel 34a, eerste lid, deze indruk kan wekken, zie ik, in het licht van de toelichting die ik hierboven al heb gegeven, geen reden tot bezorgdheid. Als de verantwoordelijke een datalek (zijnde een tekortschietende beveiliging met verlies of onrechtmatige verwerking van persoonsgegevens tot gevolg) ontdekt, zijn de nadelige gevolgen voor de bescherming van de door de inbreuk geraakte persoonsgegevens per definitie een feit en begint op dat moment de termijn voor het doen van de melding te lopen. Aangezien de melding onverwijld moet worden gedaan, is wel duidelijk dat de verantwoordelijke geenszins achterover kan leunen. Wat hier los van staat is, dat de verantwoordelijke wel moet beoordelen of het datalek dat hij heeft ontdekt een “ernstig” datalek is. Hierbij is bepalend de aard en omvang van de inbreuk en de aard van de getroffen persoonsgegevens. Een verantwoordelijke zal een dergelijke beoordeling voor de onder zijn verantwoordelijkheid verwerkte persoonsgegevens zonder al te veel moeite kunnen maken. Het Cbp zal deze afweging door middel van beleidsregels ondersteunen.
Dat hiermee een hogere drempel zou zijn opgeworpen dan in het oorspronkelijke wetsvoorstel, met een vermindering van de preventieve werking tot gevolg, zie ik niet. Het wettelijke criterium van het eerste lid biedt het Cbp ruimte om nadere uitwerking en invulling te geven aan de “drempel” dat het bij de verplichte melding aan het Cbp moet gaan om “ernstige” datalekken.

De leden van de PvdA-fractie maken zich ook zorgen over het schrappen van de meldplicht aan het Cbp indien de gegevens versleuteld zijn. Kan de regering ingaan op de mogelijkheid dat de gegevens door nieuwe technieken alsnog ontsleuteld worden, waardoor een overzicht bij het Cbp van ontvreemde versleutelde datasets van meerwaarde kan zijn voor de bescherming van persoonsgegevens?
Volgens de uitzondering van het zesde lid geldt de wettelijke meldplicht niet indien de versleuteling zodanig is dat de gelekte gegevens onbegrijpelijk of ontoegankelijk zijn voor onbevoegden. Zoals ik hiervoor al heb aangegeven is dit een strenge norm die van geval tot geval door de verantwoordelijke moet worden toegepast, naar de actuele stand van de techniek. Indien de verantwoordelijke twijfelt over de adequaatheid van de technische beschermingsmaatregelen zal een melding niet achterwege kunnen blijven. Van het Cbp zal uiteraard ook een inspanning worden verwacht om in de beleidsregels de nodige duidelijkheid te scheppen over minimaal noodzakelijke versleutelingstechnieken. Een en ander neemt niet weg dat de komst van nieuwe technieken, nieuwe risico’s kan inhouden. Een verantwoordelijke zal zich dat ook realiseren en met de diefstal van een versleutelde dataset in het achterhoofd, over een langere periode alert zijn op deze risico’s. Bij signalen van mogelijke ontsleuteling van gevoelige data zal de verantwoordelijke alsnog kunnen overwegen een kennisgeving te doen aan de betrokken personen. Het Cbp zal uiteraard de beleidsregels periodiek op de komst van nieuwe technieken aanpassen. Bij die gelegenheid zal het Cbp ook kunnen waarschuwen voor het gevaar dat uitgaat van in het verleden gestolen datasets die met de komst van nieuwe technieken te ontsleutelen zijn. Op deze wijze kunnen zowel verantwoordelijken als het Cbp op een zinvolle manier inspelen op nieuwe technologische ontwikkelingen. Hiervoor is niet nodig dat het Cbp, op basis van meldingen van verantwoordelijken,

een overzicht bijhoudt van ontvreemde versleutelde datasets en daarbij gebruikte versleutelingstechnieken.

De leden van de SP-fractie vinden de voorgestelde wijziging, waardoor slechts ernstige nadelige gevolgen voor de betrokkenen gemeld moeten worden, een ongunstige ontwikkeling. Een betrokkene wordt immers niet meer op de hoogte gesteld als er slechts sprake is van nadelige gevolgen die niet als ernstig worden bestempeld. Ik kan deze leden in zoverre gerust stellen dat de meldplicht aan de betrokkene niet is gewijzigd. Het criterium voor de meldplicht aan betrokkene is hetzelfde gebleven. Melding aan de betrokkene dient te geschieden indien de inbreuk waarschijnlijk ongunstige gevolgen zal hebben voor de persoonlijke levenssfeer van de betrokken persoon. Wel is in het getrapte model van het wetsvoorstel de melding aan de toezichthouder een voorwaarde voor het doel van een melding aan de betrokkene. Met de herformulering van de meldplicht aan de toezichthouder is verduidelijkt dat niet alle inbreuken, hoe gering ook, op de beveiliging van persoonsgegevens aan de toezichthouder behoeven te worden gemeld, maar alleen de ernstige datalekken. Het is aan het Cbp om hier door middel van beleidsregels nadere uitwerking en invulling aan te geven.

Het is voornoemde leden nog niet geheel duidelijk welk fundamenteel bezwaar de regering heeft tegen een verruiming van de reikwijdte van de meldplicht, waardoor de meldplicht kan gelden voor iedere vorm van ongeoorloofde toegang tot persoonsgegevens. Wat is er immers onredelijk aan als het ongeoorloofd toegang verschaffen tot persoonsgegevens aan de betrokkene gemeld dient te worden?
Het melden van iedere vorm van ongeoorloofde toegang tot persoonsgegevens aan de betrokkene zou weinig zinvol zijn, omdat daarmee tal van situaties onder de reikwijdte van de meldplicht zouden worden gebracht waarbij geen noemenswaardige ongunstige gevolgen voor de persoonlijke levenssfeer zijn te duchten (bijv. menselijke fouten of systeemfouten waarbij personen betrokken zijn die geen misbruik zullen maken van gegevens die zij ten onrechte hebben ingezien). Een dergelijke ruime verplichting dient naar mijn mening dan ook geen redelijk doel.

De aan het woord zijnde leden delen de vrees van het Cbp dat de wettelijke drempel voor het melden van inbreuken dermate hoog komt te liggen dat in de praktijk alleen nog datalekken zullen worden gemeld waarvan de ernstig nadelige gevolgen voor de bescherming van de verwerkte persoonsgegevens volstrekt evident zijn. Dat in combinatie met de voorgestelde wijziging van artikel 34a, vierde lid, Wet bescherming persoonsgegevens (Wbp) zal er verder toe leiden dat verantwoordelijken inbreuken pas zullen melden op het moment dat zich daadwerkelijk ernstige nadelige gevolgen hebben voorgedaan.
Zoals ook al in de toelichting bij de eerste nota van wijziging is aangegeven deel ik de vrees van het Cbp niet. De wettelijke drempel ligt weliswaar hoger dan in de Telecommunicatiewet, maar de drempel in het eerste lid bestaat enkel daarin dat het om een ernstig datalek moet gaan. Zodra een datalek wordt ontdekt zijn er *per definitie* nadelige gevolgen voor de bescherming van desbetreffende persoonsgegevens. De ernst van een datalek is niet afhankelijk van de daadwerkelijke gevolgen op de langere termijn. Of het om een ernstig datalek gaat, laat zich door de verantwoordelijke eenvoudig beantwoorden aan de hand van factoren als omvang en aard van de inbreuk en aard van de getroffen persoonsgegevens. Door het schrappen van de bijvoeglijke naamwoorden in het vierde lid is verduidelijkt dat het gaat om beschrijving van de gevolgen van de inbreuk voor de verwerking van de persoonsgegevens. Hier komt geen inschatting aan te pas van de vermoedelijke gevolgen op langere termijn.

De leden van de PVV-fractie vragen wat kan worden verstaan onder ‘ernstige nadelige gevolgen’ zoals in artikel 14, eerste lid Wbp wordt voorgesteld. Kan de regering dit met vijf voorbeelden onderbouwen? Hiervoor is, bij de beantwoording van vergelijkbare vragen van de fractie van PvdA

en SP al ingegaan op de betekenis het criterium van het eerste lid. Voorbeelden van meldingsplichtige (ernstige) datalekincidenten zijn:

- Intern wordt binnen een ziekenhuis gesignaleerd dat door een haperende beveiliging (technische storing) medische gegevens zijn ingezien door onbevoegden;
- Een journalistiek programma confronteert een bedrijf met het feit dat als gevolg van een beveiligingslek onder andere persoonlijke gegevens (zoals kopieën van paspoorten of rijbewijzen, bankgegevens en wachtwoorden) van werknemers op de server van het bedrijf door onbevoegden zijn ingezien;
- Een medewerker verliest een laptop met onversleutelde, financiële klantgegevens;
- Een bedrijf krijgt te maken met een hack waarbij klantgegevens en wachtwoorden zijn ontvreemd;
- Een overheidsdatabase met gevoelige persoonsgegevens wordt gehackt waardoor onbevoegden toegang hebben gekregen tot deze gegevens.

De leden van de D66-fractie merken op dat de regering voorstelt om het oorspronkelijke wetsvoorstel te wijzigen en de meldplicht af te zwakken tot die gevallen waarin sprake is van 'ernstige nadelige gevolgen voor de bescherming van de verwerkte persoonsgegevens'. Met deze wijziging ziet de meldplicht, volgens deze leden, alleen nog op die datalekken waarbij de ernstige nadelige gevolgen zich reeds hebben voorgedaan en niet meer op de gevallen waarbij de 'aanmerkelijke kans bestaat dat sprake zal zijn van ernstige nadelige gevolgen'. Deze leden merken op dat in de aanmerkelijke kans een redelijke aanleiding lag besloten voor een melding aan de toezichthouder. Zij zijn dan ook verbaasd over de onderhavige inperking, nu deze tot gevolg heeft dat de bescherming van burgers tegen de aanmerkelijke kans van inbreuken op hun persoonsgegevens wordt afgezwakt en er alleen nog zal worden ingegrepen indien het spreekwoordelijke kalf verdronken is. Hoe verhoudt die keuze zich tot de doelstelling van het wetsvoorstel om de gevolgen van een datalek voor betrokkenen zo veel mogelijk te beperken? Op welke wijze genieten burgers dan nog bescherming tegen inbreuken op hun gegevens indien meldingen alleen nog plaats zullen vinden indien de schade al berokkend is?
Zoals hierboven reeds aan de orde is gekomen, geven de leden van de D66-fractie een onjuiste uitleg aan het criterium van artikel 34a, eerste lid. Zodra een datalek wordt ontdekt zijn er *per definitie* nadelige gevolgen voor de bescherming van desbetreffende persoonsgegevens. Of het om een ernstig datalek gaat, laat zich door de verantwoordelijke eenvoudig beantwoorden aan de hand van factoren als omvang en aard van de inbreuk en aard van de getroffen persoonsgegevens. Dit moet worden beoordeeld op het moment van ontdekken van het datalek aangezien de melding aan de toezichthouder onverwijld dient te geschieden. De melding verschuift daarmee niet naar achteren, zoals deze leden vrezen. Het Cbp zal de afweging met beleidsregels ondersteunen.

De leden van de ChristenUnie-fractie verzoeken om een nadere invulling van het begrip 'ernstig nadelige gevolgen' in artikel I, onderdeel A, onderdelen 1, 2 en 4.
De door deze leden genoemde onderdelen betreffen de zorgplicht voor de verantwoordelijke (artikel 14 Wbp) om het bewerkerscontract zo in te richten dat de bewerker de verantwoordelijke in kennis stelt van een datalek dat onder de meldplicht van artikel 34a valt, zodat de verantwoordelijke zijn meldingsverplichtingen aan het Cbp en aan betrokken personen kan nakomen. De betekenis van dit begrip verschilt niet van de betekenis die het heeft in artikel 34a, eerste lid, waarop ik in de beantwoording van de vragen van de fracties van PvdA, SP en D66 ben ingegaan.

De leden van de ChristenUnie-fractie vragen tevens om nader toe te lichten welke lekken in het oorspronkelijke wetsvoorstel wel gemeld dienden te worden en in dit gewijzigde wetsvoorstel niet meer onder de meldplicht vallen. Het enige verschil dat het gewijzigde wetsvoorstel maakt, betreft de datalekken waarbij de verantwoordelijke passende technische beschermingsmaatregelen heeft genomen waardoor de gelekte gegevens onbegrijpelijk of ontoegankelijk zijn voor een ieder die geen

recht heeft op kennisname van de gegevens (artikel 34a lid 6). Deze lekken moesten op grond van het oorspronkelijke zesde lid wel aan de toezichthouder moeten worden gemeld, maar niet aan de personen wier persoonsgegevens waren gelekt omdat er, als gevolg van de versleuteling, geen ongunstige gevolgen voor hun persoonlijke levenssfeer zijn te duchten. Een voor de hand liggende voorbeeld hierbij is het verlies van laptops, tablets, of mobiele telefoons met (versleutelde) gevoelige persoonlijke gegevens van klanten of relaties. In het gewijzigde wetsvoorstel is ook de meldplicht aan de toezichthouder geschrapt, mits uiteraard de technische bescherming adequaat is, naar de actuele stand van de techniek. De reden hiervan is dat een organisatie die de beveiliging van zijn data goed op orde heeft en daarbij bijvoorbeeld ook heeft nagedacht over kwetsbaarheid van mobiele apparatuur en de technische beschermingsmaatregelen daarop heeft afgestemd, niet alsnog met een meldplicht voor dit soort incidenten moet worden belast. In de toelichting bij de eerste nota van wijziging is aangegeven dat een verantwoordelijke er bij twijfel over de kwaliteit van de technische beschermingsmaatregelen verstandig aan doet om te overleggen met het Cbp. In deze nota scherp ik mijn eerdere bewoordingen in zoverre aan dat bij twijfel over de kwaliteit van de beschermingsmaatregelen, melding aan het Cbp gepast is.

De leden van de ChristenUnie constateren dat het Cbp vreest dat met deze wijziging van artikel 34a, eerste lid, een onnodig hoge drempel wordt opgeworpen. Zij vragen waarom de regering deze vrees niet deelt. Deze leden vragen tevens waarom het moment van de meldplicht is verschoven tot het moment dat de ernstige gevolgen zich daadwerkelijk hebben voorgedaan. Zoals hiervoor bij de beantwoording van de vragen van de fracties van PvdA en D66 al is opgemerkt, is de regering het op dit punt niet met het Cbp eens. Er is met de wijziging van het eerste lid niet beoogd een hogere drempel op te werpen. Zodra een datalek wordt ontdekt zijn er *per definitie* nadelige gevolgen voor de bescherming van desbetreffende persoonsgegevens. Of het om een ernstig datalek gaat, laat zich door de verantwoordelijke eenvoudig beantwoorden aan de hand van factoren als omvang en aard van de inbreuk en aard van de getroffen persoonsgegevens. De ernst van het datalek moet worden beoordeeld op het moment van ontdekken van het datalek. Een verantwoordelijke kan dus niet de gevolgen van een datalek afwachten.

In reactie op de vraag van deze leden hoe de doelmatigheid van de voorgestelde bepaling wordt gecontroleerd, merk ik op dat –binnen het in dit wetsvoorstel voor de meldplicht gekozen ‘getrapte model’- de meldplicht aan de toezichthouder de kern van de regeling vormt (artikel 34a lid 1). Met de clausulering van de meldplicht (het moet gaan om ernstige datalekken) is beoogd een criterium in de wet neer te leggen waarmee niet meldingswaardige datalekken kunnen worden afgegrensd van de meldingswaardige. Het Cbp kan de balans daarin bewaken met beleidsregels die de verantwoordelijke houvast geven bij de afweging. Alleen dan kan een meldplicht voor datalekken het beoogde doel dienen en bijdragen aan een betere bescherming van persoonsgegevens.

3.2 Beslismodel meldplicht Wbp

De leden van de VVD-fractie constateren dat in de nota naar aanleiding van het verslag een beslismodel is opgenomen. Daaruit blijkt dat het mogelijk is dat zich een situatie voordoet die wel aan het Cbp moet worden gemeld maar niet aan de betrokkenen. De omgekeerde situatie, waarbij wel aan de betrokkenen maar niet aan het Cbp moet worden gemeld, kan zich volgens dit beslismodel niet voordoen. Voornoemde leden staat het voor dat de kern van het wetsvoorstel is dat ondernemingen bij geconstateerde datalekken die waarschijnlijk ongunstige gevolgen zullen hebben voor de persoonlijke levenssfeer van de betrokkene, hun verantwoordelijkheid nemen en dit lek zo spoedig mogelijk melden bij degenen wier persoonsgegevens zijn gelekt. Uit het beslismodel volgt echter dat, indien wordt voldaan aan de nieuw geformuleerde criteria, altijd moet worden gemeld bij het Cbp. Kan de regering nog eens nader ingaan op de vraag waarom is gekozen voor deze volgordelijkheid? Ligt het niet meer voor de hand dat ondernemingen melden aan de

betrokkenen in het geval van een inbreuk die waarschijnlijk ongunstige gevolgen zal hebben voor de persoonlijke levenssfeer van de betrokkene? Wat is de reden van het feit dat de toezichthouder, het Cbp, nu in de positie wordt gebracht om als eerste kennis te nemen van een brede range aan datalekken en daarover te oordelen?
De regering heeft met dit wetsvoorstel inderdaad gekozen voor een 'getrapt model', waarin de meldplicht aan de toezichthouder voorop staat en de meldplicht aan de betrokkene daarop volgend wordt geregeld. De reden hiervoor is dat de wettelijke meldplicht een tweeledig doel heeft: de meldplicht datalekken ondersteunt het toezicht door de toezichthouder op de algemene verplichting om persoonsgegevens op een goede en zorgvuldige manier te beveiligen en versterkt de positie van de burger. Eenzelfde model wordt in de hiervoor reeds aangehaalde OESO-richtlijnen uit 2013 gevolgd, en ook in de bestaande of voorgestelde regelgeving op Europees niveau (zie bijv. de EU-richtlijn voor privacy in de telecommunicatiesector en de Commissievoorstellen voor een algemene verordening gegevensbescherming en voor een richtlijn gegevensbescherming in de sectoren justitie en politie). In het herzieningsvoorstel van het Dataprotectieverdrag van de Raad van Europa wordt, bij wijze van minimumstandaard, alleen de verplichting tot het melden van een datalek aan de toezichthouder geregeld dat "de rechten en vrijheden van personen ernstig in gevaar brengt".
Juist doordat in de regeling van het wetsvoorstel een bedrijf of instantie de eerste melding van een datalek (vertrouwelijk) aan het Cbp doet (en het Cbp alle ins en outs van het datalek kent), kan het Cbp in de gaten houden of de getroffen personen vervolgens op een zorgvuldige en behoorlijke wijze worden geïnformeerd. Zo nodig kan het Cbp de melding aan de getroffen personen afdwingen, op straffe van een bestuurlijke boete (artikel 34a lid 5). Het getrapte model betekent niet dat een verantwoordelijke moet wachten op een reactie van het Cbp, voordat getroffen klanten of burgers worden ingelicht. Het inlichten van personen kan tegelijkertijd of zelfs voordat het Cbp wordt ingelicht. Daarnaast staat het verantwoordelijken vrij om klanten of burgers uit eigen beweging in te lichten over een datalek, als deze buiten de reikwijdte van de wettelijke meldplicht valt.

Omdat het Cbp in het voorgestelde model de beschikking krijgt over veel en verstrekkende informatie over datalekken, nieuwe voorbeelden van datalekken en adequate beveiliging van persoonsgegevens, zien de leden van de VVD-fractie meerwaarde in een systeem waarin het Cbp deze informatie en kennis die het opdoet, deelt met ondernemingen. Op basis daarvan zouden die ondernemingen hun digitale beveiliging nader kunnen aanpassen. Hoe kijkt de regering hiertegen aan?
Zoals ik in paragraaf 1 van de nota naar aanleiding van het verslag heb aangegeven zal het Cbp de opgedane kennis en ervaringen met het Nationaal Cyber Security Centrum en met andere toezichthouders, of met het publiek en andere belanghebbenden kunnen delen. Dat kan in periodiek overleg met andere toezichthouders en ook in het jaarverslag of andere publicaties op de website. Ik ben het met deze leden eens, dat het delen van kennis en ervaring met ondernemingen of brancheorganisaties, kan bijdragen aan een betere digitale beveiliging en het voorkomen van datalekken.

3.3 Verhouding verantwoordelijke voor de verwerking en bewerker

De leden van de D66-fractie merken op dat de wettelijke verplichting van verantwoordelijken tot het bijhouden van een overzicht van alle inbreuken vervalt. Welke stimulans resteert dan voor verantwoordelijken van dataverwerkingen om alert te zijn op inbreuken en zich rekenschap te geven van de gevolgen voor de persoonlijke levenssfeer van betrokkenen?
Deze leden gaan er mijns inziens ten onrechte vanuit dat een wettelijke verplichting voor verantwoordelijken om een overzicht bij te houden van alle inbreuken, een stimulerend effect heeft op het opsporen van datalekken. Ik zie deze samenhang niet. Voor het opsporen en onderkennen van datalekken is vooral van belang dat de organisatie de beveiliging van persoonsgegevens op orde heeft, dat deze openstaat voor externe/interne signalen die duiden op beveiligingsincidenten, dat de

bedrijfscultuur het privacybewustzijn stimuleert en dat bijvoorbeeld periodiek via audits wordt onderzocht welke zaken verbetering behoeven.

Deze leden hebben kennisgenomen van de kritiek van het Cbp van februari 2014 op de voorgenomen wijziging van het wetsvoorstel. Het Cbp meent dat de nieuwe formulering van artikel 34, zesde lid, Wbp risicovol is. Indien de meldplicht vervalt in het geval de verantwoordelijke meent dat sprake is van passende technische beschermingsmaatregelen, leidt dat tot een reëel risico dat inbreuken met ernstige nadelige gevolgen voor de bescherming van persoonsgegevens noch aan de toezichthouder, noch aan de betrokkenen worden gemeld. Hoe beschouwt de regering die kritiek en hoe denkt zij dat risico te kunnen ondervangen?
In het zesde lid is bepaald dat er geen wettelijke meldplicht bestaat als gelekte persoonsgegevens op een passende wijze middels technische maatregelen zijn beschermd waardoor de gelekte persoonsgegevens onbegrijpelijk of ontoegankelijk zijn voor eenieder die geen recht heeft op kennisname van de gegevens. Zoals hiervoor, bij de beantwoording van de vragen van de fracties van VVD en PvdA is opgemerkt is dit een strenge norm die van geval tot geval door de verantwoordelijke moet worden gehanteerd, naar de actuele stand van de techniek. Indien bij de verantwoordelijke twijfel bestaat over de kwaliteit van de technische beschermingsmaatregelen, zal een melding bij het Cbp gepast zijn. Het Cbp wordt op deze wijze in staat gesteld om de kwaliteit van de technische beschermingsmaatregelen te beoordelen. Dit is met name van belang omdat het Cbp zo nodig een melding aan betrokkene kan afdwingen indien waarschijnlijk ongunstige gevolgen voor diens persoonlijke levenssfeer te duchten zijn. Het oordeel van het Cbp is hierbij doorslaggevend (zevende lid).

4. Verhouding tot andere rechtsgebieden

4.1 Verhouding tot specifieke meldplicht op grond van de Telecommunicatiewet

De leden van de D66-fractie lezen in de eerste nota van wijziging dat de meldplicht volgens de regering ruimer lijkt te zijn dan in de Telecommunicatiewet, terwijl dat niet is beoogd. Wat wordt bedoeld met ‘lijkt’? Op grond waarvan meent de regering nu dat de onderhavige meldplicht afwijkt van de Telecommunicatiewet? Zijn er nieuwe feiten die tot deze constatering hebben geleid?
Er zijn geen nieuwe feiten. Wel is, omdat de soms abstracte bewoordingen die in Europese regelgeving worden gebruikt, vatbaar zijn voor interpretatieverschillen nog eens goed naar de bewoordingen van de meldplicht in de Telecommunicatiewet gekeken. Uit de wetsgeschiedenis van de implementatie van richtlijn 36/2009/EG blijkt dat de abstracte bewoordingen van artikel 11.3a, eerste lid, Tw neerkomen op een ruime meldplicht. Dit komt omdat een inbreuk in verband met persoonsgegevens *per definitie* nadelige gevolgen heeft voor de bescherming van de door de inbreuk geraakte persoonsgegevens. De oorspronkelijke formulering van de meldplicht in de Wbp gebruikte deels dezelfde bewoordingen, maar gaf daar een andere interpretatie aan, door te spreken over een “aanmerkelijke kans” op nadelige gevolgen voor de bescherming van persoonsgegevens. Deze kans moest bovendien “redelijkerwijs” kunnen worden “aangenomen”. Omdat de formulering van artikel 34a, eerste lid, Wbp vragen bij verschillende fracties vragen opriep, en eerder ook bij de Afdeling bestuursrechtspraak in verband met het lex certa-beginsel, is gemeend nauwer aansluiting te zoeken bij de tekst van de Tw-meldplicht, met toevoeging van het criterium “ernstig” om duidelijk te maken dat er bij de Wbp een ondergrens is van datalekken waarvoor een wettelijke meldplicht niet noodzakelijk is omdat er geen of geringe gevolgen zijn te duchten voor de persoonlijke levenssfeer.

4.2 Rol van het Cbp

De leden van de D66-fractie merken op dat de aangewezen toezichthouder, het Cbp, naast een repressieve taak ook een preventieve rol benadrukt. In hoeverre ziet de regering bij de inperking van de meldplicht datalekken naast een repressieve rol nog ruimte voor preventief optreden door de toezichthouder?
Zoals ik hiervoor reeds heb opgemerkt is de meldplicht bij eerste nota van wijziging aangescherpt, maar betekent dat geenszins dat het Cbp geen preventieve rol meer speelt. Allereerst wijs ik op het belang van het tot stand brengen van beleidsregels waarmee het criterium van artikel 34a, eerste lid (afgrenzing van meldingswaardige en niet meldingswaardige datalekken) nadere uitwerking en invulling dient te krijgen. Deze beleidsregels zullen daarnaast invulling en uitwerking kunnen geven aan de strenge norm die besloten ligt in artikel 34a, zesde lid. Het is voor bedrijven en organisaties op voorhand goed om te weten hoe het Cbp tegen de kwaliteit van bepaalde technische beschermingsmaatregelen op bijvoorbeeld mobiele apparatuur aankijkt. Zij kunnen aan de hand daarvan beter beoordelen of een concreet datalek op grond van het zesde lid van melding is uitgezonderd.
De leden van de ChristenUnie-fractie vragen hoe en door wie wordt beoordeeld of technische beschermende maatregelen na het constateren van een datalek afdoende zijn. Welke rol heeft het Cbp in dezen? Op welke wijze zal dit wetsvoorstel een preventieve werking hebben en welke preventieve taken zijn in dit opzicht voor het Cbp zijn weggelegd? De beoordeling of de technische beschermingsmaatregelen van dien aard zijn dat de gelekte gegevens onbegrijpelijk of ontoegankelijk zijn voor eenieder die geen recht heeft op de kennisname van de gegevens berust bij de verantwoordelijke. Als gezegd is dit een strenge norm (artikel 34a, zesde lid) waaraan het Cbp in beleidsregels uitwerking kan geven, zodat de opvattingen en inzichten van het Cbp op voorhand voor verantwoordelijken kenbaar zijn. Ik heb kennisgenomen van de ervaring van het Cbp dat verantwoordelijken lang niet altijd een realistisch beeld hebben van de mate waarin de toegepaste encryptiemaatregelen daadwerkelijk afdoende zijn. Dit is echter geen reden om het oordeel daarover in elk individueel geval bij het Cbp te beleggen. Bij twijfel zal een melding aan het Cbp gepast zijn; het Cbp kan zo nodig ook een melding aan de getroffen personen afdwingen. Het Cbp kan met name met beleidsregels een bijdrage in preventieve zin leveren. De preventieve werking van het wetsvoorstel ziet op het verminderen van datalekken en, zo zij zich voordoen, op het beperken van de gevolgen ervan, onder andere door een goede communicatie van de verantwoordelijke met de personen van wie de gegevens zijn gecompromitteerd.

4.3 Verhouding tot meldplicht incidenten Wet op het financieel toezicht

De leden van de SP-fractie hebben geen duidelijk antwoord ontvangen op de vraag op welke wijze de belangen van betrokkenen en belanghebbenden verzekerd zijn als een financiële onderneming een datalek geheim mag en kan houden.
De overweging bij de uitzondering van het artikel 34a, negende lid, is dat openbare kennisgevingen van datalekken aan betrokkenen in de financiële sector – mede tegen de achtergrond van de financiële crisis – te risicovol zijn om *dwingend* te worden voorgeschreven. Deze instellingen moeten een ernstig datalek echter wel melden bij het Cbp. Daarnaast geldt dat de relatie met de cliënten van een financiële onderneming wordt bestreken door de specifieke zorgplichten en de algemene zorgplicht van de financiële onderneming die per 1 januari 2014 in de Wft is opgenomen (artikel 4:24a Wft). Zoals in de nota naar aanleiding van het verslag is opgemerkt kan een financiële onderneming te allen tijde in overleg treden met de betrokken toezichthouder over het wel of niet informeren van de betrokken klanten over een datalek. Daarbij kan ook de opvatting van het Cbp worden betrokken, het Cbp is immers op de hoogte van het datalek. In dat overleg zullen de belangen van cliënten en belanghebbenden nadrukkelijk een rol spelen, net als de risico's die zijn verbonden aan een openbare kennisgeving (misbruik door kwaadwillende personen en ondermijning van het vertrouwen in het financiële stelsel). Ik verwacht dat de specifieke toezichthouders erop toe

zullen zien dat een financiële onderneming naar behoren zijn verantwoordelijkheid neemt in rechtstreeks contact met zijn cliënten.

5. Sanctionering

De leden van de VVD-fractie zijn van mening dat het goed zou zijn om het voorgestelde artikel 66, tweede lid, Wbp en het artikel 15.4, vierde lid, Telecommunicatiewet nader uit te werken. Dit geldt temeer nu het Cbp in deze artikelen de mogelijkheid wordt geboden om ondernemingen een forse boete op te leggen. Met name de vraag wanneer het Cbp hiertoe zal overgaan, heeft volgens deze leden nadere invulling nodig. Daarnaast menen zij dat het goed zou zijn om meer duidelijkheid te bieden over de hoogte van de op te leggen boetes. Wordt hier een staffel gehanteerd? Welke situatie geeft aanleiding om het maximale boetebedrag van €450.000 op te leggen? Ook ten aanzien van deze kwestie zijn deze leden van mening dat het absoluut de voorkeur heeft om op de uitwerking en invulling van deze discretionaire bevoegdheid enige democratische controle uit te kunnen oefenen. Hoe kijkt de regering aan tegen het voorstel om deze kwesties bij algemene maatregel van bestuur te regelen?
In de tweede nota van wijziging op dit wetsvoorstel, die kort geleden aan de Tweede Kamer is verzonden, wordt voorgesteld om het naleven van de meldplicht datalekken in de Wbp in de hoge categorie van het gewijzigde artikel 66 lid 2 Wbp onder te brengen. Het wettelijke boetemaximum bedraagt € 810.000, met voor rechtspersonen een mogelijke uitloop tot 10% van de jaaromzet. Voorafgaand aan het opleggen van een bestuurlijke boete, zal het Cbp eerst een bindende aanwijzing geven, tenzij het niet-naleven van de meldplicht opzettelijk is gebeurd. Het wettelijk boetemaximum biedt voldoende ruimte voor het Cbp om een boete(toemetings)beleid op te stellen waarmee van geval tot geval tot een passende en evenredige bestraffing kan worden gekomen. Het Cbp zal bij het vaststellen van beleidsregels terzake rekening moeten houden met factoren als de ernst van de overtreding, de mate waarin deze aan de overtreder kan worden verweten en de omstandigheden van het geval, waaronder de persoon van de dader (artikel 5:46, tweede lid, Awb). Voor het regelen van deze kwesties bij algemene maatregel van bestuur bevat het wetsvoorstel geen grondslag. De regering is daarvan ook geen voorstander omdat de invulling van het boete(toemetings)beleid aan de toezichthouder kan worden overgelaten.

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

6.1 Administratieve lasten en nalevingskosten

De leden van de PvdA-fractie vinden een goede afweging tussen de administratieve lasten van de meldplicht en de te bereiken effecten uiteraard belangrijk. Daarom kunnen zij zich voorstellen dat er voorkomen wordt dat bagatelzaken gemeld moeten worden. Graag horen zij de regering hiervoor mogelijkheden ziet binnen de oorspronkelijke wettekst.
Gelet op mijn antwoord op de eerdere gestelde vragen over de gewijzigde redactie van artikel 34a, eerste lid, ben ik van mening dat de oorspronkelijke wettekst onvoldoende houvast bood om tot een goede afgrenzing te komen van datalekken waarbij het wel of niet noodzakelijk is om een melding aan de toezichthouder te doen. Zoals ik heb opgemerkt is het bij nota van wijziging voorgestelde criterium betrekkelijk eenvoudig te hanteren. Of een datalek moet worden gemeld hangt af van aard en omvang van de inbreuk en de aard van de persoonsgegevens die aan onrechtmatige verwerking of misbruik zijn blootgesteld. In de voorbereiding op het van kracht worden van een wettelijke meldplicht voor datalekken zal iedere verantwoordelijke moeten inventariseren wat de risico's van een datalek voor de door hem verwerkte persoonsgegevens zijn en hoe hij de beoordeling van datalekken en de uitvoering van de meldplicht binnen de organisatie belegt. Het is voor mij lastig om in zijn algemeenheid uitspraken te doen over de precieze afbakening. In de memorie van toelichting

wordt het voorbeeld gebruikt van een hack van de ledenadministratie van een sportvereniging. Een dergelijk datalek valt normaal gesproken niet onder het bereik van deze meldplicht. Het woord 'bagatel' lijkt me in dit verband echter niet op zijn plaats, liever zou ik spreken over een niet-meldingsplichtig datalek. Bij bagatelzaken heb ik een beeld van een verkeerd geadresseerde brief of email die door de ontvanger onmiddellijk retour wordt gezonden of een telefonisch gegeven inlichting aan een persoon die niet bevoegd was deze informatie te ontvangen. Al dit soort voorvallen hebben gemeen dat een melding aan de toezichthouder niet noodzakelijk is.

De leden van de CDA-fractie en D66-fractie vragen voorts of andere manieren zijn overwogen om melding van bagatelzaken te voorkomen. Als gezegd spreek ik liever niet over bagatelzaken maar over niet-meldingsplichtige datalekken. De afgrenzing tussen beide categorieën ligt besloten in de formulering van de meldplicht aan de toezichthouder in het eerste lid van artikel 34a: het moet gaan om "ernstige nadelige gevolgen voor de bescherming van de verwerkte persoonsgegevens". Zoals hiervoor is aangegeven is dat een betrekkelijk eenvoudig te hanteren criterium waar het Cbp door middel van beleidsregels nadere uitwerking en invulling aan kan geven.

Volledigheidshalve vragen de leden van de CDA-fractie of de regering bij de beraming van de nalevingskosten nog steeds is uitgegaan van één melding per bedrijf per jaar. Daarvan kan worden gesteld dat dit een niet geheel realistische inschatting is. Immers, bij een serieus datalek zullen doorgaans gegevens van meerdere personen lekken. Deze leden wijzen op de commentaren van VNO-NCW op het wetsvoorstel waaruit blijkt dat het aantal betrokkenen bij de grotere lekken bij Nederlandse websites varieerde van 824 tot 750.000 personen per onderneming. Deze leden ontvangen graag op dit punt een verduidelijking.
Ik kan deze leden melden dat er geen nieuwe berekeningen zijn opgesteld. Hier is ook geen aanleiding voor omdat de nota van wijziging geen substantiële effecten op de beramingen van de administratieve lasten en nalevingskosten zal hebben, behoudens het schrappen van de verplichting om een overzicht van alle datalekken bij te houden. Dit scheelt jaarlijks € 543.650 aan nalevingskosten. Het informeren van meerdere getroffen personen kan geschieden via een persoonlijk elektronisch bericht in combinatie met algemene berichtgeving op de website.

De leden van de D66-fractie lezen in de eerste nota van wijziging dat de wijzigingen een beter evenwicht beogen tussen de bescherming van persoonsgegevens en de administratieve lasten en nalevingskosten. Alhoewel deze leden begrijpen dat uitvoerbaarheid een belangrijk aspect is van dit wetsvoorstel, zien zij geen onderbouwing van deze stellingname van de regering. Op grond waarvan meent de regering dat het oorspronkelijke wetsvoorstel niet langer in verhouding staat tot de administratieve lasten en nalevingskosten? Hoe verhoudt deze wijziging van het wetsvoorstel zich tot de constatering in de memorie van toelichting dat de berekende kosten en lasten slechts berusten op 'aannames' en niet op harde feiten? Beschikt de regering over nieuwe meer feitelijke informatie op grond waarvan zij meent dat deze afzwakking van de meldplicht datalekken nodig is? Het verheugt mij dat de leden van de D66-fractie de uitvoerbaarheid van een wettelijke meldplicht voor datalekken ook van belang achten. Zoals hiervoor bij de beantwoording van eerdere vragen al aan de orde kwam, heeft de regering niet beoogd de meldplicht af te zwakken maar is met een scherper oog gekeken naar baten en lasten van de meldplicht en is op grond daarvan tot een verduidelijking (eerste lid), aanscherping (zesde lid) en schrapping (achtste lid, protocolplicht) gekomen. Zoals ook eerder beschreven is, krijgt het Cbp de ruimte om door middel van beleidsregels nadere uitwerking en invulling te geven aan de algemeen geformuleerde criteria van het eerste, tweede en zesde lid. Naar mijn verwachting wordt de uitvoerbaarheid van de meldplichtregeling met deze wijzigingen gediend.

Voornoemde leden merken voorts op dat de regering niet uitsluit dat bedrijven die in goede beveiliging investeren, de risico's op een datalek kunnen verkleinen, zoals zij bij het oorspronkelijke

voorstel naar voren brachten. In hoeverre zou dat de geschatte lasten en kosten voor bedrijven kunnen verzachten? Het investeren in goede beveiliging zal de risico's op een datalek kunnen verkleinen, tegelijkertijd is moeilijk te kwantificeren in hoeverre dit rechtstreeks van invloed zal zijn op de lasten en kosten voor bedrijven die met een eventueel datalek te maken krijgen. Ook moet worden bedacht dat 100 procent veilig niet bestaat; ook bedrijven met state-of-the-art beveiligingsmaatregelen kunnen met een datalek te maken krijgen.

6.2 Bestuurlijke lasten en effecten voor de rechtspraak

De leden van de CDA-fractie vragen de regering of haar opmerking in de nota naar aanleiding van het verslag dat voor het Cbp een houdbaar financieel kader is geschapen het voornemen van de regering weergeeft om het Cbp geen extra financiële middelen meer toe te kennen of dat zij die mogelijkheid openhoudt als gevolg van het nauwlettend monitoren na inwerkingtreding van onderhavig wetsvoorstel.
In aanvulling op het hierboven gegeven antwoord over administratieve lasten en nalevingskosten verwacht de regering niet dat de nota van wijziging substantiële effecten zal hebben op de bestuurlijke lasten die eerder waren voorzien voor het Cbp. Voorafgaand aan de inwerkingtreding zal ook de voorbereiding van de uitvoering nauwlettend worden gevolgd. Mogelijke beleidsregels waarin invulling wordt gegeven aan de verplichtingen van artikel 34a Wbp behoeven de goedkeuring van de Minister van Veiligheid en Justitie en van Binnenlandse Zaken en Koninkrijksrelaties (zie onderdeel F van de tweede nota van wijziging). Na inwerkingtreding zal uiteraard worden gemonitord of de effecten voor de werklast van het Cbp overeenkomen met de verwachte effecten. Het financiële kader van het Cbp is daarbij evenwel een gegeven. In antwoord op de vraag naar de frequentie van de monitoring na inwerkingtreding en de aansluiting bij de geldende evaluatiebepaling van de Wbp, merk ik op dat de evaluatiebepaling van de Wbp (artikel 80) is uitgewerkt. Deze bepaling voorzag in een eenmalige evaluatie binnen vijf naar inwerkingtreding van de Wbp en niet in een periodieke evaluatie. De monitoring van de meldplicht datalekken kan meelopen in de reguliere begrotings- en verantwoordingscyclus van het ministerie van Veiligheid en Justitie en de rapportages daarover aan het parlement.

Deze leden vragen voorts of de regering een maximumbedrag voor ogen staat voor het totaal aan nalevingskosten dat voor rekening komt van ondernemingen, dit samenhangend met het risico dat het aantal meldingen door bedrijven hoger uitvalt dan het aantal waar de regering thans van uitgaat?
De regering heeft niet een maximumbedrag aan nalevingskosten voor ogen. Bij de voorbereiding van dit wetsvoorstel is aangenomen dat 50% van het aantal ondernemingen jaarlijks een melding zal moeten doen, zowel aan het Cbp als aan de betrokkene. De administratieve lasten voor het doen van een melding aan het Cbp zijn berekend op jaarlijks € 543.650. De nalevingskosten voor het doen van een melding aan betrokkene zijn berekend op jaarlijks € 430.355. Zoals hiervoor al is opgemerkt is de verplichting tot bijhouden van een overzicht van alle datalekken bij de eerste nota van wijziging vervallen en daarmee ook de geschatte nalevingskosten daarvan (jaarlijks € 543.650).

6.3 Gevolgen voor de rijksbegroting

Het baart de leden van de CDA-fractie zorgen dat onduidelijk is hoe de lastenstijging die uit onderhavig wetsvoorstel voortvloeit, moet worden gecompenseerd in het totaal van de toe-en afname van lasten binnen de begroting van het ministerie Veiligheid en Justitie. De regering geeft aan dat niet exact kan worden aangegeven hoe dat zal gebeuren, maar dat de Kamer hiervan op de hoogte wordt gesteld middels de gebruikelijke rapportages. Deelt de regering de opvatting dat het gezien de hoogte van de administratieve lasten en nalevingskosten gewenst is hier nu al meer inzicht in te verschaffen? Deze leden zouden het op prijs stellen als de regering de ideeën kenbaar wil

maken die zij daarover heeft ontwikkeld sinds het uitbrengen van onderhavig wetsvoorstel op 17 juni 2013.
Zoals ook in de reactie op de voorgaande vraag van deze leden is opgemerkt, is het financieel kader voor het Cbp een gegeven. In het jaar 2013 jaar zijn aan het Cbp extra financiële middelen toegekend, naar aanleiding van de motie van het lid Schouw, met het oog op de bekostiging van de taken van het Cbp nu en in de toekomst (Kamerstukken II 2012/13, 30400 VI, nrs. 100 en 71). Hiermee is een houdbaar financieel kader geschapen. Door het schrappen van de verplichting om een overzicht bij te houden van alle datalekken worden de nalevingskosten teruggedrongen. Ten slotte mag niet onvermeld blijven dat uit de eerste ervaringen die met de specifieke meldplicht voor datalekken in de Telecommunicatiewet zijn opgedaan, niet van een stortvloed aan meldingen sprake is. De prognose ging uit van 2430 meldingen per jaar; in werkelijkheid ontving ACM 211 meldingen in 2013, en in 2014 (tot en met oktober) 279 meldingen. Voor de goede orde merk ik op dat de Tw-meldplicht geldt voor ongeveer 600 bij de Autoriteit Consument en Markt geregistreerde aanbieders van openbare elektronische communicatiediensten. De Wbp-meldplicht zal voor ongeveer 132.000 verantwoordelijken gaan gelden in de private en publieke sector.

De staatssecretaris van Veiligheid en Justitie,

F. Teeven