Tweede Kamer der Staten-Generaal

2

Vergaderjaar 2012–2013

33 662

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

Nr. 5

VERSLAG

Vastgesteld 9 september 2013

De vaste commissie voor Veiligheid en Justitie, belast met het voorbereidend onderzoek van dit voorstel van wet, heeft de eer als volgt verslag uit te brengen. Onder het voorbehoud dat de hierin gestelde vragen en gemaakte opmerkingen voldoende zullen zijn beantwoord, acht de commissie de openbare behandeling van het voorstel van wet genoegzaam voorbereid.

kst-33662-5
ISSN 0921 - 7371
's-Gravenhage 2013

Inhoudsopgave **blz.**

ALGEMEEN DEEL

1. Strekking van het wetsvoorstel

De leden van de VVD-fractie hebben met belangstelling kennisgenomen van het wetsvoorstel. Zij erkennen het gevaar van datalekken voor de bescherming van persoonsgegevens en het vertrouwen dat de burger kan hebben in instanties die zijn persoonsgegevens verwerken. Om die reden zijn zij verheugd met het onderhavige wetsvoorstel. Wel hebben zij nog enkele vragen.

De leden van de PvdA-fractie hebben met belangstelling kennisgenomen van het wetsvoorstel. De regering geeft hiermee invulling aan een wens van deze leden. Zij zien het toenemende belang van een goede bescherming van de digitaal opgeslagen persoonsgegevens, vooral omdat er steeds meer informatie over mensen digitaal beschikbaar is en er met regelmaat pogingen gedaan worden om gegevens te ontvreemden. Een meldplicht kan hieraan bijdragen. Het voorstel geeft de leden van de PvdA-fractie aanleiding enkele vragen te stellen.
De aan het woord zijnde leden 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 leden van de PVV-fractie hebben met belangstelling kennisgenomen van voorliggend wetsvoorstel. Zij hebben hierover een aantal vragen en opmerkingen die verderop in het verslag aan de orde zullen komen.

De leden van de SP-fractie hebben met belangstelling kennisgenomen van het voorliggende wetsvoorstel, waarmee een meldplicht wordt ingevoerd voor datalekken. Zij zijn een groot voorstander van een dergelijke 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 zich te beschermen tegen inbreuken op hun privacy, openbaarmaking van persoonsgegevens of identiteitsfraude. Voor het vertrouwen in een zorgvuldige omgang met persoonsgegevens is het, zoals het wetsvoorstel ook regelt, van belang dat een datalek wordt gemeld aan zowel de betrokkene zelf als het Cbp. De leden zijn het eens met de constatering van de regering in de toelichting dat de meldplicht bijdraagt aan het behoud en herstel van vertrouwen in de omgang met persoonsgegevens. Dat is hard nodig nu veel mensen op dit moment onvoldoende vertrouwen hebben in een zorgvuldige omgang met hun persoonsgegevens en het gevoel hebben niet te weten waar persoonsgegevens blijven.

De leden van de CDA-fractie hebben met belangstelling kennisgenomen van het wetsvoorstel. Zij onderschrijven het doel van de voorgestelde meldplicht en van andere meldplichten met betrekking tot datalekken of andere ernstige incidenten met betrekking tot de bedrijfsvoering. Dit doel kan omschreven worden als het bevestigen en waar nodig herstellen van het vertrouwen van het publiek, de klanten, de markt, de overheid en de toezichthouders in de desbetreffende instelling of het desbetreffende bedrijf. Zij beschouwen het wetsvoorstel als een logische aansluiting op reeds bestaande meldplichten en als een logisch voorschot op Europese

voorstellen voor regelgeving voor nieuwe meldplichten. Deze leden hebben geconstateerd dat een groot aantal organisaties hun zienswijze over het wetsvoorstel hebben ingediend en dat in de heldere memorie van toelichting op gedegen wijze op deze commentaren is ingegaan. Vandaar dat deze leden slechts een beperkt aantal vragen en opmerkingen hebben.

De leden van de fractie van D66 hebben kennisgenomen van het wetsvoorstel. Zij zien het belang van een meldplicht, maar hebben nog een aantal vragen over de exacte invulling van de meldplicht. Vooraleerst willen zij 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 leden willen graag weten of de regering deze analyse deelt en waarom deze keuze toch is gemaakt. 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 leden van de ChristenUnie-fractie hebben met belangstelling kennisgenomen van het wetsvoorstel dat een meldplicht geïntroduceerd in de Wet bescherming persoonsgegevens (Wbp) voor verantwoordelijken voor de verwerking van persoonsgegevens in geval van gebleken doorbrekingen van de getroffen maatregelen ter beveiliging van persoonsgegevens. Zij hebben over het wetsvoorstel nog enige vragen en opmerkingen.

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.

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.

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 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 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.

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.

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. Voorts lezen zij 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?

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. Kan de regering voorts 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.

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 een hypothetische situatie betreft. Kan de regering aangeven hoe deze opmerking zich verhoudt tot de berichtgeving rond «Lektober»? Afgezien van bedoelde berichtgeving, vragen deze leden 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?

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?
De aan het woord zijnde leden 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?
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?
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.
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.

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 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 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.
Voorts snappen de aan het woord zijnde leden niet wat de regering bedoelt met haar reactie op het voorstel van Bits of Freedom om elk datalek te laten melden. Zij stelt dat andere varianten van lekken ook nadelig kunnen zijn voor consumenten, maar dat dat niet het onderwerp van dit wetsvoorstel is. Deze leden zijn juist van mening dat het zou moeten 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.

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.

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.
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 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 begrippen «redelijkerwijs», «aanmerkelijke kans op nadelige gevolgen» en «waarschijnlijk ongunstige gevolgen», zijn niet heel concreet. 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? Hoe wordt er voor gezorgd dat er in de praktijk geen onduidelijkheid komt te bestaan wanneer de meldplicht wel en niet geldt?

De leden van de CDA-fractie vragen aan welk tijdsbestek moet worden gedacht bij de maatstaf «onverwijld».

Voorts hebben deze leden 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. Zij 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.

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 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.
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.

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.

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?

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.

4.2 Verhouding tot meldplicht incidenten Wet op het financieel toezicht

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. De regering stelt dat cliënten ook geïnformeerd moeten worden vanuit de zorgplicht van de financiële instelling. Deze leden begrijpen 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.

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?

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.

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 van 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?

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.

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 boetebevoegdheid 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.
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?

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. Waarom is er niet voor gekozen hier direct bij aan te sluiten?
Wanneer kan de Kamer de aangekondigde nota van wijziging tegemoet zien met betrekking tot de uitbreiding van de bestuurlijke bevoegdheden van het Cbp?

De leden van de CDA-fractie merken op dat het wetsvoorstel voorziet in een stevige bestuurlijke boete van maximaal 450.000 euro, terwijl het voorstel voor een EU-verordening algemene gegevensbescherming een aanzienlijk hoger boetemaximum voor hetzelfde vergrijp kent. Zij vragen waarom niet is gekozen voor dit hogere boetemaximum.

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.
Voorts vragen deze leden 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.
De aan het woord zijnde leden snappen de voorstellen in de adviezen van het Cbp en het Nederlands genootschap Functionarissen Gegevensbescherming (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?

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?

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.

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. Daarnaast willen zij 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.

7.2 Bestuurlijke lasten en effecten voor de rechtspraak

De leden van de PvdA-fractie geven aan dat naast uitvoeringskosten aan de kant van de melders, de extra taak natuurlijk ook kosten met zich meebrengt voor het Cbp. Die kosten bestaan uit het registreren van de meldingen. Voor een geloofwaardige meldplicht is echter ook toezicht en extra onderzoek nodig als er twijfel is of een bedrijf alle relevante datalekken meldt. Deze leden vragen of het Cbp door de meldplicht een grotere takenuitbreiding krijgt dan enkel het bijhouden van een register? Zij zijn van mening dat de meldplicht vanaf het begin goed moet lopen. Daarom vragen zij de regering 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. Is de regering daartoe bereid?

De leden van de D66-fractie merken op dat de inwerkingtreding van de meldplicht voor het Cbp beheersmatig een aantal gevolgen heeft, maar 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. Heeft de regering gekeken 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 de zicht op de beheersaspecten van de onderhavige meldplicht?

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.

7.3 Positie van rijksoverheid

De leden van de SP-fractie constateren dat de meldplicht datalek 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?

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?

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 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.

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 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?

Artikel 34a, achtste lid, Wbp

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.

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?

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?

De voorzitter van de commissie,
Jadnanansing

De adjunct-griffier van de commissie,
Van Doorn