Tweede Kamer der Staten-Generaal

2

Vergaderjaar 2011–2012

32 761 Verwerking en bescherming persoonsgegevens

Nr. 31

VERSLAG VAN EEN SCHRIFTELIJK OVERLEG

Vastgesteld 15 juni 2012

De vaste commissie voor Veiligheid en Justitie heeft een aantal vragen ter beantwoording voorgelegd aan de staatssecretaris van Veiligheid en Justitie over de brief van de staatssecretaris van Veiligheid en Justitie inzake Herziening van de regels over de bescherming van persoonsgegevens binnen de Europese Unie (Kamerstuk 32 761, nr. 17), de brieven van de staatssecretaris van Buitenlandse Zaken inzake Fiche: Richtlijn gegevensbescherming opsporing en vervolging (Kamerstuk 22 112, nr. 1371) en Fiche: Verordening gegevensbescherming (Kamerstuk 22 112, nr. 1372) en het EU-voorstel: Herziening EU-wetgeving bescherming persoonsgegevens COM(2012).
Bij brief van 14 juni 2012 heeft de staatssecretaris van Veiligheid en Justitie deze vragen beantwoord. Vragen en antwoorden zijn hierna afgedrukt.

De voorzitter van de commissie,De RoonAdjunct-griffier van de commissie,
Hessing-Puts

kst-32761-31
ISSN 0921 - 7371
's-Gravenhage 2012

Inhoudsopgave

I. Vragen en opmerkingen vanuit de fracties

Vragen en opmerkingen vanuit de VVD-fractie

De leden van de VVD-fractie achten het onwenselijk en zelfs in zekere zin exemplarisch dat de Europese Commissie wel aandacht besteedt aan een vermeende daling van de administratieve lasten, maar geen berekening aanlevert van de nalevingskosten die de nieuwe regelgeving met zich meebrengt voor het Europese bedrijfsleven. Deze leden achten het essentieel dat een heldere berekening hiervan wordt opgesteld en aangeleverd. Vooral de «privacyofficer» bij grotere bedrijven moet tot een enorme kostenpost leiden waarvan de opbrengst verre van zichtbaar is.
Voornoemde leden vragen of het wenselijk is om als criterium van het begrip persoonsgegevens op te nemen dat het gaat om gegevens waarmee een persoon van andere personen kan worden onderscheiden (individualiserende gegevens). Ook VNO-NCW acht een betere omschrijving van het begrip persoonsgegevens noodzakelijk. Graag ontvangen deze leden een reactie op dit punt.
Ook vragen zij of de eisen die worden gesteld aan de doelomschrijving van de opslag van de persoonsgegevens voldoende zijn. Dient expliciet te worden opgenomen dat er ook bescherming moet zijn tegen het opvragen van persoonsgegevens bij Europese instellingen?
De aan het woord zijnde leden vinden dat kleine en grote bedrijven die zich niet expliciet bezighouden met de verwerking van persoonsgegevens geen last moeten hebben van de regelgeving. Niet de grootte, maar de aard van het bedrijf moet bepalend zijn voor het regime. Kleine webbased bedrijven die handelen in e-mailadressen dienen zich aan de (strenge) eisen te houden en grote bedrijven die soortgelijke activiteiten hebben eveneens. Kleine en grote bedrijven die slechts een salarisadministratie voeren, zoals een bouwbedrijf met meer dan 250 werknemers, moeten geen extra verplichtingen opgelegd krijgen. De drogist op de hoek die een mailing aan zijn klanten wil sturen om nieuwe haarverzorgingsproducten of bijvoorbeeld steunkousen gericht wil aanbieden (dit laatste voorbeeld is vermoedelijk de verwerking van bijzondere persoonsgegevens die de gezondheid van de betrokkene raken) moet niet verplicht zijn aan allerlei eisen te voldoen. Is dat voldoende gegarandeerd? Zo nee, gaat de staatssecretaris hierop inzetten?
De leden van de VVD-fractie vragen wat de staatssecretaris vindt van de opmerkingen van deskundigen dat de bescherming van internetgebruikers onvoldoende zou zijn gegarandeerd.
Graag ontvangen zij een reactie op het specifieke commentaar van VNO-NCW d.d. 5 maart 2012.
Kan de staatssecretaris de zorg van voornoemde leden wegnemen dat het systeem van 27 landelijk samenwerkende en één Europese toezichthouder zal leiden tot bureaucratie, een toename van ambtenaren, onnodige overlegstructuren en een geheel eigen dynamiek die niet dienstig is aan het doel van de regelgeving?

Hoe beziet de staatssecretaris de rol van de Europese Commissie in relatie tot de rol van het Europese Parlement en de nationale parlementen? Is hier sprake van evenwicht?
Deze leden vragen hoe de staatssecretaris reageert op de kritiek van belangengroepen dat de richtlijn te veel mogelijkheden zou creëren voor justitie en politie om gegevens op te vragen.
Is naar het oordeel van de staatssecretaris voldoende gewaarborgd dat geen persoonsgegevens worden verstrekt aan buitenlandse, niet-Europese, overheden zonder dat hieraan duidelijke voorwaarden worden gesteld?
Ook vragen zij of voldoende duidelijk is waar een procedure over een eventuele inbreuk moet worden gevoerd. Deze leden hechten eraan dat dit in ieder geval dichtbij de betreffende persoon kan gebeuren.
De aan het woord zijnde leden vragen hoe de staatssecretaris reageert op de zorgen van onder andere PostNL op de verscherping van de regels voor direct marketing. Deze leden erkennen dat het onwenselijk kan zijn dat ongevraagd post wordt verzonden, maar onderkennen daarnaast het economisch belang van deze industrie. Zij vragen of dit voldoende in evenwicht is.
Bijzondere aandacht is volgens deze leden nodig voor de positie van het handelsregister van de Kamer van Koophandel en soortgelijke registraties van personen of bedrijven. Graag ontvangen voornoemde leden een reactie op de bezwaren van de Kamer van Koophandel in het advies d.d. 3 maart 2012 (kenmerk JH6865/110.85.02). Is het niet wenselijk de bestaande uitzonderingen voor verwerkingen die geen risico vormen voor de persoonlijke levenssfeer te laten staan? Voornoemde leden wijzen in dit kader ook het verzoek van VNO-NCW op dit punt.
De leden van de VVD-fractie hechten aan een meldplicht voor een «security breach» en een meldplicht voor een datalek. Aan beide meldplichten kunnen wat deze leden betreft voorwaarden worden gesteld, omdat het moet gaan om gevallen waarbij daadwerkelijk risico bestaat op het openbaar maken van gevoelige persoonsgegevens. Kan de regeling hierop worden aangepast?
Is de staatssecretaris van mening dat het verstandig is, zoals VNO-NCW voorstelt, dat cruciale interpretaties van de Europese toezichthouder worden getoetst door de Europese Commissie en het Europees Parlement of de nationale lidstaten zodat ongewenste verruiming of verenging van de regelgeving kan worden voorkomen en daarmee draagvlak voor de vele verplichtingen die de regelgeving met zich meebrengt gegarandeerd blijft?
Voornoemde leden vragen of er voldoende aandacht is voor de voorlichting van Europese onderdanen over het risico van het verstrekken van persoonsgerelateerde gegevens aan bijvoorbeeld social media.
De leden van de VVD-fractie vrezen dat de implementatie van de regelgeving die nu wordt voorgesteld ook op zich voor enorme nalevingskosten zal zorgen. Graag ontvangen zij hiervan een inschatting.
Voornoemde leden vragen of het juist is dat bij de invoering van artikel 6, eerste lid, onderdelen e en f van de Verordening gegevensbescherming (hierna: de Verordening) bedrijven geen gebruik meer mogen maken van adresbestanden van derden.
Het College bescherming persoonsgegevens (CBP) stelt dat de tekst van de algemene Verordening en de Richtlijn gegevensbescherming opsporing en vervolging (hierna: de Richtlijn) voor het terrein van politie en justitie op een aantal essentiële punten behoorlijk uiteen lopen, waardoor de alomvattendheid van het wetgevend pakket in gevaar komt. Volgens het CBP moeten de volgende begrippen worden opgenomen in de Verordening en in de Richtlijn, namelijk de rechtmatigheid van de verwerking, doelbinding, accuratesse van gegevens en de noodzaak tot het stellen van heldere bewaartermijn die niet langer moet zijn dan strikt noodzakelijk. Daarnaast dienen volgens het CBP ook de verplichtingen die

van toepassing zijn op de verantwoordelijke en bewerker in beide instrumenten gelijkgeschakeld te worden. Daaronder begrepen de verplichting tot het uitvoeren van privacy impact assessments en het zorgdragen voor «privacy by design». De aan het woord zijnde leden vragen wat voor gevolgen deze suggesties van het CBP hebben voor de uitvoerbaarheid en het doel van de wetgeving. Deelt de staatssecretaris de opvatting van het CBP?

De Verordening zorgt ervoor dat de rechten van betrokkenen worden versterkt, met name het recht om te worden vergeten en het recht op dataportabiliteit. De aan het woord zijnde leden zien hier het belang van in. Hoe schat de staatssecretaris de uitvoerbaarheid hiervan in? Indien dit moeilijk uitvoerbaar is, wat zou er gedaan kunnen worden om deze uitvoerbaarheid te verbeteren? Hoe zal het recht om te worden vergeten worden gehandhaafd en uitgevoerd? Deze leden hechten hier aan, maar hopen dit zo effectief mogelijk te realiseren zonder dat het onuitvoerbaar wordt.

De Verordening voorziet in een brede informatieplicht aan personen van wie gegevens worden verwerkt. Hoe wordt dit in de praktijk uitgevoerd? Is hier volgens de staatssecretaris behoefte aan? Welk probleem lost dit op? Deze leden gaan er in ieder geval van uit dat er op een korte en bondige manier informatie moet worden verstrekt, terwijl dit ook echt een doel moet dienen. Dit is te overzien voor de verstrekker, maar ook voor de ontvanger.

De leden van de VVD-fractie merken op dat er in de Verordening wordt voorzien in robuuste sanctionering, met name in de bevoegdheid tot het vaststellen van bestuurlijke boetes door toezichthouders. De hoogte van deze boetes wordt op EU-niveau vastgesteld. Wat zou hierbij volgens de staatssecretaris de rol van de lidstaten moeten zijn? Wordt deze voldoende gewaarborgd in het voorstel? Is het voorstel op dit gebied een verbetering ten opzichte van de huidige situatie in Nederland?

Deze leden merken op dat wordt gesteld dat de Verordening deels als niet proportioneel wordt beoordeeld, met name doordat het te gedetailleerd is uitgewerkt. Voornoemde leden zien hierin eveneens een gevaar. Hoe kan dit worden verholpen zonder daarmee de doelen van het voorstel niet kunnen worden bereikt?

De aan het woord zijnde leden vragen waarom er niet is gekozen voor optie 1 uit de impact assessment, te weten een combinatie van niet-bindende instrumenten en een beperkte aanvulling van de bestaande richtlijn. Zij vernemen graag de visie van de staatssecretaris hierop.

De leden van de VVD-fractie zien een rol voor het beter informeren van gebruikers bij online gebruiksovereenkomsten. Op dit moment krijgt iemand online een ellenlange tekst waar gewoonlijk onderaan snel akkoord wordt aangevinkt. Dit kan beter kort en bondig op basis van een paar criteria, zoals dat nu ook gebeurt bij financiële producten. Kan dit door bij de discussie op Europees niveau worden ingebracht?

Voornoemde leden merken op dat er een aantal verplichtingen aan bedrijven wordt opgelegd, zoals het aanstellen van Data Protection Officers en het verplicht uitvoeren van Data Protection Impact Assessments. Welke van deze verplichtingen zijn volgens de staatssecretaris noodzakelijk en effectief, proportioneel en uitvoerbaar? Welke zijn dat niet?

Er wordt een één loketfunctie opgezet voor dataprotectie in de EU, naast de onafhankelijke dataprotectie-autoriteiten. De aan het woord zijnde leden vragen of dit in de praktijk ook wel gaat werken. Heeft dit volgens de staatssecretaris toegevoegde waarde? Wat is de Nederlandse inzet bij dit onderwerp?

Voor voornoemde leden is het van belang dat de Richtlijn het niet onmogelijk maakt om opsporing en vervolging van criminaliteit effectief te laten verlopen. Het voorstel moet dus uitvoerbaar en betaalbaar zijn.

Hoe kan dat verbeterd worden ten opzichte van wat de Europese Commissie heeft gepresenteerd?
Er wordt een aantal keer gemeld dat de voorstellen gevolgen kunnen hebben voor politie en justitie. Deze leden willen weten wat precies deze gevolgen zijn in de praktijk. Hoe kunnen deze gevolgen zo veel mogelijk verminderd worden, zodat bescherming van persoonsgegevens gewaarborgd kan blijven en politie en justitie gewoon effectief hun werk kunnen blijven doen?
De aan het woord zijnde leden merken op dat artikel 75, tweede lid, van de Verordening bepaalt dat de gerechtelijke instanties van de lidstaat waar de voor de verwerking verantwoordelijke of de verwerker is gevestigd, competent zijn om te oordelen over een vordering. Hoe verhoudt deze bepaling zich tot de competentieregels uit de Verordening (EG) nr. 44/2001 van de Raad van 22 december 2000 betreffende de rechterlijke bevoegdheid, de erkenning en de tenuitvoerlegging van beslissingen in burgerlijke en handelszaken (Brussel I)? Waarom is er niet voor gekozen om deze regels te volgen in de Verordening? Zij vragen dit in het bijzonder in gevallen waarbij er meerdere verweerders zijn, zoals in artikel 6 sub 1 Vo Brussel I, en in het geval van een forumkeuze krachtens artikel 23 Brussel I.
Artikel 76, tweede lid, voorziet in een regeling om parallelle procedures te voorkomen. Kan de staatssecretaris aangeven wat onder een parallelle procedure wordt verstaan? Hoe verhoudt artikel 76 zich tot de connexiteitregel uit de artikelen 27 en 28 Verordening Brussel I.

Vragen en opmerkingen vanuit de PvdA-fractie

De leden van de PvdA-fractie hebben met belangstelling de voorstellen met betrekking tot de Verordening en de Richtlijn gelezen. In het algemene zijn zij blij met de aanpassing van de EU-wetgeving bescherming persoonsgegevens. De wetgeving die Europese burgers moet beschermen tegen ongeoorloofd gebruik van hun persoonsgegevens moet dringend worden aangepast aan de eisen van deze tijd. Daarnaast is het noodzakelijk dat alle EU-lidstaten hetzelfde beschermingsniveau hanteren omdat persoonsgegevens niet beperkt blijven tot de landsgrenzen.
Voornoemde leden zien enerzijds een verbetering van de bescherming van de persoonsgegevens van de burger, maar zij zijn er nog niet van overtuigd dat de Verordening en Richtlijn in zijn geheel een verbetering zijn. Kan de staatssecretaris aangeven of de Verordening en de Richtlijn per saldo een betere bescherming bieden aan burgers dan onder de huidige nationale regels? Acht de staatssecretaris die bescherming op alle onderdelen of op delen van het voorstel verbeterd? Waar kan gesproken worden van een hogere beschermingsniveau en waar van een lagere beschermingsniveau? Wat is het oordeel van de staatssecretaris daarover?
De leden van de PvdA-fractie zijn zeer verheugd met de versterking van het toestemmingsvereiste in de Verordening. Zij zijn van mening dat burgers moeten weten welke persoonsgegevens worden gebruikt en voor welk doel. Zij moeten beschikking hebben en houden over hun persoonsgegevens. Dat betekent dat toestemming vereist is voor het gebruik van persoonsgegevens en als die toestemming wordt ingetrokken, ook de grond voor het gebruik van die persoonsgegevens wegvalt. Deelt de staatssecretaris dit uitgangspunt en is hij van mening dat dit principe voldoende gewaarborgd is in de nieuwe EU-regelgeving? Zo nee, waar kan op dit punt de verordening nog worden aangescherpt?
Begrijpen deze leden het goed dat volgens de voorgestelde Verordening het duidelijk moet zijn waarvoor de burger toestemming geeft en dat deze toestemming, bijvoorbeeld voor het aanvaarden van algemene voorwaarden niet gezien mag worden als toestemming voor het

verwerken van persoonlijke gegevens? Zo nee, in hoeverre wordt de doelbinding te weinig gewaarborgd in de conceptverordening?
De Europese toezichthouders hebben in een gezamenlijk opiniestuk geoordeeld over de Verordening. Over het algemeen zijn zij positief over de voorstellen die zijn gedaan. Op sommige punten hebben zij echter kritiek of maken zij zich zorgen over de Verordening. Zo zijn de gezamenlijk toezichthouders (de zogenaamde artikel 29-werkgroep) van mening dat de verordening de mogelijkheid opent voor «incompatible uses» voor zowel de private als de publieke sector dat kan leiden tot «highly undesirable results». Deze leden lezen dit commentaar zo dat er sprake is van uitholling van de doelbinding. Is de staatssecretaris bereid notie te nemen van het commentaar van de artikel 29-werkgroep en te reageren op hun kritiek op dit punt?
Voornoemde leden maken zich zorgen over het principe van de doelbinding in relatie tot de overheden. In hoeverre wijkt de doelbinding voor de overheden af van de doelbinding voor de private sector. Wat mag de overheid meer met betrekking tot de verzamelde persoonsgegevens wat een private partij niet mag. In hoeverre is dit conform, dan wel in strijd met het doelbindingsprincipe?
Deelt de staatssecretaris de mening van de Staatscommissie Grondwet dat het doelbindingsprincipe zo sterk moet zijn dat het opgenomen moet worden in de Grondwet? Zo nee, waarom niet?
De leden van de PvdA-fractie begrijpen dat naast de Verordening een apart Richtlijn is opgesteld waarin regels voor de verwerking van persoonsgegevens door politie en justitie zijn opgenomen. De opslag en verwerking van persoonsgegevens in het justitieel kader heeft de laatste jaren een grote vlucht genomen. Daarbij kan worden gedacht aan camera's in het publieke domein, toegang tot telecomgegevens, etc. De Richtlijn geeft de lidstaten veel ruimte om af te wijken van de waarborgen die genoemd zijn in de Richtlijn. Voornoemde leden vinden het spijtig dat de Richtlijn niet een ambitieniveau heeft die vergelijkbaar is met de Verordening. Zij vragen welke regels gehanteerd worden als gegevens overgedragen worden naar een ander EU-land. Is de staatssecretaris met deze leden van mening dat beperkingen die op grond van nationale wetgeving aan de verwerking van persoonsgegevens zijn gesteld ook van toepassing moeten zijn als de gegevens met andere EU-lidstaten worden uitgewisseld? Zo nee, waarom niet? Zo ja, is de staatssecretaris bereid om dit in te brengen bij de eerstvolgende mogelijkheid?
De Richtlijn maakt onderscheid tussen de verwerking van gegevens van verschillende betrokkenen. Zo worden er andere voorwaarden gesteld aan de opslag van gegevens als het gaat om een verdachte dan aan de opslag van gegevens van een slachtoffer. Deze voorwaarden zijn echter niet hard. Er is een mogelijkheid om hiervan af te wijken op grond van artikel 5, eerste lid en artikel 6, eerste en tweede lid. Kan de staatssecretaris gevallen noemen waarin het noodzakelijk is af te wijken van de voorgestelde voorwaarden? Waarom is dat in genoemde voorbeelden noodzakelijk? Voor de restcategorie zijn de voorwaarden waaronder de gegevens van deze personen verwerkt mogen worden ruim geformuleerd. Het CBP spreekt zich uit tegen deze ruime formulering en tegen de maximale bewaartermijnen voor deze categorie. Wat is de reden dat er voor deze restcategorie andere voorwaarden gelden en in hoeverre acht de staatssecretaris deze voorwaarden en de lengte van de bewaartermijnen redelijk?
De leden van de PvdA-fractie merken op dat uitwisseling van persoonsgegevens met derde landen of internationale organisaties mogelijk is zonder dat duidelijk is of de gegevens voldoende beschermd zijn. Lidstaten moeten zelf bepalen of het beschermingniveau voldoende is. Deze leden vinden deze regel weinig geruststellend. Hoe moeten lidstaten bereiken dat zij voldoende garantie krijgen dat persoonsgegevens volgens

EU-normen worden verwerkt en behandeld? Is het niet in het belang van de burger dat deze open norm nader wordt ingevuld? Zo nee, waarom niet?
Op grond van artikel 13 van de Richtlijn zijn ruime uitzonderingsgronden geformuleerd op het recht van de betrokkene om toegang te krijgen tot zijn gegevens. Waarom is dat zo? Is dat niet strijdig met het Verdrag van Lissabon?
Persoonsgegevens kunnen zonder passend beschermingsniveau en passende waarborgen doorgegeven worden aan derdelanden. Als is voldaan aan het noodzakelijkheidsvereiste mogen persoonsgegevens worden gewisseld met derde landen. Voornoemde leden zijn van mening dat persoonsgegevens slechts doorgegeven mogen worden als er duidelijke waarborgen voor de verwerking van die persoonsgegevens vaststaan. Hoe wordt omgegaan met verzoeken van derdelanden om persoonsgegevens? Hoe kan betrokkene de garantie krijgen dat zijn gegevens voldoende beschermt zijn?
De leden van de PvdA-fractie merken op dat goede wetgeving zo sterk is als de mate van handhaafbaarheid van deze regels. Nationale toezichthouders hebben de taak om klachten van schendingen van de privacywetgeving op te nemen en af te handelen. Hiervoor moeten de nationale autoriteiten de mogelijkheid hebben om afschrikkende sancties op te leggen. Een afschrikkende sanctie is de boetebevoegdheid van de toezichthoudende autoriteit. Bij monde van de staatssecretaris heeft de regering toegezegd de Kamer te informeren of de boetebevoegdheid voor het CBP nog voor de implementatie van de Verordening kan worden toegekend. Vanwege die toezegging hebben deze leden een motie (Kamerstuk 32 761, nr. 22) om de boetebevoegdheid geregeld te krijgen aangehouden. Kan de regering toezegging dat de boetebevoegdheid voor het CPB op korte termijn, maar in ieder geval voor 2013 geregeld is? Zo nee, waarom niet? Wanneer kan het CPB wel boetes gaan opleggen?
In antwoord op vragen van de leden Recourt en Heijnen (Aanhangsel van de Handelingen, vergaderjaar 2011–12, nr. 2000) over de zorgen die het CPB heeft uitgesproken dat zij niet in staat is om alle klachten af te handelen wegens tekort aan mankracht, dat het CPB in staat is om eigen afwegingen te maken en prioriteiten te stellen. Uit dit antwoord blijkt dat de staatssecretaris van mening is dat het CPB niet alle klachten moet afhandelen. De staatssecretaris heeft geantwoord dat de handhaving van regels altijd moet gebeuren binnen de kaders van de beschikbare middelen. In hoeverre is de handhavingcapaciteit van het CBP voldoende om nog effectief te kunnen handhaven? De regering heeft nooit een mededeling dan wel een signaal van de zijde van het CPB ontvangen dat meer dan de helft van de zaken blijven liggen. Heeft de staatssecretaris wel signalen van het CPB ontvangen dat, in het algemeen gesproken, het CPB een tekort aan capaciteit heeft om zijn taken goed uit te oefenen? Zo ja, welk signaal of mededeling heeft de staatssecretaris ontvangen en hoe is er omgegaan met dit signaal of deze mededeling? Hoeveel procent van de klachten die bij het CPB binnenkomen worden er wel afgehandeld? Hoeveel zaken blijven op de plank liggen? Als het CPB niet in staat is om alle zaken af te handelen, hoe moet het CPB dan effectief handhaven? Wanneer kan gesproken worden van effectieve handhaving? Hoeveel procent van de zaken moet dan tenminste zijn behandeld?
De aan het woord zijnde leden merken op dat in principe de toezichthouder van de lidstaat waar het hoofdkantoor van een onderneming zich bevindt, bevoegd is om als toezichthouder op te treden. Hoe moet worden omgegaan met deze regel als niet duidelijk is waar het hoofdkantoor is gevestigd? Zou er meer duidelijkheid komen als er criteria worden ontwikkeld welke toezichthouder verantwoordelijk is in die gevallen dat een hoofdvestiging niet is vast te stellen? Zo nee, waarom niet? Zou hiervoor niet een belangrijke taak voor de toezichthouder weggelegd moet worden? Welke toezichthouder is verantwoordelijk voor het toezicht

als het hoofdkantoor niet in een EU-lidstaat ligt, maar de organisatie wel zeer actief is in Europese landen? Wie bepaalt in een dergelijk geval welke autoriteit als toezichthouder moet optreden? Deze leden zijn van mening dat in geval het onduidelijk is welke toezichthouder bevoegd is de European Data Protection Board (EDPB) een rol toebedeeld moet krijgen en een toezichthouder moet kunnen aanwijzen. Deelt de staatssecretaris deze mening? Zo nee, waarom niet?

Vragen en opmerkingen vanuit de PVV-fractie

De leden van de PVV-fractie merken in algemene zin op dat zij tegen Europese wetgeving zijn. In Nederland kunnen namelijk prima eigen wetten worden gemaakt. Deze leden zijn voorstander van het samenwerken met andere landen. Zij zijn van mening dat dit kan op basis van aparte (bilaterale of multilaterale) verdragen met die andere landen. Voornoemde leden willen graag weten welke beleidsvrije ruimte er overblijft indien de EU-wetgeving, zoals die nu in voorligt, aangenomen wordt.
Ten aanzien van de richtlijn hebben de leden van de PVV-fractie de volgende vragen en opmerkingen.
Onder dankzegging aan de Commissie Meijers verzoeken deze leden om de volgende vragen van de Commissie Meijers, zoals gesteld in de brief van 2 maart 2012, zorgvuldig te beantwoorden. Waarom is uit oogpunt van een uniform en zo hoog mogelijk niveau van gegevensbescherming niet gekozen voor één instrument, waarbij in een aparte paragraaf heldere en uniforme regels zijn uitgewerkt ten aanzien van gegevensverwerking in de politiële en justitiële sector? Deelt de staatssecretaris de mening van zowel het CBP, de artikel 29-werkgroep en de European Data Protection Supervisor (EDPS), dat het huidige richtlijnvoorstel een te laag niveau van gegevensbescherming biedt? Deelt de staatssecretaris het oordeel van de EDPS, dat de voorgestelde Richtlijn, politie autoriteiten in de EU nog teveel ruimte biedt voor toegang tot de gegevensverwerking in de private sector? Wil de staatssecretaris zich inzetten voor een minimalisering van uitzonderingsbepalingen in de voorgestelde Richtlijn om te voorkomen dat de (implementatie van) de Richtlijn door het Hof van Justitie van de EU onverenigbaar zal worden verklaard met de fundamentele rechten zoals neergelegd in het EU Handvest? Vindt de staatssecretaris dat de voorgestelde regeling inzake de gegevensuitwisseling aan derdelanden voldoende waarborgen biedt ter bescherming van de rechten en vrijheden van personen die zich in de EU bevinden?
Voornoemde leden vragen of de staatssecretaris de mening van de Commissie Meijers deelt dat de voorgestelde regeling inzake het gebruik van profilering in de artikelen 20 en 21 van de Verordening en in artikel 9 van de Richtlijn, door de vele uitzonderingsbepalingen en de resterende discretionaire bevoegdheid voor uitvoerende instanties, nog onvoldoende waarborgen biedt ter bescherming van de bovengenoemde rechten en vrijheden van individuen en met name het non-discriminatiebeginsel.
De aan het woord zijnde leden vragen op welke wijze de staatssecretaris zich wil inzetten voor proportionele uitbreiding van de financiële en personele middelen van zowel nationale als Europese toezichthoudende instanties. Wil de staatssecretaris zich inzetten voor de toevoeging van bepalingen aan de huidige voorstellen waarbij de genoemde instanties de bevoegdheid krijgen bindende sancties op te leggen, zoals effectieve en afschrikkende boetes?
De leden van de PVV-fractie vragen of de staatssecretaris van mening is dat de verhouding tussen de e-privacy richtlijn en de Verordening moet worden verduidelijkt.
Is de staatssecretaris van mening dat op basis van artikel 50, tweede lid, van de Richtlijn een achteruitgang in collectieve rechtsbescherming wordt bewerkstelligd in Nederland en wellicht ook in andere EU-lidstaten? Vindt

de staatssecretaris dit tevens een belangrijk aandachtspunt dat een zorgvuldige behandeling behoeft en waarover de Kamer goed geïnformeerd dient te worden, zeker in het licht van het algemeen overleg over het behandelvoorbehoud en de moties die in het daaropvolgende plenaire afronding zijn ingebracht?
De aan het woord zijnde leden vragen waarom ervoor gekozen is de Verordening niet risicogericht te laten zijn. Waarom richt de Verordening zich nu op bedrijfsgrootte?
Waarom zijn er geen uitzonderingen voor verwerking gemaakt die bijvoorbeeld wel in de Nederlandse wet (in het Nederlandse Vrijstellingsbesluit) zijn opgenomen? Is de Verordening wel specifiek genoeg daar waar het verschillende typen data betreft? Wordt er onderscheid tussen on- en offline gebruik gemaakt? Wordt er gekeken naar de aard van de gegevens en de gevolgen die de Verordening heeft voor verschillende typen bedrijvigheid? Hoe wordt er geanticipeerd op voorzienbare jurisdictieconflicten? Hoe wordt voorkomen dat het voor ondernemers onmogelijk wordt om in verschillende landen te ondernemen zonder de wet te overtreden?
Deze leden vragen waarom er niet verder wordt gedifferentieerd waar het datalekken betreft. Dienen alle typen datalekken gemeld te worden? Zo ja, op welke termijn en zijn periodieke rapportages hierbij ook mogelijk? Hoe wordt dit verder uitgewerkt?
Deze leden vragen waarom in het voorstel niet wordt ingegaan op nalevingskosten (in aanvulling op de administratieve lasten)?
Hoe kijkt de Nederlandse overheid tegen de introductie van eventuele nieuwe wetgeving vanuit Europa aan? In welke mate voelt zij zich verantwoordelijk om burgers en bedrijfsleven te informeren, voor te lichten en te ondersteunen waar het (het voldoen aan) deze eventuele nieuwe wetgeving betreft?
Hoe wordt omgegaan met gegevens die via internet worden verstrekt, waarbij niet goed is vast te stellen of de gegevens van een minderjarige afkomstig zijn? Hoe wordt voorkomen dat bedrijven en organisaties deze gegevens pas mogen verwerken, bijvoorbeeld voor het beantwoorden van een vraag, wanneer zij aanvullende informatie verkrijgen die de privacy nader zouden kunnen schenden? Hierbij kan worden gedacht aan creditcardgegevens om de meerderjarigheid vast te stellen.

Welke moeilijkheden ontstaan er met het oog op fraudepreventie met de nu voorliggende EU-wetgeving? Blijven er mogelijkheden voor fraudepreventie bestaan en/of vergt dit ondersteuning, ontheffing of specifieke goedkeuring vanuit de overheid? Is hier überhaupt in voorzien?
Hoe wordt omgegaan met het recht om vergeten te worden wanneer de gegevens die iemand vrijwillig bij een aanbieder op internet heeft geplaatst openbaar zijn? Kan deze aanbieder dan verantwoordelijk worden gehouden voor de verspreiding van derden? Waarom is dit niet verder uitgewerkt en waarom is niet aangegeven wie hiervoor de verantwoordelijkheid heeft?
Hoe worden bedrijven die niet in de EU gevestigd zijn, gestimuleerd toch met een representant te gaan werken? Kan dit worden afgedwongen? Zo nee, waarom niet? Zo ja, op welke wijze?

Vragen en opmerkingen vanuit de CDA-fractie

De leden van de CDA-fractie hebben tijdens het algemeen overleg in de Tweede Kamer op 7 maart 2012 reeds diverse punten aan de orde gesteld. Daarnaast hebben zij vragen kunnen stellen tijdens de technische briefings, waarvoor zij de diverse betrokkenen langs deze weg graag dank zeggen. Veel concrete vragen hebben zij niet, daar zij zich goed realiseren

dat een en ander nog zeer in ontwikkeling is en veel nog dient te worden uitgewerkt. Een paar punten stellen deze leden wel graag nog aan de orde.
De aan het woord zijnde leden hebben bij diverse gelegenheden naar voren gebracht bijzonder veel waarde te hechten aan het actief en voorafgaand moeten geven van toestemming om gegevens te mogen gebruiken («opt-in» in plaats van «opt-out» en de motie-Van Toorenburg c.s., Kamerstukken 2011/2012, 32 761, nr. 12). Deze leden begrijpen dat de voorliggende regelgeving hier ook meer op is gebaseerd, sterker nog, uitgangspunt is uitdrukkelijke toestemming. (*Putting individuals in control of their personal data*/*Right tot be forgotten* en *Data breach notification*). Zij zijn hiermee zeer ingenomen en wat hen betreft houdt de staatssecretaris daar ook stevig aan vast.
De leden van de CDA-fractie merken op dat de indruk wordt gewekt dat er sprake is van lastenverlichting. Deze is gelegen in het feit dat de algemene meldplicht is vervallen. Daarnaast zal sprake zijn van één loketfunctie voor bedrijven. Dat zal beslist de duidelijkheid kunnen dienen, althans indien onomstotelijk vaststaat waar een hoofdvestiging gelegen is. Is inmiddels al duidelijk op basis van welke criteria dat wordt vastgesteld? Deze leden begrijpen dat veel bedrijven die op dit punt kwetsbaar zijn, Ierland als hoofdvestiging kiezen, omdat daar de regels soepel zijn. De voorzitter van het CBP pleit ervoor bij onduidelijkheid uitsluitstel te vragen bij het European Data Protection Point. Wat deze leden betreft een verstandig voorstel. Hoe denkt de staatssecretaris daarover?
Hoewel van lastenverlichting sprake zal zijn, wordt hiermee vooral gedoeld op de lasten die bedrijven ondervinden van de administratieplicht jegens de overheid. Over de uitvoeringskosten rijzen evenwel grote zorgen. Kan de staatssecretaris hierover al iets meer zeggen? Hoe omvangrijk zullen deze naar verwachting zijn?
De Kamer van Koophandel Nederland luidt de noodklok over artikel 17 waarin het recht om gegevens te kunnen laten wissen bij derden is opgenomen. Zij acht dat praktisch niet uitvoerbaar. Deelt de staatssecretaris die zorg?
De Verordening voorziet ook in een meldpunt voor datalekken. Hoe verhoudt deze zich tot het nationale meldpunt dat momenteel in Nederland onderwerp van debat is?
Momenteel is het mogelijk om, zonder daartoe door individuele burgers gemachtigd te zijn, in het algemeen belang, een privacyproces te voeren tegen de overheid. Die mogelijkheid lijkt straks niet meer te bestaan. Klopt die analyse? Deze leden hebben hier zorgen over.
De leden van de CDA-fractie hebben de staatssecretaris gevraagd of het CBP ook een voorafgaande adviserende rol zou kunnen spelen. Bij het ontwikkelen van nieuwe producten moet steeds meer al aan de tekentafel rekening worden gehouden met de bescherming van persoonsgegevens («privacy by design») en bedrijven hebben soms grote behoefte aan advies. Zouden zij, tegen betaling, een soort prejudiciële vraag kunnen stellen, dan zouden zij daar zeer mee geholpen kunnen zijn. Heeft de staatssecretaris hierover inmiddels al overleg gevoerd met het CBP?
Tot slot hechten deze leden eraan nogmaals uit te spreken dat zij volledige openheid verwachten van de regering over de stand van de onderhandelingen over de voorstellen, zodat de Kamer effectief controle kan uitoefenen op de onderhandelingen en de inzet en successen van de Nederlandse regering in de Raad.

Vragen en opmerkingen vanuit de SP-fractie

De leden van de SP-fractie hebben met belangstelling kennisgenomen van het nieuwe pakket van de Europese Commissie met voorstellen voor de bescherming van persoonsgegevens. Zij benadrukken dat dit een omvangrijk pakket is, wat van groot belang zal zijn voor de toekomstige

privacywetgeving in Nederland. Deze leden benadrukken dit pakket met voorstellen van buitengewoon groot belang te vinden en vragen de staatssecretaris hieraan veel aandacht te besteden en bij iedere gelegenheid het belang van een hoog beschermingsniveau te benadrukken. Tevens hechten zij aan de toezeggingen, gedaan in het algemeen overleg over het behandelvoorbehoud van deze voorstellen, over de informatievoorziening aan de Kamer.
De aan het woord zijnde leden vragen de staatssecretaris nog eens duidelijk aan te geven in hoeverre het na eventuele aanname van deze voorstellen nog mogelijk is in Nederland af te wijken van de Europese regels. Beogen de Europese regels de gehele privacywetgeving in alle lidstaten te harmoniseren of beogen deze Europese regels minimum-normen neer te leggen? Is het daarbij toegestaan naar boven af te wijken en zo meer bescherming te bieden? Indien dat laatste niet het geval is, waarom niet?
De leden van de SP-fractie benadrukken dat het niet alleen gaat om het maken van goede regels voor bescherming van persoonsgegevens, maar dat de regels vooral ook toegepast moeten worden in alle EU-lidstaten. Hoe kijkt de staatssecretaris aan tegen het naleven van de huidige privacyregels in andere EU-lidstaten? Hoe wordt daar op toegezien?
Deze leden constateren dat vooral op de Richtlijn, waarin regels staan voor justitie en politie, veel kritiek is gekomen. De Richtlijn zou een (te) laag niveau van gegevensbescherming bieden. Dat zeggen ook het CBP, de EDPS en de artikel 29-werkgroep. Deelt de staatssecretaris die mening? Zo ja, welke gevolgen heeft dat voor de onderhandelingsinzet? Zo nee, waarom niet?
Voornoemde leden constateren dat er soms een conflict van plichten kan bestaan bij samenloop van toepasselijk recht. Een bedrijf bijvoorbeeld kan geconfronteerd worden met een vordering voor gegevens van autoriteiten uit andere landen, bijvoorbeeld de VS, terwijl deze overdracht op basis van de EU-wetgeving niet zou zijn toegestaan. Een eerdere versie van het voorstel bevatte de duidelijke bepaling dat geen gegevens mogen worden overgedragen, zo lang er geen goede waarborgen voor de persoonsgegevens zijn. Die bepaling leek meer duidelijkheid te bieden. Waarom is die formulering verdwenen? Gaat de staatssecretaris zich er voor inzetten dat die bepaling weer terug komt?
De leden van de SP-fractie benadrukken het van groot belang te vinden dat er in alle landen een robuuste toezichthouder aanwezig is om privacyschendingen aan te pakken. Ook Europees toezicht is noodzakelijk. Hoe ziet de staatssecretaris dit voor zich?
Voornoemde leden plaatsen vraagtekens bij de capaciteit van het CBP. Er is een (privacy)-waakhond met tanden nodig, die voldoende mankracht heeft om bepaalde signalen en meldingen uit de samenleving te onderzoeken. Daarover zijn deze leden bezorgd. Vooral ook in het licht van de toekomstige meldplicht datalekken, waar deze leden groot voorstander van zijn, die naar alle waarschijnlijkheid veel werk op zal leveren voor het CBP. Graag ontvangen zij hierop een reactie.
De leden van de SP-fractie vragen wanneer het wetsvoorstel waarmee de boetebevoegdheid van het CBP wordt uitgebreid de Kamer naar verwachting zal bereiken.
Deze leden zijn al langere tijd voorstander van een meldplicht datalekken en vinden de huidige voorgestelde bepaling te beperkt. Niet de inbreuk op beveiligingsmaatregelen, maar de ongeautoriseerde toegang tot persoonsgegevens moet leidend en bepalend zijn voor de vraag of het lek gemeld moet worden. Dus ook een meldplicht indien er per ongeluk een databestand met persoonsgegevens op internet wordt geplaatst. Ook dat zou moeten worden gemeld. Gaat de staatssecretaris zich hiervoor inzetten?
De aan het woord zijnde leden vragen wat de staatssecretaris nu precies wel beschouwt als nalevingskosten en wat daar niet onder valt. In

hoeverre zijn verplichtingen van bedrijven om te investeren in een zorgvuldige omgang met persoonsgegevens nu te beschouwen als nalevingskosten?
Deze leden vragen wat de onderhandelingsinzet zal zijn op het punt dat bedrijven met minder dan 250 fte worden vrijgesteld van een aantal verplichtingen. Zou niet zo zeer de grootte van het bedrijf, maar de mate van risico bepalend moeten zijn voor de vraag of uitzonderingen moeten worden gecreëerd?
De leden van de SP-fractie vragen naar de garanties die er zijn indien gegevens worden uitgewisseld met derde landen. Vindt de staatssecretaris dat het voorstel op dit punt voldoende waarborgen bevat voor de gegevensbescherming?
Deze leden vragen de staatssecretaris te reageren op de zorgen die de Commissie Meijers heeft geuit over het gebruik van profilering op basis van persoonsgegevens.
Voornoemde leden vragen of de staatssecretaris tevreden is over de uitwerking van de rechten van betrokkenen, zoals het recht om vergeten te worden en het recht op informatie. Wat is de reactie op bijvoorbeeld de kritiek van het CBP dat de uitzonderingen op de informatieplicht te ruim geformuleerd zijn?

Vragen en opmerkingen vanuit de D66-fractie

De leden van de D66-fractie verwelkomen het feit dat de Europese Commissie een voorstel heeft gedaan om de EU-regels voor privacybescherming bij de tijd te brengen. Dit is hoognodig omdat er zich sinds het opstellen van de huidige regels veel veranderingen hebben voorgedaan.
Deze leden zijn daarbij verheugd dat het overgrote deel van de nieuwe EU-regels voor de bescherming van persoonsgegevens in de vorm van het instrument verordening is gegoten. Op deze wijze zullen de regels in elk EU-land gelijkluidend zijn. Voornoemde leden juichen toe dat personen meer controle krijgen over hun eigen data met deze Verordening. Ook moeten bedrijven in het vervolg explicieter dan voorheen aan burgers toestemming vragen als zij hun persoonsgegevens willen gebruiken en gaat voor hen een meldplicht voor datalekken gelden. Daarnaast wordt een recht om vergeten te worden voorgesteld. Naar het oordeel van deze leden zijn dit stappen vooruit.
De leden van de D66-fractie zien echter ook een aantal uitdagingen en kansen voor verbetering. De Europese Commissie heeft gekozen voor meerdere instrumenten. In aanvulling op genoemde verordening wordt voor het politiële en justitiële domein een Richtlijn voorgesteld. Volgens deze leden moet het uitgangspunt hetzelfde blijven, namelijk één alomvattend rechtskader om het verzekeren van een hoog niveau van gegevensbescherming voor de Europese burger. De aan het woord zijnde leden hebben geconstateerd dat op een aantal cruciale punten de Richtlijn en de Verordening tevens uit elkaar lopen. Is de staatssecretaris bereid om gedurende de onderhandelingen in te zetten op het bewerkstelligen van een nauwere samenhang tussen beide instrumenten? Het gaat hierbij voornamelijk om de algemene beginselen voor gegevensverwerking (zoals doelbinding en bewaartermijn), de verplichtingen die van toepassing zijn op de verantwoordelijke alsook bewerker en de bevoegdheden die worden toegekend aan de autoriteiten verantwoordelijk voor gegevensbescherming. Voornoemde leden benadrukken dat deze discrepanties hen zorgen baren.
Voor de leden van de D66-fractie is het belangrijk dat het hoogste niveau van bescherming geldt wanneer bedrijven persoonsgegevens verzamelen, zoals telecomgegevens en passagiersgegevens, en deze gegevens vervolgens worden gebruikt en verwerkt door politie en justitie. Hoe kijkt de staatssecretaris hier tegenaan? Kan een nadere toelichting worden gegeven van de regeringsinzet bij de onderhandelingen op dit punt?

Deze leden lezen dat de staatssecretaris bij het ontwerp van de Richtlijn kanttekeningen heeft geplaatst ten aanzien van de uitvoerbaarheid en werklast. Dit betreft het maken van onderscheid tussen categorieën van gegevens door politie en justitie en de informatieverplichtingen jegens degenen die met de politie en justitie in aanraking komen. Dergelijke verplichtingen zijn niet goed te verenigen met de aard van het politiewerk. Voornoemde leden ontvangen graag een nadere toelichting en precisering bij deze stelling. Waar doelt de staatssecretaris precies op?
De aan het woord zijnde leden achten het een gemiste kans dat er een apart, lager beschermingsniveau komt als de overheid persoonsgegevens gebruikt. De besluiten die de overheid neemt over burgers op basis van hun gegevens, kunnen minstens zo ingrijpend zijn als die van bedrijven. Is de staatssecretaris bereid zich bij de onderhandelingen in te zetten voor een gelijk beschermingsniveau voor alle partijen geldt die gegevens verwerken dat zo hoog mogelijke bescherming biedt? Dit zou ook moeten gelden voor de overheden en de Europese instellingen. Zo nee, waarom niet?
De voorgestelde regelgeving voorziet in nieuwe plichten voor bedrijven en nieuwe rechten voor burgers die bijdragen aan een betere bescherming van persoonsgegevens, hetgeen in beginsel positief is. Deze plichten en rechten moeten wel afdwingbaar zijn. Voornoemde leden beschouwen het als winst dat de nationale colleges bescherming persoonsgegevens boetes zullen kunnen gaan opleggen. Nu bestond op nationaal niveau in Nederland dit voornemen al langer. Deze leden vragen wanneer de Kamer dit wetsvoorstel tegemoet kan zien. Zij zijn benieuwd naar de samenloop tussen het Europese en de nationale trajecten. Deze leden vragen hoe de staatssecretaris aankijkt tegen strafrechtelijke sancties voor gevallen van zware overtreding van deze regels. Ook vragen zij de staatssecretaris om zijn visie op het «minder dan 250 fte»-criterium toe te lichten. Graag zouden zij zien dat daarbij expliciet wordt ingegaan op de stelling van het CBP dat niet de grootte van het bedrijf, maar de mate van risico verbonden aan de verwerking bepalend dient te zijn voor het creëren van eventuele uitzonderingen.
Voor de leden van de D66-fractie is het een belangrijk punt dat Europese burgers beschermd worden door Europese regels, ook als derde landen gebruik maken van gegevens van Europese burgers. De regering stelt dat het probleem van conflicterende jurisdicties nog niet volledig sluitend lijkt te zijn geregeld. Deze leden hebben over dit onderwerp meerdere malen vragen gesteld. Kan de regering een nadere toelichting geven van de regeringsinzet op deze punten? Welke ondergrens wordt gehanteerd? In een brief van het CBP over onderhavige materie aan de vaste Kamercommissie voor Veiligheid en Justitie d.d. 2 maart 2012 meldt het CBP dat een eerdere openbaar geworden conceptversie van de verordening een dergelijke bepaling bevatte in artikel 42: «No judgment of a court or tribunal and no decision of an administrative authority of a third country requiring a controller or processor to disclose personal data shall be recognized or be enforceable in any matter , without prejudice to an mutual assistance treaty or an international agreement in force between the requesting third country and the Union or a Member State».« Kan de staatssecretaris inzicht verschaffen in de reden(en) dat deze formulering verdwenen is uit het voorstel? Kan de staatssecretaris tevens duidelijkheid verschaffen of zij voorstander zou zijn van het (her-)introduceren van een dergelijke bepaling? Zo nee, waarom niet?
De leden van de D66-fractie benadrukken ten slotte dat de uitwerking en verdere onderhandelingen over onderhavige voorstellen hun buitengewone belangstelling heeft. Zij worden dan ook graag tijdig en frequent geïnformeerd over de voortgang hiervan.

Vragen en opmerkingen vanuit de GroenLinks-fractie

De leden van de GroenLinks-fractie hebben nog enkele navolgende vragen over de herziening van de EU-wetgeving over de bescherming van persoonsgegevens.
Op welke wijze spant de regering zich in om een aantal algemene beginselen voor gegevenswerking van zo groot belang zijn en aan de basis liggen van gegevensbescherming dat zij zowel in de Verordening als de Richtlijn te laten opnemen? Zij wijzen in het bijzonder op beginselen als de rechtmatigheid van de gegevensverwerking, doelbinding, accuratesse van gegevens en de noodzaak tot het stellen van een heldere bewaartermijn die niet langer moeten worden bewaard dan strikt noodzakelijk is voor het doel.
Voornoemde leden merken op dat artikel 6, vierde lid, van de Verordening in latere fases van gegevensverwerking het principe van doelbinding doorbreekt. Op welke wijze spant de staatssecretaris zich in om deze dreigende uitholling van het principe van doelbinding ongedaan te maken?
In de Verordening zijn voor de overheid afwijkende bepalingen opgenomen over het gebruik van bijzondere persoonsgegevens, onverenigbaar gebruik, privacy impact assessments en over de mogelijkheid van de overheid om beperkingen aan te brengen op de principes en rechten voor bepaalde belangen. Deelt de staatssecretaris het standpunt dat door deze bepalingen wordt afgeweken van de doelstelling om te komen tot een alomvattend privacykader, een normenstelsel dat zowel voor de publieke als voor de private sector zou gelden. Deelt de staatssecretaris de mening dat zonder dat allesomvattende privacykader onzekerheid ontstaat bij burgers en verantwoordelijken over de vraag welke normen waarom wel of niet in welke situaties voor hen van toepassing zijn? Zo ja, op welke wijze spant de staatssecretaris zich in opdat deze afwijkende bepalingen worden aangepast?
Voornoemde leden vragen op welke wijze de staatssecretaris zich inspant om de verplichtingen die van toepassing zijn op de verantwoordelijke en bewerker in zowel de Verordening als de Richtlijn gelijk te schakelen, waaronder de verplichting tot het uitvoeren van privacy impact assessments en het zorgdragen voor privacy by design.
In artikel 22 van de Verordening worden verplichtingen rond «accountability» vastgelegd. Dit betekent dat bedrijven dienen te investeren in een zorgvuldige omgang met persoonsgegevens. Dit vertaalt zich in plichten als het zorgdragen voor «privacy by design», het doen van «privacy impact assessments» en het garanderen van adequate beveiliging. Op welke wijze spant de staatssecretaris zich in om deze bepaling in de verordening te behouden evenals om de uitvoering ervan in de praktijk te realiseren, zowel met betrekking tot het overheidsdomein als met betrekking tot het stimuleren hiervan in het private domein?
Artikel 51, tweede lid, van de Verordening stelt dat de dataprotectieautoriteit van de lidstaat waar een verantwoordelijke zijn hoofdvestiging heeft, wordt geacht de leidende autoriteit te zijn die bevoegd is toezicht te houden op de verwerkingen van dit bedrijf in andere EU-lidstaten. Op welke wijze spant de staatssecretaris zich in om de Verordening op te laten nemen dat indien de hoofdvestiging van een bedrijf niet eenduidig kan worden vastgesteld de EDPB de bevoegdheid krijgt om te bepalen welke dataprotectie-autoriteit de leiding neemt bij een zaak en hoe de onderlinge rolverdeling met andere nationale toezichthouders is?
Op welke wijze spant de staatssecretaris zich in voor het versterken van de rechten van de burger, in het bijzonder voor het behoud van de door de ontwerpverordening gegarandeerde versterking van het toestemmingsvereiste zoals opgenomen in de artikelen 4 en 7 van de conceptverordening?

In de Verordening worden bedrijven met minder dan 250 werknemers vrijgesteld van een aantal verplichtingen. Deelt de staatssecretaris het standpunt dat in het huidige tijdgewricht vaak juist bedrijven met slechts enkele medewerkers voor de bescherming van persoonsgegevens zeer risicovolle verwerkingen doen en dat om die reden niet de grootte van een bedrijf, maar de mate van risico verbonden aan de verwerking bepalend moet zijn als besloten wordt om uitzonderingen te creëren? Zo ja, op welke wijze spant de staatssecretaris zich in opdat de Verordening op dit punt wordt aangepast?

II. Reactie van de staatssecretaris van Veiligheid en Justitie

VVD

De leden van de VVD-fractie hebben ten aanzien van de voorgestelde ontwerprichtlijn en de ontwerpverordening de volgende vragen:

– De leden van de VVD-fractie achten het onwenselijk en zelfs in zekere zin exemplarisch dat de Europese Commissie wel aandacht besteedt aan een vermeende daling van de administratieve lasten, maar geen berekening aanlevert van de nalevingskosten die de nieuwe regelgeving met zich meebrengt voor het Europese bedrijfsleven. Deze leden achten het essentieel dat een heldere berekening hiervan wordt opgesteld en aangeleverd. Met name de «privacyofficer» bij grotere bedrijven moet tot een enorme kostenpost leiden waarvan de opbrengst verre van zichtbaar is.

Het is niet zo dat de Europese Commissie in het geheel geen aandacht schenkt aan de invloed van uit de conceptontwerpverordening voortvloeiende stijging van de lasten voor het bedrijfsleven. In de Impact Assessment, opgesteld door de diensten van de Commissie (SEC 2012, 72), en gelijktijdig uitgebracht met de voorstellen wordt de uitbreiding van de informatieverplichtingen voor verantwoordelijken begroot op € 180 mln per jaar. De verplichtingen tot het melden van datalekken worden geraamd op € 20 mln – naar moet worden aangenomen – ook op jaarbasis. Beide kostenposten hebben betrekking op de EU als geheel. Het is echter onduidelijk of hiermee alle nalevingskosten zijn afgedekt. Ik ben overigens met de leden van de VVD-fractie teleurgesteld over het feit dat de Commissie aan de feitelijke lasten en nalevingskosten zo weinig aandacht schenkt. Ik heb dat in Brussel dan ook inmiddels duidelijk ter sprake gebracht, en zal dat ook blijven doen.

– Is het wenselijk om als criterium van het begrip persoonsgegevens op te nemen dat het gaat om gegevens waarmee een persoon van andere personen kan worden onderscheiden (individualiserende gegevens)? Ook VNO-NCW acht een betere omschrijving van het begrip «persoonsgegevens» noodzakelijk. Graag een reactie van de regering op dit punt.

Het is niet zonder meer wenselijk dat onder het begrip persoonsgegevens ook die gegevens moeten worden begrepen waarmee een persoon van andere personen kan worden onderscheiden door middel van (directe of indirecte) individualisering, zoals het College bescherming persoonsgegevens (Cbp) bepleit. Dit criterium acht ik onvoldoende duidelijk, en daardoor geen goede toevoeging aan een begrip dat naar zijn aard toch al tal van interpretatieproblemen oplevert. VNO/NCW – MKB Nederland (hierna: VNO/NCW) wijst er terecht op dat een uitbreiding van dit begrip leidt tot hogere lasten en kosten van naleving. Ik ben het met VNO/NCW eens dat de context waarin gegevens verzameld worden een relevant aandachtspunt is bij beantwoording van de vraag of een gegeven als

persoonsgegeven moet worden aangemerkt. Ik meen echter dat dit niet noodzakelijkerwijs in de ontwerpverordening moet zijn neergelegd.

– Zijn de eisen aan de doelomschrijving van de opslag van de persoonsgegevens voldoende?

Artikel 5, onder b, van de ontwerpverordening regelt dat persoonsgegevens voor welbepaalde, uitdrukkelijk omschreven en gerechtvaardigde doeleinden moeten worden verwerkt. Die omschrijving stemt overeen met artikel 6, onder b, van de huidige ontwerprichtlijn 95/46/EG. Ik acht het behoud van deze bepaling van groot belang, omdat daarmee duidelijk wordt gemaakt dat niet de wetgever, maar de verantwoordelijke de doelomschrijving in concreto vaststelt. Verwerken omvat overigens mede de opslag van persoonsgegevens.

– Dient expliciet te worden opgenomen dat er ook bescherming moet zijn tegen het opvragen van persoonsgegevens bij Europese instellingen?

Verordening (EG) nr. 45/2001 van het Europees Parlement en de Raad van 18 december 2000 (PbEG 2001, 8) regelt de bescherming van persoonsgegevens door de communautaire instellingen en organen. Er is dus ook op communautair niveau voorzien in een behoorlijk niveau van gegevensbescherming. Niettemin is de vraag gerechtvaardigd waarom die ontwerpverordening niet meteen is aangepast aan de nieuwe ontwerpverordening, aangezien het ongewijzigd laten voortbestaan van verordening (EG) nr. 45/2001 leidt tot verschillen in het beschermingsniveau dat de lidstaten en de EU moeten handhaven.

– De leden van de VVD-fractie vinden dat kleine en grote bedrijven die zich niet expliciet bezig houden met de verwerking van persoonsgegevens geen last moeten hebben van de regelgeving. Het zou dus niet de grootte van het bedrijf moeten zijn dat bepalend is voor het regime, maar de aard van het bedrijf. Kleine webbased bedrijven die handelen in e-mailadressen dienen zich aan de (strenge) eisen te houden en grote bedrijven die soortgelijke activiteiten hebben eveneens. Kleine en grote bedrijven die slechts een salarisadministratie voeren (denk aan bouwbedrijf met meer dan 250 werknemers) moet geen extra verplichtingen opgelegd krijgen. De drogist op de hoek die een mailing aan zijn klanten wil sturen om nieuwe haarverzorgingsproducten of bijvoorbeeld steunkousen gericht wil aanbieden (N.B. dit laatste voorbeeld is vermoedelijk de verwerking van bijzondere persoonsgegevens die de gezondheid van de betrokkene raken) moet niet verplicht zijn aan allerlei eisen te voldoen. Is dat voldoende gegarandeerd, zo nee, gaat de regering hierop inzetten?

Ik ben het met deze leden eens dat voor de private sector het maken van een onderscheid in verplichtingen gerechtvaardigd is, en dat voor dit onderscheid niet moet worden aangesloten bij de omvang van de onderneming, maar bij het risico dat de verwerking van persoonsgegevens door de onderneming voor de persoonlijke levenssfeer oplevert. Ik ben overigens wel van oordeel dat voor directmarketingactiviteiten voor alle ondernemingen – groot en klein – regels moeten worden gesteld die betrokkenen beschermen tegen excessen. Tenslotte associeer ik het aanbod van producten door een drogist via direct marketing aan zijn klanten niet als het verwerken van gegevens betreffende de gezondheid. Een drogist valt niet aan te merken als een zorgaanbieder of zorgverlener, ook niet als de drogist eenvoudige zelfzorggeneesmiddelen te koop aanbiedt.

– Wat vindt de regering van de opmerkingen van deskundigen dat de bescherming van internetgebruikers onvoldoende zou zijn gegarandeerd?

Het is mij niet duidelijk op welke deskundigen deze leden doelen. Een specifieke reactie op specifieke uitlatingen kan ik dan ook niet geven. De ontwerpverordening beoogt in elk geval het niveau van gegevensbescherming voor internetgebruikers te verhogen, onder meer door het recht om te worden vergeten en het recht op dataportabiliteit. Los van de vraag naar de uitvoeringsmodaliteiten van deze rechten, moet die stap positief worden gewaardeerd. Iets anders is dat de ontwerpverordening nog aanleiding geeft tot de nodige vragen over de toepasselijkheid van veel bepalingen op internetgebruik en gebruik van sociale media. Dat is in dit stadium van behandeling onvermijdelijk.

– Graag ontvangen de leden van de VVD-fractie een reactie op het specifieke commentaar van VNO-NCW d.d. 5 maart 2012.

Ik geef deze reactie hieronder puntsgewijs.
- Op de definitie van persoonsgegevens is hierboven reeds een reactie gegeven.
- Ik acht de toevoeging van elementen aan de definitie van «verwerking» die geassocieerd zijn aan organisatorische belangen en de mogelijkheden om diensten aan te bieden geen winstpunt. De verwerking van persoonsgegevens is een activiteit die ook buiten het organisatorisch belang van overheid en bedrijfsleven vraagt om bescherming van de belangen van betrokkenen.
- Ik ben het met VNO/NCW eens dat onder artikel 6, onderdeel f, van de ontwerpverordening ten onrechte niet mede de belangen van derde partijen zijn begrepen.
- Het is ontegenzeglijk zo dat artikel 7, eerste lid, van de ontwerpverordening leidt tot verzwaring van de last van de verantwoordelijke en de verplichting inderdaad ook zelfstandig leidt tot verwerking van persoonsgegevens. En het is de vraag of dat wenselijk is. Maar voor zover dat inderdaad te zijner tijd leidt tot de vaststelling van een verplichting, is dat niet in strijd met het beginsel van dataminimalisatie. Het betreft dan immers gegevens die op grond van een verplichting verwerkt worden.
- Ik ben het met VNO/NCW eens dat artikel 8 van het voorstel nog onvoldoende rekening houdt met de omstandigheid dat werkelijk betrouwbare middelen om identiteit, leeftijd en toestemming via internet vast te stellen nog onvoldoende beschikbaar lijken. Gebruik van een creditcard lijkt mij ook geen oplossing, niet zozeer vanuit het oogpunt van dataminimalisatie, maar meer vanuit het gebrek aan mogelijkheden vast te stellen dat de gebruiker van de creditcard in een online transactie ook de kaarthouder is.
- Bij artikel 9 snijdt VNO/NCW een bekend keuzeprobleem aan. Bij de beantwoording van de vraag welke gegevens als bijzondere persoonsgegevens moeten worden aangemerkt is de keuze tussen een open systeem van bijzondere persoonsgegevens – waarin een gegeven bijzonder wordt door context van de verwerking – en een gesloten systeem waarin de wetgever bepaalt wat bijzondere persoonsgegevens zijn en onder welke voorwaarden elk bijzonder persoonsgegeven mag worden verwerkt. Beide systemen hebben voor- en nadelen.
- Ik ben het met VNO/NCW eens dat in artikel 9 ten onrechte geen mogelijkheden worden opengelaten voor de verwerking van strafrechtelijke gegevens ten behoeve van de gerechtvaardigde belangen van particulieren.
- Wat de artikelen 13, 14 en 17 betreft is het de vraag op welke wijze de daarin neergelegde rechten van betrokkene volledig door de verantwoordelijke kunnen worden gehonoreerd indien de desbetreffende

gegevens voorafgaand aan de uitoefening van het recht aan derde partijen zijn verstrekt. Uitgangspunt hierbij moet wel zijn dat de verantwoordelijke een redelijke inspanning moet verrichten om ook bij derden correcties of wissing te bewerkstelligen. Zou dat niet het geval zijn, dan verliest het recht op correctie teveel aan inhoud. Maar anderzijds geldt dat derde partijen onder omstandigheden een gerechtvaardigd belang kunnen hebben de gegevens, niettegenstaande de wens van betrokkene, toch verder te verwerken. Bovendien is het de vraag of het technisch en economisch haalbaar is alle derden te achterhalen. Die vragen zullen nog moeten worden beantwoord.

– Ik deel de mening van VNO/NCW niet dat artikel 20, dat handelt over profiling sectorspecifiek is en daarom niet in de ontwerpverordening thuishoort. Het tegendeel is geval. Profileren is een speciale techniek, die zowel in de publieke als in de private sector kan worden gebruikt. Aan een regeling van het profileren bestaat juist grote behoefte in verband met de specifieke risico's voor de persoonlijke levenssfeer die deze techniek met zich brengt. Overigens ben ik het met VNO/NCW eens dat het begrip profileren kan worden gedefinieerd. Daarvoor biedt Resolutie CM (2010) 73 van de Raad van Europa een bruikbaar voorbeeld.
– Het is duidelijk dat in de ontwerpverordening de rol van de bewerker ten opzichte van de verantwoordelijke meer wordt uitgewerkt. Ik het met VNO/NCW eens dat dit vraagt om een duidelijke bepaling van de rechtsverhouding tussen verantwoordelijke en bewerker enerzijds en betrokkenen en derden anderzijds. Dit lijkt echter geen kwestie van de formulering van de begripsbepaling van «bewerker». Die bepaling is ten opzichte van de huidige richtlijn onveranderd gebleven.
– Ik zie geen overwegende bezwaren tegen het introduceren van een gezamenlijke of gedeelde verantwoordelijkheid, zoals artikel 24 van de ontwerpverordening doet. Integendeel, de wetgevingspraktijk leert dat daaraan behoefte bestaat. Voorwaarde daarvoor is echter dat de onderlinge rechtsverhouding tussen de desbetreffende verantwoordelijken helder geregeld is, en dat er geen misverstand over mag bestaan tot welke verantwoordelijke de betrokkene zich kan richten wanneer hij een beroep op een van zijn rechten doet.
– Het is inderdaad de vraag of veel ondernemingen zich aangetrokken voelen tot het vertegenwoordigen van niet in de EU gevestigde verantwoordelijken. Ook onder het huidige stelsel ontbreken prikkels om dergelijke aanwijzingen te doen. Stimulering van de aanstelling van een vertegenwoordiger in de EU door een niet in de EU gevestigde verantwoordelijke voor de verwerking van persoonsgegevens is in de eerste plaats mogelijk door in de EU een aantrekkelijk gegevensbeschermingsrecht aan te bieden dat niet alleen voor de betrokkene, maar ook voor de verantwoordelijke duidelijke voordelen biedt. Ook verantwoordelijken hebben belang bij een goed gegevensbeschermingsrecht.
– Wat de documentatieverplichting van artikel 28 betreft, is het uitgangspunt dat het accountabilitybeginsel met zich brengt dat aan verantwoordelijken meer eisen worden gesteld wat betreft de verantwoording van hun doen en laten met betrekking tot verwerkte persoonsgegevens. Dit houdt onder omstandigheden ook in dat er meer informatie wordt gegenereerd, opgeslagen en openbaargemaakt met betrekking tot de verwerking dan thans nog het geval is. Wel ben ik van oordeel dat beter moet worden nagedacht over de vraag of de documentatieverplichting over de volle breedte voor elke verantwoordelijke gelijkelijk moet gelden. Ik ben van oordeel dat daarin moet en kan worden gedifferentieerd naar gelang het risico van de verwerking. Wellicht kan ook aan een vrijstellingsregeling worden gedacht. Tenslotte is zo dat bij gedeelde verantwoordelijkheid aan de documentatieplicht gepaste eisen worden gesteld. Dit acht ik onvermijdelijk.

– Ik ben het met VNO/NCW eens dat het voorstel voor de meldplicht datalekken in de ontwerpverordening nog een aantal vragen oproept. Zo is deze, zowel in de relatie naar ondernemingen, als in de relatie naar de toezichthouders, nogal ongenuanceerd. Een meldplicht voor elk datalek lijkt weinig zinvol. Ook betrokkenen zijn hier uiteindelijk niet mee geholpen. Dat wil echter niet zeggen dat op nationaal niveau de ontwikkeling van wetgeving moet worden stopgezet. De DigiNotar-zaak heeft mij geleerd dat een meldplicht wel degelijk toevoegde waarde heeft.
– Een redelijke interpretatie van artikel 33 lijkt op te leveren dat ook de Europese Commissie beseft dat een Privacyeffectbeoordeling (PIA) alleen moet worden gehouden in de gevallen waarin de ontwerpverordening dit uitdrukkelijk aangeeft, en daarnaast in die gevallen waarin het aannemelijk is dat er sprake is van een verhoogd risico op aantasting van de persoonlijke levenssfeer. Ik zal de opmerkingen van VNO/NCW over de redactie van de bepaling bij de standpuntbepaling betrekken.
– Ik sta niet afwijzend ten opzichte van een wat ruimere taakomschrijving van de Data Protection Officer. Ik ben echter ook van oordeel dat de nationale en Europese wetgever zich niet meer dan strikt noodzakelijk is met de bedrijfshuishoudingen moet bemoeien. Overigens voorziet artikel 34, vierde lid, van de ontwerpverordening in de mogelijkheid van aanstelling van collectieve Data Protection Officers in de private sector.
– Aanpassing van de modelcontracten zal na vaststelling van de ontwerpverordening wellicht nodig zijn. Ik vertrouw erop dat de Europese Commissie daartoe tijdig het initiatief neemt.
– Wat de uitoefening van toezichtsbevoegdheden betreft, meen ik dat een toezichthouder verplicht is zijn bevoegdheden op redelijke wijze toe te passen met inbegrip van de beginselen van proportionaliteit en subsidiariteit. Dat brengt met zich dat een onderzoek niet onredelijk lang mag duren. Voor zover de ontwerpverordening dit niet reeds zelf regelt, moet worden aangenomen dat de uitoefening van taken en bevoegdheden door de toezichtouder mede wordt beheerst door de Algemene wet bestuursrecht. De Algemene wet bestuursrecht biedt voldoende garantie voor een behoorlijke uitoefening van bevoegdheden. Ik zie in de ontwerpverordening overigens geen aanleiding te veronderstellen dat er reden is voor discriminatoir optreden van toezichthouders. Dit neemt overigens niet weg dat een toezichthouder naar mijn oordeel gerechtigd is recidive van overtredingen te betrekken bij de vraag of in een volgend geval een sanctie wordt opgelegd.
– Ik betreur het met VNO/NCW dat in artikel 66 niet is voorzien in een meer transparante rol bij de vaststelling van algemene standpunten over de interpretatie van de ontwerpverordening. Inderdaad zou een rol voor het bedrijfsleven daarbij niet misplaatst zijn.
– Ik zie geen aanleiding om in de ontwerpverordening de vrijheid van meningsuiting op een andere wijze te benaderen dan in richtlijn 95/46/EG is gebeurd. Naar het mij voorkomt is er ook geen sprake van een wezenlijk andere benadering.
– De verwerking van persoonsgegevens met betrekking tot de gezondheid en de arbeidsverhoudingen is door de Commissie in belangrijke mate overgelaten aan de lidstaten. Ik acht dat een verstandige keuze. Dit stelt de lidstaten in staat het eigen gegevensbeschermingsrecht voor sectoren die per lidstaat zeer verschillend zijn georganiseerd met toepassing van maatwerk te regelen. De uitzonderingen op het verbod om gegevens betreffende de gezondheid te verwerken hebben mijn aandacht. Tegelijk moet worden gewaakt tegen een al te brede uitleg van deze verbodsbepaling. Leveranciers van sportartikelen of manicures, waarop VNO/NCW wijst, zijn naar mijn oordeel niet aan te

merken als zorgaanbieders die gegevens betreffende de gezondheid verwerken.

– Kan de regering de zorg van de leden van de VVD-fractie wegnemen dat het systeem van 27 landelijk samenwerkende en één Europese toezichthouder zal leiden tot bureaucratie, een toename van ambtenaren, onnodige overlegstructuren en een geheel eigen dynamiek die niet dienstig is aan het doel van de regelgeving?

De keuze voor een samenwerkingsmechanisme waarbij 28 toezichthouders gaan samenwerken is een keuze die onverbrekelijk samenhangt met het doel van de ontwerpverordening. In het huidige systeem onder de ontwerprichtlijn is er sprake van implementatie- en interpretatieverschillen die in de afgelopen 15 jaar hebben geleid tot nadelen voor de Europese Unie en het bedrijfsleven bij de handhaving van het gegevensbeschermingsrecht. Een samenwerkingsmechanisme bij de handhaving is dus noodzakelijk. Een mechanisme waaraan zoveel partijen moeten deelnemen brengt echter onvermijdelijk met zich dat regels moeten worden gesteld met betrekking tot de uitoefening van bevoegdheden, feitelijke werkzaamheden, de beslistermijnen en de overige regels met betrekking tot de besluitvorming. Een alternatief daarvoor zie ik eigenlijk niet.

– Hoe beziet de regering de rol van de Europese Commissie in relatie tot de rol van het Europese parlement en de Nationale parlementen? Is hier sprake van evenwicht?

De verhouding tussen Europese Commissie, Europees Parlement en de nationale parlementen is geregeld in het Verdrag betreffende de Europese Unie en het Verdrag betreffende de werking van de Europese Unie en de daarbij behorende protocollen en verklaringen, en niet in de ontwerpverordening. Ik moet ook overigens terughoudendheid in acht nemen waar het gaat om de posities van parlementen.

– Hoe reageert de regering op de kritiek van belangengroepen dat de ontwerprichtlijn teveel mogelijkheden zou creëren voor justitie en politie om gegevens op te vragen?

De verwerking van persoonsgegevens door de verantwoordelijke in de private sector is geregeld in de ontwerpverordening. De ontwerprichtlijn regelt de gegevensverwerking door politie en justitie, ten behoeve van de opsporing en de vervolging van strafbare feiten. De ontwerprichtlijn bevat echter geen regels over de toegang van de politieautoriteiten tot de persoonsgegevens van de private sector. De vraag onder welke omstandigheden politie en justitie gegevens kunnen opvragen van de private sector moet worden beantwoord door de ontwerpverordening en de ontwerprichtlijn in hun onderlinge samenhang te bezien. De ontwerpverordening geeft regels voor de rechtmatigheid van de gegevensverwerking, dit is onder meer het geval als de verwerking noodzakelijk is om aan een wettelijke verplichting te voldoen waaraan de verantwoordelijke is onderworpen (artikel 6, eerste lid, onderdeel c). De ontwerprichtlijn geeft eveneens regels voor de rechtmatigheid van de gegevensverwerking door politie en justitie. De betreffende gronden zijn limitatief opgesomd en zijn beperkt tot de uitvoering van een wettelijke taak door een bevoegde autoriteit, ten behoeve van de opsporing en vervolging van strafbare feiten, de nakoming van een wettelijke verplichting waaraan de verantwoordelijke is onderworpen, de bescherming van een vitaal belang van de betrokkene of een andere persoon of om een onmiddellijke en ernstige bedreiging van de openbare veiligheid te voorkomen (artikel 7). Uit deze bepaling vloeit voort dat het opvragen van gegevens aan de

private sector een wettelijke regeling veronderstelt. Ik kan de mening van belangengroepen, dat de ontwerprichtlijn voor politie en justitie teveel mogelijkheden zou creëren om gegevens op te vragen, niet delen. Naar mijn oordeel bevat het vereiste van een wettelijke grondslag voldoende waarborgen voor een afgewogen en evenwichtige regeling die op democratische wijze tot stand komt, met volledige betrokkenheid van het parlement.

– Is naar het oordeel van de regering voldoende gewaarborgd dat geen persoonsgegevens worden verstrekt aan buitenlandse, niet-Europese, overheden zonder dat hieraan duidelijke voorwaarden worden gesteld?

De ontwerpverordening biedt verschillende mogelijkheden voor de rechtmatige doorgifte van persoonsgegevens aan derde landen, ook als de ontvanger van de gegevens de overheid van het desbetreffende land is. Deze leden doelen dan ook vermoedelijk op de vraag of de doorgifte van persoonsgegevens naar derde landen ten aanzien waarvan niet is vastgesteld dat daar een passend niveau van gegevensbescherming bestaat en de doorgifte moet plaatsvinden ingevolge de wetgeving van het desbetreffende of een rechterlijk bevel uit dat land. Uit overweging 90 wordt voldoende duidelijk dat de ontwerpverordening beoogt het conflict van verplichtingen dat door dergelijke wetten en bevelen mede wordt veroorzaakt het hoofd te bieden. Het is mij echter nog niet geheel duidelijk hoe artikel 42 van de ontwerpverordening dit conflict precies oplost. Ik heb daarom de behoefte eerst eens naar de Commissie te luisteren.

Voor wat betreft de ontwerprichtlijn merk ik op dat deze geen bevoegdheden of verplichtingen bevat tot het verstrekken van persoonsgegevens aan derde landen. De voorgestelde regeling gaat ervan uit dat duidelijke voorwaarden worden gesteld aan de gegevensverstrekking, rekening houdend met het niveau van gegevensbescherming in het betreffende land. De regels van de ontwerprichtlijn zijn van toepassing als een dergelijke verstrekking aan de orde is, bijvoorbeeld naar aanleiding van een verdrag. Hieronder zal ik, onder meer naar aanleiding van vragen van de PvdA-fractie, nader ingaan op de verstrekking van persoonsgegevens aan derde landen.

– Is voldoende duidelijk waar een procedure over een eventuele inbreuk moet worden gevoerd? De leden van de VVD-fractie hechten eraan dat dit in ieder geval dichtbij de betreffende persoon kan gebeuren.

Het territorialiteitsbeginsel is uitgangspunt bij de bepaling van de bevoegdheid van de toezichthouders. Dat beginsel is nader uitgewerkt in de regel dat bij het verrichten van activiteiten van een verantwoordelijke in meer dan één lidstaat, de toezichthouder van de lidstaat waar de belangrijkste vestiging van de verantwoordelijke zich bevindt bevoegd is. Die keuze is op zichzelf genomen duidelijk en ook verklaarbaar uit hoofde van een effectieve handhaving, ervan uitgaande dat goed valt vast te stellen dat een vestiging als «de belangrijkste vestiging» kan worden aangemerkt. Maar toegegeven moet worden dat die regel als belangrijk nadeel heeft dat de betrokkene zich soms moet wenden tot een toezichthouder in een andere lidstaat dan de zijne. De daaruit mogelijk voortvloeiende problemen acht ik – met het Cbp – voldoende ernstig om daarvoor de aandacht te vragen.

– Hoe reageert de regering op de zorgen van onder andere PostNL op de verscherping van de regels voor direct marketing. De leden van de VVD-fractie erkennen dat het onwenselijk kan zijn dat ongevraagd post wordt verzonden, maar erkennen daarnaast het economisch belang van deze industrie en vragen zich af of dit voldoende in evenwicht is.

Artikel 19, tweede lid, van de ontwerpverordening is mijn optiek een belangrijke verduidelijking van het al bestaande recht van verzet van de betrokkene op grond van artikel 14, onder b, van ontwerprichtlijn 95/46/EG. Ik acht het niet zonder meer een kwestie van onevenwichtigheid wanneer dit recht wordt verduidelijkt en tot de essentie ervan teruggebracht. Op de specifieke zorgen van PostNL kan ik niet ingaan, aangezien PostNL zich niet tot mij heeft gericht.

– Bijzondere aandacht is volgens de leden van de VVD-fractie nodig voor de positie van het handelsregister van de Kamer van Koophandel en soortgelijke registraties van personen of bedrijven. Graag een reactie van de regering op de bezwaren van de Kamer van Koophandel (zie memo 3 maart 2012).

Het memo van de Kamer van Koophandel waarop deze leden doelen is niet aan mij gezonden, zodat een specifieke bespreking daarvan achterwege moet blijven. In reactie op een memo dat de Kamers van Koophandel, de Dienst Wegverkeer en het Kadaster gezamenlijk aan mij hebben gezonden, kan ik meedelen dat de ontwerpverordening wat mij betreft voldoende ruimte moet openlaten voor het nationale recht om de openbare registers zonder al te veel veranderingen te laten doorfunctioneren. Ik vraag mij af of dat wel in voldoende mate het geval is.

– Is het niet wenselijk de bestaande uitzonderingen voor verwerkingen die geen risico vormen voor de persoonlijke levenssfeer te laten staan, zie in dit kader ook het verzoek van VNO-NCW op dit punt?

In het huidige recht kunnen verwerkingen waarbij sprake is van zodanige risico's dat de inbreuk op de fundamentele rechten en vrijheden van de betrokkene onwaarschijnlijk is, worden vrijgesteld van de meldplicht. Die meldplicht keert in de ontwerpverordening niet meer terug. Dat betekent dat de bestaande uitzonderingen op de meldplicht niet zonder meer zullen terugkeren in de ontwerpverordening. Ik ben er voorstander van dat op het pakket verplichtingen dat de ontwerpverordening op verantwoordelijken legt meer differentiatie mogelijk wordt, zodanig dat wordt aangesloten bij het risico dat de verwerking met zich brengt. Op manier wordt het bedrijfsleven meer proportioneel belast.

– De leden van de VVD-fractie hechten aan een meldplicht voor een »security breach» en een meldplicht voor een«datalek». Aan beide meldplichten kunnen wat de leden van de VVD-fractie betreft voorwaarden worden gesteld omdat het moet gaan om gevallen waarbij daadwerkelijk risico bestaat op het openbaar maken van gevoelige persoonsgegevens. Kan de regeling hierop worden aangepast?

De ontwerpverordening bevat alleen een regeling voor een meldplicht voor datalekken waarbij het risico op verlies of onrechtmatige verwerking van persoonsgegevens aanwezig is. Andere meldplichten passen niet in het kader van de ontwerpverordening. Deze keuze acht ik juist. Artikel 32 van de ontwerpverordening waar de meldplicht voor datalekken is neergelegd, roept nog veel vragen op. Zo lijkt het de bedoeling te zijn dat elk datalek gemeld moet worden. Dat roept de vraag op of een minder vergaande regeling niet tot de mogelijkheden behoort teneinde verantwoordelijken en toezichthouders niet onevenredig te belasten.

– Zou het – zoals VNO-NCW – voorstelt niet verstandig zijn als cruciale interpretaties van de Europese toezichthouder worden getoetst door EC/EP of de Nationale lidstaten zodat ongewenste verruiming of verenging van de regelgeving kan worden voorkomen en daarmee

draagvlak voor de vele verplichtingen die de regelgeving met zich meebrengt gegarandeerd blijft?

Het is een gemis dat de opinies van de artikel 29 Werkgroep tot stand komen zonder inbreng van belanghebbende partijen. Ik ben er voorstander van dat min of meer vergelijkbare documenten van het Europees Comité voor Gegevensbescherming niet aan dat manco lijden.

– Is er voldoende aandacht voor de voorlichting van Europese onderdanen over het risico van het verstrekken van persoonsgerelateerde gegevens aan bijvoorbeeld social media?

Ik zie het geven van voorlichting over de gevolgen van het verwerken van persoonsgegevens via sociale media niet primair als een taak van de Nederlandse of de Europese overheid. De exploitanten van de sociale media dienen invulling te geven aan hun verplichting betrokkenen daarover zorgvuldig, volledig en begrijpelijke taal te informeren, zodat betrokkenen zelf in staat zijn te beslissen of zij instemmen met de beoogde verwerking.

– De leden van de VVD-fractie vrezen dat de implementatie van de regelgeving die nu wordt voorgesteld ook op zich voor enorme nalevingskosten zal zorgen. Graag hiervan een inschatting beschikbaar stellen.

Het is op zichzelf genomen aannemelijk dat de uitbreiding van de verplichtingen van de verantwoordelijke leidt tot een verhoging van de nalevingskosten. Het zou echter een langdurig onderzoek vergen om dit voor het Nederlandse bedrijfsleven in kaart te brengen. Daar komt nog bij dat een dergelijk onderzoek onder alle omstandigheden grote onzekerheden met zich brengt, omdat de ontwerpverordening voorziet in de mogelijkheid van uitzonderingen op de verplichtingen, zonder dat duidelijk is wat de reikwijdte van die uitzonderingen zal zijn. Ik acht het bovendien niet mijn taak, maar die van de Europese Commissie om dergelijke berekeningen uit te voeren. In mijn beantwoording van de eerste vraag van deze leden heb ik de beschikbare cijfers gegeven.

– Is het juist dat bij invoering van art. 6 lid 1e en f van de ontwerpverordening bedrijven geen gebruik meer mogen maken van adresbestanden van derden?

Het verschil tussen het voorgestelde artikel 6, eerste lid, onder e en f, van de ontwerpverordening en artikel 7, eerste lid, onder e en f, van ontwerprichtlijn 95/46/EG is dat de rechtvaardigingsgrond voor het verwerken van persoonsgegevens in de ontwerpverordening voortaan beperkt blijft tot het publieke belang waarvan de verantwoordelijke zelf de drager is, respectievelijk het gerechtvaardigde private belang dat de verantwoordelijke zelf formuleert. In geen van beide gevallen mag de verantwoordelijke nog langer (mede) namens of ten behoeve van derden gegevens verwerken, zoals dat onder de ontwerprichtlijn nog wel is toegestaan. Dat betekent niet dat bedrijven geen gebruik meer zouden kunnen maken van adresbestanden van derden, maar dat zij de belangen van derden niet langer tot de hunne kunnen maken, buiten het verband van een gezamenlijke directe verantwoordelijkheid of een bewerkersovereenkomst. Het doelbindingsvereiste wordt daarmee strikter gehandhaafd.

– Het Cbp stelt dat de tekst van de algemene ontwerpverordening en de ontwerprichtlijn voor het terrein van politie en justitie op een aantal essentiële punten behoorlijk uiteen lopen, waardoor de alomvattendheid van het wetgevend pakket in gevaar komt. Volgens het Cbp moeten de volgende begrippen worden opgenomen in de ontwerpverordening en in

de ontwerprichtlijn: 1) rechtmatigheid van de verwerking, 2) doelbinding, 3) accuratesse van gegevens, 4) de noodzaak tot het stellen van heldere bewaartermijn (niet langer dan strikt noodzakelijk). Daarnaast dienen volgens het Cbp ook de verplichtingen die van toepassing zijn op de verantwoordelijke en bewerker in beide instrumenten gelijkgeschakeld te worden, waaronder de verplichting tot het uitvoeren van privacy impact assessments en het zorgdragen voor privacy by design. De leden van de fractie van de VVD vragen zich af wat voor gevolgen deze suggesties van het Cbp hebben voor de uitvoerbaarheid en het doel van de wetgeving en of de regering de opvatting van het Cbp deelt.

Het Cbp heeft er op gewezen dat de tekst van de ontwerprichtlijn en de ontwerpverordening op een aantal essentiële punten behoorlijk uiteen lopen, waardoor de alomvattendheid van het wetgevend pakket in gevaar komt. Het Cbp heeft erop aangedrongen dat tijdens de onderhandelingen scherp in de gaten worden gehouden dat de samenhang tussen de beide instrumenten gewaarborgd wordt en op een aantal punten fors wordt versterkt. Dat is volgens het Cbp in de eerste plaats het geval voor de algemene beginselen voor gegevensverwerking. In het bijzonder begrippen als de rechtmatigheid van de verwerking, doelbinding, accuratesse van gegevens, en de noodzaak tot heldere bewaartermijnen dienen zowel in de ontwerpverordening als de ontwerprichtlijn te worden opgenomen. Daarnaast dienen ook de verplichtingen die van toepassing zijn op de verantwoordelijke en bewerker in beide instrumenten gelijkgeschakeld te worden, waaronder de verplichting tot het uitvoeren van privacy impact assessments en het zorgdragen voor privacy by design. Tenslotte dienen de bevoegdheden die worden toegekend aan de gegevensbeschermingsautoriteiten naar het oordeel van het Cbp gelijk getrokken te worden.

Naar aanleiding van de inbreng van het Cbp merk ik op hier in beginsel positief tegenover te staan, met dien verstande dat rekening moet worden gehouden met het verschil in toepassingsbereik van de beide rechtsinstrumenten. Het Cbp erkent dit tot op zekere hoogte ook, omdat het College opmerkt dat een zeker onderscheid in de regels begrijpelijk is, zeker gelet op het specifieke karakter van de politie- en justitiesector. Daarbij merk ik op dat bepaalde beginselen inzake gegevensverwerking, zoals de rechtmatigheid van de verwerking, de doelbinding, de accuratesse en de noodzaak tot het stellen van een heldere bewaartermijn, in de beide rechtsinstrumenten zijn opgenomen. Daarvoor kan worden verwezen naar artikel 4 van de ontwerprichtlijn en artikel 5 van de ontwerpverordening. Op dat punt lijkt het verschil niet erg groot, en lijkt ook de samenhang nauwelijks in het geding. Ten aanzien van de verplichtingen voor de verantwoordelijke en de bewerker zijn de verschillen groter. Anders dan de ontwerprichtlijn kent de ontwerpverordening een verplichting voor de verantwoordelijke of de bewerker tot het verrichten van privacy impactassessments (artikel 33). Vooralsnog staat de regering tamelijk gereserveerd ten opzichte van een dergelijke verplichting voor politie en justitie, omdat het weinig aantrekkelijk lijkt om de gegevensverwerking in een opsporingsonderzoek of een concrete strafzaak vooraf door een toezichthoudend orgaan te laten toetsen. Dit zal snel kunnen leiden tot het door elkaar lopen van de taken van het toezichthoudend orgaan en die van de rechterlijke macht. Bovendien zal de taakuitvoering van politie en justitie daardoor ernstig kunnen worden belemmerd. Een andere zaak is, dat nieuwe wettelijke regels op het gebied van de opsporing en vervolging van strafbare feiten aan een privacy impact assessment wordt onderworpen. Tijdens de behandeling van het rapport van de Commissie Brouwer-Korf heeft de regering dit, naar aanleiding van een motie van het lid Franken (Kamerstukken I, 2010/11, 31 051, D) toegezegd (Handelingen Eerste Kamer 17 mei 2011, EK 27-11-48). Dan gaat het echter om de

totstandkoming van nieuwe wetgeving, waarbij van een beperking van het grondrecht van de bescherming van de persoonlijke levenssfeer sprake is. Minder gereserveerd staat de regering ten opzichte van de toepassing van de regels op het gebied van de privacy by design. Hiervoor zijn in de beide rechtsinstrumenten regels opgenomen. Daarvoor kan worden verwezen naar artikel 19 van de ontwerprichtlijn en artikel 23 van de ontwerpverordening. Deze regels vertonen een hoge mate van overeenstemming. Tenslotte kan de regering zich vinden in de door het Cbp voorgestelde gelijktrekking van de bevoegdheden van de gegevensbeschermingsautoriteiten.

– De ontwerpverordening gegevensbescherming zorgt ervoor dat de rechten van betrokkenen worden versterkt, met name het recht om te worden vergeten en het recht op dataportabiliteit. De leden van de VVD-fractie zien hier het belang van in. Hoe schat de regering de uitvoerbaarheid hiervan in? Indien dit volgens de regering moeilijk uitvoerbaar is, wat zou er gedaan kunnen worden om deze uitvoerbaarheid te verbeteren? Hoe zal het recht om te worden vergeten worden gehandhaafd/uitgevoerd? De VVD hecht hier aan, maar hoopt dit zo effectief mogelijk te realiseren zonder onuitvoerbaar te worden.

Ook ik hecht aan het belang van het recht om te worden vergeten en het recht op dataportabiliteit. Tegelijk moet worden bedacht dat beide rechten naar hun aard niet absoluut van karakter van zijn. Gerechtvaardigde belangen van de verantwoordelijke of van een derde kunnen vergen dat een verzoek van de betrokkene om zijn gegevens te wissen niet wordt ingewilligd. Wat het recht om te worden vergeten betreft, lijkt het recht om gegevens te wissen in de verhouding tussen betrokkene en verantwoordelijke eerder en eenvoudiger uitvoerbaar dan in de verhouding tussen betrokkenen, verantwoordelijke en derden. Via internet en sociale media kunnen gegevens zo snel en zo grootschalig worden verspreid dat het in veel gevallen niet goed mogelijk lijkt te achterhalen welke derden over de gegevens beschikken en aan wie die derden de gegevens op hun beurt hebben verstrekt. Het is dan aangewezen dat van de verantwoordelijke niet veel meer kan worden gevergd dan dat hij een redelijke, althans niet onevenredige inspanning verricht de derden mee te delen dat de betrokkene verzoekt zijn gegevens te wissen. Een dergelijke benadering is thans reeds geldend recht (art. 38 Wbp). De ontwerpverordening biedt aanknopingspunten voor het vorenoverwogene, maar roept ook vragen op, zoals de verplichte overname van verantwoordelijkheid voor publicaties door derden die op basis van rechtmatig verwerkte persoonsgegevens plaatsvond.

Het recht op dataportabiliteit is van andere orde, aangezien de betrokkene de uitoefening van dat recht veel meer in eigen hand heeft dan het recht om te worden vergeten. De vraag bij dit recht is nog wel hoe moet worden vastgesteld of een gebruikte dataset algemeen gebruikelijk is en of er voor een nieuwe verantwoordelijke die een dataset krijgt aangeboden wel een acceptatieplicht bestaat. Dit zal vermoedelijk sectorgewijs moeten worden vastgesteld.

– De ontwerpverordening voorziet in een brede informatieplicht aan personen van wie gegevens worden verwerkt. Hoe wordt dit in de praktijk uitgevoerd en is hier volgens de regering behoefte aan, welk probleem lost dit op? De leden van de VVD-fractie gaan er in ieder geval van uit dat er op korte en bondige manier informatie moet worden verstrekt, terwijl dit ook echt een doel moet dienen. Dit is te overzien voor de verstrekker, maar ook voor de ontvanger.

De informatieplicht is een essentieel onderdeel van de ontwerpverordening, evenals van de huidige ontwerprichtlijn. Informatie door de verantwoordelijke over diens identiteit, de doeleinden van de verwerking, de gegevens die hij verwerkt, en het verstrekkingenregime stellen de betrokkene in staat om te beoordelen wat er met zijn persoonsgegevens gebeurt en of hij daarop invloed wil uitoefenen. Aan die verplichting kan op uiteenlopende manieren uitvoering worden gegeven, eenprivacyverklaring op websites en in algemene voorwaarden, mededelingen op adreswikkels van tijdschriften of telefonische mededelingen. Uit artikel 11 van de ontwerpverordening volgt dat de informatie op transparante en gemakkelijk toegankelijke wijze moet worden gegeven.

– Er wordt in de ontwerpverordening voorzien in robuuste sanctionering, met name in de bevoegdheid tot het vaststellen van bestuurlijke boetes door toezichthouders. De hoogte van deze boetes wordt op EU-niveau vastgesteld. Wat zou hierbij volgens de regering de rol van de lidstaten moeten zijn en wordt deze voldoende gewaarborgd in het voorstel? Is het voorstel op dit gebied volgens de regering een verbetering ten opzichte van de huidige situatie in Nederland?

Waar de Europese wetgever de bevoegdheid tot het vaststellen van bestuurlijke boetebesluiten, de beboetbare feiten en het boetemaximum vaststelt, is er voor de wetgevers van de lidstaten geen ruimte meer om terzake nog wetgeving vast te stellen. Dat er in de hele EU een geharmoniseerd boetemaximum wordt vastgesteld, is beslist een verbetering van het handhavingsniveau.

– De regering stelt in het fiche dat de ontwerpverordening deels als niet proportioneel wordt beoordeeld, met name doordat het te gedetailleerd is uitgewerkt. De VVD-fractie ziet hierin eveneens een gevaar. Hoe kan dit volgens de regering worden verholpen zonder daarmee de doelen van het voorstel niet kunnen worden bereikt?

Dat zou kunnen worden bereikt door veel van de grondslagen voor het vaststellen van gedelegeerde handelingen door de Commissie te laten vervallen. Dat zou ook kunnen gebeuren door bij de vormgeving van rechten en verplichtingen meer verantwoordelijkheid te geven aan verantwoordelijke overheden en bedrijven, en aan betrokkenen zelf.

– De leden van de VVD-fractie vragen zich af waarom er niet is gekozen voor optie 1 uit de impact assessment en zou hierover graag de visie van de regering vernemen.

Optie 1 uit het Policy Impact Assessment hield in dat Commissie voorstellen zou doen voor «soft law» als interpretatieve verklaringen bij de huidige ontwerprichtlijn, bewustwordingscampagnes voor betrokkenen en stimuleringscampagnes voor verantwoordelijken. Daarnaast zou een beperkte wijziging van de ontwerprichtlijn worden voorgesteld. Ik ben het met de Commissie eens dat als gevolg van het niet bindende karakter van soft law de garantie zou ontbreken dat er daadwerkelijk een einde komt aan de implementatie- en interpretatieverschillen in de diverse lidstaten. Ik herinner eraan dat ook het Nederlands bedrijfsleven heeft aangegeven dit als een probleem te zien. Ook kan een aanpak met soft law de uiteenlopende bevoegdheden op het gebied van de handhaving niet voorkomen, aangezien die bij behoud van het huidige stelsel de bevoegdheid zouden blijven van de wetgevers van de lidstaten.

– De VVD-fractie ziet een rol voor het beter informeren van gebruikers bij online gebruiksovereenkomsten. Op dit moment krijgt iemand online een ellenlange tekst waar gewoonlijk onderaan snel akkoord wordt aange-

vinkt. Dit kan beter kort en bondig op basis van een paar criteria, zoals dat nu ook gebeurt bij financiële producten. Kan dit door Nederland bij de discussie ingebracht worden?

Ik ben het met deze leden eens dat de invulling van de informatieplicht en het verlenen van toestemming voor het verwerken van persoonsgegevens het beste op korte en bondige wijze onder de aandacht van de betrokkene kan worden gebracht. De artikelen 7 en 11 van de ontwerpverordening bieden daarvoor al de nodige regels. Het voorstel zal ik op deze punten zeker ondersteunen.

– Er wordt een aantal verplichtingen aan bedrijven opgelegd, zoals het aanstellen van Data Protection Officers en het verplicht uitvoeren van Data Protection Impact Assessments. Welke van deze verplichtingen zijn volgens de regering, a) noodzakelijk/effectief, b) proportioneel, c) uitvoerbaar? En welke zijn dat bij a, b en c niet?

Ik acht zowel het aanstellen van een Data Protection Officer als het uitvoeren van Data Protection Impact Assessments in algemene zin zinvol en uitvoerbaar. Of het noodzakelijk, effectief en proportioneel is moet van geval tot geval worden vastgesteld. Het zal zeker niet in alle gevallen waarin gegevens worden verwerkt noodzakelijk zijn dergelijke verplichtingen uit de voeren. Hoe groter het risico op de bescherming van de persoonlijke levenssfeer is dat aan de verwerking is verbonden, des te meer aanleiding zal er zijn een Data Protection Officer aan te stellen of een Data Protection Impact Assessment uit te voeren.

– Er wordt een One Stop Shop opgezet voor dataprotectie in de EU, naast de onafhankelijke dataprotectie-autoriteiten. De leden van de VVD-fractie vragen zich af of dit in de praktijk ook wel gaat werken. Heeft dit volgens de regering toegevoegde waarde? Wat is de Nederlandse inzet bij dit onderwerp?

De one stop shop procedure in gevallen van grensoverschrijdend nalevingstoezicht en handhaving beschouw ik als een belangrijk winstpunt op het gebied van toezicht en handhaving. Het bedrijfsleven heeft aangegeven hier ook veel winst in te zien. Het scheelt immers het onderhouden van contacten met uiteenlopende toezichthouders in verschillende lidstaten, met een telkens verschillend talenregime. Ik ben niet pessimistisch over de kansen op succes van het mechanisme. Onder het huidige regime werken de toezichthouders in individuele zaken ook al onderling samen en kunnen zij onder omstandigheden ook al ten behoeve van collegatoezichthouders onderzoekshandelingen in eigen land verrichten. Er is dus al de nodige ervaring beschikbaar.

– Voor de VVD is het van belang dat de ontwerprichtlijn het niet onmogelijk maakt om opsporing en vervolging van criminaliteit effectief te laten verlopen. Het voorstel moet dus uitvoerbaar en betaalbaar zijn. Hoe kan dat verbeterd worden ten opzichte van wat de commissie heeft gepresenteerd? In het fiche wordt een aantal keer gemeld dat de voorstellen gevolgen kunnen hebben voor politie en justitie. De leden van de VVD-fractie willen tevens weten wat precies deze gevolgen zijn in de praktijk? Hoe kunnen deze gevolgen zo veel mogelijk verminderd worden, zodat bescherming van persoonsgegevens kan blijven gewaarborgd en politie en justitie gewoon effectief hun werk kunnen blijven doen?

In antwoord op de gestelde vragen merk ik op dat er op dit moment nog geen gedetailleerd beeld bestaat van de precieze gevolgen van de voorstellen voor politie en justitie in de praktijk. Inmiddels is het voorstel voor de ontwerprichtlijn voorgelegd aan vertegenwoordigers van politie

en justitie, die hebben aangegeven dat sommige onderdelen van het voorstel gevolgen kunnen hebben voor de effectiviteit van de opsporing en de vervolging. Zoals ook in het BNC-fiche is aangegeven, heeft dit vooral betrekking op het maken van onderscheid tussen de verschillende categorieën van personen en categorieën van persoonsgegevens, de verplichting tot het informeren van de betrokkene over de gegevensverwerking, het recht op verwijdering van gegevens en de melding van datalekken. Voor wat betreft het maken van onderscheid tussen categorieën van personen betekent dit dat politie en justitie, voor zover mogelijk, van ieder gegeven moeten vermelden of dit een verdachte, een veroordeelde of een slachtoffer betreft, en de graad van betrouwbaarheid van het betreffende gegevens moeten vermelden. Voor wat betreft het informeren van de betrokkene betekent dit dat politie en justitie in beginsel een persoon die in aanraking komt met de politie moeten informeren over een aantal aspecten rond de gegevensverwerking zoals de doelen van de verwerking, de periode gedurende welke de gegevens worden opgeslagen en de ontvangers van de gegevens. Voor wat betreft het recht op verwijdering betekent dit dat gegevens worden gemarkeerd als de juistheid daarvan door de betrokkene wordt betwist, hetgeen bij opsporing en vervolging bij uitstek aan de orde is. Voor wat betreft de melding van datalekken betekent dit dat de politie binnen 24 uur de toezichthoudende instantie informeert over iedere inbreuk in verband met persoonsgegevens, welk begrip in de ontwerprichtlijn zeer ruim is omschreven (artikel 3, negende lid), samen met aanbevelingen voor maatregelen om de nadelige gevolgen van de inbreuk te verminderen en een omschrijving van de maatregelen om de inbreuk aan te pakken. Gedurende de onderhandelingen over de ontwerprichtlijn zal nagegaan moeten worden welke mogelijkheden beschikbaar en haalbaar zijn om de uitvoerbaarheid en haalbaarheid van de maatregelen te verbeteren en de gevolgen van de maatregelen zodanig te verminderen dat politie en justitie effectief hun werk kunnen blijven doen.

– Artikel 75 lid 2 van de ontwerpverordening bepaalt dat de gerechtelijke instanties van de lidstaat waar de voor de verwerking verantwoordelijke of de verwerker is gevestigd, competent zijn om te oordelen over een vordering. Hoe verhoudt deze bepaling zich tot de competentieregels uit het EEX en waarom is er niet voor gekozen om deze regels te volgen in de ontwerpverordening? In het bijzonder in gevallen waarbij er meerdere verweerders zijn (art. 6 sub 1 EEX) en in het geval van een forumkeuze krachtens art. 23 EEX.

Artikel 75, tweede lid, van de ontwerpverordening stelt andere regels dan de EEX-Ontwerpverordening. In dat opzicht geldt de ontwerpverordening als bijzonder recht ten opzichte van het algemene recht van de EEX-Ontwerpverordening, voor zover het betreft geschillen die worden beheerst door het burgerlijk procesrecht. Wanneer de verwerende partij een bestuursorgaan is zal het geschil in veel lidstaten, Nederland niet uitgezonderd, worden beheerst door het bestuursprocesrecht. De EEX-Ontwerpverordening is niet van toepassing op het bestuursprocesrecht. Hoewel het Explanatory Memorandum geen specifieke toelichting op de gemaakte keuze bevat, is hier van belang dat tussen verantwoordelijke en betrokkene relatief vaak een ongelijkwaardige verhouding bestaat. Dat verklaart naar alle waarschijnlijkheid het keuzerecht van de betrokkene in artikel 75, tweede lid, tweede volzin, van de ontwerpverordening.

– Artikel 76 lid 2 voorziet in een regeling om parallelle procedures te voorkomen. Kan de regering aangeven wat onder een parallelle procedure wordt verstaan en hoe verhoudt artikel 76 zich tot de connexiteit-regel uit het EEX (art. 27 en 28 EEX).

Het is zeker denkbaar dat een verantwoordelijke in meer dan één lidstaat een vestiging heeft die aanknopingspunt vormt voor het opwerpen van een geschil. Dat kan heel goed hetzelfde geschil of een sterk vergelijkbaar geschil zijn. Hierboven gaf ik al aan dat de ontwerpverordening als bijzonder recht geldt ten opzichte van de EEX-Ontwerpverordening.

PvdA

– De leden van de PvdA-fractie hebben met belangstelling de voorstellen van de EU met betrekking tot de EU-ontwerpverordening bescherming persoonsgegevens en de ontwerprichtlijn gegevensbescherming opsporing en vervolging, gelezen. In het algemene zijn de leden blij met de aanpassing van de EU-wetgeving bescherming persoonsgegevens. De wetgeving die Europese burgers moet beschermen tegen ongeoorloofd gebruik van hun persoonsgegevens moet dringend worden aangepast aan de eisen van deze tijd. Daarnaast is het noodzakelijk dat alle EU-lidstaten hetzelfde beschermingsniveau hanteren, omdat persoonsgegevens niet beperkt blijven tot de landsgrenzen.
De leden van de PvdA-fractie zien enerzijds een verbetering van de bescherming van de persoonsgegevens van de burger, maar de leden zijn er nog niet van overtuigd dat de ontwerpverordening en ontwerprichtlijn in zijn geheel een verbetering is. Kan de regering aangeven of de ontwerpverordening en de ontwerprichtlijn per saldo een betere bescherming biedt aan burgers dan onder de huidige nationale regels. Acht de regering die bescherming op alle onderdelen van het voorstel verbeterd of op delen? Waar kan volgens de regering gesproken worden van een hogere beschermingsniveau en waar van een lagere beschermingsniveau? En wat is uw oordeel daarover?

Naar mijn oordeel biedt de Ontwerpverordening per saldo een betere bescherming aan burgers dan onder de huidige nationale regels. De huidige nationale regels op het gebied van de bescherming van persoonsgegevens zijn opgenomen in de Wet bescherming persoonsgegevens, de Wet politiegegevens voor wat betreft de verwerking van persoonsgegevens ten behoeve van de uitvoering van de politietaak als bedoeld in de artikelen 2 en 6, eerste lid, van de Politiewet 1993, en de Wet justitiële en strafvorderlijke gegevens voor wat betreft persoonsgegevens betreffende de toepassing van het strafrecht of de strafvordering en de verwerking van persoonsgegevens in een strafvorderlijk onderzoek. De Wet bescherming persoonsgegevens vormt de weerslag van de Europese Privacyrichtlijn 95/46/EG, die in 1995 is vastgesteld. De Wet politiegegevens en de Wet justitiële en strafvorderlijke gegevens zijn beïnvloed door het Europese kaderbesluit dataprotectie, dat in 2008 is vastgesteld. De commissie stelt nu een pakket voor tot herziening van de bestaande EU-regels op het gebied van de gegevensbescherming. Dit betreft een ontwerpverordening in de plaats van de huidige Privacyrichtlijn, en een ontwerprichtlijn in de plaats van het huidige kaderbesluit. In zijn algemeenheid vormen de ontwerpverordening en de ontwerprichtlijn een nadere uitwerking van de huidige Europese regels.

De ontwerpverordening belooft in zijn algemeenheid een hoger beschermingsniveau dan ontwerprichtlijn 95/46/EG nu kan bieden. Zeker wanneer dit wordt gezien in het perspectief van de EU als geheel. Dat valt toe te schrijven aan het feit dat burgers hun rechten in de gehele EU op dezelfde manier kunnen inroepen tegen verantwoordelijken, en op dezelfde manier toegang kunnen krijgen tot toezichthouders. Daarenboven worden strengere eisen gesteld aan het verlenen van toestemming en worden de rechten van betrokkenen uitgebreid met het recht om te worden vergeten en het recht op dataportabiliteit. De uitwerking van het accountabilitybeginsel leidt tot een uitbreiding van de verplichtingen van verantwoorde-

lijken, waarmee uiteindelijk ook wordt beoogd de positie van betrokkenen te verbeteren. Daarnaast geldt dat met de conceptontwerpverordening natuurlijk niet alleen wordt beoogd de rechten van burgers te beschermen. Ook de positie van verantwoordelijken verdient aandacht. Dat hoort bij een evenwichtig voorstel. Ik zie die aandacht niet als een verlaging van het beschermingsniveau.

Voor wat betreft de ontwerprichtlijn ben ik van oordeel dat deze in ieder geval een hoger beschermingsniveau biedt dan het huidige kaderbesluit 2008/977/JBZ. Het huidige kaderbesluit is uitsluitend van toepassing op persoonsgegevens die tussen de lidstaten worden uitgewisseld of die worden verstrekt aan Europol of Eurojust. Daar komt bij dat sommige onderwerpen in de ontwerprichtlijn meer gedetailleerd zijn geregeld, zoals de instemming van de betrokkene met de gegevensverwerking, het recht op toegang voor de betrokkene en de taken en bevoegdheden van het toezichthoudende orgaan. Andere onderwerpen zijn geheel nieuw, zoals de verplichting tot het melden van datalekken, het recht te worden vergeten en de verplichting tot het houden van privacy impact assessments. In het licht van het totale pakket van nationale regels het gebied van de bescherming van persoonsgegevens die worden verwerkt ten behoeve van de opsporing en vervolging van strafbare feiten kunnen echter geen algemene uitspraken worden gedaan over het verschil in het niveau van gegevensbescherming tussen de ontwerprichtlijn en de nationale regelgeving.

– De leden zijn zeer verheugd met de versterking van het toestemmingsvereiste. De leden van de PvdA-fractie zijn van mening dat burgers moeten weten welke persoonsgegevens worden gebruikt en waarvoor. Zij moeten beschikking hebben en houden over hun persoonsgegevens. Dat betekent dat toestemming vereist is voor het gebruik van persoonsgegevens en als die toestemming wordt ingetrokken, ook de grond voor het gebruik van die persoonsgegevens wegvalt. Deelt de regering dit uitgangspunt en is de regering van mening dat dit principe voldoende gewaarborgd is in de nieuwe EU-regelgeving? Zo nee, waar kan op dit punt de ontwerpverordening nog worden aangescherpt?

De belangrijkste verandering in het toestemmingsvereiste is dat een einde wordt gemaakt aan de situatie waarin sprake is van twee verschillende vormen van toestemming. De ondubbelzinnige toestemming als rechtvaardigingsgrond voor de verwerking van persoonsgegevens in het algemeen en de uitdrukkelijke toestemming voor de verwerking van bijzonder persoonsgegevens. Dat is een winstpunt. En het is inderdaad zo dat verwerking van gegevens moet worden beëindigd wanneer een toestemming wordt ingetrokken en er geen andere rechtvaardigingsgrond rest. Maar er zijn zeker nog vragen over de exacte betekenis van de artikelen 6, eerste lid, onder a, en 7 van de ontwerpverordening. Zo is het de vraag of de rechtszekerheid niet gebiedt dat een toestemming expliciet wordt verleend. Ook is het de vraag of de bewijslast voor de verantwoordelijke niet met zich brengt dat juist meer persoonsgegevens verwerkt moeten worden dan zonder die eis nodig zou zijn. Tenslotte is de toevoeging dat geen beroep op een toestemming kan worden gedaan wanneer sprake is van een «aanzienlijke onevenwichtigheid» tussen betrokkene en verantwoordelijke een regel die zonder enige twijfel aanleiding zal geven tot interpretatieproblemen en conflicten.

– Begrijpen de leden het zo goed dat volgens de voorgestelde EU-ontwerpverordening het duidelijk moet zijn waarvoor de burger toestemming geeft en dat deze toestemming, bv voor het aanvaarden van algemene voorwaarden, niet gezien mag worden als toestemming voor

het verwerken van persoonlijke gegevens? Zo nee, in hoeverre wordt de doelbinding te weinig gewaarborgd in de conceptontwerpverordening?

Artikel 6, eerste lid, onder a, van de ontwerpverordening regelt dat toestemming wordt gegeven voor de verwerking van persoonsgegevens voor een of meer specifieke doeleinden. Uit artikel 4, onder (8), van de ontwerpverordening vloeit voort dat toestemming op informatie over de verwerking moet berusten. In zoverre moet het de betrokkene dus voorafgaand duidelijk worden gemaakt wat de strekking van de toestemming is. Wanneer het verlenen van toestemming deel uitmaakt van het aanvaarden van, bijvoorbeeld, algemene voorwaarden, moet het verlenen van toestemming «duidelijk afzonderlijk» worden weergegeven van de andere voorwaarden.

– De Europese toezichthouders hebben in een gezamenlijk opiniestuk geoordeeld over de conceptontwerpverordening. Over het algemeen zijn zij positief over de voorstellen die zijn gedaan. Echter, op sommige punten hebben zij kritiek of maken zij zich zorgen over de ontwerpverordening. Zo zijn de gezamenlijk toezichthouders (Article 29 Working Party) van mening dat de ontwerpverordening de mogelijkheid opent voor «incompatible uses» voor zowel de private als de publieke sector dat kan leiden tot «highly undesirable results» (pagina 16). Met andere woorden, zo lezen de leden dit commentaar, is er sprake van uitholling van de doelbinding. Is de regering bereid notie te nemen van het commentaar van de Article 29 Working Party en te reageren op hun kritiek op dit punt?

Het standpunt van de artikel 29 Werkgroep en van de Europese Toezichthouder voor de Gegevensbescherming over de verhouding tussen de artikelen 5, onder b en 6, vierde lid, van de ontwerpverordening is mij bekend. Ik ben van oordeel dat het voorstel van de Commissie een nuttige bijdrage levert aan de discussie over de vraag wat de betekenis van het vereiste van doelbinding is in een omgeving waarin het verder verwerken van gegevens via internet en sociale media veel gemakkelijker en goedkoper is, en dit bovendien voor zeer velen ook veel vanzelfsprekender lijkt dan 20 jaar geleden nog het geval was toen richtlijn 95/46/EG werd ontworpen. Het is naar mijn mening de vraag of het in de thans bestaande verhoudingen nog wel reëel is onverkort vast te houden aan doelbinding als enig ijkpunt voor de verwerking van persoonsgegevens, of dat niet meer nadruk moet worden gelegd op compenserende waarden als dataminimalisatie. Dat is geen kwestie van het uithollen van doelbinding, maar het eigentijds invullen van die eis. Ik wijs erop dat dit vraagstuk bij de totstandkoming van de Wet bescherming persoonsgegevens ook al onder ogen is gezien. Dit heeft geleid tot artikel 9 van de Wbp dat de verantwoordelijke ook nu al een redelijk ruime armslag verschaft voor het zogeheten nevengebruik, mits hij zich daarvan in een door hem zelf te verrichten belangenafweging rekenschap geeft tegenover betrokkenen en de toezichthouders.

– De leden maken zich zorgen over het principe van de doelbinding in relatie tot de overheden. In hoeverre wijkt de doelbinding voor de overheden af van de doelbinding voor de private sector. Maw wat mag de overheid meer met betrekking tot de verzamelde persoonsgegevens wat een private partij niet mag. En in hoeverre is dit conform, dan wel in strijd met het doelbindingsprincipe?

De ontwerpverordening bepaalt niet zelf voor welke doeleinden publieke of private partijen in concreto persoonsgegevens mogen verwerken. Wel is er een betekenisvol verschil in de rechtvaardigingsgronden voor de verwerking van persoonsgegevens voor beide sectoren. Artikel 6, eerste lid, onder c en e, van de ontwerpverordening zijn specifiek bedoeld voor

de gegevensverwerking in de publieke sector. Gegevens mogen door de overheid worden verwerkt wanneer daartoe een wettelijke verplichting bestaat en gegevens mogen worden verwerkt wanneer de verwerking noodzakelijk is voor de vervulling van een taak van algemeen belang of een taak die deel uitmaakt van de uitoefening van het openbaar gezag dat aan de voor verwerking verantwoordelijke is opgedragen. Die rechtvaardigingsgronden verschillen niet wezenlijk van de rechtvaardigingsgronden die al in richtlijn 95/46/EG zijn opgenomen. Voor de publieke sector betekent dit dat de wetgever van geval tot geval moet vaststellen in welke gevallen persoonsgegevens worden verwerkt, en welke voorwaarden en beperkingen daaraan worden verbonden. Algemene beperkingen op deze bevoegdheid vloeien voort uit artikel 8, tweede lid, EVRM, artikel 52 van het Handvest voor de Grondrechten van de EU en de Grondwet.

– Deelt u de mening van de Staatscommissie Grondwet dat het doelbindingsprincipe zo sterk moet zijn dat het opgenomen moet worden in de Grondwet? Zo nee, waarom niet?

In antwoord op deze vraag verwijs ik deze leden graag naar het kabinetsstandpunt naar aanleiding van het rapport van de Staatscommissie Grondwet. Dit betreft de brief van 24 oktober 2011 van de Minister van Binnenlandse Zaken en Koninkrijksrelaties aan de Voorzitter van de Tweede Kamer der Staten-Generaal, Kamerstukken II 2011/12, 31 570, nr. 20.

– Naast de ontwerpverordening is een apart conceptontwerprichtlijn opgesteld waarin de verwerking van de persoonsgegevens door politie en justitie zijn opgenomen. De opslag en verwerking van persoonsgegevens in het justitieel kader heeft de laatste jaren een grote vlucht genomen. Camera's in het publieke domein, toegang tot telecomgegevens etc. De ontwerprichtlijn geeft de lidstaten veel ruimte om af te wijken van de waarborgen die genoemd zijn in de ontwerprichtlijn. Het spijt de leden van de PvdA-fractie dat de ontwerprichtlijn niet een ambitieniveau heeft vergelijkbaar met de ontwerpverordening.

De leden vragen zich af welke regels gehanteerd worden als gegevens overgedragen worden naar een ander EU-land. Is de regering met de leden van de PvdA van mening dat beperkingen die op grond van nationale wetgeving aan de verwerking van persoonsgegevens zijn gesteld ook van toepassing moeten zijn als de gegevens met andere EU-lidstaten worden uitgewisseld? Zo nee, waarom niet? Zo ja, is de regering bereid om dit in te brengen bij de eerstvolgende mogelijkheid?

De ontwerprichtlijn bevat een afzonderlijk hoofdstuk over de doorgifte van persoonsgegevens naar derde landen of internationale organisaties (hoofdstuk V). De hoofdregel is dat de doorgifte van persoonsgegevens aan een derde land of een internationale organisatie slechts kan plaatsvinden nadat de Commissie heeft besloten dat het betreffende derde land of internationale organisatie een passend niveau van gegevensbescherming waarborgt. Daarbij wordt rekening gehouden met verschillende aspecten, zoals de algemene en sectorale wetgeving, het bestaan van effectieve en afdwingbare rechten, het bestaan en de effectieve werking van onafhankelijke toezichthoudende autoriteiten en de internationale verbintenissen die het betrokken derde land of de internationale organisatie is aangegaan (artikel 34, eerste lid). Wanneer de Commissie hierover geen besluit heeft vastgesteld, kan de doorgifte van persoonsgegevens naar een ontvanger in een derde land of internationale organisatie plaatsvinden indien in een juridisch bindend instrument, zoals een verdrag, passende garanties voor de bescherming van de persoonsgegevens zijn geboden, of de verantwoordelijke alle omstandigheden heeft

beoordeeld en heeft geconcludeerd dat er passende waarborgen bestaan voor de bescherming van persoonsgegevens (artikel 35). In afwijking van deze regeling kan de doorgifte naar een derde land of internationale organisatie slechts plaatsvinden als dit noodzakelijk is voor bepaald omschreven doeleinden, zoals de voorkoming van een onmiddellijke en ernstige bedreiging voor de openbare veiligheid van een lidstaat of derde land (bijvoorbeeld een aanslag), of als dit in afzonderlijke gevallen noodzakelijk is met het oog op de preventie, het onderzoek, de opsporing, of de vervolging van strafbare feiten of de tenuitvoerlegging van straffen (artikel 36, onderdeel c en onderdeel d).
In antwoord op de vraag van de PvdA-fractie naar de mogelijkheid om beperkingen op grond van de nationale wetgeving toe te passen op de uitwisseling van gegevens met andere lidstaten acht ik enige terughoudendheid op zijn plaats. Het beginsel dat nationale beperkingen van kracht blijven bij de verstrekking van persoonsgegevens aan andere lidstaten vormt op het eerste gezicht een aantrekkelijke mogelijkheid om vergaande nationale regels van toepassing te kunnen laten blijven als de gegevens in een andere lidstaat verder worden verwerkt. Het huidige kaderbesluit bevat een dergelijke mogelijkheid (artikel 12, eerste lid). Ditzelfde geldt voor de ontwerprichtlijn (artikel 37). Het bezwaar van een dergelijke regeling is echter dat de Nederlandse opsporingsdiensten kunnen worden geconfronteerd met aanvullende specifieke regels voor de verwerking van gegevens die van de andere lidstaten zijn verkregen. In theorie kunnen politie en justitie dan worden geconfronteerd met 27 verschillende regimes voor de verwerking van persoonsgegevens. Dat acht ik minder goed uitvoerbaar voor politie en justitie. Daar komt bij dat hiermee afbreuk wordt gedaan aan de harmonisatie van de regels, die met de ontwerprichtlijn juist wordt beoogd. Ik ben dan ook voornemens eerst nadere afstemming met politie en justitie te doen plaatsvinden, om te bezien in hoeverre de regeling van artikel 12 van het huidige kaderbesluit dataprotectie in de praktijk functioneert en of het met het oog op de bescherming van persoonsgegevens wenselijk is een dergelijke regeling in de ontwerprichtlijn te continueren.
– De ontwerprichtlijn maakt onderscheid tussen de verwerking van gegevens van verschillende betrokkenen. Zo worden er andere voorwaarden gesteld aan de opslag van gegevens als het gaat om een verdachte dan aan de opslag van gegevens van een slachtoffer. Deze voorwaarden zijn echter niet hard. Er is een mogelijkheid om hiervan af te wijken (art 5 lid 1, art. 6 lid 1 en 2). Kan de regering gevallen noemen waarin het noodzakelijk is af te wijken van de voorgestelde voorwaarden? Waarom is dat in genoemde voorbeelden noodzakelijk? Voor de restcategorie zijn de voorwaarden waaronder de gegevens van deze personen verwerkt mogen worden ruim geformuleerd. Het Cbp spreekt zich uit tegen deze ruime formulering en tegen de maximale bewaartermijnen voor deze categorie. Wat is de reden dat er voor deze restcategorie andere voorwaarden gelden en in hoeverre acht de regering deze voorwaarden en de lengte van de bewaartermijnen redelijk?
In antwoord op de gestelde vragen merk ik op dat de artikelen 5 en 6 van de ontwerprichtlijn verplichten tot het, voor zover mogelijk, maken van onderscheid tussen categorieën van personen en categorieën van persoonsgegevens. De toevoeging «voor zover mogelijk» biedt de lidstaten de ruimte om hiervan af te wijken. Op grond van de opzet en structuur van de informatiehuishouding bij politie en justitie kan dit noodzakelijk zijn, omdat het bepaald niet zeker is dat de informatiesystemen van politie en justitie technisch de mogelijkheid bieden om bij de vastlegging van gegevens onderscheid te maken naar categorieën van personen en categorieën van persoonsgegevens. Dit betekent in de eerste plaats dat alle informatiesystemen die bij politie en justitie in gebruik zijn nader moeten worden onderzocht op een dergelijke mogelijkheid, waarna het vraagstuk van de haalbaarheid van aanpassing van de systemen aan

de orde is. Het CBP heeft geconstateerd dat de verwerking van gegevens van personen die in geen van de in artikel 5 genoemde categorieën vallen, nogal ruim is geformuleerd en dringt erop aan dat aan de gegevensverwerking op dit punt nadere voorwaarden worden gesteld, met name op het gebied van maximale bewaartermijnen van gegevens in deze restcategorie. Het is dus niet zo dat in de ontwerprichtlijn voor deze restcategorie andere voorwaarden worden voorgesteld, dan wel een langere bewaartermijn, zoals de leden van de PvdA-fractie kennelijk veronderstellen. Hieronder zal ik, in antwoord op een vraag van de fractie van D66, nader ingaan op de wenselijkheid van het maken van onderscheid tussen de categorieën van personen en categorieën van persoonsgegevens, zoals door de Commissie voorgesteld.
– Uitwisseling van persoonsgegevens met derde landen of internationale organisatie is mogelijk zonder dat duidelijk is of de gegevens voldoende beschermd zijn. Lidstaten moeten zelf bepalen of het beschermingniveau voldoende is. De PvdA-fractie vindt deze regel weinig geruststellend. Hoe moeten lidstaten bereiken dat zij voldoende garantie krijgen dat persoonsgegevens volgens EU-normen worden verwerkt en behandeld? Is het niet in het belang van de burger dat deze open norm nader wordt ingevuld? Zo nee, waarom niet?
Het belangrijkste doel van de ontwerpverordening is te bereiken dat de verwerking van persoonsgegevens kan rekenen op een hoog beschermingsniveau in de EU. Wanneer dat hoge beschermingsniveau kan worden geboden, bestaat tegelijk de garantie dat persoonsgegevens binnen de EU, en overigens ook de EER, vrijelijk kunnen circuleren. De ontwerpverordening kan niet garanderen dat derde landen hetzelfde niveau van gegevensbescherming bieden. De EU heeft in derde landen geen rechtsmacht. Die beperking zal moeten worden aanvaard. Niettemin zijn er een aantal mechanismen om te bereiken dat persoonsgegevens die aan derde landen worden doorgegeven op een zekere mate van bescherming kunnen rekenen. In de eerste plaats kan de Europese Commissie vaststellen dat in een derde land een passend niveau van gegevensbescherming bestaat. Een dergelijke beslissing wordt pas gegeven na een grondig onderzoek van het recht van het desbetreffende land. In de tweede plaats kunnen gegevens worden doorgegeven in het kader van bindende bedrijfsvoorschriften. Deze voorschriften worden, na goedkeuring door een bevoegde toezichthouder in de EU, vastgesteld door een bedrijf dat deze voorschriften binnen het concern wereldwijd hanteert. In de derde plaats kan gegevensoverdracht plaatsvinden op grond van de goedgekeurde modelcontracten die bepaalde garanties kunnen bieden. Die goedkeuring wordt verleend door de Commissie of door een toezichthouder. Voor de gevallen waarin deze drie mogelijkheden geen oplossing kunnen bieden, moet de verantwoordelijke de nodige inspanningen verrichten om te beoordelen of de beoogde doorgifte plaatsvinden onder het bieden van toereikende garanties. De toezichthouder kan dan op grond van ontwerpverordening toestemming verlenen voor de doorgifte. Het is inderdaad ook in het belang van de betrokkene dat deze regeling in concreto wordt ingevuld, maar het is zeer twijfelachtig of dat altijd goed kan plaatsvinden door het vaststellen van regelgeving. De ervaringen onder ontwerprichtlijn 95/46/EG leren dat van geval tot geval moet worden bezien hoe de garanties voor de bescherming van de persoonlijke levenssfeer het best kunnen worden verleend.

Voor wat betreft de ontwerprichtlijn merk ik nog op dat de vaststelling van de toereikende waarborgen op grond van artikel 35 van de ontwerprichtlijn bij de regering nog vragen oproept met betrekking tot de uitvoerbaarheid en de mogelijke werklast voor politie en justitie. Op dit punt is er sprake van een buitengewoon lastige afweging. De door de Commissie voorgestelde hoofdregel, namelijk dat de gegevensuit-

wisseling met derde landen beperkt is tot die landen die een passend niveau van gegevensbescherming waarborgen, zal voor de burger de meeste zekerheid kunnen bieden dat de gegevensverwerking plaatsvindt in overeenstemming met de EU-normen. Daar staat echter tegenover dat de criminaliteit is geglobaliseerd en dat de Nederlandse samenleving wordt geconfronteerd met vormen van criminaliteit (zoals drugs- of mensenhandel) die ernstige gevolgen hebben voor de veiligheid en het welbevinden van de burgers en die hun oorsprong vinden in landen die niet altijd over een niveau van gegevensbescherming beschikken dat volledig vergelijkbaar is met dat van de Europese Unie. Als in een concreet opsporingsonderzoek blijkt dat de hoofddaders hun verblijf hebben in een ander land, of aldaar activiteiten ontplooien die aan de Nederlandse samenleving raken, dan kan het noodzakelijk zijn om samen te werken met de opsporingsautoriteiten in het betreffende land. De uitwisseling van gegevens vormt een logisch onderdeel van een dergelijke samenwerking. Het is dan weinig realistisch om te het oordeel van de Commissie over het niveau van gegevensbescherming in het betreffende land af te wachten, als het opsporingsonderzoek tot doortastend optreden noopt. Het is evenzeer weinig realistisch om de samenwerking met de betreffende autoriteiten te verbreken omdat de Commissie van oordeel is dat het betreffende land geen passend niveau van gegevensbescherming kan garanderen. In een dergelijk geval zal er ruimte moeten zijn voor flexibiliteit, door de beperking van de aard en de omvang van de gegevensverstrekking of door het maken van aanvullende afspraken over het gebruik van de te verstrekken gegevens. Naar het oordeel van de regering heeft de Commissie een lovenswaardige poging gedaan om een goed evenwicht te vinden tussen het belang van een zo hoog mogelijk niveau van bescherming voor persoonsgegevens die aan derde landen worden verstrekt en het belang van de criminaliteitsbestrijding om door middel van samenwerking tussen de betrokken opsporingsdiensten het hoofd te kunnen bieden aan ernstige vormen van grensoverschrijdende criminaliteit. Of het door de Commissie voorgestelde systeem voor de praktijk werkbaar is zal, in nauwe afstemming met politie en justitie, nader moeten worden bekeken. Hierover zal ook de discussie in de Raad afgewacht moeten worden, zodat kennis genomen kan worden van de inzichten van de andere lidstaten hieromtrent.

– Op grond van art. 13 zijn ruime uitzonderingsgronden geformuleerd op het recht van de betrokkene om toegang te krijgen tot zijn gegevens. Waarom is dat en is dat niet strijdig met het Verdrag van Lissabon?

In antwoord op de gestelde vragen merk ik op dat de uitzonderingsgronden van artikel 13 van de ontwerprichtlijn overeenkomen met die van het huidige kaderbesluit dataprotectie. Met de wet van 6 oktober 2011 (Stb. 490), die op 1 april 2012 in werking is getreden (Stb. 2012, 129), zijn de regels van dit kaderbesluit in de Nederlandse wetgeving geïmplementeerd. Overigens wijken de weigeringsgronden van dit kaderbesluit inhoudelijk nauwelijks af van die welke voorheen op grond van de nationale wetgeving (de Wet politiegegevens en de Wet justitiële en strafvorderlijke gegevens) van toepassing waren. De weigeringsgronden zijn ruim geformuleerd omdat deze zowel betrekking hebben op de opsporing als op de vervolging. Het Verdrag van Lissabon staat niet in de weg aan dergelijke weigeringsgronden. In dit verdrag is vastgelegd dat eenieder recht heeft op bescherming van zijn persoonsgegevens (artikel 16, eerste lid, VWEU), daarbij zijn echter geen nadere waarborgen gegeven omtrent de reikwijdte van dit recht. In het Handvest voor de Grondrechten van de Europese Unie is het recht op bescherming van persoonsgegevens vastgelegd. Eenieder heeft recht van inzage in de over hem verzamelde gegevens en op rectificatie daarvan (artikel 16, eerste lid). Beperkingen op de uitoefening van de in het Handvest erkende rechten en vrijheden zijn echter mogelijk; deze moeten bij wet worden gesteld en de wezenlijke inhoud van die rechten en vrijheden eerbiedigen

(artikel 52, eerste lid, Handvest van de Grondrechten). Met inachtneming van het evenredigheidsbeginsel kunnen slechts beperkingen worden gesteld indien zij noodzakelijk zijn en daadwerkelijk beantwoorden aan de door de Unie erkende doelstellingen van algemeen belang of aan de eisen van de bescherming van rechten en vrijheden van anderen. Dit alles overziend, lijken de regels van het Handvest evenmin in de weg te staan aan de weigeringsgronden van artikel 13 van de ontwerprichtlijn.
– Persoonsgegevens kunnen zonder passend beschermingsniveau en passende waarborgen doorgegeven worden aan derde landen. Als is voldaan aan de noodzakelijkheidsvereiste mogen persoonsgegevens worden gewisseld met derde landen. De PvdA-fractie is van mening dat persoonsgegevens slechts doorgegeven mogen worden als er duidelijke waarborgen voor de verwerking van die persoonsgegevens vaststaan. Hoe gaat de regering om met verzoeken van derde landen om persoonsgegevens en hoe kan betrokkene de garantie krijgen dat zijn gegevens voldoende beschermt zijn?
Hierboven ben ik, in antwoord op een vraag van de PvdA-fractie over dit onderwerp, reeds nader ingegaan op de voor de Commissie voorgestelde regeling voor de verstrekking van persoonsgegevens aan derde landen en de afwegingen die daarbij aan de orde zijn. De regering is van oordeel dat het uitwisselen van persoonsgegevens met derde landen alleen geoorloofd is als er daadwerkelijk, zowel in wet- en regelgeving als in de praktijk, toereikende gegevensbescherming bestaat in het betreffende land. De Nederlandse opsporingsinstanties werken reeds langere tijd samen met buitenlandse opsporingsdiensten. Met sommige landen worden daarvoor speciale samenwerkingsovereenkomsten gesloten, waarin voor de gegevensbescherming naar het nationale recht wordt verwezen. Daarbij kan ook worden voortgebouwd op de ervaringen met de toepassing van rechtshulp- of uitleveringsovereenkomsten met de betreffende landen. Bij de beoordeling van het beschermingsniveau, en daaruit voortvloeiend, de eventuele noodzaak om aanvullende afspraken te maken, zullen uiteraard ook de eerdere ervaringen rond de samenwerking met deze landen betrokken kunnen worden. En zoals ook hierboven in antwoord op een andere vraag van de PvdA-fractie reeds is aangegeven, kunnen verschillende maatregelen worden getroffen om te komen tot een passende uitwisseling, zoals het maken van aanvullende afspraken, de aanpassing van de gegevensverstrekking naar aard en omvang, het maken van een onderscheid tussen de gegevens van Nederlanders of van ingezetenen van het betreffende land of het betrekken van het landelijk parket van het openbaar ministerie ten behoeve van een extra toetsing van de voorgenomen gegevensverstrekking.

Toezichthouder

– Goede wetgeving is zo sterk als de mate van handhaafbaarheid van deze regels. Nationale toezichthouders hebben de taak om klachten van schendingen van de privacywetgeving op te nemen en af te handelen. Hiervoor moeten de nationale autoriteiten de mogelijkheid hebben om «afschrikkende sancties» op te leggen. Een afschrikkende sanctie is de boetebevoegdheid van de toezichthoudende autoriteit. Bij monde van staatssecretaris Teeven heeft de regering toegezegd de Kamer te informeren of de boetebevoegdheid voor het College bescherming persoonsgegevens nog voor de implementatie van de EU-ontwerpverordening kan worden toegekend. Vanwege die toezegging heeft de PvdA haar motie (Kamerstuk 32 761-22) om de boetebevoegdheid geregeld te krijgen aangehouden. Kan de regering toezeggen dat de boetebevoegdheid voor het CPB op korte termijn, maar in ieder geval voor 2013 geregeld is? Zo nee, waarom niet en wanneer kan het CPB wel boetes gaan opleggen?

In antwoord op vragen van de leden Recourt en Heijnen (2012Z04593) over de zorgen die het Cbp heeft uitgesproken dat het College niet in staat is om alle klachten af te handelen wegens tekort aan mankracht, dat het CPB in staat is om eigen afwegingen te maken en prioriteiten te stellen. Uit dit antwoord blijkt dat de regering van mening is dat het Cbp niet alle klachten moet afhandelen. «De handhaving van regels moet altijd gebeuren binnen de kaders van de beschikbare middelen», zo is het antwoord van de staatssecretaris. In hoeverre is de handhavingcapaciteit van het College voldoende om nog effectief te kunnen handhaven?
Ik ben van oordeel dat de wetgever zorg dient te dragen voor een zodanige financiering en bestaffing van het Cbp dat dit orgaan in staat is zijn taak op redelijke wijze te kunnen uitoefenen. Ik meen dat dit in de afgelopen jaren steeds het geval is geweest. Het zal altijd zo zijn dat het aantal handhavingsvraagstukken varieert qua aantal en aard, en het zal ook altijd zo zijn dat handhavingsinstanties, het Cbp niet uitgezonderd, op een verstandige manier hun capaciteit inzetten en daarom moeten prioriteren.
– De regering heeft nooit een mededeling dan wel een signaal van de zijde van het Cbp ontvangen dat meer dan de helft van de zaken blijven liggen. Heeft u wel signalen van het Cbp ontvangen dat, in het algemeen gesproken, het Cbp een tekort aan capaciteit heeft om zijn taken goed uit te oefenen? Zo ja, welk signaal of mededeling heeft de regering ontvangen en hoe is de regering omgegaan met dit signaal of mededeling?
Het Cbp vraagt al geruime tijd aandacht voor een vermeend tekort aan middelen, mensen en bevoegdheden. Dergelijke signalen worden uiteraard serieus genomen, maar dat wil niet zeggen dat daar vanzelfsprekend onmiddellijk gehoor aan wordt gegeven. Hoe begrijpelijk de wens tot uitbreiding van middelen soms ook is, deze wensen moeten worden beoordeeld tegen de achtergrond van de budgettaire situatie, tegen de eigen mogelijkheden die het bestuursorgaan zelf heeft zijn eigen situatie te beïnvloeden en tegen de achtergrond van de eisen die de Europese en Nederlandse wetgeving stelt in vorm van het handhaven van een redelijk handhavingsniveau.
– Hoeveel procent van de klachten die bij het Cbp binnenkomen worden er wel afgehandeld? Hoeveel zaken blijven op de plank liggen? Als het Cbp niet in staat is om alle zaken af te handelen hoe moet het CPB effectief handhaven. Wanneer kan gesproken worden van effectieve handhaving? Hoeveel procent van de zaken moet dan tenminste zijn behandeld?
Het laatst beschikbare jaarverslag van het Cbp is het verslag over 2011. Dat verslag meldt dat er 129 klachten zijn binnengekomen en 85 onderzoeken zijn gehouden. Die aantallen zeggen naar mijn mening als zodanig niet veel. Niet elke ontvangen klacht is goed in behandeling te nemen door formele omstandigheden. Niet elke ontvangen klacht is zwaar genoeg om onderwerp van een langdurig onderzoek te kunnen zijn. Het Cbp moet ook inhoudelijk een zekere schifting aanbrengen in de klachten en zijn beschikbare capaciteit daar zo goed mogelijk op afstemmen. Ik heb er vertrouwen dat het Cbp dit naar behoren doet.
– In principe is de toezichthouder van de lidstaat waar het hoofdkantoor van een onderneming zich bevindt, bevoegd om als toezichthouder op te treden. Hoe moet worden omgegaan met deze regel als niet duidelijk is waar de hoofdvestiging is gevestigd. Zou er meer duidelijk komen als er criteria worden ontwikkeld welke toezichthouder verantwoordelijk is in die gevallen dat een hoofdvestiging niet is vast te stellen? Zo nee, waarom niet? Zou hiervoor niet een belangrijke taak voor de weggelegd moet worden? Welke toezichthouder is verantwoordelijk voor de toezicht als het hoofdkantoor niet in een EU-lidstaat ligt, maar de organisatie wel zeer actief is in Europese landen? Wie bepaalt in zo'n geval welke autoriteit als toezichthouder moet optreden? De leden zijn van mening dat in geval het onduidelijk is welke toezichthouder bevoegd is de European Data

Protection Board een rol toebedeeld moet krijgen en een toezichthouder moet kunnen aanwijzen. Deelt de regering deze mening? Zo nee, waarom niet?
Ik ben het met deze leden eens dat het in concreto inderdaad wel eens lastig kan zijn om vast te stellen waar de hoofdvestiging van een onderneming is gevestigd. Er zijn voor dit soort gevallen onder het huidige recht door de artikel 29 Werkgroep al de nodige vuistregels geformuleerd. Ik vraag mij af of het zinvol is voor dit soort gevallen nadere regels op te stellen. Dat zal niet eenvoudig zijn, omdat de feiten in afzonderlijke zaken zeer van elkaar kunnen verschillen. Ik geef daarom de voorkeur aan meer praktische oplossingen, zoals een consultatie van de European Data Protection Board, al dan niet gecombineerd met de aanwijzing van een coördinerend toezichthouder, zoals ook het Cbp bepleit.
De ontwerpverordening geeft geen uitdrukkelijke regeling voor de vaststelling van de bevoegdheid van de toezichthouder wanneer de hoofdvestiging buiten de EU is gelegen. Ik zal deze kwestie zeker aan de orde stellen bij de bespreking van de ontwerprichtlijn.

PVV

– In algemene zin: De Partij voor de Vrijheid is tegen Europese wetgeving. In Nederland kunnen wij namelijk prima onze eigen wetten maken. Wanneer wij willen samenwerken met andere landen – ook daar is de PVV groot voorstander van – dan kan dat op basis van aparte verdragen met die andere landen. We spreken dan van bilaterale of multilaterale verdragen.

– Verder wil de PVV graag weten welke beleidsvrije ruimte er overblijft indien de EU-wetgeving, zoals die nu in voorligt, aangenomen wordt.

De keuze van de Commissie om met een voorstel voor een ontwerpverordening te komen heeft tot gevolg dat het gegevensbeschermingsrecht in verdere mate geharmoniseerd wordt dan nu het geval is. Daaruit vloeit voort dat in er in algemene zin in elk geval geen sprake is van een uitbreiding van de mogelijkheden om op nationaal niveau regels vast te stellen. Toch is het niet zo dat die mogelijkheden in het voorstel volledig ontbreken. De lidstaten behouden vrijheid om op het terrein van het arbeidsrecht aanvullende wetgeving vast te stellen. Op het terrein van het gezondheidsrecht is er een verplichting tot het stellen van aanvullende regels. Dit is belangrijk, omdat er tussen de lidstaten grote verschillen bestaan op deze gebieden.

Voor de regelgeving die geen betrekking heeft op specifiek benoemde terreinen is er sprake van een geschakeerd beeld. Op veel gebieden is rechtvaardiging voor de verwerking van persoonsgegevens afhankelijk van hetzij nadere regelgeving van de EU, hetzij nadere regelgeving van de lidstaten. In veel gevallen zal dit neerkomen op de noodzaak regels vast te stellen op nationaal niveau. Het is ook nog onvoldoende duidelijk hoe de verhouding is van de ontwerpverordening tot bestaande regels van nationaal recht. De Europees Toezichthouder voor de Gegevensbescherming heeft terecht de aandacht gevraagd voor deze vragen.

Voor wat betreft de ontwerprichtlijn merk ik nog op dat deze een afzonderlijke paragraaf bevat over de doorgifte van persoonsgegevens naar derde landen of internationale organisaties (hoofdstuk V). Deze regels zijn hierboven toegelicht, naar aanleiding van een vraag van de fractie van de PvdA. De regels zijn van toepassing op de verstrekking van persoonsgegevens aan een derde land, ook in het geval dat Nederland een bilateraal of multilateraal verdrag met het betreffende land sluit. Dit

betekent dat in het betreffende derde land sprake dient te zijn van een passend beschermingsniveau, als bedoeld in artikel 34, eerste lid, van de ontwerprichtlijn, behoudens de mogelijkheid van passende garanties, bedoeld in artikel 35, eerste lid,van de ontwerprichtlijn, of de afwijkingen die in artikel 36 van de ontwerprichtlijn zijn beschreven.
Aanvullend kan worden opgemerkt dat de ontwerprichtlijn ervan uitgaat dat de internationale overeenkomsten die door de lidstaten voorafgaand aan de inwerkingtreding van de ontwerprichtlijn zijn gesloten, indien nodig binnen vijf jaar na de inwerkingtreding van de ontwerprichtlijn worden gewijzigd (artikel 60). De Nederlandse regering is minder gelukkig met deze bepaling, omdat dit ertoe kan leiden dat over een onbekend aantal verdragen met derde landen, bijvoorbeeld op het gebied van rechtshulp of uitlevering, moet worden heronderhandeld. De regering geeft de voorkeur aan de handhaving van de regeling van het huidige kaderbesluit dataprotectie. Op basis van die regeling blijven bestaande verplichtingen of verbintenissen op grond van bilaterale of multilaterale overeenkomsten onverminderd van kracht (artikel 26).

– Onder dankzegging aan de Commissie Meijers verzoekt de PVV verder om de onderstaande vragen van de Commissie Meijers (zoals gesteld in de brief van 2 maart 2012 met kenmerk CM1206) zorgvuldig te beantwoorden:

– Waarom is uit oogpunt van een uniform en zo hoog mogelijk niveau van gegevensbescherming niet gekozen voor één instrument, waarbij in een aparte paragraaf heldere en uniforme regels zijn uitgewerkt ten aanzien van gegevensverwerking in de politiële en justitiële sector?
– Deelt de regering de mening van zowel het College Bescherming Persoonsgegevens (CBP), de Artikel 29 Werkgroep voor Gegevensbescherming en de Europese Toezichthouder voor Gegevensbescherming (EDPS), dat het huidige ontwerprichtlijnvoorstel een te laag niveau van gegevensbescherming biedt?
– Deelt de regering het oordeel van de EDPS dat de voorgestelde ontwerprichtlijn, politie autoriteiten in de EU nog teveel ruimte biedt voor toegang tot de gegevensverwerking in de private sector?
– Wil de regering zich inzetten voor een minimalisering van uitzonderingsbepalingen in de voorgestelde ontwerprichtlijn, om te voorkomen dat de (implementatie van) de ontwerprichtlijn door het Hof van Justitie van de EU onverenigbaar zal worden verklaard met de fundamentele rechten zoals neergelegd in het EU Handvest?
– Vindt de regering dat de voorgestelde regeling inzake de gegevensuitwisseling aan derde staten voldoende waarborgen biedt ter bescherming van de rechten en vrijheden van de zich in de Europese Unie bevindende personen?

Ten aanzien van profilering:

– Deelt de regering de mening van de Commissie Meijers dat de voorgestelde regeling inzake het gebruik van profilering in Artikel 20 en 21 van de concepterordening en in Artikel 9 van de conceptrichtlijn, door de vele uitzonderingsbepalingen en de resterende discretionaire bevoegdheid voor uitvoerende instanties, nog onvoldoende waarborgen biedt ter bescherming van de bovengenoemde rechten en vrijheden van individuen en met name het non-discriminatiebeginsel?

Ten aanzien van de toezichthoudende autoriteiten:

– Op welke wijze wil de regering zich inzetten voor proportionele uitbreiding van de financiële en personele middelen van zowel nationale als Europese toezichthoudende instanties?

– Wil de regering zich inzetten voor de toevoeging van bepalingen aan de huidige voorstellen waarbij de genoemde instanties de bevoegdheid krijgen bindende sancties op te leggen, zoals effectieve en afschrikkende boetes?

In antwoord op de vraag van de PVV-fractie kan ik meedelen dat ik graag voldoe aan het verzoek van deze fractie om de vragen van de Commissie Meijers zorgvuldig te beantwoorden. Bij brief van de Minister van Veiligheid en Justitie aan de Voorzitter van de Tweede Kamer der Staten-Generaal van 27 april 2012, Kamerstukken II 2011/12, 32 761, nr. 29, is een uitgebreide schriftelijke reactie gegeven op de schriftelijke vragen van de Commissie-Meijers van 2 maart 2012, nr. CM1206. Ik verwijs de leden van de PVV-fractie graag naar deze brief.

Overige vragen:

– Bent u van mening dat de verhouding tussen de e-Privacy Ontwerprichtlijn en de ontwerpverordening moet worden verduidelijkt?

Artikel 89 van de ontwerpverordening bevat enkele bepalingen met betrekking tot de verhouding van ontwerprichtlijn 2002/58/EG tot de ontwerpverordening. De bedoeling daarvan is dat de ontwerpverordening de rechten en verplichtingen bevat voor het gehele gegevensbeschermingsrecht, voor zover daarin niet specifiek wordt voorzien in ontwerprichtlijn 2002/58/EG. Als beginsel is dit op zichzelf genomen een voldoende duidelijk uitgangspunt. Toch kan niet op voorhand worden uitgesloten dat hier interpretatievragen rijzen. Aangezien ontwerprichtlijn 2002/58/EG is geïmplementeerd in de nationale wetgeving, zullen de lidstaten bij inwerkingtreding van de ontwerpverordening zorgvuldig moeten nagaan of die nationale wetgeving ook voldoende is toegesneden op de ontwerpverordening.

– Bent u van mening dat op basis van art. 50 lid 2 conceptontwerprichtlijn een achteruitgang in collectieve rechtsbescherming wordt bewerkstelligd in Nederland (wellicht ook in andere EU-lidstaten)? Vindt u dit tevens een belangrijk aandachtspunt dat een zorgvuldige behandeling behoeft en waarover de Kamer goed geïnformeerd dient te worden, zeker in het licht van het (AO) behandelvoorbehoud en de moties die in het daaropvolgende VAO zijn ingebracht?

Ik ben van mening dat niet op voorhand gezegd kan worden dat artikel 50, tweede lid, van de ontwerprichtlijn en 73, tweede lid, van de ontwerpverordening een achteruitgang voor Nederland betekent van het recht om collectiefbelangacties in te stellen. Ik wijs erop dat een specifiek voor het gegevensbeschermingsrecht bedoelde collectiefbelangactie momenteel ontbreekt. Wat artikel 50, derde lid, van de ontwerprichtlijn en artikel 73, derde lid, van de ontwerpverordening betreft, kan zelfs wel worden volgehouden dat er sprake is van een uitbreiding. Artikel 3:305a, vierde en vijfde lid, van het Burgerlijk Wetboek bieden de mogelijkheid dat een individuele belanghebbende zich verzet tegen een collectiefbelangactie die mede betrekking heeft op zijn belang, terwijl het recht een collectiefbelangactie in te stellen in geval van een datalek op grond van artikel 73, derde lid, van de ontwerpverordening ook onafhankelijk van een individuele klacht kan worden uitgeoefend. In het algemeen overleg van 7 maart 2012 heb ik toegezegd de Kamer specifiek over de ontwikkelingen rond het collectief actierecht te informeren.

– Waarom is er gekozen de ontwerpverordening niet risicogericht te laten zijn en waarom richt de ontwerpverordening zich nu op bedrijfsgrootte?

Het is mij niet bekend waarom de Commissie deze keuze heeft gemaakt.

– Waarom zijn er geen uitzonderingen voor verwerking gemaakt die bijvoorbeeld wel in de Nederlandse wet (in het Nederlandse Vrijstellingsbesluit) zijn opgenomen?

Het Vrijstellingsbesluit Wbp bevat de voorwaarden waaronder aan verantwoordelijken in de zin van de Wbp vrijstelling wordt verleend van de verplichting om een verwerking van persoonsgegevens te melden bij het Cbp of de functionaris voor de gegevensbescherming. Die meldplicht is niet in de ontwerpverordening opgenomen en verdwijnt dus. Er is dan ook geen reden meer voor vrijstelling van die verplichting. Niettemin is het voorstelbaar dat de ontwerpverordening een voorziening bevat die vrijstelling verleent van andere verplichtingen, en die zou zijn opgezet volgens de principes van de Vrijstellingsbesluit Wbp.

– Is de Ontwerpverordening wel specifiek genoeg daar waar het verschillende typen data betreft? Wordt er een onderscheid tussen on- en offline gebruik gemaakt? Wordt er gekeken naar de aard van de gegevens en de gevolgen die de Ontwerpverordening heeft voor verschillende typen bedrijvigheid?

Het is zeker voorstelbaar dat in de ontwerpverordening ten aanzien van de omvang van de rechten en verplichtingen van verantwoordelijken en ten aanzien van de rechtvaardigingsgronden voor het verwerken van bijzondere persoonsgegevens meer wordt gedifferentieerd naar de aard van de gegevens, het type van bedrijvigheid en de vraag of gegevens meer online of offline worden gebruikt.

– Hoe wordt er geanticipeerd op voorzienbare jurisdictieconflicten? Hoe wordt voorkomen dat het voor ondernemers onmogelijk wordt om in verschillende landen te ondernemen zonder de wet te overtreden?

Hoofdstuk V van de ontwerpverordening bevat een groot aantal bepalingen die het grensoverschrijdend verkeer van persoonsgegevens regelen. Met deze bepalingen bevat de ontwerpverordening een beter uitgewerkte verzameling grondslagen voor deze typen verwerkingen. De regering is van mening dat er op dit onderdeel van het gegevensbeschermingsrecht sprake is van een verbetering ten opzichte van richtlijn 95/46/EG. Waar het gaat om verplichtingen krachtens buitenlands recht aan in de Europese Unie gevestigde verantwoordelijken om buiten toestemming van de betrokkene gegevens te verstrekken aan de overheid van een derde land, beoogt de ontwerpverordening blijkens overweging 90 een oplossing te bieden. Hoe die oplossing precies luidt blijkt nog onvoldoende duidelijk uit de artikelen 42 en 44 van de ontwerpverordening.

– Waarom wordt er niet verder gedifferentieerd waar het datalekken betreft? Dienen alle typen datalekken gemeld te worden? Zo ja op welke termijn en zijn periodieke rapportages hierbij ook mogelijk? Hoe wordt dit verder uitgewerkt?

Volgens artikel 31 van de ontwerpverordening dienen alle datalekken zonder uitzondering te worden gemeld bij de toezichthoudende autoriteiten. In beginsel moet dat binnen 24 uur gebeuren. Volgens artikel 32 van de ontwerpverordening dienen alle datalekken die waarschijnlijk een nadelig effect hebben op de persoonsgegevens of de persoonlijke levenssfeer van de betrokkene ook aan de betrokkene te worden gemeld. In beginsel moet dit onverwijld gebeuren. Over de invulling van het criterium nadelig effect bevat overweging 67 enige voorbeelden. Beide

bepalingen voorzien in de mogelijkheid van de vaststelling van gedelegeerde handelingen door de Commissie. Met die gedelegeerde handelingen kan een nadere invulling worden gegeven aan beide bepalingen. De Commissie heeft daarvoor nog geen voorstellen aangekondigd.

– Waarom wordt in het voorstel niet ingegaan op nalevingskosten (in aanvulling op de administratieve lasten)?

De Commissie heeft zich wat betreft de administratieve lasten en nalevingskosten beperkt tot een berekening van de voordelen die de ontwerpverordening oplevert in termen van verhoging van het harmonisatieniveau en het afschaffen van verplichtingen zoals de meldplicht. De Commissie heeft enige cijfers bijgevoegd over de effecten van de verplichtingen en de daarmee gemoeide nalevingskosten die de ontwerpverordening oplevert voor het bedrijfsleven. Het is de vraag of die cijfers volledig zijn. Ik verwijs de leden van de PVV-fractie graag naar mijn antwoord op de eerste vraag van de leden van de VVD-fractie.

– Hoe kijkt de Nederlandse overheid tegen de introductie van eventuele nieuwe wetgeving vanuit Europa aan? In welke mate voelt zij zich verantwoordelijk om burgers en bedrijfsleven te informeren, voor te lichten en te ondersteunen waar het (het voldoen aan) deze eventuele nieuwe wetgeving betreft?

Te zijner tijd zal samen met het Cbp worden bezien of de komende inwerkingtreding van de nieuwe regels specifieke publieksvoorlichting vereist.

– Hoe wordt omgegaan met gegevens die via internet worden verstrekt waarbij niet goed vast te stellen is of de gegevens van een minderjarige afkomstig zijn? Hoe wordt er voorkomen dat bedrijven en organisaties deze gegevens pas mogen verwerken (bijvoorbeeld voor het beantwoorden van een vraag) wanneer zij aanvullende informatie verkrijgen (die de privacy nader zouden kunnen schenden) zoals bijvoorbeeld creditcardgegevens (om de meerderjarigheid vast te stellen)?

De voorstellen van de Commissie voor de bescherming van de belangen van jeugdigen geven aanleiding tot het stellen van vragen. Het succes van die voorstellen is in belangrijke mate afhankelijk van de ontwikkeling van betrouwbare en gebruiksvriendelijke methoden om online identiteit en leeftijd van een persoon te kunnen vaststellen, zonder dat dit leidt tot de proliferatie van meer persoonsgegevens dan wenselijk is. Die methoden zijn nu nog onvoldoende voorhanden, zodat nog onzekerheid bestaat over de uitvoerbaarheid van de voorstellen.

– Welke moeilijkheden ontstaan er met het oog op fraudepreventie met de nu voorliggende EU-wetgeving? Blijven er mogelijkheden voor fraudepreventie bestaan en/of vergt dit ondersteuning, ontheffing of specifieke goedkeuring vanuit de overheid? Is hier überhaupt in voorzien?

Voor zover de leden van de PVV-fractie bedoelen te vragen of de ontwerpverordening de vaststelling van regels die de onderlinge verstrekking van persoonsgegevens in het belang van de fraudebestrijding tussen uitvoeringsinstanties in de sociale zekerheid, bestuursorganen en toezichthouders bemoeilijkt, lijkt dit niet het geval te zijn. Wel zijn er nog vragen bij de rechtvaardigingsgronden voor de verwerking van bijzondere persoonsgegevens – in het bijzonder gegevens betreffende de gezondheid en strafrechtelijke gegevens – door verzekeringsmaatschappijen en andere private partijen. De verwerking van laatstbedoelde categorieën van gegevens is belangrijk uit oogpunt van fraudebestrijding.

– Hoe wordt omgegaan met «het recht om vergeten te worden» wanneer de gegevens die iemand vrijwillig bij een aanbieder op internet heeft geplaatst openbaar zijn? Kan deze aanbieder dan verantwoordelijk worden gehouden voor de verspreiding van derden? Waarom is dit niet verder uitgewerkt en waarom is niet aangegeven wie hiervoor de verantwoordelijkheid heeft?

Er moet van worden uitgegaan dat – al dan niet via een intermediair – vrijwillig op internet geplaatste gegevens ook voor anderen toegankelijk zijn wanneer de desbetreffende site of het platform geen toegangsrestricties heeft. De betrokkene, en niet de verantwoordelijke, is primair verantwoordelijk voor de verstrekking van zijn gegevens. Het is ook de betrokkene die zichzelf primair moet vergewissen van hetgeen met de gegevens gebeurt nadat hij ze heeft verstrekt. Wanneer hij het recht om te worden vergeten gaat uitoefenen zal dat tot gevolg hebben dat de verantwoordelijke – in dit geval degene die er een website of platform op nahoudt – primair zorg moet dragen voor het wissen van de gegevens en op wie een inspanningsverplichting rust ervoor te zorgen dat de gegevens die na verstrekking door de betrokkene zijn doorverstrekt aan derden ook bij die derden worden gewist. Er is op zichzelf genomen geen onduidelijkheid over de vraag op wie een verplichting rust, maar meer over de vraag of die verplichting wel in alle opzichten uitvoerbaar is.

– Hoe worden niet in de Unie gevestigde bedrijven gestimuleerd toch met een representant te gaan werken? Kan dit worden afgedwongen, zo nee, waarom niet? Zo ja, op welke wijze?

Stimulering van de aanstelling van een vertegenwoordiger in de EU door een niet in de EU gevestigde verantwoordelijke voor de verwerking van persoonsgegevens is in de eerste plaats mogelijk door in de EU een aantrekkelijk gegevensbeschermingsrecht aan te bieden dat niet alleen voor de betrokkene, maar ook voor de verantwoordelijke duidelijke voordelen biedt. Ook verantwoordelijken hebben belang bij een goed gegevensbeschermingsrecht. Het niet aanstellen van een vertegenwoordiger in de gevallen waarin dit wel verplicht is, is – net als nu het geval is – met een bestuurlijke boete bedreigd. De uitvoerbaarheid van deze maatregel is afhankelijk van de begrensde mogelijkheden een dergelijke maatregel buiten het grondgebied van de EU ten uitvoer te leggen.

CDA

De leden van de CDA-fractie hebben tijdens het algemeen overleg d.d. 7 maart jl. reeds diverse punten aan de orde gesteld. Daarnaast hebben zij vragen kunnen stellen tijdens de technische briefings, waarvoor zij de diverse betrokkenen langs deze weg graag dank zeggen. Veel concrete vragen hebben genoemde leden niet, daar zij zich goed realiseren dat een en ander nog zeer in ontwikkeling is en veel nog dient te worden uitgewerkt. Een paar punten stellen de leden van de CDA-fractie in deze schriftelijke inbreng wel graag nog aan de orde.

– De leden van de CDA-fractie hebben bij diverse gelegenheden naar voren gebracht bijzonder veel waarde te hechten aan het actief en voorafgaand moeten geven van toestemming om gegevens te mogen gebruiken (vide discussie «opt-in» in plaats van «opt-out» en de motie-Van Toorenburg c.s., Kamerstukken II 2011/2012, 32 761, nr. 12). Genoemde leden begrijpen dat de voorliggende regelgeving hier ook meer op is gebaseerd, sterker nog, uitgangspunt is uitdrukkelijke toestemming. (Putting individuals in control of their personal data/Right tot be forgotten en Data breach notification). Genoemde leden zijn

hiermee zeer ingenomen en wat hen betreft houdt de Staatssecretaris daar ook stevig aan vast.

Het is inderdaad zo dat de ontwerpverordening de toestemming van de betrokkene als rechtvaardigingsgrond voor de verwerking van persoonsgegevens heeft versterkt. Ik kan mij hierin vinden en zal daar stevig aan vasthouden.

– De indruk wordt gewekt dat er sprake is van lastenverlichting. Deze is gelegen in het feit dat de algemene meldplicht is vervallen. Daarnaast zal sprake zijn van één loketfunctie voor bedrijven. Dat zal beslist de duidelijkheid kunnen dienen, althans indien onomstotelijk vast staat waar een hoofdvestiging gelegen is. Is inmiddels al duidelijk op basis van welke criteria dat wordt vastgesteld? De leden van de CDA-fractie begrijpen dat veel bedrijven die op dit punt kwetsbaar zijn Ierland als hoofdvestiging kiezen, omdat daar de regels zo soepel zijn. De voorzitter van het College bescherming persoonsgegevens (Cbp) pleit ervoor bij onduidelijkheid uitsluitstel te vragen bij het European Data Protection Point. Wat het CDA betreft een verstandig voorstel. Hoe denkt de Staatssecretaris daarover?

De vaststelling van de criteria met behulp waarvan wordt bepaald waar een vestiging van een verantwoordelijke is gelegen, is onderwerp geweest van een intensieve bespreking in de betrokken raadswerkgroep. De Commissie heeft na deze besprekingen laten weten nader over de implicaties van dit onderdeel van het voorstel te willen nadenken. De vaststelling van een ontwerpverordening voor het algemene gegevensbeschermingsrecht heeft mede tot doel te voorkomen dat bedrijven in verschillende lidstaten van de EU verschillend worden behandeld. Ik meen met de leden van de CDA-fractie dat het voorstel van het Cbp om de European Data Protection Board een zekere rol toe kennen bij onduidelijkheid over de bevoegdheid van een van de Europese toezichthouders constructief is.

– Hoewel van lastenverlichting sprake zal zijn, wordt hiermee vooral gedoeld op de lasten die bedrijven ondervinden van de administratieplicht jegens de overheid. Over de uitvoeringskosten rijzen evenwel grote zorgen. Kan de Staatssecretaris hierover al iets meer zeggen? Hoe omvangrijk zullen deze naar verwachting zijn?

Het lijkt inderdaad plausibel dat de nalevingskosten die voortvloeien uit de ontwerpverordening hoger zullen zijn dan de nalevingskosten die uit richtlijn 95/46/EG voortvloeien. De Commissie heeft dit maar gedeeltelijk willen narekenen. Ik verwijs deze leden graag naar het antwoord op de eerste vraag van de leden van de VVD-fractie. Ik kan dus niet precies aangeven wat de omvang van die kosten is.

– De Kamer van Koophandel Nederland luidt de noodklok over artikel 17 (het recht om gegevens te kunnen laten wissen bij derden). Zij acht dat praktisch niet uitvoerbaar. Deelt de Staatssecretaris die zorg, zo vragen de leden van de CDA-fractie.

Ik ben niet van oordeel dat artikel 17 volledig onuitvoerbaar zou zijn. Het is veeleer de vraag of het recht om te worden vergeten *in alle opzichten* volledig uitvoerbaar is. Ook de inspanningsverplichting van een verantwoordelijke om bij derden te bewerkstelligen dat de van hem afkomstige en door derden verwerkte gegevens zullen worden gewist, zal vermoedelijk niet volledig kunnen voorkomen dat de persoonsgegevens waarop een verzoek om deze te wissen betrekking heeft in het verkeer zullen blijven. De verantwoordelijke zal niet in alle gevallen onder alle omstandigheden kunnen overzien welke derden de gegevens in enig stadium

rechtmatig zijn gaan verwerken. Het recht om te worden vergeten zal dan ook niet als een absoluut recht van de betrokkene kunnen worden aangemerkt. Mijn zorg ligt dan ook niet zozeer bij het recht om te worden vergeten als zodanig, maar bij de mogelijke verkeerde indruk die ontstaat bij de naamgeving ervan.

– De ontwerpverordening voorziet ook in een meldpunt voor datalekken. Hoe verhoudt deze zich tot het nationale meldpunt die momenteel in Nederland onderwerp van debat is, zo vragen de leden van de CDA-fractie.

De ontwerpverordening voorziet in een meldplicht voor datalekken bij de toezichthouder. In Nederland is dat het Cbp. Het door mij in december 2011 in consultatie gegeven wetsvoorstel, waarin op nationaal niveau een meldplicht datalekken wordt voorgesteld, voorziet ook in een meldplicht bij het Cbp. In zoverre is er sprake van overeenstemming tussen beide voorstellen.

– Momenteel is het mogelijk om, zonder daartoe door individuele burgers gemachtigd te zijn, in het algemeen belang een privacyproces te voeren tegen de overheid. Die mogelijkheid lijkt straks niet meer te bestaan. Klopt die analyse? De leden van de CDA-fractie hebben hier zorgen over.

De uitleg die de leden van de CDA-fractie geven aan de collectiefbelang-actie lijkt mij niet geheel juist. In het huidige recht is het op grond van artikel 3:305a van het Burgerlijk Wetboek mogelijk voor een stichting of een vereniging met volledige rechtsbevoegdheid die blijkens de statuten bepaalde belangen behartigt, een rechtsvordering in te stellen die strekt tot bescherming van gelijksoortige belangen van andere personen. Dat belang is een collectief belang, en niet noodzakelijkerwijs het algemeen belang. De rechtsvordering kan elke verplichting tot een geven, een doen of een nalaten betreffen, en behoeft niet specifiek de uitoefening van rechten die verband houden met de gegevensbescherming te betreffen. Evenmin hoeft de wederpartij niet steeds de overheid te zijn. Verder is het zo dat een gedraging waarop de rechtsvordering betrekking heeft niet aan die vordering ten grondslag kan worden gelegd wanneer degene die door die gedraging in het bijzonder wordt getroffen zich daartegen verzet. Ook heeft de uitspraak van de rechter in een collectiefbelangproces in beginsel geen gevolg ten aanzien van degene ten aanzien van wiens bescherming die uitspraak strekt, maar die zich daartegen toch verzet. Met die laatste twee regels wordt bereikt dat niemand gedwongen kan worden tot betrokkenheid tegen zijn zin in een collectiefbelangactie.
Artikel 73, tweede lid, van de ontwerpverordening geeft een specifiek collectiefactierecht voor organisaties die zich blijkens hun statuten sterk maken voor de rechten en belangen van betrokkenen in de zin van de ontwerpverordening. Dit collectiefactierecht is anders van aard dan het collectiefactierecht uit het Burgerlijk Wetboek. Het is bestuursrechtelijk van aard en maakt alleen het collectief indienen van een handhavings-klacht bij de toezichthouder mogelijk. Hoewel het tweede lid van artikel 73 dit niet uitdrukkelijk regelt, lijkt het mij moeilijk voorstelbaar dat beoogd is met deze bepaling het collectiefactierecht uit het burgerlijk recht uit te sluiten. Ik zal niettemin in de onderhandelingen in Brussel aandacht vragen voor de verhouding van artikel 73 tot het bestaande recht van de lidstaten. Het lijkt overigens wel voldoende duidelijk dat het collectiefac-tierecht van artikel 73, tweede lid, ontwerpverordening uitsluitend kan worden uitgeoefend op verzoek van een of meer betrokkenen. Een algemene handhavingsklacht zonder de medewerking van individuele betrokkenen lijkt dus uitgesloten.
Artikel 73, derde lid, van de ontwerpverordening geeft echter één uitzondering op die regel. Een handhavingsklacht kan wel door een

collectiefbelangorganisatie worden ingediend, zonder de medewerking van een individuele belanghebbende in geval van een datalek. Bij de noodzaak voor die uitzondering zijn vragen te stellen.

– De leden van de CDA-fractie hebben de Staatssecretaris gevraagd of het Cbp ook een voorafgaande adviserende rol zou kunnen spelen. Bij het ontwikkelen van nieuwe producten moet steeds meer al aan de tekentafel rekening worden gehouden met de bescherming van persoonsgegevens (privacy by design) en bedrijven hebben soms grote behoefte aan advies. Zouden zij, tegen betaling, een soort prejudiciële vraag kunnen stellen, dan zouden zij daar zeer mee geholpen kunnen zijn. Heeft de Staatssecretaris hierover inmiddels al overleg gevoerd met het Cbp?

Ik zal op dit onderwerp in een afzonderlijke brief terugkomen. Ik zal in die brief ook ingaan op een aantal andere onderwerpen die in het algemeen overleg van 7 maart 2012 aan de orde zijn gesteld.

– Tot slot hecht de CDA-fractie eraan nogmaals uit te spreken dat zij volledige openheid verwacht van de regering over de stand van de onderhandelingen over de voorstellen, zodat de Kamer effectief controle kan uitoefenen op de onderhandelingen en de inzet en successen van de Nederlandse regering in de Raad.

Voor zoveel nodig herinner ik de leden van de CDA-fractie aan de toezeggingen terzake die door mij zijn gedaan in het algemeen overleg van 7 maart 2012.

SP

De leden van de SP-fractie hebben met belangstelling kennis genomen van het nieuwe pakket van de Europese Commissie met voorstellen voor de bescherming van persoonsgegevens. De leden benadrukken dat dit een omvangrijk pakket is, wat van groot belang zal zijn voor de toekomstige privacywetgeving in Nederland. De leden benadrukken bij de regering dit pakket met voorstellen van buitengewoon groot belang te vinden en vragen de regering hieraan veel aandacht te besteden en bij iedere gelegenheid het belang van een hoog beschermingsniveau te benadrukken. Tevens hechten zij aan de toezeggingen, gedaan in het Algemeen Overleg over het behandelvoorbehoud van deze voorstellen, over de informatievoorziening aan de Kamer.

Algemeen

– De leden van de SP-fractie vragen de regering nog eens duidelijk aan te geven in hoeverre het na eventuele aanname van deze voorstellen (ontwerpverordening en ontwerprichtlijn) nog mogelijk is in Nederland af te wijken van de Europese regels. Beogen de Europese regels de gehele privacywetgeving in alle lidstaten te harmoniseren? Of beogen deze Europese regels minimumnormen neer te leggen, waarbij het is toegestaan naar boven af te wijken (méér bescherming te bieden)? Indien dat laatste niet het geval is, waarom niet?

De keuze van de Commissie om met een voorstel voor een ontwerpverordening te komen heeft tot gevolg dat het gegevensbeschermingsrecht in verdere mate geharmoniseerd wordt dan nu nog het geval is. Daaruit vloeit voort dat in er in algemene zin in elk geval geen sprake is van een uitbreiding van de mogelijkheden om op nationaal niveau regels vast te stellen. Toch is het niet zo dat die mogelijkheden in het voorstel volledig ontbreken. Zo behouden de lidstaten vrijheid om op het terrein van het arbeidsrecht aanvullende wetgeving vast te stellen. Op het terrein van het

gezondheidsrecht is er een verplichting tot het stellen van aanvullende regels. Dit is belangrijk, omdat er tussen de lidstaten grote verschillen bestaan op deze gebieden, en die het kader van gegevensbescherming verre te buiten gaan.
Voor de regelgeving die geen betrekking heeft op specifiek benoemde terreinen is er sprake van een geschakeerd beeld. Op veel gebieden is rechtvaardiging voor de verwerking van persoonsgegevens afhankelijk van hetzij nadere regelgeving van de EU, hetzij nadere regelgeving van de lidstaten. In veel gevallen zal dit neerkomen op de noodzaak regels vast te stellen op nationaal niveau. Het is ook nog onvoldoende duidelijk hoe de verhouding is van de ontwerpverordening tot bestaande regels van nationaal recht. De Europees Toezichthouder voor de Gegevensbescherming heeft terecht de aandacht gevraagd voor deze vragen.
Wat de ontwerprichtlijn betreft geldt de algemene regel dat een ontwerprichtlijn voor de lidstaten verbindend is ten aanzien van te bereiken resultaat, maar dat het aan de lidstaten is gelaten de vorm en de middelen te kiezen waarmee dat resultaat wordt bereikt. Bij de ontwerprichtlijn gaat het beoogde resultaat verder dan het beoogde resultaat van kaderbesluit 2008/977/JBZ ter vervanging waarvan de ontwerprichtlijn dient. In zoverre is er minder ruimte voor de lidstaten om aanvullende regels te stellen. Toch bevat de ontwerprichtlijn op enkele onderdelen wel degelijk verwijzingen naar de mogelijkheid op onderdelen nog nadere regels vast te stellen.

– De leden van de SP-fractie benadrukken dat het niet alleen gaat om het maken van goede regels voor bescherming van persoonsgegevens, maar dat de regels vooral ook toegepast moeten worden in alle EU-lidstaten. Hoe kijkt de regering aan tegen het naleven van de huidige privacyregels in andere EU-lidstaten? Hoe wordt daar op toegezien?

Ik ben het met deze leden eens dat goede toepassing en handhaving van de regels van groot belang is. Ik moet mij echter onthouden van een oordeel over de wijze waarop in andere lidstaten van de EU de regels van gegevensbescherming worden nageleefd. De handhaving vindt daar, net als in Nederland, plaats door onafhankelijke toezichthouders.

– De leden van de SP-fractie constateren dat met name op de ontwerprichtlijn, waarin regels staan voor justitie en politie, veel kritiek is gekomen. De ontwerprichtlijn zou een (te) laag niveau van gegevensbescherming bieden. Dat zeggen ook het CBP, de EDPS en de art. 29-werkgroep.
Deelt de regering die mening? Zo ja, welke gevolgen heeft dat voor de onderhandelingsinzet? Zo niet, waarom niet?
Voor de beantwoording van deze vragen verwijs ik de leden van de SP-fractie graag naar de eerder, naar aanleiding van vragen van de fractie van de PVV, genoemde brief van de Minister van Veiligheid en Justitie aan de Voorzitter van de Tweede Kamer der Staten-Generaal van 27 april 2012.
– De leden van de SP-fractie constateren dat er soms een conflict van plichten kan bestaan bij samenloop van toepasselijk recht. Een bedrijf bijvoorbeeld kan geconfronteerd worden met een vordering voor gegevens van autoriteiten uit andere landen, bijvoorbeeld de VS, terwijl deze overdracht op basis van de EU-wetgeving niet zou zijn toegestaan. Een eerdere versie van het voorstel bevatte de duidelijke bepaling dat géén gegevens mogen worden overgedragen, zo lang er geen goede waarborgen voor de persoonsgegevens zijn. Die bepaling leek meer duidelijkheid te bieden. Waarom is die formulering verdwenen? Gaat de regering zich er voor inzetten dat die bepaling weer terug komt?
In overweging 90 van de ontwerpverordening heeft de Commissie voldoende duidelijk gemaakt dat zij zich bewust is van het ontstaan van mogelijke conflicten van plichten wanneer de verstrekking van gegevens

verplicht is op grond van buitenlands recht en een rechtvaardigingsgrond voor die verstrekking in het Europese recht ontbreekt. Ik acht dat een belangrijk gegeven. Het is mij nog niet helemaal duidelijk hoe met de artikelen 42 en 44 van de ontwerpverordening die problemen worden opgelost. Ik ben er primair in geïnteresseerd van de Commissie te vernemen hoe deze bepalingen in het licht van overweging 90 moeten worden begrepen.

Toezicht

– De leden van de SP-fractie benadrukken het van groot belang te vinden dat er in alle landen een robuuste toezichthouder aanwezig is om privacyschendingen aan te pakken. Ook Europees toezicht is noodzakelijk. Hoe ziet het kabinet dit voor zich?

Er is reeds in alle lidstaten en ook op Europees niveau een toezichthouder aangesteld. De ontwerpverordening voorziet in een eenvormig stelsel van bevoegdheden en bestuurlijk strafrecht voor deze toezichthouders. Het lijdt weinig twijfel dat het handhavingsniveau daarmee aanmerkelijk wordt versterkt.

– De leden van de SP-fractie plaatsen vraagtekens bij de capaciteit van het College Bescherming Persoonsgegevens. We hebben een (privacy-) waakhond met tanden nodig, die voldoende mankracht heeft om bepaalde signalen en meldingen uit de samenleving te onderzoeken. Daarover zijn de leden bezorgd. Vooral ook in het licht van de toekomstige meldplicht datalekken, waar de aan het woord zijnde leden groot voorstander van zijn, die naar alle waarschijnlijkheid veel werk op zal leveren voor het CBP. Graag een reactie.

Ik ben van oordeel dat het CBP zodanig met financiële en personele middelen moet worden uitgerust dat het in staat is zijn taken op redelijke wijze te vervullen. Naar mijn oordeel is daarvan thans sprake. Wat betreft de eventuele toename van taken van het Cbp als gevolg van het wetsvoorstel meldplicht datalekken zal in de memorie van toelichting terzake een korte beschouwing worden opgenomen.

– De leden van de SP-fractie vragen wanneer het wetsvoorstel waarmee de boetebevoegdheid van het CBP wordt uitgebreid de Kamer naar verwachting zal bereiken.

Ik zal op dit onderwerp in een afzonderlijke brief terugkomen. Ik zal in die brief ook ingaan op een aantal andere onderwerpen die in het algemeen overleg van 7 maart 2012 aan de orde zijn gesteld.

Specifieke vragen, op onderdelen

Meldplicht datalekken

– De leden van de SP-fractie zijn al langere tijd voorstander van een meldplicht datalekken, en vinden de huidige voorgestelde bepaling te beperkt: Niet de inbreuk op beveiligingsmaatregelen, maar de ongeautoriseerde toegang tot persoonsgegevens moet leidend zijn en bepalend zijn voor de vraag of het lek gemeld moet worden. Dus ook een meldplicht indien er per ongeluk een databestand met persoonsgegevens op internet wordt geplaatst. Ook dat zou moeten worden gemeld. Gaat de regering zich hiervoor inzetten?

Ik ben er geen voorstander van om de meldplicht datalekken zo breed op te rekken dat ook elk geval van ongeautoriseerde toegang onder deze meldplicht valt. Een binding van de meldplicht aan een andere reeds bestaande verplichting met betrekking tot de bescherming van persoonsgegevens is juist vanwege deze band beter handhaafbaar. Noch richtlijn 95/46/EG, noch de Wbp, noch de ontwerpverordening kennen een regeling voor de rechtmatige toegang tot persoonsgegevens. Het is niet mogelijk om een dergelijke regeling in wetgeving op te nemen, omdat richtlijn 95/46/EG daarin niet voorziet en het zeer de vraag is of op nationaal niveau de ruimte bestaat een dergelijk voorschrift vast te stellen. Daarnaast moet de overheid zich in algemene zin niet zonder dringende noodzaak bemoeien met de interne huishouding van niet tot de overheid behorende bedrijven of instellingen.

Behalve dit aspect geldt uit oogpunt van handhaafbaarheid nog dat het in concreto bijzonder moeilijk kan zijn een goed onderscheid te maken tussen ongeautoriseerde toegang tot gegevens – die overigens niet noodzakelijkerwijs een extern negatief effect op de persoonsgegevens van de betrokkene hoeft te hebben – en verkeerde handelingen met persoonsgegevens nadat op wel geautoriseerde wijze toegang tot die gegevens is verkregen. Het door deze leden aangehaalde voorbeeld van een verwerking die per ongeluk op internet is geplaatst, hoeft niet het gevolg te zijn van ongeautoriseerde toegang tot die gegevens.

Nalevingskosten

– De leden van de SP-fractie vragen wat de regering nu precies wel beschouwt als «nalevingskosten» en wat daar niet onder valt. In hoeverre zijn verplichtingen van bedrijven om te investeren in een zorgvuldige omgang met persoonsgegevens nu te beschouwen als nalevingskosten? Volgens de in Nederland gehanteerde definitie vallen onder nalevingskosten alle kosten die een bedrijf of instelling moet maken om te kunnen voldoen aan wet- en regelgeving. Daaronder vallen dus ook de kosten die gemoeid zijn met investeringen in een zorgvuldige omgang met persoonsgegevens.

Bedrijven met minder dan 250 fte

– De leden van de SP-fractie vragen de regering wat de onderhandelingsinzet zal zijn op het punt dat bedrijven met minder dan 250 fte worden vrijgesteld van een aantal verplichtingen. Zou niet zo zeer de grootte van het bedrijf, maar de mate van risico bepalend moeten zijn voor de vraag of uitzonderingen moeten worden gecreëerd?

Ik ben het met de leden van de SP-fractie eens dat niet de omvang van het bedrijf, maar de aard van de gegevensverwerking en de daarmee gemoeide risico's bepalend moeten zijn voor de zwaarte van de verplichtingen die de ontwerpverordening op verantwoordelijken legt. Mijn inzet is er dus niet op gericht dat ondernemingen of instellingen met minder dan 250 fte principieel moeten worden vrijgesteld van de verplichtingen van de ontwerpverordening.

Uitwisseling met derde landen

– De leden van de SP-fractie vragen naar de garanties die er zijn indien gegevens worden uitgewisseld met derde landen. Vindt de regering dat het voorstel op dit punt voldoende waarborgen bevat voor de gegevensbescherming?

Hoofdstuk V van de ontwerpverordening bevat een groot aantal bepalingen die het grensoverschrijdend verkeer van persoonsgegevens regelen. Met deze bepalingen bevat de ontwerpverordening een beter uitgewerkte verzameling grondslagen voor deze typen verwerkingen. De regering is van mening dat er op dit onderdeel van het gegevensbeschermingsrecht sprake is van een verbetering ten opzichte van richtlijn 95/46/EG, ook waar het gaat om de daarbij in acht te nemen waarborgen.

Profilering

– De leden van de SP-fractie vragen de regering te reageren op de zorgen die de commissie Meijers heeft geuit over het gebruik van profilering op basis van persoonsgegevens.

In de eerder, naar aanleiding van vragen van de fractie van de PVV, genoemde brief van de Minister van Veiligheid en Justitie aan de Voorzitter van de Tweede Kamer der Staten-Generaal van 27 april 2012, is een reactie gegeven op de brief van de Commissie-Meijers. Ik verwijs de leden van de SP-fractie graag naar die brief.

Rechten van betrokkenen

– De leden van de SP-fractie vragen de regering of zij tevreden zijn over de uitwerking van de rechten van betrokkenen, zoals het «recht om vergeten te worden» en het «recht op informatie». Wat is de reactie op bijvoorbeeld de kritiek van het CBP dat de uitzonderingen op de informatieplicht te ruim geformuleerd zijn?

In het voorgaande is bij de beantwoording van de vragen van de leden van de fracties van CDA en VVD reeds ingegaan op enige aspecten van het recht om te worden vergeten. Ik verwijs de leden van de SP-fractie graag naar deze passages.
Aannemende dat de leden van de SP-fractie wat betreft hun vraag naar de informatieplicht doelen op de specifieke opmerkingen van het Cbp bij de ontwerprichtlijn, kan ik deze leden verwijzen naar de reactie in de eerdergenoemde brief van de Minister van Veiligheid en Justitie van 27 april 2012.

D66

– De leden van de D66-fractie verwelkomen het feit dat de Commissie een voorstel heeft gedaan om de EU-regels voor privacybescherming bij de tijd te brengen. Dit is hoognodig omdat zich sinds het opstellen van de huidige regels veel veranderingen hebben voorgedaan. Zij zijn daarbij verheugd dat het overgrote deel van de nieuwe EU-regels voor Bescherming Persoonsgegevens in de vorm van het instrument «Ontwerpverordening» is gegoten. Op deze wijze zullen de regels in elk EU-land gelijkluidend zijn. Deze leden juichen toe dat personen meer controle krijgen over hun eigen data met deze Ontwerpverordening. Ook moeten bedrijven in het vervolg explicieter dan voorheen aan burgers toestemming vragen als zij hun persoonsgegevens willen gebruiken en gaat voor hen een meldplicht voor datalekken gelden. Daarnaast wordt een «right to be forgotten» voorgesteld. Naar het oordeel van de leden van de fractie van D66 zijn dit stappen vooruit.

De leden van de D66-fractie zien echter ook een aantal uitdagingen en kansen voor verbetering. De Europese Commissie heeft gekozen voor meerdere instrumenten (in aanvulling op genoemde Ontwerpverordening wordt voor het politiële en justitiële domein een Ontwerprichtlijn voorgesteld), maar volgens D66 moet het uitgangspunt hetzelfde blijven:

één alomvattend rechtskader om het verzekeren van een hoog niveau van gegevensbescherming voor de Europese burger. De aan het woord zijnde leden hebben geconstateerd dat op een aantal cruciale punten de ontwerprichtlijn en de ontwerpverordening tevens uit elkaar lopen. Is de regering bereid om gedurende de onderhandelingen in te zetten op het bewerkstelligen van een nauwere samenhang tussen beide instrumenten? Het gaat hierbij voornamelijk om de algemene beginselen voor gegevensverwerking (zoals doelbinding en bewaartermijn), de verplichtingen die van toepassing zijn op de verantwoordelijke alsook bewerker en de bevoegdheden die worden toegekend aan de autoriteiten verantwoordelijk voor gegevensbescherming. De aan het woord zijnde leden benadrukken dat deze discrepanties hen zorgen baren.

Ik ben van mening dat de keuze die de Commissie heeft gemaakt met betrekking tot de instrumenten verdedigbaar is. Er zijn belangrijke verschillen tussen het algemene gegevensbeschermingsrecht en het gegevensbeschermingsrecht voor politie en justitie. Die verschillen zijn ook gerechtvaardigd, omdat op het terrein van politie en justitie de onderzoeksbelangen steeds zullen moeten afgewogen tegen het belang van de bescherming van persoonsgegevens, hetgeen tot andere uitkomsten kan leiden dan bij de verwerking van persoonsgegevens door bedrijven of overheidsinstellingen. Voor de beantwoording van de vragen over het uit elkaar lopen van de ontwerprichtlijn en de ontwerpverordening verwijs ik de leden van de fractie van D66 naar het antwoord op een soortgelijke vraag van de fractie van de VVD.

– Voor de leden van de D66-fractie is het belangrijk dat het hoogste niveau van bescherming geldt wanneer bedrijven persoonsgegevens verzamelen (zoals telecomgegevens en passagiersgegevens) en deze gegevens vervolgens worden gebruikt en verwerkt door politie en justitie. Hoe kijkt de regering hier tegenaan? Kan een nadere toelichting worden gegeven van de regeringsinzet bij de onderhandelingen op dit punt?
De voorstellen van de Commissie voor een ontwerpverordening en een ontwerprichtlijn brengen op zichzelf geen verandering in de bestaande situatie. Die houdt in dat bedrijven die gegevens voor hun eigen doeleinden verwerken onderworpen zijn aan de regels van het algemene gegevensbeschermingsrecht. Als deze gegevens vervolgens van belang blijken voor politie en justitie zal daarvoor hetzij op EU-niveau, hetzij op nationaal niveau een wettelijke voorziening nodig zijn. Ik acht dit de juiste weg. Daarbij merk ik op dat ik mij kan voorstellen dat de fractie van D66 het hoogste niveau van gegevensbescherming bepleit voor persoonsgegevens die worden verzameld door bedrijven en die vervolgens worden gebruikt door politie en justitie. Tegelijkertijd ben ik van mening dat het gebruik van een begrip als «het hoogste niveau van gegevensbescherming» de discussie eenvoudig kan vertroebelen zolang het niet duidelijk is wat hiermee precies wordt bedoeld. Ten aanzien van de doelbinding zal het hoogste niveau van gegevensbescherming er toe moeten leiden dat gegevens uitsluitend mogen worden verwerkt voor het doel waarvoor zij zijn verzameld. Gelet op andere belangen dan die van de bescherming van persoonsgegevens is een dergelijke zienswijze echter niet houdbaar, omdat politie en justitie vrijwel dagelijks baat hebben bij het gebruik van verkeersgegevens van gebruikers van telecommunicatiediensten. Dit neemt niet weg dat ik van oordeel ben, en zo denk ik ook de inbreng van de fractie van D66 te mogen begrijpen, dat er zeer goede waarborgen dienen te gelden voor het gebruik van persoonsgegevens door politie en justitie, zodat de burger er op kan vertrouwen dat zijn persoonsgegevens slechts op grond van een zorgvuldige wettelijke regeling, waarbij is voorzien in afdoende wettelijke waarborgen voor een zorgvuldige gegevensverwerking, kunnen worden gebruikt voor de opsporing en vervolging van strafbare feiten.

De persoonsgegevens die door aanbieders in de private sector, zoals banken, luchtvaartmaatschappijen en telecommunicatiedienstverleners, ten behoeve van de eigen bedrijfsvoering worden verwerkt, vallen onder de reikwijdte van de ontwerpverordening. De gevallen waarin, en de omstandigheden waaronder, de gegevens door politie en justitie kunnen worden gevorderd ten behoeve van de opsporing en vervolging van strafbare feiten zijn uitgewerkt in het Wetboek van Strafvordering. Dit betreffen de bevoegdheden op het gebied van het vorderen van verkeersgegevens (de artikelen 126n/u tot en met 126 nb/ub Sv en de artikelen 126zh/zja Sv) en het vorderen van gegevens (de artikelen 126 nc/uc tot en met 126ng/ug Sv, en de artikelen 126 zk/zo Sv). De regels over de bescherming van de persoonsgegevens, die door politie en justitie worden verwerkt, zijn neergelegd in de Wet politiegegevens en de Wet justitiële en strafvorderlijke gegevens. Deze regels hebben betrekking op de doelbinding, de bewaartermijnen, de verstrekking van de gegevens aan derden en de beveiliging van de gegevens.
Zoals ik eerder, in antwoord op vragen van de VVD-fractie heb aangegeven, gaat de ontwerprichtlijn ervan uit dat de verwerking van persoonsgegevens door politie en justitie in beginsel slechts plaatsvindt op grond van een wettelijke grondslag (artikel 7). Voor een dergelijke grondslag kan worden verwezen op de eerdergenoemde bepalingen van het Wetboek van Strafvordering. Ik acht dit een juist uitgangspunt, omdat hiermee verzekerd is dat het gebruik van gegevens van private bedrijven ten behoeve van opsporing en vervolging slechts kan plaatsvinden op basis van een wettelijke regeling, die tot stand is gekomen in nauwe samenspraak met het parlement. Overigens zijn de bepalingen van de ontwerprichtlijn van toepassing op de verdere verwerking van de gegevens door politie en justitie. Op dit moment zie ik geen aanleiding tot aanvulling van de regels van de ontwerprichtlijn vanwege het mogelijke gebruik van gegevens van private aanbieders door politie en justitie.

– Deze leden lezen in de brief van staatssecretaris Teeven (32 761, nr. 17) het volgende: «Ook bij de ontwerprichtlijn heb ik kanttekeningen ten aanzien van de uitvoerbaarheid en werklast. Dit betreft het maken van onderscheid tussen categorieën van gegevens door politie en justitie en de informatieverplichtingen jegens degenen die met de politie en justitie in aanraking komen. Dergelijke verplichtingen zijn niet goed te verenigen met de aard van het politiewerk.» Zij ontvangen graag een nadere toelichting en precisering bij deze stelling. Waar doelt de staatssecretaris precies op?

In de ontwerprichtlijn wordt voorgesteld dat de lidstaten erop toezien dat de verschillende categorieën van persoonsgegevens die worden verwerkt, voor zover mogelijk worden onderscheiden naar de graad van juistheid en betrouwbaarheid en dat persoonsgegevens die op feiten zijn gebaseerd worden onderscheiden van persoonsgegevens die op een persoonlijk oordeel zijn gebaseerd (artikel 6). Afgezien van de technische haalbaarheid van een dergelijk onderscheid – dit is hierboven, naar aanleiding van een vraag van de PvdA-fractie aan de orde gekomen – is het probleem van een dergelijke verplichting dat de graad van betrouwbaarheid van gegevens voor de politie niet eenduidig is vast te stellen. De verklaring van een verdachte kan afwijken van die van een getuige zonder dat duidelijk is welke verklaring het meest betrouwbaar is. De aard van het politiewerk is er juist op gericht om zoveel mogelijk informatie te verzamelen ten behoeve van de oordeelsvorming van de officier van justitie en de rechter. Daar komt bij dat de ontwerprichtlijn geen nadere aanknopingspunten biedt geeft voor een onderscheid naar de graad van betrouwbaarheid van gegevens. Weliswaar wordt bij bepaalde eenheden van de politie, de zogenaamde criminele inlichtingen eenheden (CIE's), gewerkt met gradaties voor de beoordeling van de betrouwbaarheid van

verklaringen van informanten (het zogenaamde 4x4 formulier) maar dit betreft een specifiek deelterrein van de opsporing. Dit geldt eveneens voor het onderscheid tussen feiten en een persoonlijk oordeel. Het zal in de praktijk niet altijd eenvoudig zijn om een onderscheid te maken tussen een feit en een persoonlijk oordeel. Dit alles klemt temeer daar er aan een dergelijk onderscheid geen gevolgen zijn verbonden voor wat betreft de verdere verwerking van de gegevens. Daardoor is het niet duidelijk wat de betrokkene hier precies aan heeft, terwijl de lasten voor politie en justitie aanzienlijk kunnen zijn.
Daarnaast wordt in de ontwerprichtlijn voorgesteld dat de lidstaten erop toezien dat wanneer persoonsgegevens worden verzameld, de verantwoordelijke alle passende maatregelen treft om de betrokkene ten minste bepaalde informatie te verschaffen, zoals de doeleinden van de gegevensverwerking, de periode gedurende welke de gegevens worden opgeslagen en de ontvangers en categorieën ontvangers van de gegevens (artikel 11, eerste lid). De informatieverstrekking aan de betrokkene kan worden uitgesteld, beperkt of achterwege gelaten, onder meer om te voorkomen dat afbreuk wordt gedaan aan de opsporing of vervolging van strafbare feiten. Bepaalde categorieën van gegevensverwerking kunnen geheel of gedeeltelijk onder deze uitzonderingsgronden worden gebracht. Het probleem van een dergelijke verplichting is dat het voor politie en justitie lastig uitvoerbaar zal kunnen zijn om alle personen, die met de politie in aanraking komen in verband met de opsporing van strafbare feiten, te informeren over de gegevensverwerking. Dit kan betekenen dat een groep voetbalvandalen, die door de politie wordt gefilmd met het oog op mogelijke aanhouding vanwege openlijke geweldpleging, moet worden ingelicht over de doeleinden van de gegevensverwerking. En gelet om de inhoud omvang van de voorgestelde informatieplicht, lijkt een informatieformulier («bijsluiter») dat aan de betrokkene kan worden uitgereikt, nauwelijks haalbaar. Verder zal het in de praktijk niet vaak mogelijk zijn om tijdens een opsporingsonderzoek gegevens te verstrekken aan personen, aangevers, getuigen of slachtoffers, vanwege het zogenaamde afbreukrisico. Dat wil zeggen dat de verdachten op de hoogte raken van het politieonderzoek en hun gedrag aanpassen. Als ervoor wordt gekozen de betrokkenen in een later stadium te informeren, moet de organisatie erop zijn ingericht om te voorkomen dat dit aan de aandacht ontsnapt. Als dit gebeurt dan kan de vraag aan de orde zijn van de consequenties van een dergelijke nalatigheid. In ieder geval moet rekening worden gehouden met een aanzienlijke verhoging van de werklast voor de politie, die afbreuk zal doen aan de beschikbare personele capaciteit voor de opsporing van strafbare feiten.

– De leden van de D66-fractie achten het een gemiste kans dat er een apart, lager beschermingsniveau komt als de overheid persoonsgegevens gebruikt. De besluiten die de overheid neemt over burgers op basis van hun gegevens, kunnen minstens zo ingrijpend zijn als die van bedrijven. Is de regering bereid zich bij de onderhandelingen in te zetten voor één – zo hoog – beschermingsniveau die voor alle partijen geldt die gegevens verwerken, dus ook de overheden en de Europese instellingen? Zo nee, waarom niet?

Ik ben het niet eens met de leden van de D66-fractie als zij stellen dat er sprake is van een lager beschermingsniveau voor alle gevallen waarin de overheid gegevens verwerkt. Wel is het zo dat voor de overheid afzonderlijke rechtvaardigingsgronden gelden voor de verwerking van persoonsgegevens, en dat de mate waarin de Uniewetgever of de nationale wetgever regels kan of moet stellen voor specifieke verwerkingen in de sfeer van de overheid nu eenmaal ruimer is. Dat laatste acht ik gerechtvaardigd. De overheid heeft in de samenleving een bijzondere verantwoordelijkheid, die afwijkt van de verantwoordelijkheden van het

bedrijfsleven. De overheid moet, anders dan het bedrijfsleven, ook garant staan voor de verwerkelijking van andere grondrechten dan alleen de bescherming van persoonsgegevens. Veiligheid, belastingheffing en sociale zekerheid kunnen niet worden georganiseerd wanneer er niet op een zekere schaal persoonsgegevens worden verwerkt. Het is dan ook veeleer de vraag of de overheid haar taken wel voldoende kan uitoefenen wanneer aangedrongen wordt op vermindering van de mogelijkheden om gegevens te verwerken.

– De voorgestelde regelgeving voorziet in nieuwe plichten voor bedrijven en nieuwe rechten voor burgers die bijdragen aan een betere bescherming van persoonsgegevens; hetgeen in beginsel positief is. Maar deze plichten en rechten moeten wel afdwingbaar zijn. De leden van de D66-fractie beschouwen het als winst dat de nationale colleges bescherming persoonsgegevens boetes zullen kunnen gaan opleggen. Nu bestond op nationaal niveau in Nederland dit voornemen al langer en vragen zij de regering wanneer de Kamer dit wetsvoorstel tegemoet kan zien, waarbij de aan het woord zijnde leden zeggen benieuwd te zijn naar de samenloop tussen beide (het Europese en nationale) trajecten.

Ik zal op dit onderwerp in een afzonderlijke brief terugkomen. Ik zal in die brief ook ingaan op een aantal andere onderwerpen die in het algemeen overleg van 7 maart 2012 aan de orde zijn gesteld.

– Zij vragen de regering eveneens hoe deze aankijkt tegen strafrechtelijke sancties voor gevallen van zware overtreding van deze regels.

Ik ben voorstander van handhaving van de gegevensbeschermingswetgeving door middel van een bestuurlijke boete. Tegen het voorstel van de Commissie terzake heb ik dan ook geen principieel bezwaar. Wel kan ik mij voorstellen dat over de exacte hoogte van de boetes en de vraag of alle overtredingen wel met juiste sanctie worden bedreigd nog de nodige discussie plaatsvindt.

– Ten slotte, vragen zij de regering om haar visie op het «minder dan 250 fte»-criterium toe te lichten. Graag zouden zij zien dat daarbij expliciet wordt ingegaan op de stelling van het CBP dat «niet de grootte van het bedrijf, maar de mate van risico verbonden aan de verwerking» bepalend dient te zijn voor het creëren van eventuele uitzonderingen.

Ik verwijs de leden van de D66-fractie graag naar mijn antwoorden terzake op gelijkluidende vragen van de leden van de SP-fractie.

– Voor de leden van de D66-fractie is het een belangrijk punt dat Europese burgers beschermd worden door Europese regels, ook als derde landen gebruik maken van gegevens van Europese burgers. In het fiche over de ontwerpverordening stelt de regering dat het probleem van conflicterende jurisdicties nog niet volledig sluitend lijkt te zijn geregeld. Leden van deze fractie hebben over dit onderwerp meerdere malen vragen gesteld. Kan de regering een nadere toelichting geven van de regeringsinzet op deze punten? Welke ondergrens hanteert de regering?

In overweging 90 van de ontwerpverordening heeft de Commissie voldoende duidelijk gemaakt dat zij zich bewust is van het ontstaan van mogelijke conflicten van plichten wanneer de verstrekking van gegevens verplicht is op grond van buitenlands recht en een rechtvaardigingsgrond voor die verstrekking in het Europese recht ontbreekt. Ik acht dat een belangrijk gegeven. Het is mij nog niet helemaal duidelijk hoe met de artikelen 42 en 44 van de ontwerpverordening die problemen worden opgelost. Ik ben er primair in geïnteresseerd van de Commissie te

vernemen hoe deze bepalingen in het licht van overweging 90 moeten worden begrepen. Ik richt mij er dus in de eerste plaats op te luisteren naar de Commissie.

– In een brief van het College Bescherming Persoonsgegevens (CBP) over onderhavige materie aan de vaste Kamercommissie voor Veiligheid en Justitie (d.d. 2 maart 2012) meldt het CBP het volgende: «Een eerdere – openbaar geworden – conceptversie van de ontwerpverordening bevatte zo'n bepaling in artikel 42: «No judgment of a court or tribunal and no decision of an administrative authority of a third country requiring a controller or processor to disclose personal data shall be recognized or be enforceable in any matter , without prejudice to an mutual assistance treaty or an international agreement in force between the requesting third country and the Union or a Member State».« Kan de regering inzicht verschaffen in de reden(en) dat deze formulering verdwenen is uit het voorstel? Kan de regering tevens duidelijkheid verschaffen of zij voorstander zou zijn van het (her-)introduceren van een dergelijke bepaling? En zo niet, waarom niet.

Het is mij niet bekend waarom die bepaling niet in het voorstel, dat door de Commissie is ingediend, is opgenomen. Een dergelijke bepaling gaat uit van een zeer rigide model voor het doorgeven van persoonsgegevens uit de EU naar derde landen, wanneer een voorschrift van vreemd recht of een rechterlijke beslissing van een vreemde jurisdictie een verantwoordelijke of bewerker daartoe dwingt. Natuurlijk verdient het de voorkeur om dergelijke doorgiften te laten plaatsvinden op de grondslag van een rechtshulpverdrag, een ander bilateraal verdrag, of een bindend EU-besluit, maar met de totstandkoming van dergelijke instrumenten is doorgaans veel tijd gemoeid. Een dergelijke rigiditeit helpt de verantwoordelijke die in een acuut conflict van plichten verzeild raakt naar mijn mening niet. Daar zal dus een aanvullende oplossing voor gezocht moeten worden. Bij de verdere vormgeving van oplossing zullen bovendien ook andere elementen moeten worden betrokken zoals de vraag of het gegevensverstrekking in bulk betreft, of dat het om individuele gevallen gaat en de vraag naar de aard van de betrokken gegevens.

– De leden van de D66-fractie benadrukken ten slotte dat de uitwerking en verdere onderhandelingen over onderhavige voorstellen hun buitengewone belangstelling heeft. Zij worden dan ook graag tijdig en frequent geïnformeerd over de voortgang hiervan.

Voor zoveel nodig herinner ik de leden van de D66-fractie aan de toezeggingen terzake die door mij zijn gedaan in het algemeen overleg van 7 maart 2012.

GroenLinks

De leden van de fractie van GroenLinks hebben nog enkele navolgende vragen over de herziening van de EU-wetgeving over de bescherming van persoonsgegevens.

– Op welke wijze spant de regering zich in om een aantal algemene beginselen voor gegevenswerking van dermate groot belang zijn en aan de basis liggen van gegevensbescherming dat zij zowel in de ontwerpverordening als de ontwerprichtlijn te laten opnemen, in het bijzonder beginselen als de rechtmatigheid van de gegevensverwerking, doelbinding, accuratesse van gegevens, en de noodzaak tot het stellen van een heldere bewaartermijn (niet langer bewaren dan strikt noodzakelijk voor het doel)?

Voor de beantwoording van deze vraag verwijs ik de leden van de fractie van GroenLinks naar het antwoord op een soortgelijke vraag van de fractie van de VVD.

– Artikel 6, vierde lid van de ontwerpverordening doorbreekt in latere fases van gegevensverwerking het principe van doelbinding. Op welke wijze spant de regering zich om deze dreigende uitholling van het principe van doelbinding ongedaan te maken?

Er zal in de ontwerpverordening hoe dan ook een regeling moeten worden opgenomen voor de verwerking van persoonsgegevens voor andere doeleinden dan die waarvoor zij oorspronkelijk zijn verzameld. Een dergelijke regeling ligt ook ten grondslag aan artikel 6, eerste lid, onder c, van richtlijn 95/46/EG en is nader uitgewerkt in artikel 9 van de Wbp. Als een dergelijke regeling ontbreekt zal het gegevensbeschermingsrecht zodanig rigide worden dat het maatschappelijke en economische ontwikkelingen blokkeert in plaats van stimuleert. Waar het mij om gaat is dat een regeling voor de zogeheten verdere verwerking de juiste voorwaarden biedt, waaronder die verdere verwerking nodig is. Artikel 6, vierde lid, van de ontwerpverordening biedt daarvoor in elk geval een bruikbaar beginpunt voor verdere discussie.

– In de ontwerpverordening zijn voor de overheid afwijkende bepalingen opgenomen over het gebruik van bijzondere persoonsgegevens, onverenigbaar gebruik, privacy impact assessments, en over de mogelijkheid van de overheid om beperkingen aan te brengen op de principes en rechten voor bepaalde belangen. Deelt de regering het standpunt dat door deze bepalingen wordt afgeweken van de doelstelling om te komen tot een alomvattend privacykader, een normenstelsel dat én voor de publieke en én voor de private sector zou gelden. En deelt de regering de mening dat zonder dat allesomvattende privacykader onzekerheid ontstaat bij burgers en verantwoordelijken over de vraag welke normen waarom wel of niet in welke situaties voor hen van toepassing zijn? Zo ja, op welke wijze spant de regering zich in opdat deze afwijkende bepalingen worden aangepast?

Ik ben het niet eens met de stellingname van de leden van de fractie van GroenLinks dat afbreuk wordt gedaan aan de doelstelling om een alomvattend wettelijk kader voor gegevensbescherming wanneer dat kader verschillende verplichtingen bevat voor overheid, bedrijfsleven en individuele burgers. Dat voor de overheid afzonderlijke rechtvaardigingsgronden gelden voor de verwerking van persoonsgegevens, en dat de mate waarin de Uniewetgever of de nationale wetgever regels kan of moet stellen voor specifieke verwerkingen in de sfeer van de overheid ruimer is, en dat er onder omstandigheden uitzonderingen op de rechten van de betrokkene moeten worden aanvaard acht ik gerechtvaardigd. De overheid heeft in de samenleving een bijzondere verantwoordelijkheid, die afwijkt van de verantwoordelijkheden van het bedrijfsleven. De overheid moet, anders dan het bedrijfsleven, ook garant staan voor de verwerkelijking van andere grondrechten dan alleen de bescherming van persoonsgegevens. Veiligheid, belastingheffing en sociale zekerheid kunnen niet worden georganiseerd wanneer er niet op een zekere schaal persoonsgegevens worden verwerkt. Het is dan ook veeleer de vraag of de overheid haar taken wel voldoende kan uitoefenen wanneer aangedrongen wordt op vermindering van de mogelijkheden om gegevens te verwerken. Daar staat tegenover dat de overheid, anders dan het bedrijfsleven, onderworpen is aan veel verschillende controlemechanismen op de uitoefening van haar bevoegdheden. Ik geloof niet dat verantwoordelijken en betrokkenen aan meer onzekerheid over het geldende recht zijn blootgesteld, wanneer er sprake is van verschil tussen

bevoegdheden en verantwoordelijkheden van overheid en bedrijfsleven. De regels moeten natuurlijk wel duidelijk zijn.

– Op welke wijze spant de regering zich in om de verplichtingen die van toepassing zijn op de verantwoordelijke en bewerker in zowel de ontwerpverordening en de ontwerprichtlijn gelijk te schakelen, waaronder de verplichting tot het uitvoeren van privacy impact assessments en het zorgdragen voor privacy by design?

Voor de beantwoording van deze vraag verwijs ik de leden van de fractie van GroenLinks naar het antwoord op een soortgelijke vraag van de fractie van de VVD. Voor wat betreft de ontwerpverordening merk ik nog op dat de verplichting tot het uitvoeren van privacy impact assessments blijkens artikel 33, eerste lid, van de ontwerpverordening gelijkelijk op de verantwoordelijke en de bewerker rust. Wat de doorwerking van de verplichting tot installeren van privacy by design of privacy by default betreft, kan inderdaad de vraag worden gesteld of die verplichting noodzakelijkerwijs alleen op de verantwoordelijke rust, of dat die ook vatbaar is voor nadere vormgeving of uitwerking door de bewerker. Het zou niet misstaan wanneer in artikel 26 van de ontwerpverordening wordt opgenomen of, en zo ja hoe, de bewerker die verplichting op grond van een bewerkersovereenkomst kan overnemen van de verantwoordelijke. Ik zal aandacht vragen voor dit punt in de onderhandelingen.

– In artikel 22 van de ontwerpverordening worden verplichtingen rond «accountability» vastgelegd. Dit betekent dat bedrijven dienen te investeren in een zorgvuldige omgang met persoonsgegevens. Dit vertaalt zich in plichten als het zorgdragen voor «privacy by design», het doen van «privacy impact assessments» en het garanderen van adequate beveiliging. Op welke wijze spant de regering zich in om deze bepaling in de ontwerpverordening te behouden alsmede om de uitvoering ervan in de praktijk te realiseren, zowel met betrekking tot het overheidsdomein als met betrekking tot het stimuleren hiervan in het private domein?

Artikel 22 van de ontwerpverordening bevat inderdaad de uitwerking van het accountabilitybeginsel. Als zodanig ben ik daar voorstander van, maar ik ben wel van oordeel dat het pakket aan verplichtingen evenwichtig moet zijn aan het pakket aan bevoegdheden dat er tegenover staat en ook verantwoord moet zijn wanneer rekening gehouden wordt met de specifieke risico's van de verwerking waar het in concreto om gaat. Dat evenwicht is naar mijn mening nog onvoldoende bereikt in deze bepaling. Daarvoor zal ik de aandacht zeker vragen. Wanneer dat evenwicht is bereikt, zal ook de uitvoering van deze bepaling in de praktijk gemakkelijker worden aanvaard.

Artikel 51 (2) van de conceptverordening stelt dat de dataprotectie-autoriteit van de lidstaat waar een verantwoordelijke zijn hoofdvestiging heeft, wordt geacht de «leidende autoriteit» te zijn die bevoegd is toezicht te houden op de verwerkingen van dit bedrijf in andere EU-lidstaten. Op welke wijze spant de regering zich in om de ontwerpverordening op te laten nemen dat indien de hoofdvestiging van een bedrijf niet eenduidig kan worden vastgesteld de European Data Protection Board (EDPB) de bevoegdheid krijgt om te bepalen welke dataprotectie-autoriteit de leiding neemt bij een zaak en hoe de onderlinge rolverdeling met andere nationale toezichthouders is?

Deze suggestie – afkomstig van het Cbp – acht ik nuttig. Ik zal daarvoor tijdens de onderhandelingen in Brussel de aandacht vragen.

– Op welke wijze spant de regering zich in voor het versterken van de rechten van de burger, in het bijzonder voor het behoud van de door de ontwerpverordening gegarandeerde versterking van het toestemmingsvereiste (betreft artikelen 4 en 7 van de conceptontwerpverordening)?

De versterking van het toestemmingsvereiste, in die zin dat het verschil tussen uitdrukkelijke en ondubbelzinnige toestemming wordt afgeschaft, is een verbetering ten opzichte van ontwerprichtlijn 95/46/EG. Dat neemt echter niet weg dat artikel 7 van de ontwerpverordening ook de nodige vragen oproept. Zo leidt de verplichting van de verantwoordelijke om bij te houden of een toestemming is verleend tot nalevingskosten en, belangrijker, ook de tot de verwerking van meer persoonsgegevens. De rechtsgevolgen van het intrekken van een toestemming zijn nog onvoldoende in kaart gebracht. De regeling van de onevenwichtigheid tussen partijen is evenmin voldoende duidelijk.

– In de ontwerpverordening worden bedrijven met minder dan 250 werknemers vrijgesteld van een aantal verplichtingen. Deelt de regering het standpunt dat in het huidige tijdgewricht vaak juist bedrijven met slechts enkele medewerkers voor de bescherming van persoonsgegevens zeer risicovolle verwerkingen doen en dat om die reden niet de grootte van een bedrijf, maar de mate van risico verbonden aan de verwerking bepalend moet zijn als besloten wordt om uitzonderingen te creëren en zo ja, op welke wijze spant de regering zich in opdat de conceptontwerpverordening op dit punt wordt aangepast?

Dit standpunt van de leden van de GroenLinks-fractie deel ik. Ik heb inmiddels nadrukkelijk aandacht gevraagd voor dit punt in de onderhandelingen. Andere lidstaten hebben dit ook gedaan.