Tweede Kamer der Staten-Generaal

2

Vergaderjaar 2015–2016

32 317 JBZ-Raad

32 761 Verwerking en bescherming persoonsgegevens

Nr. 363 **BRIEF VAN DE MINISTER VAN VEILIGHEID EN JUSTITIE**

Aan de Voorzitter van de Tweede Kamer der Staten-Generaal

Den Haag, 30 november 2015

In het algemeen overleg van 7 oktober 2015 over de JBZ Raad (Kamerstuk 32 317, nr. 356) deed ik de toezegging uw Kamer een brief te sturen met een appreciatie van het arrest van het Hof van Justitie van de Europese Unie (hierna: HvJEU) van 6 oktober 2015 in de zaak Maximilian Schrems/Data Protection Commissioner (C-362/14). Met deze brief voldoe ik aan die toezegging. Ik doe dat mede namens de Ministers van Economische Zaken en Binnenlandse Zaken en Koninkrijksrelaties.

0. Leeswijzer

Het arrest betreft een ingewikkelde materie. Mij is gebleken dat over de reikwijdte van het arrest veel misverstanden bestaan. Ik zet daarom eerst kort uiteen wat de geldende regels voor het verkeer van persoonsgegevens met landen buiten de EU en de EER zijn. Daarna ga ik kort in op de positie van de Verenigde Staten daarin en de betekenis van het besluit dat door het HvJEU ongeldig is verklaard. Vervolgens schets ik de inhoud van het arrest en geef ik een allereerste beoordeling. Daarna schets ik de consequenties ervan in feitelijk opzicht, aan welke oplossingsrichtingen wordt gewerkt en welke consequenties ik zie voor de wetgeving op EU- en nationaal niveau.

1. Doorgifte persoonsgegevens aan derde landen

Op grond van artikel 25, eerste lid, van richtlijn 95/46/EG (hierna: richtlijn) mogen persoonsgegevens slechts worden doorgegeven ter verdere verwerking naar een derde land indien dat land een passend niveau van bescherming waarborgt. Deze regel beoogt te voorkomen dat het beschermingsniveau van de richtlijn wordt ontgaan door de verwerking van persoonsgegevens van EU-burgers in een derde land te laten plaatsvinden. Op grond van artikel 25, zesde lid, van de richtlijn is de Commissie bevoegd om bij besluit vast te stellen dat een derde land een passend beschermingsniveau waarborgt. Dergelijke besluiten worden toereikendheidsoordelen of *adequacy findings* genoemd. Zij zijn

kst-32317-363
ISSN 0921 - 7371
's-Gravenhage 2015

gebaseerd op een bestudering van de wetgeving en de internationaalrechtelijke verplichtingen van het desbetreffende land waarin die waarborgen zijn neergelegd. Er zijn momenteel 11 landen met een toereikendheidsoordeel.

Als er een toereikendheidsoordeel is dan mogen persoonsgegevens, mits verwerkt in overeenstemming met de richtlijn zonder verdere garanties worden doorgegeven. Als er geen toereikendheidsoordeel is, moet de doorgifte op een andere door de richtlijn geregelde grondslag plaatsvinden. Toepassing van andere grondslagen veroorzaakt in de regel meer administratieve lasten en nalevingskosten van de verantwoordelijke voor de gegevensverwerking.

1.1 Passendheid niveau gegevensbescherming Verenigde Staten

De Verenigde Staten beschikken niet over een algemeen toereikendheidsoordeel van de Commissie. Een dergelijk oordeel is moeilijk te geven omdat de Verenigde Staten geen samenhangend gegevensbeschermingsrecht kennen. Voor de publieke sector is er op federaal niveau de *Privacy Act of 1974*. Die wet heeft enkele elementen die ook in het EU-gegevensbeschermingsrecht herkenbaar zijn. De rechten die de wet toekent op inzage, correctie en toegang tot de rechtsbescherming kunnen alleen worden ingeroepen door Amerikaanse staatsburgers en vreemdelingen die rechtmatig hoofdverblijf in de VS houden. Voor de private sector is gegevensbescherming in de VS een onderdeel van het consumenten- en mededingingsrecht dat bovendien per sector verschilt. Het overheidstoezicht op de bescherming van persoonsgegevens is ook niet afzonderlijk geregeld. Ook dat is onderdeel van het toezicht dat op de desbetreffende sector wordt uitgeoefend. Er bestaat bovendien gegevensbeschermingsrecht op het niveau van de deelstaten.

1.2 Safe Harbour-beschikking

Het gegevensverkeer tussen de EU en de VS is omvangrijk als gevolg van de nauwe economische banden tussen de VS en Europa. Om dit verkeer te faciliteren is *beschikking van de Commissie nr. 2000/520/EG van 26 juli 2000 overeenkomstig Richtlijn 95/46/EG van het Europees parlement en de Raad betreffende de gepastheid van de bescherming geboden door de Veiligehavenbeginselen voor de bescherming van de persoonlijke levenssfeer en de daarmee verband houdende Vaak gestelde vragen, die door het Ministerie van Handel van de Verenigde Staten zijn gepubliceerd* (PbEG L 215) vastgesteld (hierna: beschikking). De beschikking maakt het mogelijk dat bedrijven die in de VS zijn gevestigd zich vrijwillig bij het *US Department of Commerce* aanmelden. Aanmelding houdt de belofte in dat het bedrijf zich conformeert aan de «Veiligehavenbeginselen» (*Safe Harbour principles*). Die beginselen weerspiegelen enkele beginselen van Europees gegevensverwerkingsrecht, zoals de transparantieverplichting, toestemming voor verdere verwerking, de verwerking van bijzondere persoonsgegevens, de beveiligingsplicht en de rechten van inzage en correctie. Overheidstoezicht is geïntegreerd in het toezicht dat de *Federal Trade Commission* of het *US Department of Transportation* op de desbetreffende sector uitoefent. Met nadruk wijs ik erop dat de beschikking alleen betrekking heeft op bedrijven en alleen betrekking heeft op bedrijven die in de VS zijn gevestigd. Bovendien zijn er sectoren uitgezonderd van de werking van de beschikking, zoals de telecommunicatie- en de luchtvaartsector. De beschikking is niet van toepassing op de verwerking van gegevens door de overheid, met inbegrip van politie, rechtshandhaving en de inlichtingendiensten. Als een bedrijf zich heeft aangemeld dan kunnen zonder aanvullende garanties persoonsgegevens uit de EU naar dat bedrijf in de VS worden doorge-

geven. Momenteel hebben zich meer dan 4000 ondernemingen aangemeld. Daaronder bevindt zich ook Facebook.

2. Arrest

2.1 Feiten

Schrems is gebruiker van Facebook. Daartoe heeft hij met Facebook Ireland Ltd. een gebruikersovereenkomst gesloten. Facebook Ireland verzorgt de Europese activiteiten van Facebook en is een dochteronderneming van Facebook Inc., gevestigd in de Verenigde Staten. Op grondslag van die overeenkomst worden persoonsgegevens van Schrems verwerkt. Onderdeel van die verwerking is doorgifte van de gegevens uit de EU naar de Verenigde Staten en opslag van de gegevens op servers in dat land. Naar aanleiding van de onthullingen van Edward Snowden over de ruime toegang die de inlichtingendiensten van de VS hebben tot gegevens van de gebruikers van diensten zoals die van Facebook, heeft Schrems een klacht ingediend bij de Ierse gegevensbeschermingstoezichthouder. Schrems heeft gesteld dat het recht van de Verenigde Staten onvoldoende daadwerkelijke bescherming biedt tegen de ruime toegang die de overheid heeft tot de verwerkte gegevens. De Ierse *Data Protection Commissioner* heeft de klacht afgewezen. Hij heeft zijn beslissing gemotiveerd met de stelling dat de klacht feitelijke grondslag mist omdat Schrems niet aannemelijk heeft gemaakt dat de inlichtingendiensten van de VS zich daadwerkelijk toegang hadden verschaft tot de gegevens die op Schrems betrekking hebben. De Commissioner heeft er ook op gewezen dat de beschikking een bindend oordeel geeft dat de VS voldoende waarborgen voor een passend niveau van gegevensbescherming bieden voor zover het verkeer van persoonsgegevens in overeenstemming met die beschikking plaatsvindt. De Commissioner oordeelde dat de beschikking hem de mogelijkheid ontzegde de klacht van Schrems op feitelijke juistheid te onderzoeken omdat hij zich moest conformeren aan dat oordeel.

2.2 Prejudiciële vragen

Schrems is tegen de beslissing van de Data Protection Commissioner in beroep gegaan bij het Ierse *High Court of Justice*. De Ierse rechter is, zakelijk weergegeven, op basis van het door Schrems overlegde bewijsmateriaal tot de vaststelling gekomen dat in de VS daadwerkelijk sprake is van een zeer ruime toegang van de overheid tot de door Facebook verwerkte gegevens. De rechter overwoog daarbij dat het doeleinde van die toegang, de bestrijding van criminaliteit en terrorisme, op zichzelf genomen legitiem is. Hij heeft echter ook overwogen dat de toegang tot de gegevens onevenredig groot was, dat de bij de toepassing van de bevoegdheden in acht te nemen waarborgen niet transparant zijn, en dat burgers van de EU geen rechtsbescherming in de VS wordt geboden wanneer de op hen betrekking hebbende gegevens aan de overheid worden verstrekt. Omdat het Schrems in feite niet om de bevoegdheden van de Commissioner te doen is maar om de rechtmatigheid van de beschikking in het licht van de onthullingen van Snowden, overweegt de rechter dat die laatste vraag moet worden beantwoord. De rechter wijst erop dat nadat de beschikking totstandgekomen is het Handvest van de Grondrechten (HvdG) bindende kracht heeft gekregen. Artikel 7 HvdG garandeert de burger het recht op bescherming van het privéleven en artikel 8 HvdG garandeert het recht op bescherming van persoonsgegevens. De rechter acht het zeer de vraag of de beschikking met de artt. 7 en 8 HvdG verenigbaar is, gegeven de ruime toegang van de overheid van de VS tot de gegevens en het gebrek aan waarborgen en adequate rechtsbescherming. De rechter heeft daarom het HvJEU de vraag

voorgelegd of de beschikking terecht de Commissioner de bevoegdheid ontnam de klacht van Schrems te onderzoeken, gezien de waarschijnlijkheid dat de beschikking niet in overeenstemming is met de artikelen 7 en 8 HvdG.

2.3 Uitspraak

2.3.1 Verhouding bevoegdheden Commissie en bevoegdheden toezichthouders

Het HvJEU wijst er allereerst op dat art. 8, derde lid, HvdG en artikel 16 VWEU verplichten tot het garanderen van het recht op bescherming van persoonsgegevens in de Unie en dat het toezicht op de naleving van de regels die dit grondrecht uitwerken wordt opgedragen aan onafhankelijke toezichthouders. De toezichthouders moeten op grond van artikel 28 van de richtlijn zijn toegerust met onderzoeks- en sanctiebevoegdheden om die taken te kunnen uitvoeren. Die bevoegdheden kunnen zij slechts op het eigen grondgebied uitoefenen. Niettemin is de doorgifte van gegevens naar een derde land een onderdeel van het begrip verwerking van persoonsgegevens en kunnen de bevoegdheden van de toezichthouder zich uitstrekken tot de vraag of de doorgifte in overeenstemming is met de richtlijn. Het HvJEU wijst erop dat de artikelen 25 en 26 van de richtlijn een stelsel in het leven roepen dat de Commissie in staat stelt bindende besluiten vast te stellen met de strekking dat een derde land een toereikend niveau van gegevensbescherming kent. Die besluiten zijn geldig zolang de geldingsduur niet is verstreken, zij niet zijn ingetrokken of door het HvJEU nietig of ongeldig zijn verklaard. Artikel 28 van de richtlijn voorziet niet in een uitzondering op de regel dat het toezicht op gegevensbescherming zich uitstrekt over alle aspecten van het verwerken van persoonsgegevens met inbegrip van het doorgeven van persoonsgegevens aan een derde land. Zou dat anders zijn dan zou aan betrokkenen het recht, gegarandeerd door artikel 8 HvdG, worden ontzegd om de verenigbaarheid van de verwerking met artikel 8 HvdG te onderzoeken. Alleen al daarom kan een toereikendheidsoordeel van de Commissie niet aan een nationale toezichthouder de bevoegdheid ontnemen om de verenigbaarheid van een gegevensverwerking die mede bestaat in de doorgifte van gegevens naar een derde land te toetsen aan het HvdG en de richtlijn en zo nodig handhavingsmaatregelen te treffen.

2.3.2 Toegang toezichthouders tot de rechter

Het HvJEU voegt daar nog enkele belangrijke overwegingen aan toe. Een nationale toezichthouder is niet bevoegd een besluit van de Commissie nietig of ongeldig te verklaren. Die bevoegdheid is alleen voorbehouden aan het HvJEU. Om het HvJEU in staat te stellen zijn bevoegdheden uit te oefenen, moet verzekerd zijn dat tegen besluiten van toezichthouder beroep op de nationale rechter openstaat, en dat de toezichthouder in staat is zelf toegang tot de rechter te zoeken. De nationale rechter is in staat een zaak naar het HvJEU te verwijzen voor een prejudiciële beslissing.

2.3.3 Betekenis van een passend niveau van gegevensbescherming

Het HvJEU toetst vervolgens of de stellingen van Schrems en de overwegingen van de Ierse rechter over het niveau van gegevensbescherming in de VS consequenties hebben voor de beschikking. Het HvJEU beoordeelt of de beschikking in overeenstemming is met de artikelen 25 en 26 van de richtlijn, gelezen in het licht van art. 8 HvdG. Het gaat er volgens het HvJEU om te beoordelen of het niveau van gegevensbescherming dat de beschikking biedt «passend» is in de zin van artikel

25, eerste lid, van de EU-privacyrichtlijn. «Passend» betekent volgens het HvJEU niet noodzakelijkerwijs hetzelfde als identiek aan het Unierecht, maar het desbetreffende land moet op grond van de eigen wetgeving en de internationaalrechtelijke verplichtingen die het is aangegaan een beschermingsniveau van de fundamentele rechten en vrijheden bieden dat gelijkwaardig is aan het niveau dat Unie garandeert in de richtlijn. Anders zou het niveau dat Unie biedt eenvoudig kunnen worden ontgaan door gegevensverwerkingen in het derde land te vestigen dat een dergelijk niveau niet biedt. De Commissie moet daarom bij de beoordeling van het beschermingsniveau een oordeel geven over het interne recht van het derde land en zij moet bovendien dat oordeel met regelmatige tussenpozen evalueren om rekening te houden met veranderingen in de omstandigheden die zich van tijd tot tijd voordoen. Daarbij moet bovendien rekening worden gehouden met de omstandigheden, zoals de effecten van inbreuken op de bescherming van gegevens op de bescherming van het privéleven als geheel en het aantal datasubjecten dat daardoor wordt geraakt.

2.3.4 Doorwerking van het Handvest voor de Grondrechten in toereikendheidsoordelen

Het Safe Harbour-regime berust in wezen op zelfregulering. Dit is volgens het HvJEU op zichzelf niet onverenigbaar met de richtlijn. Het HvJEU wijst er echter op dat het Safe Harbour-regime alleen van toepassing is op in de VS gevestigde bedrijven en niet op overheidsorganisaties in de VS. Bovendien is de zelfregulering als zodanig, blijkens artikel 1 van de beschikking, de enige normering waaraan de Commissie het niveau van gegevensbescherming heeft getoetst. De interne wetgeving van de VS en de internationaalrechtelijke verplichtingen zijn daarbij niet betrokken. Uit Annex I, § 4, van de beschikking blijkt bovendien dat de wetgeving van de VS voorrang heeft boven het Safe Harbour-regime en dat toepassing van dat regime wordt beperkt door de vereisten van nationale veiligheid, publieke belangen of de belangen van de rechtshandhaving. Het HvJEU concludeert dat inmenging in de grondrechten van datasubjecten door de autoriteiten in de VS mogelijk is. Het HvJEU acht dit op zichzelf genomen legitieme gronden voor een inmenging. De beschikking vermeldt echter niet aan welke beperkingen die inmenging is onderworpen en ook niet welke rechtsbescherming daartegen openstaat. Het HvJEU wijst erop dat Commissie in een aantal uit 2013 daterende mededelingen zelf de conclusie had getrokken dat de autoriteiten in de VS in staat zijn zich toegang te verschaffen tot de persoonsgegevens en deze verder te verwerken op een wijze die niet verenigbaar is met het doel van de doorgifte en verder ging dan strikt noodzakelijk voor de bescherming van de nationale veiligheid. Ook heeft de Commissie geconstateerd dat er voor datasubjecten geen toegang tot een rechterlijke of administratieve voorziening openstaat om de rechten op inzage, correctie en wissing uit te oefenen.

2.3.5 Toetsing van artikel 1 van de Safe Harbour-beschikking

Het HvJEU wijst erop dat naar Unierecht een regeling niet beperkt is tot het strikt noodzakelijke wanneer zij algemeen toestaat dat alle persoonsgegevens van alle personen van wie het betreft naar een derde land worden doorgegeven en bewaard zonder dat enig onderscheid wordt gemaakt, enige beperking wordt gesteld of enige uitzondering wordt gemaakt op grond van het nagestreefde doel zonder te voorzien in objectieve criteria ter begrenzing van de toegang van de autoriteiten en het later gebruik ervan. Een zodanig veralgemeende toegang van de autoriteiten tot de inhoud van elektronische communicatie moet, aldus het HvJEU, worden beschouwd als een aantasting van de wezenlijke

inhoud van het grondrecht op bescherming van de eerbiediging van het privéleven. Wanneer elke beroepsmogelijkheid voor de justitiabelen ontbreekt om de rechten op toegang, correctie of wissing in te roepen is bovendien de wezenlijke inhoud van het grondrecht op een effectieve voorziening in rechte aangetast. Een dergelijk niveau van gegevensbescherming oordeelt het HvJEU niet «passend» in de zin van artikel 25 van de richtlijn. Artikel 1 van de beschikking, waarin het toereikendheidsoordeel wordt gegeven, is daarom niet in overeenstemming met artikel 25 van de richtlijn.

2.3.6 Toetsing van artikel 3 van de Safe Harbour-beschikking

Het HvJEU wijst er ook op dat artikel 3 van de beschikking een beperking van de toetsingsmogelijkheden van de nationale toezichthouders inhoudt, doordat zij naast de bevoegdheden die zij slechts op hun nationale grondgebied kunnen uitoefenen, alleen de doorgiften onder het Safe Harbour-regime kunnen opschorten wanneer die niet of niet langer in overeenstemming met het Safe Harbour-regime zouden plaatsvinden. Dat sluit uit dat datasubjecten de verenigbaarheid van het Safe Harbour-regime met hoger recht zouden kunnen laten toetsen. Artikel 3 van de beschikking is daarom ook niet in overeenstemming met artikel 25 van de richtlijn.

2.3.7 Ongeldigheid beschikking

Op deze vaststellingen baseert het HvJEU het oordeel dat de beschikking ongeldig is. Het HvJEU verklaart verder voor recht dat een besluit van de Commissie op grond artikel 25 van de richtlijn, gelezen in het licht van de artikelen 7, 8 en 47 HvdG, de nationale toezichthouders niet afdoet aan de verplichting van nationale toezichthouders om klachten van belanghebbenden over de bescherming van zijn rechten en vrijheden in het land waarop de beschikking betrekking heeft te onderzoeken. Het belet hun evenmin de wettelijke onderzoeksbevoegdheden te gebruiken bij dat onderzoek. Het is nu aan de Ierse toezichthouder de klacht met voortvarendheid en zorgvuldigheid te onderzoeken en te beslissen of de doorgifte van gegevens van abonnees van Facebook naar de VS moet worden opgeschort.

3. Eerste beoordeling van de uitspraak

De uitspraak van het HvJEU past in een reeks van uitspraken waarin aan het belang van het grondrecht op bescherming van persoonsgegevens en het grondrecht op bescherming van het privéleven een bijzonder zwaar gewicht wordt toegekend in relatie tot andere belangen. Eerder oordeelde het HvJEU dat deze rechten zwaarder wogen dan het belang van de openbaarheid bij het verstrekken van landbouwsubsidies (C-92/09 en C-93/09, Volker en Markus Schecke en Eifert), het belang van de overheid bij het bewaren van verkeersgegevens door telecommunicatiebedrijven (C-293/12 en C-594/12, Digital Rights Ireland Ltd en Kärntner Landesregierung e.a.) of het belang van de vrijheid van ondernemerschap voor zoekmachine-exploitanten en de vrijheid van informatiegaring (C-131/12, Google Spain SL en Google Inc.). In laatstgenoemde twee zaken heeft het HvJEU bovendien al geoordeeld dat het HvdG het toetsingskader is voor alle bindende EU-besluiten, ook wanneer die besluiten dateren van voor de totstandkoming van het HvdG.

Een aantal aspecten van de uitspraak vallen op. Het HvJEU laat het systeem van de beoordeling van de toereikendheid van het recht van derde landen als zodanig in stand. Ook een systeem van zelfregulering dat een derde land kan bieden, ziet het HvJEU niet als prohibitief. Het HvJEU

heeft niet een rechtstreeks oordeel gegeven over het niveau van gegevensbescherming in de VS, maar is afgegaan op de vaststellingen door de Ierse rechter en hetgeen door de Commissie in mededelingen uiteengezet is. Maar uit de uitspraak volgt wel dat een beoordeling van het recht van het derde land ook inhoudt dat de Commissie zich een beeld moet vormen van het gehele stelsel van wettelijke bevoegdheden van derde landen. Dat is met inbegrip van de bevoegdheden om ten behoeve van de nationale veiligheid inbreuk te kunnen maken op het recht op bescherming van persoonsgegevens. Dat is een opvallend oordeel omdat nationale veiligheid de verantwoordelijkheid van de lidstaten is (art. 4, tweede lid, VEU en art. 72 VWEU). Naast de toepasselijke regels moet de Commissie ook de praktijk waarmee de regels worden uitgevoerd en gehandhaafd beoordelen om vast te stellen of sprake is van een passend beschermingsniveau. Verder valt op dat in het arrest geen aandacht uitgaat naar de consequenties van de ongeldigverklaring voor burgers en bedrijven. Uit de overwegingen blijkt niet of die consequenties op enigerlei wijze door het HvJEU zijn meegewogen in de beslissing. Het HvJEU heeft ook geen rechterlijk overgangsrecht vastgesteld om de gevolgen van de ongeldigverklaring te regelen.

4. Consequenties van de uitspraak

4.1 Feitelijke consequenties

De onmiddellijke consequentie van de uitspraak is dat een belangrijke rechtsgrondslag voor de doorgifte van gegevens uit de Unie naar de VS is komen te vervallen. Het moet ervoor worden gehouden dat de doorgiften op grond van de beschikking niet alleen niet langer rechtmatig zijn, maar in beginsel ook in het verleden onrechtmatig zijn geweest. Tot hoever dit terugwerkt is, mede omdat het HvJEU hieraan geen overwegingen heeft gewijd, onduidelijk. Wel is duidelijk dat de uitspraak lasten veroorzaakt voor de bedrijven die van de beschikking gebruik maken of daarvan gebruik hadden willen maken. De ontstane rechtsonzekerheid en de stijging van de nalevingskosten die het gevolg van de uitspraak zijn, zijn de oorzaken van de zorg die ik over het arrest heb uitgesproken.

Aan Amerikaanse zijde betreft het de meer dan 4000 bedrijven die zich bij het *US Department of Commerce* hebben ingeschreven. Hoeveel bedrijven het in Europa of Nederland betreft is onduidelijk. Voor die bedrijven geldt immers geen specifiek op Safe Harbour gerichte meld- of inschrijfplicht. Omdat er vanaf 2012 een vrijstelling van de meldplicht bestaat voor doorgiften krachtens de beschikking, is het niet mogelijk met behulp van het meldingenregister van het Cbp na te gaan hoeveel bedrijven gegevens op de grondslag van Safe Harbour naar de VS doorgeven. Nederland heeft net als de Commissie en enkele andere lidstaten dit probleem zien aankomen. Daarom is al in 2014 aan het bedrijfsleven gevraagd naar de mogelijke consequenties van een eventuele opschorting van de beschikking. Uit het antwoord is helaas geen afgerond beeld naar voren gekomen. Voldoende duidelijk is dat het voor een betrekkelijk klein aantal grote bedrijven betrekkelijk grote consequenties heeft. Dat zijn vooral de grote bedrijven in de ICT-sector. De kans bestaat echter dat juist het midden- en kleinbedrijf betrekkelijk zwaar getroffen kan worden. Het is voor grote bedrijven minder bezwaarlijk om zich te voorzien van kostbare juridische en technische bijstand om overeenkomsten met Amerikaanse zakenpartners op te stellen die voldoen aan de eisen van de richtlijn, of om intern bindende bedrijfsvoorschriften op te stellen. Een van de aantrekkelijke kanten van het Safe Harbour-regime vanuit handelsoptiek was nu juist dat persoonsgegevens zonder aanvullende garanties naar Amerikaanse bedrijven konden worden doorgegeven. Deze verlaagde drempel voorkwam aanvullende nalevings-

kosten. Die lagere kosten kunnen juist voor een kleiner bedrijf de doorslaggevende factor zijn voor het uitbreiden van de activiteiten naar de VS. Navraag bij andere lidstaten leert dat het overal moeilijk is een zelfs maar enigszins afgerond beeld van de kosten te krijgen. Er is geen centrale registratie van bedrijven die gegevens naar de VS doorgeven. Bedrijven zijn bovendien terughoudend met het doen van mededelingen over vertrouwelijke zakelijke aangelegenheden.

4.2 Alternatieve grondslagen

Zolang geen instrument op Unieniveau bestaat dat de beschikking kan vervangen, dienen bedrijven zich te beraden op alternatieve grondslagen voor de doorgifte van gegevens naar de VS. De voor bedrijven meest voor de hand liggende alternatieven zijn:

– De doorgifte is noodzakelijk voor de uitvoering van een overeenkomst tussen de betrokkene en de verantwoordelijke, of voor het totstandkomen daarvan.
– De doorgifte vindt plaats op grond van een door de Commissie goedgekeurde modelcontractsbepaling die bepaalde waarborgen biedt.
– De doorgifte vindt plaats met toepassing van intern bindende bedrijfsvoorschriften (*Binding Corporate Rules*). Deze regelingen worden door bedrijven die in concernverband georganiseerd zijn en vennootschapsrechtelijke vestigingen hebben buiten de EU zelf vastgesteld. Daarmee ontstaat een eigen interne privacycode die geldt voor het hele concern. Die regelingen moeten echter worden goedgekeurd door alle betrokken nationale toezichthouders. Daarbij worden Europese toetsingsnormen gehanteerd.
– De doorgifte vindt plaats krachtens een grondslag die het nationaal recht biedt. In Nederland is dat een vergunning van de Minister van Veiligheid en Justitie op grond van art. 77, tweede lid, van de Wbp.

Minder voor de hand liggend is toestemming van de betrokkene. De richtlijn laat ook voldoende ruimte voor een beoordeling van het passend beschermingsniveau door de verantwoordelijke zelf. Op enkele consequenties van deze keuzes wordt in het onderstaande teruggekomen. Welke keuze ook wordt gehanteerd, altijd moet worden bedacht dat de autoriteiten van de VS over ruime mogelijkheden beschikken om ten behoeve van de rechtshandhaving of de nationale veiligheid gegevens te vorderen van degene die daarover de feitelijke beschikking heeft en zich binnen de rechtsmacht van de VS bevindt. Dat kan doordat het bedrijf waaraan de gegevens zijn doorgegeven in de VS is gevestigd, of deel uitmaakt van een vennootschapsrechtelijke groep met een vertakking in de VS. Dat geldt doorgaans ook voor de gevallen waarin de gegevens worden verwerkt op servers die zich buiten de VS bevinden. Ook wanneer de gegevens zich op servers in de VS bevinden zonder dat er sprake is van rechtstreekse vennootschapsrechtelijke of contractuele banden kunnen vorderingsbevoegdheden worden uitgeoefend. De uitspraak van het HvJEU verandert hieraan niets.

5. Mogelijke oplossingen

5.1 Oplossingen op EU-niveau

Met de uitspraak van het HvJEU is een besluit van de Commissie ongeldig verklaard. Het ligt daarmee voor de hand dat de oplossing van het probleem een nieuwe rechtmatige grondslag te creëren of een andere grondslag aan te wijzen allereerst op Europees niveau moet worden gezocht.

De Commissie heeft zich in een eerste reactie als volgt over het arrest uitgelaten. De Commissie wijst erop dat de uitspraak van het HvJEU een oordeel van de hoogste rechter op Unieniveau is en als zodanig moet worden uitgevoerd. De Commissie ziet het arrest verder als een steun in de rug voor de al lopende onderhandelingen met de VS over een vernieuwd Safe Harbour-regime. Daarnaast zal de Commissie op zeer korte termijn met de gezamenlijke toezichthouders uit de lidstaten (de Artikel 29 Werkgroep) gaan overleggen over aanbevelingen voor de tussenliggende periode. Tenslotte zal de Commissie op zeer korte termijn op hoog niveau met het georganiseerde bedrijfsleven spreken over de ontstane situatie. Dat laatste gesprek heeft inmiddels plaatsgevonden. Concrete mededelingen zijn daarover niet gedaan. Ik ga op de andere punten in het onderstaande in.

5.1.1 Nieuwe Safe Harbour-beschikking

Het HvJEU heeft in zijn arrest nadrukkelijk gewezen op de verplichting van de Commissie om eenmaal vastgestelde toereikendheidsoordelen regelmatig te evalueren, omdat de situatie in het desbetreffende land van tijd tot tijd verandert. De Safe Harbour-beschikking is, voor zover mij bekend, ten minste twee maal geëvalueerd. De Commissie heeft de evaluatierapporten echter niet bekendgemaakt en evenmin willen delen in het daarvoor aangewezen Comité, het zogenaamde Artikel 31 Comité. Naar aanleiding van vragen van het lid van uw Kamer Gesthuizen (Aanhangsel Handelingen II 2010/11, 828) is in dat Comité herhaalde malen aangedrongen op het bekendmaken van deze rapporten. De Commissie heeft daaraan geen gehoor willen geven.
Eerst na de onthullingen van Edward Snowden heeft de Commissie twee mededelingen gedaan over, respectievelijk, het «Herstel van vertrouwen in de EU-VS gegevensstromen», COM (2013) 846 en de «Werking van de veiligehavenregeling («Safe Harbour») uit het oogpunt van EU-burgers en in de EU gevestigde bedrijven», COM (2013) 847. Uw Kamer is daarover geïnformeerd bij brief van de Minister van Buitenlandse Zaken van 17 januari 2014 (Kamerstuk 22 112, nr. 1777). De in deze mededelingen aangekondigde herziening van de Safe Harbour-beschikking heeft de steun gekregen van de toenmalige Staatssecretaris van Veiligheid en Justitie en van uw Kamer. In de mededeling betreffende de Safe Harbour-beschikking somt de Commissie 13 verbeterpunten op. Twee daarvan betreffen de toegang van de Amerikaanse autoriteiten in het belang van de nationale veiligheid, het openbaar belang en de opsporing van strafbare feiten. De Commissie meent dat bedrijven die met vorderingen tot het verstrekken van gegevens worden geconfronteerd moeten worden aangemoedigd daarover een zekere mate van openbaarheid te verschaffen. Verder meent de Commissie dat de autoriteiten zelf die toegang moeten beperken tot de gevallen waarin daartoe een dringende noodzaak bestaat en dit overigens proportioneel is.
De al sinds einde 2013 lopende onderhandelingen hebben volgens de Commissie in zoverre resultaat gehad dat er uitzicht is op verbetering op alle punten van inhoudelijke aard. Echter, over de twee punten betreffende de nationale veiligheid moeten de gesprekken inhoudelijk nog beginnen. De Commissie ziet de uitspraak van het HvJEU als een belangrijke stimulans om die gesprekken te versnellen. De Commissie heeft inmiddels bekendgemaakt de onderhandelingen op technisch en politiek niveau voort te zetten. Uitvoering van dat voornemen is inmiddels ter hand genomen en ook op het werkprogramma van de Commissie voor 2016 geplaatst. Waar het lid van uw Kamer Van Wijngaarden in het algemeen overleg van 7 oktober 2015 vroeg naar kansen voor een betere gegevensbescherming, meen ik dat die liggen in de voortzetting en spoedige afronding van deze onderhandelingen. Ik meen dat een nieuw Safe Harbour-regime dat voldoet aan de uitgangspunten die de

Commissie in 2013 heeft geformuleerd bijdraagt aan verbetering van het niveau van gegevensbescherming dat Europese burgers momenteel hebben. Het vertrouwen in de diensten die bedrijven in de VS bieden kan daarmee groeien. Dat vertrouwen is een belangrijke factor bij de groei van de digitale economie.
Op ambtelijk niveau is er inmiddels door mijn ministerie gesproken met een vertegenwoordiger van het *US Department of Commerce* en daar is die boodschap ook uitgesproken. Ik zal de kwestie mijnerzijds binnenkort met de Amerikaanse regering bespreken tijdens mijn bezoek aan de VS. Ik wijs er echter op dat het onvermijdelijk is dat de Commissie het hele onderhandelingsdossier nu opnieuw moet beoordelen in het licht van het arrest. Verder valt niet te verwachten dat de onderhandelingen met de VS op zeer korte termijn zijn afgerond.

5.1.2 Andere maatregelen op EU-niveau

De Commissie heeft er terecht op gewezen dat het arrest geen einde maakt aan het rechtmatig gegevensverkeer tussen de Unie en de VS. De richtlijn biedt daarvoor andere grondslagen. In het bovenstaande is daarvan al een overzicht gegeven. Het is echter zo dat na de ongeldigverklaring van de beschikking rechtsonzekerheid is ontstaan en dat het tijd vergt om passende contracten of binding corporate rules op te stellen. De toezichthouders zullen voor de tussenliggende periode moeten vaststellen hoe zij willen omgaan met het inmiddels onrechtmatig geworden gegevensverkeer. Daarover vindt thans beraad plaats tussen de Commissie en de toezichthouders. Dat beraad moet leiden tot een gedragslijn die in de hele Unie gevolgd kan worden. Dat lijkt mij de best denkbare weg. De toezichthouders zijn zowel ieder afzonderlijk als verenigd in de Artikel 29 Werkgroep onafhankelijk. Ik heb bij dat beraad geen betrokkenheid. Uit een eerste verklaring van 16 oktober 2015 blijkt dat de Artikel 29 Werkgroep de eerste oplossing ziet in onderhandelingen tussen lidstaten en de EU enerzijds en de VS anderzijds. Op de positie van de lidstaten kom ik hieronder nog terug.
Op grond van artikel 26, vierde lid, van de richtlijn kan de Commissie modelbepalingen voor contracten vaststellen. Deze bepalingen bevatten de nodige waarborgen voor de persoonlijke levenssfeer die bij doorgiften in acht moeten worden genomen. De Commissie heeft bepalingen voor contracten tussen verantwoordelijken onderling en in contracten tussen verantwoordelijken en bewerkers vastgesteld. Wanneer een contract de passende bepalingen bevat, dan kunnen persoonsgegevens zonder aanvullende garanties aan het derde land worden doorgegeven. Zolang de besluiten van de Commissie geldig zijn, zijn deze voorwaarden naar mijn mening een rechtmatige grondslag voor de doorgifte. De Werkgroep heeft zich in evenbedoelde verklaring ook op dat standpunt gesteld. De Werkgroep merkt zowel de modelcontractbepalingen als binding corporate rules vooralsnog aan als bruikbare alternatieven. De Werkgroep zet haar analyse van de alternatieven echter voort. Indien eind januari 2016 nog geen bruikbare oplossing met de VS is bereikt acht de werkgroep de weg vrij voor noodzakelijk en gepast handelen, waaronder gecoördineerde handhavingsacties. Volledigheidshalve meld ik nog dat de toezichthouder van de Duitse deelstaat Sleeswijk-Holstein zich sinds 14 oktober 2015 op het standpunt stelt dat doorgiften van gegevens krachtens de genoemde modelbepalingen na het arrest voor onrechtmatig moeten worden gehouden. Bij gebruik van deze voorwaarden stelt deze toezichthouder boetes in het vooruitzicht.

5.2 Mogelijke oplossingen op nationaal niveau

Zoals hierboven uiteengezet, bestaan er voor doorgiften krachtens de beschikking enige alternatieven. Enkele van die alternatieven verdienen in de Nederlandse context enige aandacht. De artikelen 25 en 26 van de richtlijn zijn in de artikelen 76, 77 en 78 van de Wet bescherming persoonsgegevens (Wbp) op specifieke wijze geïmplementeerd.

Artikel 76, eerste lid, van de Wbp gaat er vanuit dat het primair aan de verantwoordelijke zelf is zich een oordeel te vormen over het niveau van gegevensbescherming in het derde land waarnaar hij gegevens wil overbrengen. De richtlijn biedt daartoe de ruimte. Het is daarom onder het geldende recht nog mogelijk een dergelijke verantwoordelijkheid te nemen. Toegegeven moet worden dat deze mogelijkheid voor doorgiften naar de VS sinds het arrest niet aantrekkelijker voor bedrijven is geworden.

Lidstaten hebben niet de mogelijkheid om een derde land zelf aan te merken als land met een passend niveau van gegevensbescherming. Dat zou ingaan tegen de harmonisatiedoelstelling van de richtlijn. Wel kan op grond van artikel 25, tweede lid, van de richtlijn toestemming voor een afzonderlijke individuele doorgifte of categorie doorgiften worden verleend. Deze regel is geïmplementeerd in artikel 77, tweede lid, van de Wbp. Die bepaling verleent mij de bevoegdheid tot het verlenen van een vergunning voor de doorgifte van gegevens naar een derde land dat geen voldoende waarborgen voor een passend beschermingsniveau biedt. Dergelijke vergunningen worden uitsluitend na een positief advies van het Cbp verleend. Aan de vergunning worden voorwaarden verbonden ten behoeve van de bescherming van de persoonlijke levenssfeer en de fundamentele rechten en vrijheden. Het aantal vergunningen dat wordt verleend fluctueert sterk. Op jaarbasis gaat het om 60 tot 130 vergunningen per jaar. Ik houd er rekening mee dat als gevolg van het arrest het aantal vergunningaanvragen zal stijgen. Het is vooralsnog onduidelijk in welke mate.

Een specifieke toepassing van de verlening van vergunningen is vergunningverlening voor intern bindende bedrijfsvoorschriften. Dergelijke vergunningen worden tot dusverre verleend aan verantwoordelijken. Die kunnen dan binnen een vennootschapsrechtelijke groep gegevens naar de verbonden vestigingen in derde landen overbrengen. Uit het bedrijfsleven is al voor het arrest de vraag gesteld naar de mogelijkheid om deze vergunningen ook aan bewerkers te kunnen verlenen, overigens onder het stellen van voorwaarden voor de bescherming van de persoonlijke levenssfeer. Bewerkers bieden hun diensten aan vele verantwoordelijken op een bovennationale schaal aan, zodat dergelijke vergunningen de lasten potentieel aanmerkelijk kunnen verlagen voor het bedrijfsleven. Het is niet uitgesloten dat deze vergunningen ook een oplossing kunnen bieden voor de gevolgen van het verval van de beschikking. Ik ben dan ook voornemens om in samenspraak met het Cbp en het bedrijfsleven beleidsregels op te stellen voor de verlening van deze vergunningen. De materie is technisch ingewikkeld, zodat daar enige tijd mee gemoeid is.

Tenslotte kent artikel 78, vierde lid, van de Wbp nog een regeling voor de opschorting van de doorgifte van gegevens naar derde landen in afwijking van een bestaand toereikendheidsoordeel. Toepassing van deze bepaling is niet meer aan de orde. De beschikking is door het HvJEU immers al ongeldig verklaard.

De Artikel 29 Werkgroep wijst op de noodzaak van overleg tussen de lidstaten en de VS. De Werkgroep noemt lidstaten zelfs primair als gesprekspartners, voor de EU-instellingen. Als gezegd, lidstaten hebben onder de richtlijn slechts beperkte bevoegdheden tot het nemen van besluiten. Teveel eigen actie van de lidstaten zou de harmonisatie niet bevorderen. In het voorgaande ben ik al ingegaan op de mogelijkheden die ik in het bilateraal overleg met de VS zal benutten.

6. Consequenties voor de wetgeving

6.1 Wetgeving op EU-niveau

Het ligt voor de hand dat de Commissie zal nagaan of het arrest gevolgen heeft voor andere toereikendheidsoordelen. De Commissie heeft zich daarover nog niet uitgelaten. Ik zie daar op dit moment ook geen aanwijzingen voor. Mocht de Commissie vaststellen dat er wel consequenties zijn, dan moet zij volgens artikel 25, vijfde lid, van de richtlijn met het desbetreffende derde land onderhandelingen openen om een geconstateerd gebrek te herstellen.

Op dit moment is de Algemene verordening gegevensbescherming onderwerp van onderhandeling in de triloog. In september 2015 is op het hoofdstuk voor de doorgifte naar derde landen een voorlopige consensus bereikt tussen Raad en Europees parlement. Dat akkoord is goeddeels gebaseerd op het voorstel dat in 2012 door de Commissie is ingediend. Dat voorstel reflecteert de eerdergenoemde artikelen 25 en 26 van de richtlijn. De kans is niet uitgesloten dat het akkoord moet worden opengebroken als gevolg van het arrest. Ik zal uw Kamer over eventuele ontwikkelingen terzake berichten in de kwartaalrapportages over het verloop van de onderhandelingen.

Het arrest heeft vooralsnog geen gevolgen voor het onlangs door de Commissie en de VS geparafeerde parapluverdrag. Ik informeerde uw Kamer daarover in mijn brief van 1 oktober 2015 (Kamerstukken II 2015/16, 32 761, nr. 87). Dat verdrag bevat bepalingen van gegevensbeschermingsrecht die toepassing vinden bij de uitoefening van Uniebevoegdheden op het gebied van de justitiële en politiële samenwerking in de zin van het VWEU. Dat betreft bij uitstek een regeling voor de publieke sector. De Safe Harbour-beschikking bevat een regeling die uitsluitend toepassing vindt in de private sector.

Het arrest heeft vooralsnog ook geen gevolgen voor enige specifieke verdragen die door de EU met de VS zijn gesloten waarin de VS zijn aangemerkt als een derde land met een passend beschermingsniveau voor enkele specifieke doorgiften. Het betreft de verdragen inzake passagiersgegevens (PNR) en gegevens betreffende het betalingsverkeer (TFTP). Beide verdragen bevatten specifieke waarborgen voor de persoonlijke levenssfeer.

6.2 Wet bescherming persoonsgegevens

In artikel 28, derde lid, derde gedachtestreepje, van de richtlijn is geregeld dat toezichthouders de bevoegdheid moeten hebben «om in rechte op te treden in geval van inbreuken op ter uitvoering van de richtlijn vastgestelde bepalingen, of om die inbreuken onder de aandacht van het gerecht te brengen». Een gelijkluidende bepaling is opgenomen in artikel 2, eerste lid, Additioneel Protocol bij het op 28 januari 1981 te Straatsburg totstandgekomen Verdrag tot bescherming van personen met betrekking tot de geautomatiseerde verwerking van persoonsgegevens (Trb. 2003, 122).

Het eerste zinsdeel van die bepaling is geïmplementeerd in de artikelen 61 en 66 van de Wbp. Die bepalingen kennen het Cbp bestuursrechtelijke handhavingsbevoegdheden toe. Tegen besluiten van het Cbp staat krachtens de Algemene wet bestuursrecht bezwaar en beroep open. Het laatste zinsdeel van het artikelonderdeel is tot dusverre zodanig geïnterpreteerd dat het Cbp via het doen van aangifte bij het openbaar ministerie de meest ernstige overtredingen van de Wbp via de strafrechtelijke weg aan de rechter kan voorleggen.

Uit rechtsoverweging 65 van het arrest volgt echter dat die uitleg niet meer voldoende is. Eventuele strijdigheid van toereikendheidsoordelen met hoger recht moet niet slechts via het beroep tegen een besluit over een handhavingsklacht aan de nationale rechter kunnen worden voorgelegd, oordeelt het HvJEU. Het HvJEU legt evengenoemde bepaling zodanig uit dat toezichthouders ook de rechter ambtshalve moeten kunnen benaderen als zij gerede twijfel over de rechtmatigheid van het handelen van de Commissie hebben. De nationale rechter kan dan beslissen of er reden is de desbetreffende zaak naar het HvJEU te verwijzen, omdat alleen het HvJEU bevoegd is bindende EU-besluiten ongeldig te verklaren.

Dat betekent dat een voorziening moet worden getroffen om dit mogelijk te maken. Daartoe moet de Wbp worden aangepast. Ik zal daarover in overleg met het Cbp treden.

Tenslotte is in artikel 44, aanhef en onder d, van het Vrijstellingsbesluit Wbp geregeld dat vrijstelling van meldplicht van artikel 27 Wbp bestaat voor verantwoordelijken die gegevens doorgeven naar de VS op grond van de Safe Harbour-beschikking. Die vrijstelling is in 2012 in het kader van de vermindering van de administratieve lastendruk voor bedrijven ingevoerd. Die vrijstelling zal moeten ingetrokken.

De Minister van Veiligheid en Justitie,
G.A. van der Steur