

Vergaderjaar 2010–2011

**32 554**

**Wijziging van de Wet politiegegevens en van de Wet justitiële en strafvorderlijke gegevens in verband met de implementatie van het kaderbesluit van de Raad van de Europese Unie 2008/977/JBZ over de bescherming van persoonsgegevens die worden verwerkt in het kader van de politieke en justitiële samenwerking in strafzaken en de implementatie van het Besluit van de Raad 2009/371/JBZ van 6 april 2009 tot oprichting van de Europese politiedienst (Europol)**

**Nr. 6**

**NOTA NAAR AANLEIDING VAN HET VERSLAG**

Ontvangen 15 juni 2011

Met veel belangstelling heb ik kennis genomen van het uitgebreide verslag van de vaste commissie voor Veiligheid en Justitie over dit wetsvoorstel. Ik hecht veel waarde aan de bescherming van persoonsgegevens. Dit kan ook blijken uit het feit dat in het Regeerakkoord, getiteld «Vrijheid en verantwoordelijkheid», verschillende maatregelen zijn aangekondigd ter verbetering van de informatieveiligheid en de bescherming van persoonsgegevens. Gelet op het grote aantal vragen en opmerkingen is het verheugend te constateren dat gegevensbescherming ook door de leden van de aan het woord zijnde fracties van belang wordt geacht. Ik hoop de gestelde vragen en ingebrachte opmerkingen dan ook naar volle tevredenheid te kunnen beantwoorden. Omwille van de overzichtelijkheid is bij de beantwoording van de vragen en opmerkingen de volgorde van het verslag aangehouden. Van de gelegenheid is gebruik gemaakt om, mede naar aanleiding van een vraag van de leden van de VVD-fractie over artikel I, onderdeel H, een nota van wijziging aan te bieden.

**I. Inleiding**

De leden van de VVD-fractie hebben met belangstelling kennisgenomen van het voorliggende wetsvoorstel en opgemerkt dat in het nader rapport wordt gerefereerd aan de aankondiging van de Europese Commissie inzake een algehele herziening van het gehele Europeesrechtelijke kader voor de bescherming van persoonsgegevens. Die herziening zou aanleiding kunnen zijn het hieromtrent in de Wet bescherming persoonsgegevens (Wbp), de Wet politiegegevens (Wpg) en de Wet justitiële en strafvorderlijke gegevens (Wjsg) bepaalde opnieuw op zijn onderlinge samenhang te bezien. Zij hebben gevraagd of het kabinet al meer zicht heeft op de details van de voorgestelde herziening van het gehele

Europeesrechtelijke kader (inclusief tijdpad) en hebben het kabinet verzocht hier concreet op in te gaan.

De Commissie heeft in november 2010 een Mededeling aan het Europees Parlement en de Raad uitgebracht, onder de titel «Een integrale aanpak van de bescherming van persoonsgegevens in de Europese Unie», waarin kaders worden geschetst voor een herziening van de privacyrichtlijn (richtlijn nr. 95/46/EG). De Commissie is voornemens ook de herziening van het onderhavige kaderbesluit hierin te betrekken. Naar aanleiding van de Mededeling is, bij brief van 21 december 2010, een BNC-fiche aan uw Kamer gezonden waarin de essentie van het voorstel en de eerste Nederlandse beoordeling van de Mededeling zijn opgenomen (Kamerstukken II 2010/11, 22 112, nr. 1116). In het fiche is onder meer aangegeven dat de Nederlandse regering de voornemens van de Commissie tot herziening van het kaderbesluit enigszins prematuur acht. Het kaderbesluit dataprotectie is in het merendeel der lidstaten, waaronder Nederland, nog niet geïmplementeerd. Ook de evaluatie van het kaderbesluit heeft nog niet plaatsgevonden. Deze evaluatie is voorzien voor november 2014. Ik verwijs de leden van de VVD-fractie overigens graag naar de inhoud van dit fiche voor de weergave van de inhoud van de herziening van het Europeesrechtelijke kader voor de bescherming van persoonsgegevens. In de Mededeling kondigt de Commissie voor medio 2011 een uitgewerkt voorstel aan tot herziening van het wettelijk kader voor gegevensbescherming in de EU. Dat voorstel is nog niet uitgebracht. Tijdens de JBZ-Raad van 24 februari 2011 zijn Raadsconclusies vastgesteld over de Mededeling.

De leden van de PvdA-fractie hebben met belangstelling kennisgenomen van het onderhavige wetsvoorstel en zien in dat het op sommige momenten erg belangrijk kan zijn om bepaalde gegevens uit te wisselen in verband met een strafrechtelijk proces of onderzoek. Zij zijn van mening dat bij de uitwisseling van persoonsgegevens tussen de EU en derde staten de gegevensbescherming en de privacyrechten van betrokkene voorop staan en hebben gevraagd of de regering kan bevestigen dat bij dit wetsvoorstel de privacyrechten van betrokkene vooropstaan.

Met dit wetsvoorstel wordt een Europees kaderbesluit geïmplementeerd. Het kaderbesluit geeft regels voor de bescherming van persoonsgegevens die, kort gezegd, door de rechtshandhavingdiensten van de lidstaten worden uitgewisseld. Daarbij moet worden onderkend dat een ruime uitwisseling van persoonsgegevens in het belang is van de rechtshandhaving. Niettemin bestaat er bij de rechtshandhavingdiensten soms een zekere terughoudendheid tot het delen van gegevens, vanwege de vrees dat gevoelige opsporingsgegevens in te ruime kring bekend worden. Ook de betrokkene zelf heeft, om voor de hand liggende redenen, weinig belang bij een ruime gegevensuitwisseling door de rechtshandhavingdiensten. Een gemeenschappelijke noemer is echter dat de uitgewisselde gegevens zorgvuldig worden verwerkt, omdat noch de rechtshandhavingdiensten, noch de betrokkene er baat bij hebben dat gevoelige opsporingsgegevens in verkeerde handen komen. Het kaderbesluit bevat normen om te komen tot een zorgvuldige gegevensverwerking, waarbij de privacy van de betrokkenen zoveel mogelijk wordt beschermd. Daarbij nemen de rechten van de betrokkene weliswaar een zeer belangrijke plaats in maar deze moeten worden afgewogen tegen andere belangen. Immers, als alleen het belang van de betrokkene in de beoordeling zou worden betrokken, dan zouden vrijwel geen persoonsgegevens kunnen worden uitgewisseld ten behoeve van de opsporing en vervolging van strafbare feiten omdat daarmee de privacyrechten van de betrokkene kunnen worden aangetast. Op dit punt weerspiegelt het kaderbesluit een evenwicht in de verschillende belangen. Zo heeft een aantal lidstaten zich

verzet tegen regels voor verwerking van persoonsgegevens die uitsluitend op nationaal niveau worden verwerkt. Nu gelden de regels van het kaderbesluit alleen voor gegevens die worden uitgewisseld tussen de lidstaten. De Nederlandse regering had dit graag anders gezien maar dit bleek niet haalbaar. Hierop zal hieronder, bij de beantwoording van de vragen van de leden van de fractie van de SP, nader in worden gegaan.

De leden van de PVV-fractie hebben met belangstelling kennisgenomen van het voorliggende wetsvoorstel. Zij hebben een aantal vragen, die hieronder aan de orde komen.

De leden van de CDA-fractie hebben met belangstelling kennisgenomen van het voorliggende wetsvoorstel en vinden het een goede zaak dat duidelijk wordt geregeld hoe het precies zit met de regels op het gebied van de verwerking en uitwisseling van persoonsgegevens, de waarborgen als ze worden uitgewisseld en het toezicht op de gegevensverwerking. Wel hebben deze leden nog enkele vragen, opmerkingen en wensen, die hieronder aan de orde komen.

De leden van de SP-fractie hebben kennisgenomen van het onderhavige wetsvoorstel. Naar het oordeel van deze leden is het goed dat hiermee waarborgen worden geboden voor de bescherming van persoonsgegevens bij verstrekking aan andere lidstaten en autoriteiten die zijn belast met opsporing en vervolging. Zorgvuldige gegevensverwerking is naar het oordeel van deze leden van groot belang. Deze leden hebben naar aanleiding van dit voorstel en de toelichting daarop vragen en opmerkingen, die hieronder aan de orde komen.

De leden van de D66-fractie hebben kennisgenomen van het voorliggende wetsvoorstel en zijn tevreden dat eindelijk een meer uniform kader wordt gecreëerd voor de bescherming van persoonsgegevens bij het uitwisselen daarvan in het kader van de politieke en justitiële samenwerking. Zij zien grote kansen voor een nauwere Europese samenwerking op strafrechtelijk gebied en achten een adequaat beschermingsniveau van persoonsgegevens randvoorwaardelijk. Deze leden zijn kritisch over het niveau van bescherming dat door dit kaderbesluit wordt opgelegd en zien de implementatie van onderhavig kaderbesluit dan ook als een ondergrens in Europees verband en te laag voor de Nederlandse regelgeving. Zij hebben de regering gevraagd te blijven ijveren voor verhoging van het beschermingsniveau van de grondrechten van Nederlandse burgers.

Het kabinet zal blijven ijveren voor een hoog beschermingsniveau van de grondrechten van de Nederlandse burgers. Het recht op de bescherming van de persoonlijke levenssfeer behoort daartoe (artikel 10 GW). Het Kabinet hecht veel waarde aan een goede bescherming van persoonsgegevens, zoals ook uit het regeerakkoord kan blijken. Dit neemt niet weg dat het recht op de bescherming van de persoonlijke levenssfeer geen absoluut recht is, maar moet worden afgewogen tegen andere belangen, zoals het belang van de opsporing en vervolging van strafbare feiten. De uitkomst van deze afweging is dan ook niet alleen afhankelijk van de toepassing van juridische beginselen of regels maar tevens van politieke en maatschappelijke opvattingen of overtuigingen over de bestrijding van criminaliteit en de wenselijkheid van samenwerking tussen de betrokken instanties en partijen op basis van gedeelde belangen. In de lidstaten worden op dit punt verschillende accenten gelegd en afwegingen gemaakt. Het kaderbesluit dataprotectie is het resultaat van een EU-breed onderhandelingstraject. De Nederlandse regering acht het van groot belang dat deze regels tot stand zijn gekomen – tot nu toe waren er geen gemeenschappelijke regels op dit gebied – ook met het oog op de verdere

intensivering van de politieke en justitiële samenwerking tussen de lidstaten. De uitwisseling van gegevens is daarvoor essentieel.

De leden van de D66-fractie hebben opgemerkt dat het wetsvoorstel midden november is aangeboden aan de Tweede Kamer, terwijl het kaderbesluit uiterlijk 27 november 2010 dient te zijn geïmplementeerd. Deze leden zouden graag de reden vernemen waarom die termijn niet gehaald is. Bovendien hebben zij gevraagd waarom de zin «Het streven is dit wetsvoorstel voor die datum in werking te laten treden» nog in de toelichting op artikel III staat, hoewel dit praktisch onmogelijk is. Voorts hebben deze leden in algemene zin de opmerkingen van de Raad van State over de omzettingstabel onderschreven en hopen zij op navolging.

Het kaderbesluit is op 27 november 2008 door de Raad vastgesteld en kent een implementatietermijn van twee jaar. Hoewel deze termijn op het eerste gezicht voldoende zou moeten zijn- de implementatietermijn van kaderbesluiten was doorgaans 18 maanden – blijkt een dergelijke termijn in de praktijk telkens weer minder ruim als bedacht wordt dat daarin het gehele implementatieproces afgerond moet worden. Dat wil zeggen dat de benodigde wet- en regelgeving wordt opgesteld en uitgewerkt, dat de ontwerp teksten worden afgestemd met de betrokken departementen en voorgelegd aan de uitvoeringsinstanties en dat vervolgens de procedure voor de totstandkoming van wet- en regelgeving wordt doorlopen. Begin 2009 zijn een wetsvoorstel en een ontwerp voor een algemene maatregel van bestuur opgesteld. Deze teksten zijn in het voorjaar en de zomer van 2009 afgestemd met de betrokken partijen. Het wetsvoorstel is op 5 oktober 2009 in consultatie gegeven. Het laatste advies is op 21 januari 2010 ontvangen. Nadat de inhoud van de adviezen was verwerkt en afgestemd met de betrokken departementen is het wetsvoorstel door tussenkomst van de Ministerraad op 9 juni 2010 voor advies aan de Raad van State voorgelegd. Op 19 juli 2010 is het advies van de Raad van State ontvangen. Daarna is het advies van de Raad verwerkt en afgestemd met de betrokken partijen, waarna het wetsvoorstel op 23 november 2010 bij Uw Kamer is ingediend. Samenvattend kan worden opgemerkt dat de implementatie van het kaderbesluit is vertraagd vanwege de noodzakelijke voorbereiding van de wijziging van meerdere wetten en algemene maatregelen van bestuur, de afstemming van deze wijzigingen met de betrokken departementen, de weerbarstigheid van de materie en de discussie over de financiële paragraaf. Op basis van de ervaringen moet worden vastgesteld dat een implementatietermijn van twee jaar te kort is voor de implementatie van dergelijke kaderbesluiten. Dit kan tevens blijken uit het feit dat Nederland – zacht uitgedrukt – bepaald niet de enige lidstaat is die de implementatietermijn niet heeft gehaald. Volgens informatie die is verkregen van het secretariaat van de Raad van de Europese Unie heeft op dit moment namelijk alleen Letland het kaderbesluit dataprotectie geïmplementeerd.

De leden van de D66-fractie hebben er terecht op gewezen dat het praktisch onmogelijk was om – zoals per abuis in de memorie van toelichting is gemeld – het wetsvoorstel voor de implementatiedatum van 27 november 2010 in werking te laten treden. Deze zin had moeten luiden: Het streven is dit wetsvoorstel zo spoedig mogelijk na die datum in werking te laten treden.

De leden van de ChristenUnie-fractie hebben met belangstelling kennisgenomen van het onderhavig wetsvoorstel. Zij onderschrijven het belang van een gemeenschappelijk kader voor de bescherming van persoonsgegevens die tussen de lidstaten worden uitgewisseld en hebben in dit stadium op een enkel punt nog behoefte aan een toelichting, zoals hieronder aan de orde komt.

## II. De reikwijdte van het kaderbesluit dataprotectie

De leden van de SP-fractie hebben aangegeven het standpunt van de regering te delen dat gemeenschappelijke regels voor de bescherming van de gegevens die tussen opsporings- en vervolgingsdiensten worden uitgewisseld eigenlijk niet langer mogen ontbreken. Deze leden menen echter dat deze regels er eigenlijk al meteen hadden moeten zijn vanaf het moment dat persoonsgegevens tussen die diensten werden uitgewisseld. Zij hebben om een reactie gevraagd.

De gemeenschappelijke regels voor de uitwisseling van persoonsgegevens tussen de lidstaten ten behoeve van de opsporing en vervolging van criminaliteit hebben zich geleidelijk en stapsgewijs ontwikkeld. De uitwisseling van persoonsgegevens tussen politiediensten van de lidstaten is gedurende de afgelopen decennia steeds meer geïntensiveerd. Aanvankelijk vond deze uitwisseling plaats op basis van het Verdrag van Schengen. Daarbij waren de nationale bepalingen voor de bescherming van persoonsgegevens, gekoppeld aan internationale afspraken en beginselen voor de bescherming van die gegevens, van toepassing. Een belangrijke kenbron vormden de richtsnoeren van de Raad van Europa, neergelegd in het Verdrag van 28 januari 1981 tot bescherming van het individu in verband met de geautomatiseerde registratie van persoonsgegevens en de Aanbeveling nr. R(87)15 van het Comité van Ministers van de Raad van Europa van 17 september 1987 tot regeling van het gebruik van persoonsgegevens op politieel gebied. Voor gemeenschappelijke organen, zoals Europol en Eurojust, golden afzonderlijke en specifieke regels voor dataprotectie. In een brief aan Uw Kamer van 5 februari 2007 (Kamerstukken II 2006/07, 23 490, nr. 444) is de ontwikkeling van de uitwisseling van persoonsgegevens op Europees niveau in relatie tot de bescherming van persoonsgegevens geschetst. De beschreven situatie leidde tot een minder overzichtelijk geheel van regels voor de bescherming van persoonsgegevens die tussen de lidstaten worden uitgewisseld. In op 27 juli 2010 heeft de Commissie een Mededeling gepubliceerd, waarin een overzicht wordt gegeven van de EU-rechtsinstrumenten voor de verzameling, bewaring en uitwisseling van persoonsgegevens voor doeleinden in verband met de rechtshandhaving of de migratie (COM (2010)385 final). Daaruit blijkt dat er een groot aantal informatiesystemen binnen de Unie in gebruik is, waarvoor specifieke regels voor de gegevensbescherming gelden.

Met de vaststelling van het Haags programma, onder het Nederlandse Voorzitterschap, is het beschikbaarheidsbeginsel de leidraad geworden voor de uitwisseling van informatie tussen de lidstaten. Dit betekent dat een rechtshandhavingfunctionaris in een lidstaat informatie, die hij voor de uitoefening van zijn taak nodig heeft, kan verkrijgen van een andere lidstaat en dat de betrokken rechtshandhavingdienst in die andere lidstaat de informatie voor het aangegeven doel beschikbaar stelt, rekening houdend met lopende onderzoeken in die lidstaat. Het kabinet is een groot voorstander van gemeenschappelijke regels voor de bescherming van persoonsgegevens, niet alleen vanwege de mede uit het Haags Programma voortvloeiende intensivering van de gegevensuitwisseling maar ook vanwege de werkbaarheid voor de praktijk. Er is sprake van een groeiprocess.

Dit alles overziende kan – zoals de leden van de SP-fractie aangeven – worden geoordeeld dat deze regels er wellicht eerder hadden kunnen zijn, maar daarbij moet bedacht worden dat de uitwisseling van politieke en justitiële gegevens voor veel lidstaten een gevoelig onderwerp betreft, ten aanzien waarvan zij van oudsher gewend zijn in een hoge mate van zelfstandigheid te beslissen over de vraag of dergelijke gegevens aan een

andere lidstaat worden verstrekt en welke regels daarbij van toepassing zijn. Het kabinet is in ieder geval verheugd dat het kaderbesluit is vastgesteld en acht dit een goede basis voor de intensivering van de politieke en justitiële samenwerking binnen de EU. Mede voortbouwend op de ervaringen met de regels van het kaderbesluit acht het kabinet het van belang dat het gemeenschappelijk kader in de nabije toekomst verder wordt uitgewerkt.

### **III. De inhoud van het kaderbesluit**

De leden van de PvdA-fractie hebben opgemerkt dat in het kaderbesluit de doelbinding is geregeld. Het verwerken van persoonsgegevens moet rechtmatig, adequaat, ter zake dienend en niet excessief zijn in verhouding tot het doel waarvoor zij worden verzameld. Deze leden hebben erop gewezen dat deze regel vrij strikt lijkt maar direct wordt ondergraven door de mogelijkheid om verwerking van persoonsgegevens ook toe te staan voor een «ander doel». Wel moet dit andere doel verenigbaar zijn met het oorspronkelijke doel. De leden hebben zich afgevraagd welke andere doelen hiermee bedoeld worden en of de regering voorbeelden wil geven die aangeven waarom het noodzakelijk is dat persoonsgegevens in zo'n geval moeten worden verwerkt. Verder hebben zij gevraagd of dit betekent dat deze persoonsgegevens in andere databases worden opgenomen en welke databases het hier betreft.

In antwoord op deze vragen merk ik op dat het beginsel van doelbinding een essentieel beginsel is voor de bescherming van persoonsgegevens. Hiermee wordt bedoeld op het beginsel dat persoonsgegevens slechts worden verzameld en verwerkt voor welbepaalde en gerechtvaardigde doelen. Die doelen moeten zodanig zijn omschreven dat de doelen, waarvoor persoonsgegevens kunnen worden verwerkt, nauw worden ingekaderd. Zo moet de politie persoonsgegevens kunnen verwerken ten behoeve van een goede uitvoering van haar taak, te weten de politietak als bedoeld in de artikelen 2 en 6 PW 1993. Dit betreft de opsporing van strafbare feiten, de handhaving van de openbare orde en de verlening van hulp aan hen die deze hulp behoeven. De verzameling van persoonsgegevens voor andere doelen, bijvoorbeeld de inning van belastingen, het verlenen van gezondheidszorg of het aanbieden van onderwijs, is hiermee niet verenigbaar en vanuit het oogpunt van gegevensbescherming niet toelaatbaar. Dit neemt niet weg dat derden belang kunnen hebben bij de verstrekking van persoonsgegevens die door de politie of het openbaar ministerie rechtmatig zijn verzameld ten behoeve van de uitvoering van hun wettelijke taken. Politiegegevens kunnen bijvoorbeeld worden verstrekt aan slachtoffers van misdrijven, om in rechte voor hun belangen op te kunnen komen, aan het Bureau BIBOB, ten behoeve van de uitvoering van de wettelijke taken door het bureau BIBOB, of aan directeurs van penitentiaire inrichtingen, ten behoeve van de benoeming of het ontslag van personeel. Justitiële gegevens kunnen worden verstrekt aan ambtenaren van de reclassering, ten behoeve van de hulpverlening aan veroordeelde personen, of aan de burgemeesters ten behoeve van het advies over de verlening van een Koninklijke onderscheiding. De personen en instanties, aan wie politiegegevens, justitiële of strafvorderlijke gegevens worden of kunnen worden verstrekt, zijn opgesomd in het Besluit politiegegevens en het Besluit justitiële gegevens. Vereist is dat de gegevensverstrekking nodig is met het oog op een zwaarwegend algemeen belang. Met dit criterium wordt tot uitdrukking gebracht dat de verstrekking voor de samenleving van meer dan gewone betekenis is. Toepassing van dit criterium impliceert een belangenafweging, waarbij het belang dat gediend wordt met de verstrekking wordt afgewogen tegen het belang van de persoonlijke levenssfeer van degene op wie de gegevens verstrekking hebben. De gegevensverstrekking brengt met zich

mee dat de verstrekte persoonsgegevens in andere databases worden opgenomen, namelijk de databases van de personen of instanties aan wie de gegevens zijn verstrekt. Deze personen en instanties zijn op hun beurt verplicht tot de bescherming van persoonsgegevens en gehouden het gebruik van de gegevens te beperken tot het doel waarvoor deze zijn verkregen. Daarbij geldt een geheimhoudingsverplichting, zodat de gegevens uitsluitend in uitzonderlijke gevallen verder verstrekt mogen worden.

De leden van de PVV-fractie hebben gevraagd of er aanwijzingen bestaan dat het wel eens is voorgekomen dat lidstaten doelloos gegevens verzamelen en of hiervan voorbeelden gegeven kunnen worden. Verder hebben deze leden gevraagd of zij het goed hebben begrepen dat het College bescherming persoonsgegevens (Cbp) zal worden belast met de advisering en het toezicht, en hoe zich dit verhoudt tot hetgeen het Cbp heeft aangegeven, namelijk dat zij de nadruk willen leggen op handhaving in plaats van advisering.

De vraag of er aanwijzingen bestaan van het doelloos verzamelen van gegevens moet ontkennend worden beantwoord, hiervan kunnen dan ook geen voorbeelden gegeven worden. Het Cbp is inderdaad belast met de advisering over wetgeving en het toezicht op de naleving van het bij of krachtens de Wet politiegegevens en de Wet justitiële en strafvorderlijke gegevens bepaalde. Dit betreft een wettelijke taak van het College, die is vastgelegd in artikel 35 Wpg en de artikelen 27, 39r en 51 Wjsg, juncto artikel 51 van de Wbp. Op dit punt strekt het kaderbesluit niet tot aanvulling van de bestaande wettelijke regelingen. Tot de adviestaak die is opgenomen in artikel 51 van de Wbp behoort de wetgevingsadvisering. De maatschappelijke adviseringstaak, die betrekking heeft op de invulling van de inhoudelijke verplichtingen van de Wbp door burgers en bedrijven, behoort strikt genomen niet tot de wettelijke taak van het Cbp. Het Cbp heeft ervoor gekozen meer de nadruk te gaan leggen op handhaving in plaats van de maatschappelijke advisering. Dit betreft een eigen keuze van het Cbp, die door het kabinet wordt gerespecteerd.

De leden van de CDA-fractie hebben gevraagd wat precies onder de verdere verwerking van gegevens moet worden verstaan. Ook hebben zij gevraagd hoe het nu zit als de betrokkene niet wil dat zijn gegevens verder worden verwerkt voor een ander doel, maar de verstrekkende lidstaat hiertegen geen bezwaar heeft.

Onder de verdere verwerking van gegevens wordt verstaan de verwerking van gegevens voor andere doelen dan waarvoor zij zijn verkregen. Dit is bijvoorbeeld aan de orde als gegevens, die zijn verzameld ten behoeve van de opsporing van een strafbaar feit, worden gebruikt voor het verrichten van de zogenaamde openbare orde toets van personen die een verblijfsvergunning hebben aangevraagd. Deze gegevens, die zijn verzameld ten behoeve van het doel van de opsporing, worden dan verder verwerkt voor een ander doel, namelijk de toepassing van de Vreemdelingenwetgeving. Dit is ook aan de orde als gegevens, die aan een andere lidstaat zijn verstrekt ten behoeve van de opsporing van een bepaald strafbaar feit, worden gebruikt voor de opsporing van andere strafbare feiten. In het Nederlandse rechtssysteem is de mogelijkheid van de verdere verwerking van gegevens voor een ander doel afhankelijk van een afweging door de verantwoordelijke, aan de hand van wettelijke kaders, in plaats van de instemming van de betrokkene. De verantwoordelijke dient af te wegen in hoeverre de verdere verwerking verenigbaar is met het oorspronkelijke doel van de gegevensverwerking. Hieraan ligt ook een praktische overweging ten grondslag omdat de betrokkene niet altijd eenvoudig te vinden zal zijn, en bovendien doorgaans geen belang zal

hebben bij de verdere verwerking van zijn persoonsgegevens. Het ligt niet voor de hand om de verdere verwerking in een andere lidstaat afhankelijk te doen zijn van de instemming van de betrokkene omdat dit voor de nationale situatie evenmin het geval is. De samenwerking tussen de lidstaten bij de aanpak van gemeenschappelijke problemen zou ernstig gehinderd kunnen worden als verzamelde politie- en justitiële gegevens zonder toestemming van de betrokkene niet gebruikt zouden kunnen worden voor bijvoorbeeld de screening van personen die in aanmerking willen komen voor een bepaalde maatschappelijke functie waarbij zij veelvuldig in aanraking zullen komen met jonge kinderen. Daar komt bij dat een dergelijke werkwijze grote consequenties zal hebben voor de werklast van politie en justitie.

De leden van de CDA-fractie hebben opgemerkt dat persoonsgegevens die van een andere lidstaat zijn verkregen onder bepaalde voorwaarden kunnen worden doorgegeven aan particuliere instanties en hebben gevraagd wat voor soort instanties dit zijn. Ook hebben zij gevraagd of de regering hier een omschrijving dan wel enkele voorbeelden van kan geven.

De verstrekking van persoonsgegevens aan particuliere instanties kan aan de orde zijn in gevallen waarin rechtshandavingsinstanties nauw samenwerken met particuliere instanties bij de bestrijding van criminaliteit. Een voorbeeld betreft het weren van personen, die worden verdacht van betrokkenheid bij het beramen of plegen van terroristische misdrijven, van internationale vluchten door luchtvaartmaatschappijen. Het weren van de zogenaamde bolletjesslikkers betreft een soortgelijk voorbeeld. In dergelijke gevallen kan de verstrekking van gegevens over de betreffende personen, zoals personalia of het strafbare feit dat aanleiding geeft tot verhoogde waakzaamheid, aan de luchtvaartmaatschappij noodzakelijk zijn. Een ander voorbeeld betreft de verstrekking van persoonsgegevens over hooligans aan buitenlandse voetbalorganisaties, zodat maatregelen getroffen kunnen worden bij de opvang en begeleiding van deze personen rond voetbalwedstrijden. Het belang van de handhaving van de openbare orde en de voorkoming van strafbare feiten weegt op tegen het belang van de betrokkene dat zijn persoonsgegevens niet worden verwerkt. Voor de gegevensverstrekking gelden strenge eisen op het gebied van de noodzakelijkheid en de proportionaliteit. Dit vloeit voort uit het kaderbesluit (artikel 3, tweede lid). De verstrekking van persoonsgegevens door de rechtshandavingsinstanties dient beperkt te zijn tot de gegevens die noodzakelijk zijn voor het doel waarvoor deze worden verstrekt. De verdere verwerking moet in verhouding staan tot dat doel. Daarbij geldt voor de betrokkene het recht op kennisgeving, zodat deze op de hoogte kan komen van de persoonsgegevens die over hem of haar worden verwerkt.

De leden van de CDA-fractie hebben gevraagd of ik kan aangeven wie de verantwoordelijke is die kan weigeren dat de betrokkene het recht heeft op het corrigeren, wissen of het afschermen van gegevens en hebben met betrekking tot artikel 18 van het kaderbesluit gevraagd bij welke rechterlijke instantie beroep kan worden aangetekend.

De verantwoordelijke die belast is met het beoordelen van een verzoek om correctie of afscherming van gegevens is degene die het doel en de middelen voor de gegevensverwerking vaststelt. Bij de politiegegevens is dit de korpsbeheerder, bij justitiële gegevens is dit de minister van Veiligheid en Justitie en bij strafvorderlijke gegevens is dit het College van procureurs-generaal. Een weigering tot correctie van persoonsgegevens geldt als een besluit in de zin van de Algemene wet bestuursrecht, waartegen beroep kan worden ingesteld. Het beroepsschrift tegen een



besluit van de korpsbeheerder wordt ingediend bij de rechtbank binnen wier rechtsgebied het regiokorps zetelt (artikel 8:7, eerste lid, Awb). Het beroepsschrift tegen een besluit van de minister van Veiligheid en Justitie of het College van procureurs-generaal wordt ingediend bij de rechtbank te 's-Gravenhage.

De leden van de CDA-fractie hebben opgemerkt dat over het kaderbesluit voor 27 november 2014 door de Commissie advies zal worden uitgebracht. Zij hebben gevraagd hoe dit getoetst zal worden.

De lidstaten moeten uiterlijk op 27 november 2013 aan de Commissie verslag uitbrengen over de nationale maatregelen die zij hebben genomen om te zorgen voor volledige naleving van dit kaderbesluit. Op basis van de inbreng van de lidstaten brengt de Commissie een verslag uit aan het Europees Parlement en de Raad. In het verslag kunnen voorstellen tot wijziging van het kaderbesluit worden gedaan. Het verslag van de Commissie zal worden behandeld volgens de procedure van codecisie. Dat wil zeggen dat het Europees Parlement, de Raad en de Commissie het onderling eens moeten worden over de naar aanleiding van het verslag te treffen maatregelen.

De leden van de SP-fractie hebben gevraagd of de regering tevreden is met het bereikte niveau van gegevensbescherming dat in het kaderbesluit dataprotectie is neergelegd, of de door Nederland ingebrachte wensen zijn verwezenlijkt en of er op punten water bij de wijn is gedaan. Verder hebben zij gevraagd of het kaderbesluit volledig moet worden geïmplementeerd of dat er sprake is van minimumharmonisatie. Zij hebben om een toelichting op deze punten gevraagd. Voorts hebben zij gevraagd of het kaderbesluit dataprotectie Nederland dwingt om het niveau van gegevensbescherming naar beneden bij te stellen.

In zijn algemeenheid is de regering tevreden met het bereikte niveau van gegevensbescherming dat in het kaderbesluit dataprotectie tot uitdrukking komt. Het kaderbesluit voorziet in een samenhangend systeem van regels bij de uitwisseling van gegevens tussen de opsporings- en vervolgingsinstanties van de lidstaten en biedt de nodige rechtswaarborgen voor de Europese burger, bijvoorbeeld op het punt van het recht op kennisneming en het toezicht op de gegevensverwerking. Dit is temeer van belang vanwege de toenemende intensivering van de politieke en justitiële samenwerking. Naar het oordeel van de regering waarborgt het kaderbesluit een adequaat niveau van gegevensbescherming waarbij tevens rekening wordt gehouden met de binnen de Europese Unie breed gevoelde noodzaak tot verdere intensivering van de samenwerking tussen de opsporingsdiensten, ook op het gebied van de gegevensuitwisseling. Over dit punt is destijds uitgebreid van gedachten gewisseld met de leden van de Eerste Kamer (Kamerstukken II 2007/08, 23 490, CX). Daarmee is niet gezegd dat het resultaat van de onderhandelingen over het kaderbesluit voor Nederland optimaal is. Zo gaf de Nederlandse regering de voorkeur aan een ruim toepassingsbereik van het kaderbesluit, dat wil zeggen dat de regels van het kaderbesluit ook van toepassing zijn op gegevens die in de lidstaten zelf worden verwerkt ten behoeve van de opsporing en vervolging van strafbare feiten. Dit bleek in Brussel echter niet haalbaar, omdat een aantal lidstaten daartegen grote bezwaren had. Ook is de situatie blijven bestaan dat op deelterreinen van de politieke en justitiële samenwerking binnen de Unie specifieke dataprotectieregimes van kracht blijven. Hierbij kan worden gedacht aan de regels voor de gegevensverwerking door Europol en Eurojust, de verwerking van gegevens in het Schengen Informatie Systeem (SIS) en de regels voor de uitwisseling van gegevens op basis van het kaderbesluit tot omzetting van het Verdrag van Prüm. Deze regels gelden in aanvulling op, of naast die

van het kaderbesluit, waardoor de rechtshandhavingdiensten worden geconfronteerd met verschillende regimes voor persoonsgegevens die worden uitgewisseld in het kader van de politieke en justitiële samenwerking. Het zou beter zijn als er een gemeenschappelijk alomvattend kader zou gelden voor de gegevensverwerking ten behoeve van de opsporing en vervolging van strafbare feiten, maar dit is een ideaal dat slechts op langere termijn zal kunnen worden gerealiseerd. Het kaderbesluit dwingt Nederland niet om het niveau van gegevensbescherming naar beneden bij te stellen. In het kaderbesluit is vastgelegd dat de lidstaten, ter bescherming van de op nationaal niveau verzamelde of verwerkte persoonsgegevens, uitgebreidere waarborgen kunnen bieden dan die waarin het kaderbesluit voorziet (artikel 1, vijfde lid). Als Nederland op bepaalde onderdelen een hoger niveau van gegevensbescherming heeft, dan doet het kaderbesluit daaraan geen afbreuk.

De leden van de SP-fractie hebben de regering gevraagd of er lidstaten zijn waarover Nederland zich zorgen maakt met betrekking tot het niveau van de bescherming van persoonsgegevens. Zij hebben gevraagd of er lidstaten zijn die momenteel nog geen toereikend niveau van gegevensbescherming hebben, en zo ja, welke landen dat zijn. Ook hebben zij gevraagd of het kaderbesluit daarin verbetering gaat brengen, niet alleen op papier maar ook in de praktijk. Zij hebben om een toelichting gevraagd.

Alle lidstaten van de Europese Unie zijn gebonden aan de normen van het kaderbesluit en dienen deze in hun nationale wetgeving om te zetten. Deze normen hebben betrekking op de persoonsgegevens die tussen de lidstaten worden uitgewisseld in het kader van de politieke en justitiële samenwerking in strafzaken. Het kaderbesluit is niet van toepassing op de persoonsgegevens die in een lidstaat worden verwerkt in het kader van de opsporing of de vervolging van strafbare feiten en die niet aan een andere lidstaat worden verstrekt. Op dit punt raakt het kaderbesluit niet aan het niveau van de bescherming van persoonsgegevens in de betreffende lidstaat. De Commissie houdt nauwgezet toezicht op de uitvoering van de Europese regels door de lidstaten. Daarnaast verplicht het kaderbesluit tot het inrichten van een nationale toezichthoudende autoriteit die de opgedragen taken in volstrekte onafhankelijkheid verricht en over de nodige onderzoeksbevoegdheden beschikt om de naleving van de regels af te dwingen. Daarbij moet ook worden bedacht dat ook de Privacyrichtlijn van 1995 (richtlijn 95/46/EG, Pb EG, L. 281/31) voorziet in uitgebreide regels voor gegevensbescherming in de voormalige eerste pijler, zodat het merendeel der lidstaten over een ruime ervaring beschikt met de bescherming van persoonsgegevens. In het geval dat er in de samenwerking met bepaalde lidstaten twijfels zouden bestaan over de zorgvuldigheid van de gegevensverwerking, vanwege ervaringen in het verleden, kan er aanleiding bestaan tot terughoudendheid in de gegevensuitwisseling met de bevoegde instanties van die lidstaten. Hierop zal hieronder, bij de beantwoording van de vragen van de leden van deze fractie over de uitwisseling van gegevens met EU-lidstaten of met derde landen, nader in worden gegaan.

De leden van de SP-fractie hebben gevraagd of de regering de mening van deze leden deelt dat het uitwisselen van politieke, justitiële en strafvorderlijke gegevens met EU-lidstaten of met derde landen alleen geoorloofd is als er daadwerkelijk, zowel in theorie, als in de praktijk toereikende gegevensbescherming bestaat in het andere land. Ook hebben zij gevraagd of Nederland zo nodig ook daadwerkelijk doorgifte of verstrekking van persoonsgegevens zal weigeren bij twijfel over het niveau van gegevensbescherming in het andere land en of het kaderbesluit dat toe staat. Verder hebben deze leden dezelfde vraag gesteld over

derde landen. In dit kader hebben deze leden gevraagd wanneer Nederland zal instemmen met de doorgifte van persoonsgegevens door een andere lidstaat aan een derde staat, wanneer deze gegevens door Nederland zijn doorgegeven aan die EU-lidstaat. Zij hebben gevraagd ten aanzien van welke landen dit niet het geval zal zijn en hoe dit wordt bepaald.

De regering deelt de mening van de leden van de SP-fractie dat het uitwisselen van politieke, justitiële en strafvorderlijke gegevens met EU-lidstaten of met derde landen alleen geoorloofd is als er daadwerkelijk, zowel in wet- en regelgeving, als in de praktijk toereikende gegevensbescherming bestaat in het andere land.

Voor wat betreft de lidstaten heeft de regering niet bij voorbaat zorgen, omdat alle lidstaten gebonden zijn aan de gemeenschappelijke regels op het gebied van de bescherming van persoonsgegevens. De Europese Commissie beoordeelt de implementatie van deze regels en houdt toezicht op de naleving ervan. In de lidstaten is er dus sprake van een toereikend niveau van gegevensbescherming. Als het al zo zou zijn dat er op grond van de ervaringen van de rechtshandhavingdiensten met de uitwisseling van persoonsgegevens met bepaalde lidstaten aanleiding bestaat tot twijfels over de wijze waarop de gegevens worden beschermd, kan met inachtneming van de kaders van de Europese afspraken terughoudendheid worden betracht in de verstrekking van de gegevens.

Ook is het mogelijk om de verstrekking van aanvullende gegevens afhankelijk te stellen van een rechtshulpverzoek, zodat de officier van justitie is betrokken. In het uiterste geval zou Nederland zonedig de doorgifte of verstrekking kunnen weigeren. Het kaderbesluit staat daaraan niet in de weg omdat dit geen bevoegdheden of verplichtingen bevat over de verstrekking van persoonsgegevens aan andere lidstaten.

Voor wat betreft derde landen onderschrijft de regering in zijn algemeenheid eveneens het standpunt van de SP. Daarbij moet wel worden opgemerkt dat de bronlanden van criminaliteit die zich tevens uitstrekt tot het Nederlandse grondgebied, in andere werelddelen kunnen zijn gelegen, waarbij andere normen gelden op het gebied van de bescherming van persoonsgegevens. In het belang van het welslagen van een opsporingsonderzoek of van de vervolging kan het noodzakelijk zijn met dergelijke landen gegevens uit te wisselen. Het kaderbesluit geeft geen normen voor de rechtstreekse verstrekking van persoonsgegevens aan derde landen. Wel geeft het kaderbesluit regels voor de verstrekking van persoonsgegevens, die van een andere lidstaat zijn ontvangen, aan een derde land. Deze beperking houdt verband met de reikwijdte van het kaderbesluit, dat van toepassing is op gegevens die tussen de lidstaten worden verstrekt. Bij de implementatie van het kaderbesluit is de Nederlandse regering uitgegaan van een zoveel mogelijk extensieve werking van de regels van het kaderbesluit, dat wil zeggen dat de regels van het kaderbesluit ook gelden voor de gegevens die uitsluitend op nationaal niveau worden verwerkt (Kamerstukken II 2010/11, 32 554, nr. 3, blz. 8). Anders zouden de rechtshandavingsautoriteiten met verschillende verstrekkingssystemen kunnen worden geconfronteerd, afhankelijk van de vraag of een persoonsgegeven eerder van een andere lidstaat is verkregen. Het kaderbesluit bindt de verdere verstrekking van persoonsgegevens aan een derde land in beginsel aan het vereiste van een toereikend beschermingsniveau. Of het beschermingsniveau toereikend is wordt beoordeeld met inachtneming van alle omstandigheden die op de doorgifte van de gegevens of op een groep van gegevensverwerkingen van invloed zijn. In het bijzonder wordt rekening gehouden met de aard van de gegevens, met het doel en de duur van de voorgenomen verwerking of verwerkingen, het land van herkomst en het land of het internationale orgaan van eindbestemming van de gegevens, de algemene en sectorale rechtsregels die in het derde land of het interna-

tionale orgaan gelden, alsmede de beroepscodes en de veiligheidsmaatregelen die in het land of het orgaan van toepassing zijn. In afwijking hiervan kunnen persoonsgegevens worden doorgegeven als de nationale wetgeving van de lidstaat die de gegevens doorgeeft daarin voorziet wegens gerechtvaardigde specifieke belangen van de betrokkene of gerechtvaardigde doorslaggevende belangen, met name zwaarwegende openbare belangen. Tevens kunnen persoonsgegevens worden doorgegeven als het derde land of het ontvangende orgaan of de ontvangende internationale instantie garanties bieden die door de betrokken lidstaat conform de nationale wetgeving toereikend worden geacht (artikel 13, derde lid). Bij de samenwerking met derde landen zal van geval tot geval moeten worden afgewogen welke mogelijkheden er zijn voor de verstrekking van persoonsgegevens. De Nederlandse opsporingsinstanties werken reeds langere tijd samen met buitenlandse opsporingsdiensten. Met sommige landen worden daarvoor speciale samenwerkingsovereenkomsten gesloten, waarin voor de gegevensbescherming naar de regels van 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. Op grond van de beoordeling van het niveau van gegevensbescherming kunnen verschillende maatregelen worden getroffen. Bij de verstrekking van politiegegevens aan derde landen zal altijd grote terughoudendheid worden betracht met «zachte» opsporingsgegevens, zoals CIE-gegevens. Verder kan worden gekozen voor (gedeeltelijke) anonimisering van de gegevens. Voorts kan onderscheid worden gemaakt in persoonsgegevens van Nederlanders en die van ingezetenen van het betreffende land, waarbij uiterste terughoudendheid wordt betracht met de verstrekking van persoonsgegevens van Nederlanders. Tenslotte zal het landelijk parket van het openbaar ministerie worden betrokken in die gevallen waarin behoefte bestaat aan een extra toetsing van de voorgenomen gegevensverstrekking door officieren van justitie die over de nodige ervaring beschikken in de strafrechtelijke samenwerking met andere landen.

De doorgifte van persoonsgegevens aan een derde land zal aan dezelfde criteria worden getoetst als de rechtstreekse verstrekking van de gegevens aan die betreffende staat door Nederland zelf. Dat wil zeggen dat sprake moet zijn van een toereikend beschermingsniveau voor de voorgenomen gegevensverwerking. Dit is bij de beantwoording van de vorige vragen van de leden van deze fractie reeds aan de orde gekomen. Het beschermingsniveau wordt beoordeeld met inachtneming van alle omstandigheden die op de doorgifte van gegevens van invloed zijn. Het feit dat de doorgifte door een andere lidstaat aan dezelfde criteria wordt getoetst als de rechtstreekse verstrekking door Nederland zelf betekent dat de praktische betekenis van deze bepaling voor de opsporingspraktijk waarschijnlijk gering zal zijn. Immers, in die gevallen waarin doorgifte wordt overwogen zal het belanghebbende land zich rechtsreeks kunnen richten tot de lidstaat die de gegevens heeft verstrekt aan de lidstaat die de doorgifte daarvan overweegt.

Ook de leden van de D66-fractie wilden graag een appreciatie van de regering van het beschermingsniveau dat de minimumnormen in het kaderbesluit pogen te garanderen. Tevens hebben deze leden de regering verzocht de Kamer nauw te betrekken bij haar inzet aangaande de algehele herziening van het Europeesrechtelijk kader voor de bescherming van persoonsgegevens.

In antwoord op de vraag van de leden van de D66-fractie over de appreciatie van het beschermingsniveau van het kaderbesluit kan worden verwezen naar de beantwoording van de vragen over dit onderwerp van de leden van de SP-fractie.

Voor wat betreft de inzet bij de algehele herziening van het Europeesrechtelijke kader voor de bescherming van persoonsgegevens merkt de regering op gaarne bereid te zijn de Kamer nauw te betrekken bij haar inzet aangaande de algehele herziening van het Europese kader dienaangaande. Dit kan blijken uit het feit dat de Kamer reeds is geïnformeerd over de inhoud van de Mededeling over de herziening van de privacyrichtlijn en de voorlopige reactie van de regering daarop (Kamerstukken II, 2010/11, 22 122, nr. 1116). Hiervoor kan ook worden verwezen naar de brief van 5 februari 2010, waarin is aangegeven op welke wijze Uw Kamer bij het Europees beleids- en besluitvormingsproces wordt betrokken (Kamerstukken 2009/10, 32 317, nr. 1). De regering zal zich voor de betrokkenheid van de Kamer bij het Europees beleids- en besluitvormingsproces uiteraard conformeren aan de in die brief aangegeven kaders.

De leden van de D66-fractie zouden graag een nadere toelichting ontvangen op de regels omtrent het doorgeven van gegevens aan derde landen. Zij hebben gevraagd welke eisen precies aan het beschermingsniveau van die persoonsgegevens door die landen en/of instanties worden gesteld.

Voor de doorgifte van gegevens aan een derde land is onder meer vereist dat het betreffende land een toereikend beschermingsniveau voor de voorgenomen gegevensverstrekking garandeert. Het kaderbesluit bepaalt dat het beschermingsniveau wordt beoordeeld met inachtneming van alle omstandigheden die op de doorgifte van gegevens of op een groep van gegevensverstrekkingen van invloed zijn. In het bijzonder wordt rekening gehouden met de aard van de gegevens, met het doel en met de duur van de voorgenomen verwerking of verwerkingen, het land van herkomst en het land of het internationale orgaan van eindbestemming van de gegevens, de algemene en sectorale rechtsregels die in het derde land of het internationale orgaan gelden, alsmede de beroepscodes en de veiligheidsmaatregelen die in het land of het orgaan van toepassing zijn. Dit is hierboven nader toegelicht, naar aanleiding van een vraag van de leden van de fractie van de SP.

#### **IV. Het toepassingsgebied van het kaderbesluit**

De leden van de CDA-fractie hebben de regering gevraagd nader toe te lichten waarom het kaderbesluit niet van toepassing is op de inlichtingen- en veiligheidsdiensten, nu de activiteiten van deze diensten buiten de reikwijdte van het Verdrag betreffende de Europese Unie vallen. Ook de leden van de SP-fractie hebben geconstateerd dat het kaderbesluit niet van toepassing is op de inlichtingen- en veiligheidsdiensten en hebben gevraagd welke regels en waarborgen dan voor de uitwisseling van gegevens door deze diensten gelden.

Naar aanleiding van de gestelde vragen moet voorop worden gesteld dat de activiteiten van de inlichtingen- en veiligheidsdiensten van de lidstaten niet onder de reikwijdte van het EU-Verdrag vallen. Dit betekent dat de rechtsinstrumenten van de Unie niet op de activiteiten van deze diensten van toepassing zijn. Een aantal lidstaten, waaronder Nederland, heeft erop aangedrongen om dit expliciet in het kaderbesluit vast te leggen, zodat daarover geen misverstand zou kunnen ontstaan. De regels en waarborgen die voor de gegevensverwerking en -uitwisseling door deze diensten gelden, zijn opgenomen in de nationale wetgeving van de

lidstaten. Voor de activiteiten van deze diensten gelden geen gemeenschappelijke regels op het niveau van de Europese Unie.

## **V. De verhouding met regels in bestaande EU-overeenkomsten en bilaterale afspraken**

De leden van de CDA-fractie hebben gevraagd wat moet worden verstaan onder het recht van toegang in het Europolbesluit en wie het gemeenschappelijk toezichthoudend orgaan wordt. Deze leden hebben tevens gevraagd wie het gemeenschappelijk controleorgaan op grond van het besluit tot oprichting van Eurojust wordt en wie de partners zijn met wie informatie moet worden uitgewisseld.

Het Europolbesluit geeft de betrokkene het recht op kennisneming van de hem betreffende persoonsgegevens die door Europol worden verwerkt en het recht deze gegevens in begrijpelijke vorm te ontvangen, dan wel om hem betreffende persoonsgegevens te laten controleren (artikel 30 van het Besluit 2009/371/JBZ, PbEU L 121/37). De regels omtrent het recht op kennisneming voor de gegevens die bij Europol worden verwerkt vormen specifieke bepalingen ten opzichte van het in het kaderbesluit geregelde recht van toegang (artikel 17 van het Besluit 2009/371/JBZ). Er is een gemeenschappelijk controleorgaan ingericht, dat is samengesteld uit vertegenwoordigers van de nationale toezichthoudende instanties van de lidstaten en dat toeziet op de werkzaamheden van Europol (artikel 34 van het Besluit 2009/371/JBZ). Voor Nederland wordt aan dit controleorgaan deelgenomen door vertegenwoordigers van het College bescherming persoonsgegevens. Voor wat betreft Eurojust is eveneens een gemeenschappelijk controleorgaan opgericht, dat is samengesteld uit de vertegenwoordigers van de rechterlijke macht van de lidstaten en dat toeziet op de activiteiten van Eurojust, teneinde de verwerking van persoonsgegevens in overeenstemming met het Eurojustbesluit te verzekeren (artikel 23 van het Besluit 2009/JBZ, PbEU L 63/1). De partners met wie door Eurojust informatie kan worden uitgewisseld zijn derde landen of organisaties, zoals internationale organisaties en andere organen van publiekrechtelijke aard die zijn gegrondvest op een overeenkomst tussen twee of meer staten en Interpol (artikel 26a van het Besluit 2009/426/JBZ, PbEG L 138/14).

## **VI. Uitgangspunten voor de implementatie van het kaderbesluit dataprotectie**

De leden van de CDA-fractie hebben gevraagd wanneer de aangekondigde algemene maatregel van bestuur klaar zal zijn en hoe die precies zal luiden.

In de memorie van toelichting bij het wetsvoorstel is aangegeven dat de belangrijkste aanpassingen, die uit het kaderbesluit dataprotectie voortvloeien, deels in de algemene maatregelen van bestuur en deels op het niveau van de wet plaatsvinden (Kamerstukken II 2010/11, 32 554, nr. 3, blz. 15). Inmiddels is een eerste ontwerp voor een algemene maatregel van bestuur opgesteld, strekkende tot wijziging van het Besluit politiegegevens en het Besluit justitiële en strafvorderlijke gegevens in verband met de implementatie van het kaderbesluit dataprotectie. Het ontwerp voor de algemene maatregel van bestuur bevat nadere regels over de ontvangst van gegevens uit het buitenland en van andere lidstaten, de verstrekking van gegevens aan andere lidstaten, de verstrekking van gegevens aan Europol en Eurojust en de doorgifte van gegevens aan derde landen en aan personen en instanties met een publieke taak. Het ontwerp voor deze algemene maatregel van bestuur zal voor advies aan de Raad van State worden voorgelegd, zodra het

wetvoorstel door de Kamer is aanvaard. Een ontwerp voor deze algemene maatregel van bestuur, dat tijdens de consultatie van het wetsvoorstel ter informatie is meegezonden, is ter kennisneming bij deze nota naar aanleiding van het verslag gevoegd.

## **VII. De Nederlandse wetgeving op het gebied van de verwerking van persoonsgegevens ten behoeve van de opsporing en vervolging van strafbare feiten en de wijze waarop daarin reeds rekening wordt gehouden met de uitwisseling van gegevens met andere landen.**

De leden van de PvdA-fractie hebben gevraagd of onder de huidige Wpg en Wjsg gegevens worden verzameld voor een ander doel dan waarvoor zij zijn verworven en verwerkt. Deze leden hebben tevens gevraagd welke doelen dit zijn en waarom juist deze doelen om bepaalde persoonsgegevens vragen.

In antwoord op deze vragen moet voorop worden gesteld dat onder de huidige Wpg en Wjsg persoonsgegevens uitsluitend kunnen worden verzameld en verwerkt ten behoeve van de in die wetten omschreven doelen. Voor de Wpg betreft dit bepaalde doelen binnen de politietaak, voor de Wjsg betreft dit de in de Wjsg voor de verschillende categorieën van persoonsgegevens omschreven doelen. Daarbij wordt onderscheid gemaakt tussen justitiële gegevens, strafvorderlijke gegevens en de persoonsgegevens in persoonsdossiers. De verstrekking van de persoonsgegevens aan derden, ten behoeve van verdere verwerking voor andere doelen, is mogelijk in die gevallen waarin dit bij algemene maatregel van bestuur is voorzien. Voor de politiegegevens is dit uitgewerkt in het Besluit politiegegevens, voor justitiële gegevens is dit uitgewerkt in het Besluit justitiële gegevens. In deze algemene maatregelen van bestuur zijn de ontvangende personen en instanties opgesomd, aan wie bepaalde categorieën van politiegegevens of justitiële gegevens kunnen worden verstrekt ten behoeve van een goede uitvoering van hun taak. Daarbij kan het bijvoorbeeld gaan om de behartiging van de belangen van slachtoffers, het bieden van hulp en steun aan veroordeelde personen (reclassering) of de benoeming of het ontslag van gevangenispersoneel. Hiervoor kan worden verwezen naar de artikelen 4:1 tot en met 4:3 van het Bpg en de artikelen 13 tot en met 22 van het Bgj. Deze doelen brengen met zich mee dat bepaalde persoonsgegevens nodig zijn. Zo kan het bijvoorbeeld voor een slachtoffer van belang zijn te beschikken over de personalia van een dader of over een proces-verbaal waarin verklaringen zijn opgenomen van getuigen van een verkeersongeval, ten behoeve van het instellen van een vordering bij de civiele rechter. Een ander voorbeeld is dat de reclassering baat heeft bij de verstrekking van politiegegevens ten behoeve van de begeleiding van de verdachte of de veroordeelde. De Minister van Justitie heeft behoefte aan de verstrekking van politiegegevens over strafbaar handelen van gevangenenbewaarders ten behoeve van de bescherming van de integriteit van het gevangenispersoneel. De gegevensverstrekking stelt de ontvangende partij in staat tot een goede uitvoering van de taak, met het oog waarop de gegevens worden verstrekt. Daarnaast bieden zowel de Wpg als de Wjsg de verantwoordelijke de mogelijkheid om zelfstandig te besluiten tot de verstrekking van politiegegevens of van justitiële of strafvorderlijke gegevens aan derden, met het oog op bepaalde doelen die nauw samenhangen met de rechtshandhaving, zoals het voorkomen en opsporen van strafbare feiten, het handhaven van de openbare orde en het verlenen van hulp aan hen die deze behoeven. Gedacht kan worden aan de samenwerking met gemeenten bij de aanpak van drugsdealers om overlast en onveiligheid tegen te gaan of samenwerking met gemeenten, energiebedrijven en woningbouwverenigingen om hennepcultuur tegen te gaan, en aan de

verstrekking van strafvorderlijke gegevens door het openbaar ministerie aan de KNVB of aan openbaar vervoersbedrijven, ten behoeve van het handhaven van de openbare orde en veiligheid. De gegevensverstrekking dient het belang van de rechtshandhaving in meer ruime zin, omdat de samenwerking met de ontvangende instanties een bijdrage kan leveren aan de voorkoming en opsporing van strafbare feiten of de handhaving van de openbare orde.

De leden van de CDA-fractie hebben opgemerkt dat politiegegevens alleen mogen worden verstrekt als bij de ontvangende instantie voldoende waarborgen aanwezig zijn voor een juist gebruik van de verstrekte gegevens en voor de bescherming van de persoonlijke levenssfeer. Zij hebben gevraagd hoe dit wordt getoetst en in het bijzonder in nog niet zo lang geleden tot de Europese Unie toegetreden landen als Bulgarije en Roemenië.

Hierboven is, naar aanleiding van vragen van de leden van de SP reeds aangegeven dat alle lidstaten van de Europese Unie gebonden zijn aan de normen van het kaderbesluit en deze in hun nationale wetgeving dienen om te zetten. De Commissie houdt nauwgezet toezicht op de uitvoering van de Europese regels door de lidstaten. Daarnaast verplicht het kaderbesluit tot het inrichten van een nationale toezichthoudende autoriteit die de opgedragen taken in volstrekte onafhankelijkheid verricht en over de nodige onderzoeksbevoegdheden beschikt om de naleving van de regels af te dwingen. Bij hun toetreding in 2007 hebben Bulgarije en Roemenië het volledige «acquis communautaire» overgenomen, zodat ook de gegevensbeschermingsregels van de voormalige eerste pijler van de Europese Unie, waaronder de Privacyrichtlijn van 1995, in deze lidstaten volledig van toepassing zijn. Tot dusver is gebleken dat er in deze landen tekortkomingen zijn op het gebied van de rechtsstaat, de corruptiebestrijding en – ten aanzien van Bulgarije – de bestrijding van de georganiseerde misdaad. Om die tekortkomingen aan te pakken is op Europees niveau het Coöperatie- en Verificatie Mechanisme (CVM) ingesteld (Besluit 2006/928/EG van 13 december 2006, Pb EU L 354). Uit rapporten van de Commissie over beide landen blijkt dat de situatie op de voornoemde terreinen nog te wensen overlaat. Daarbij moet wel worden opgemerkt dat uit deze rapporten niet zozeer blijkt van tekortkomingen op het specifieke terrein van de bescherming van persoonsgegevens als van het tekort schieten van de structuren en uitvoering op het gebied van de rechtshandhaving. In de Kamerbrief waarin de interim-rapporten van de Europese Commissie over de voortgang van Bulgarije en Roemenië onder het Coöperatie- en verificatiemechanisme (CVM) aan u worden aangeboden (Kamerstukken 2010/11, 23 987, nr. 115) werd u geïnformeerd over de Nederlandse inzet gelet op de geconstateerde tekortkomingen en de toetreding van Bulgarije en Roemenië tot Schengen. Op het terrein van gegevensuitwisseling draaien beide landen al volledig mee binnen de Europese Unie (inclusief het gebruik van het Schengen informatie-systeem, SIS). Daarom dient een goede naleving van de geldende dataprotectieregels door beide landen via de kaders binnen de EU en op nationaal niveau gerealiseerd te worden. Ingeval er aanwijzingen zouden zijn dat de gemeenschappelijke regels over gegevensbescherming niet voldoende worden nageleefd, dan kunnen aanvullende maatregelen worden getroffen. Deze maatregelen zijn hierboven, naar aanleiding van een vraag van de SP-fractie over het toereikend beschermingsniveau in derde landen, aan de orde gekomen. Hierbij kan worden opgemerkt dat deze landen vanwege hun geografische ligging als doorvoerland worden gebruikt voor bepaalde vormen van ernstige criminaliteit waarin Nederland de eindbestemming is, zoals mensenhandel en de handel in verdovende middelen. Er is dus aan Nederlandse zijde een duidelijk



belang bij de uitwisseling van informatie ten behoeve van de criminaliteitsbestrijding.

### **VIII. De implementatie van de inhoud van het kaderbesluit**

De leden van de CDA-fractie hebben gevraagd naar de verwerking van gevoelige politiegegevens in de Wet justitiële en strafvorderlijke gegevens, nu in de toelichting op artikel 6 van het kaderbesluit louter de Wet politiegegevens is genoemd.

De verwerking van gevoelige gegevens is reeds geregeld in artikel 5 van de Wpg. Voor de gevoelige justitiële en strafvorderlijke gegevens zijn in de Wjsg echter geen specifieke regels opgenomen. Gevoelige justitiële gegevens worden niet verwerkt in de registers van de dienst Just-ID. Het is echter heel wel denkbaar dat gevoelige gegevens door het openbaar ministerie in een strafdossier worden opgenomen. Daarom wordt voorgesteld in de Wjsg specifieke bepalingen op te nemen over de verwerking van gevoelige gegevens. Dit betreft het voorgestelde artikel 39c, derde lid, en 40, derde lid, Wjsg (artikel II, onderdelen I en O).

De leden van de CDA-fractie hebben gevraagd hoe de regering aankijkt tegen feit dat noch de Wpg noch de Wjsg bepalingen bevat over een besluit dat voor betrokkene een nadelig rechtsgevolg heeft en of de regering nader kan toelichten waarom hieraan geen behoefte is, zoals bij de toelichting op artikel 7 van het kaderbesluit vermeld is.

Het kaderbesluit dataprotectie bepaalt dat een besluit dat voor de betrokkene een nadelig rechtsgevolg heeft of wezenlijke consequenties heeft voor hem, en dat uitsluitend op een geautomatiseerde gegevensverwerking berust die bestemd is om bepaalde aspecten van zijn persoonlijkheid te beoordelen, alleen mag worden genomen als dit is toegestaan bij de wet. Het kaderbesluit strekt ertoe dat, daar waar dit aan de orde zou zijn, voorzien is in een wettelijke regeling waarin waarborgen zijn opgenomen voor de bescherming van de gerechtvaardigde belangen van de betrokkene. Voor de implementatie betekent dit dat de lidstaten nagaan in hoeverre dergelijke geautomatiseerde verwerkingen aan de orde zijn, teneinde deze te toetsen aan het vereiste van de wettelijke grondslagen, in de daarvoor in aanmerking komende gevallen, in een dergelijke grondslag te voorzien. Zoals in de memorie van toelichting is aangegeven kennen noch de Wpg noch de Wjsg dergelijke verwerkingen, waarbij een besluit met wezenlijke consequenties voor de betrokkene uitsluitend op een geautomatiseerde gegevensverwerking berust die bestemd is om bepaalde aspecten van zijn persoonlijkheid te beoordelen. Daar waar geautomatiseerde verwerking van politiegegevens of van justitiële of strafvorderlijke gegevens aan de orde is, is menselijke tussenkomst voorzien voor de waardering van de uitkomsten dan wel het geven van opvolging aan het resultaat van de geautomatiseerde gegevensverwerking. Een voorbeeld betreft de verstrekking van een verklaring omtrent het gedrag (VOG), waarbij justitiële gegevens worden geraadpleegd en getoetst op relevantie voor de afgifte van de verklaring. Een ander voorbeeld betreft de geautomatiseerde bevraging van vingerafdrukken door contactpunten van andere lidstaten. Een dergelijke bevraging vindt plaats op basis van hit/no hit. De koppeling van de gegevens vindt echter plaats door het nationale contactpunt van de verzoekende staat, en voor de verstrekking van de persoonsgegevens is een rechtshulpverzoek vereist. Indien politie of justitie in de toekomst wel zouden overgaan tot het nemen van besluiten die voor de betrokkenen een nadelig rechtsgevolg of wezenlijke consequenties hebben en die uitsluitend op een geautomatiseerde gegevensverwerking berusten, zal daarvoor alsnog voorzien moeten worden in een adequate wettelijke regeling.

Verder hebben de leden van de CDA-fractie erop gewezen dat in de toelichting op de artikelen 8, 9, 12, 13, 14 en 15 van het kaderbesluit melding wordt gemaakt van het feit dat in nadere regeling zal worden voorzien in het Besluit politiegegevens en/of het Besluit justitiële gegevens. Zij hebben gevraagd wanneer en op welke termijn hierin zal worden voorzien.

Zoals in antwoord op een andere vraag van de leden van deze fractie, over de aangekondigde algemene maatregel van bestuur hiervoor is vermeld, zal het ontwerp voor deze algemene maatregel van bestuur voor advies aan de Raad van State worden voorgelegd zodra het wetsvoorstel door de Kamer is aanvaard.

Voorts hebben de leden van de CDA-fractie gesteld dat uit de toelichting op artikel 16 van het kaderbesluit blijkt dat noch de Wpg noch de Wjsg de verplichting tot het informeren van de betrokkene kennen over het verzamelen en verwerken van persoonsgegevens door de bevoegde autoriteiten. Zij hebben gevraagd waarom dit zo is en of hier toch niet in moet worden voorzien.

Op grond van artikel 16 van het kaderbesluit zien de lidstaten erop toe dat de betrokkene overeenkomstig het nationaal recht wordt geïnformeerd over het verzamelen en verwerken van persoonsgegevens door hun bevoegde autoriteiten. Aan de lidstaten wordt op dit punt dus de nodige beleidsruimte gelaten. De Wet politiegegevens en de Wet justitiële en strafvorderlijke gegevens kennen thans geen algemene verplichting voor politie en justitiële autoriteiten om de betrokkene te informeren over de verwerking van gegevens die op zijn persoon betrekking hebben. Een algemene verplichting tot het informeren van de betrokkene dat over hem persoonsgegevens worden verwerkt, verdraagt zich niet goed met de aard van de werkzaamheden van politie en justitie. De uitvoering van de politietaak omvat zeer uiteenlopende werkzaamheden, zoals de beheersing van grootschalige manifestaties, in het kader van de handhaving van de openbare orde, of de bemiddeling tussen maatschappelijke organisaties bij de opvang van dakloze of anderszins hulpbehoevende personen. Het informeren van de betrokkene over de gegevensverwerking is niet alleen zeer bewerkelijk in de praktijk, bijvoorbeeld bij de aanhouding van groepen van personen in verband met grootschalige ordeverstoringen, maar ook onmogelijk, bijvoorbeeld bij het fotograferen van onbekende personen die zich bij voetbalwedstrijden misdragen. Een verplichting tot het informeren van de betrokken personen over de gegevensverwerking door de politie zou een aanzienlijke verzwaring van de werklast opleveren, die voor een belangrijk deel overbodig is omdat de betrokkene er in de gevallen waarin hij met de politie in aanraking komt redelijkerwijs van op de hoogte kan zijn dat de politie persoonsgegevens over hem verwerkt. Voor wat betreft de opsporingstaak geldt dat opsporingsbevoegdheden, bijvoorbeeld observaties, heimelijk toegepast moeten kunnen worden. Immers, de betrokken personen zouden waarschijnlijk direct hun gedrag aanpassen zodra zij kennis zouden hebben van het feit dat de politie in hen is geïnteresseerd. Een verplichting tot het informeren van de betrokkene zou dus niet alleen forse uitvoeringslasten met zich meebrengen maar ook het opsporingsonderzoek ernstig kunnen belemmeren. Een algemene verplichting tot het informeren van de betrokkene over de gegevensverwerking door politie en justitie acht ik dan ook niet wenselijk. Uit de wet- en regelgeving kan de betrokkene opmaken in welke gevallen en onder welke voorwaarden politie en justitie persoonsgegevens over hem kunnen verwerken. Daarnaast bestaat er voor de betrokkene een recht op kennisneming van de over hem verwerkte persoonsgegevens, met dien verstande dat de betreffende rechtshandavingsinstantie bepaalde weigeringsgronden in

kan roepen. Naar het oordeel van het kabinet wordt met het voorgaande in voldoende mate voorzien in de vereiste kenbaarheid voor de betrokkene over de gegevensverwerking door politie en justitie.

De leden van de SP-fractie hebben om een toelichting gevraagd op artikel 14 van het kaderbesluit, over de doorgifte aan particuliere instanties in de lidstaten. Deze leden stelden vast dat de Wpg en de Wjsg nu nog geen bepalingen kennen over de doorgifte van persoonsgegevens aan particuliere instanties in het buitenland en veronderstelden dat dit wel niet voor niets zal zijn geweest. Zij hebben gevraagd om welke particuliere instanties het gaat en zouden hierop graag een toelichting ontvangen.

De doorverstrekking van politiegegevens aan een particuliere instantie in het buitenland is op basis van de huidige regelgeving niet mogelijk. In het Besluit politiegegevens is bepaald dat politiegegevens die aan een ander land zijn verstrekt ten behoeve van de goede uitvoering van de politietaken in dat land, voor een ander doel kunnen worden verwerkt voor zover dit noodzakelijk is voor de goede uitvoering van de politietaken in dat land (art. 5:1, tweede lid, Bpg). Dit kan betekenen dat binnen dat land gegevens verstrekt kunnen worden aan een particuliere instantie. Hierboven zijn, in antwoord op vragen van de leden van de fractie van het CDA, voorbeelden gegeven van gevallen waarin de mogelijkheid van verstrekking van persoonsgegevens aan personen of instanties met een particuliere taak, zoals een luchtvaartmaatschappij of een voetbalorganisatie wenselijk kan zijn. De regering is dan ook verheugd dat het kaderbesluit rekening houdt met de mogelijkheid van de noodzaak van doorgifte van verstrekte persoonsgegevens in een andere lidstaat en aan personen en instanties met een particuliere taak.

De leden van de ChristenUnie-fractie hebben opgemerkt dat met de implementatie van het kaderbesluit de geldende regels op een enkel punt worden verruimd. Zo voorziet het kaderbesluit dataprotectie in de mogelijkheid om persoonsgegevens, die door een andere lidstaat zijn verstrekt ten behoeve van de opsporing van strafbare feiten, verder te verwerken ten behoeve van de vervolging van strafbare feiten of van andere strafbare feiten. Hiermee wordt de doelbinding, die aan de Nederlandse wetgeving ten grondslag ligt, verruimd. De leden van deze fractie hebben de regering verzocht nader toe te lichten waarom deze verruiming noodzakelijk is en daarbij verzocht de stelling in de memorie van toelichting dat deze verruiming goed aansluit bij de behoeften van de praktijk, nader toe te lichten.

Op grond van het Besluit politiegegevens geldt een strikte doelbinding voor het gebruik van verstrekte politiegegevens door het ontvangende land. De gegevens worden verstrekt onder de algemene voorwaarde dat deze slechts verder kunnen worden verwerkt voor het doel waarvoor ze zijn verstrekt. Dit betreft het concrete opsporingsonderzoek ten behoeve waarvan de gegevens zijn verstrekt. Dit betekent dat als het ontvangende land de verstrekte gegevens wil gebruiken in een ander opsporingsonderzoek, aanvullend toestemming moet worden gevraagd aan de bevoegde Nederlandse autoriteiten. In de praktijk blijkt dit systeem niet alleen zeer bewerkelijk, omdat daarvoor aanvullende toestemming moet worden gevraagd, maar biedt dit ook weinig toegevoegde waarde, omdat het gebruik van de verstrekte politiegegevens voor andere opsporingsonderzoeken bezwaarlijk kan worden geweigerd. Om deze reden heeft verruiming op dit punt, waartoe het kaderbesluit reden geeft, mijn instemming. Aan de zijde van de Nederlandse politie ligt hier eveneens een duidelijk inhoudelijk belang, omdat het vanuit het oogpunt van de werklast en de efficiency nuttig is dat politiegegevens, die van een andere lidstaat zijn ontvangen, ook voor andere opsporingsonderzoeken kunnen

worden gebruikt zonder dat daarvoor aanvullende instemming vereist is. Voor wat betreft het gebruik van politiegegevens in het kader van strafvervolging ligt het in de rede dat persoonsgegevens, die zijn verstrekt ten behoeve van een bepaald opsporingsonderzoek, in beginsel ook kunnen worden gebruikt in de betreffende strafzaak. Daarbij wordt in de lidstaten doorgaans wel een justitieel rechtshulpverzoek vereist, indien de gegevens worden gebruikt ten behoeve van het bewijs in die strafzaak. Dit aanvullende toestemmingsvereiste heeft ten doel de actualiteit van de eerder verstrekte gegevens te kunnen controleren en te voorkomen dat gevoelige of «zachte» politiegegevens bij de verdachte bekend raken. De Schengen Uitvoeringsovereenkomst bevat hiervoor een grondslag (artikel 39, tweede lid, SUO). Ditzelfde geldt voor het kaderbesluit 2006/960/JBZ van de Raad van 18 december 2006 betreffende de vereenvoudiging van de uitwisseling van informatie en inlichtingen tussen de rechtshandhavingsautoriteiten van de lidstaten van de Europese Unie (PbEU L 386), ook bekend als het Zweedse kaderbesluit (artikel 3, vijfde lid). Dergelijke regels worden door het kaderbesluit onverlet gelaten (Overwegingen 39 en 40). In het kaderbesluit is de verruiming van de doelbinding beperkt tot de preventie, het onderzoek, de opsporing of de vervolging van andere strafbare feiten of de tenuitvoerlegging van andere straffen dan die waarvoor de gegevens waren verstrekt of beschikbaar gesteld en andere gerechtelijke of administratieve procedures daarmee die rechtstreeks verband houden (artikel 11, onderdelen a en b). Het verdere gebruik van de gegevens ten behoeve van een onmiddellijke en ernstige bedreiging van de openbare veiligheid (artikel 11, onderdeel c), betreft een algemeen aanvaarde verruiming, die ook in verschillende andere EU-rechtsinstrumenten terug te vinden is. Daarvoor kan worden gewezen op artikel 23, eerste lid, onderdeel c, van de Overeenkomst, door de Raad vastgesteld overeenkomstig artikel 34 van het Verdrag betreffende de Europese Unie, betreffende de wederzijdse rechtshulp in strafzaken tussen de lidstaten van de Europese Unie, met verklaringen, ook bekend als de EU-rechtshulpovereenkomst en artikel 8, derde lid, van het eerdergenoemde Zweedse kaderbesluit.

### **IX. De inhoud van het wetsvoorstel op hoofdlijnen**

De leden van de VVD-fractie wilden expliciet van de regering vernemen op welke punten dit wetsvoorstel afwijkt van het kaderbesluit, en bij afwijking wat de motivering van die afwijking is.

In de memorie van toelichting bij het wetsvoorstel zijn de uitgangspunten voor de implementatie van het kaderbesluit geschetst (Kamerstukken II, 2010/11, 32 554, nr. 3, blz. 8/9). Tevens is een overzicht opgenomen van de wijze waarop de verplichtingen van het kaderbesluit zijn opgenomen in de Nederlandse wetgeving (Kamerstukken II, 2010/11, 32 554, nr. 3, blz. 11/14). In zijn algemeenheid kan worden opgemerkt dat op het punt van het toepassingsbereik van de regels is afgeweken van het kaderbesluit, omdat ervoor gekozen is de regels van het kaderbesluit ook van toepassing te laten zijn op gegevens die uitsluitend op nationaal niveau worden verwerkt. Overigens wijkt het wetsvoorstel inhoudelijk niet af van het kaderbesluit, met dien verstande dat geen wettelijke regels zijn opgenomen voor geautomatiseerde individuele besluiten (artikel 7). Verder zijn geen wettelijke regels opgenomen over het informeren van de betrokkene. Op dit punt laat het kaderbesluit de lidstaten de ruimte voor eigen afwegingen. Op dit punt is hierboven ingegaan, naar aanleiding van vragen van de fractie van het CDA.

De leden van de PvdA-fractie hebben gevraagd welke mogelijkheden landen hebben om te weigeren persoonsgegevens te verstrekken.

Het kaderbesluit bevat geen bevoegdheden of verplichtingen tot het verstrekken van persoonsgegevens. Dergelijke bevoegdheden of verplichtingen kunnen onderdeel vormen van EU-rechtsinstrumenten, zoals een richtlijn of een overeenkomst, over de uitwisseling van gegevens ten behoeve van bepaalde doelen op het terrein van de opsporing of vervolging van strafbare feiten, waarvoor de Europese Unie bevoegd is. In deze afspraken kunnen tevens weigeringsgronden worden opgenomen. Gewezen kan worden op het Raadsbesluit 2008/615/JBZ over de verbetering van de grensoverschrijdende samenwerking, in het bijzonder bij de bestrijding van terrorisme en grensoverschrijdende criminaliteit (PbEU L 210), dat voorziet in de verplichting van de lidstaten om DNA-profielen en vingerafdrukken ter beschikking te stellen ten behoeve van de vergelijking van gegevens. Ook van belang is het eerdergenoemde Zweedse kaderbesluit, waarin een verplichting voor de lidstaten is opgenomen om voor het verstrekken van informatie en inlichtingen aan de bevoegde rechtshandhavingsautoriteiten van een andere lidstaat geen striktere voorwaarden toe te passen dan de op nationaal niveau toepasselijke voorwaarden voor het verstrekken van en verzoeken om informatie en inlichtingen. De verstrekking van de informatie of inlichtingen mag worden geweigerd als de wezenlijke nationale veiligheidsbelangen van de aangezochte lidstaat zouden worden geschaad, het welslagen van een lopend onderzoek of de veiligheid van personen in gevaar worden gebracht of het verzoek niet in verhouding staat tot de doeleinden waarvoor de betrokken informatie of inlichtingen zijn gevraagd. Ook geldt een weigeringsgrond voor het verzoek dat betrekking heeft op een strafbaar feit dat naar het recht van de aangezochte lidstaat strafbaar is met een gevangenisstraf van maximaal een jaar. De mogelijkheden die landen hebben om te weigeren persoonsgegevens te verstrekken kunnen dus uit deze en andere EU-rechtsinstrumenten voortvloeien. De regels van kaderbesluit dataprotectie zijn van toepassing *als* persoonsgegevens worden verstrekt. Deze regels betreffen de doelbinding, het gebruik van de ontvangen gegevens voor andere doelen, de bewaartermijnen, de rechten van de betrokkene en dergelijke.

#### *De verenigbaarheid van de verdere verwerking*

De leden van de PvdA-fractie hebben opgemerkt dat volgens het voorgestelde artikel 3 van de Wjsg justitiële gegevens uitsluitend voor een ander doel verwerkt kunnen worden als deze verwerking niet onverenigbaar is met het doel waarvoor de gegevens zijn verkregen en hebben gevraagd wanneer sprake is van onverenigbaarheid met het doel waarvoor de gegevens zijn verkregen, en of de regering dit kan toelichten. Verder hebben deze leden gevraagd of het niet voor de hand ligt dat, wanneer politiegegevens of justitiële gegevens worden verzocht van een ander land en waar het een ander doel betreft, de betrokkene altijd om toestemming moet worden gevraagd.

Het kaderbesluit dataprotectie geeft regels voor de doelbinding. Dat wil zeggen dat het verzamelen en verwerken van persoonsgegevens wordt gebonden aan bepaalde doelen. Daarbij geldt uiteraard dat die doelen zo specifieke mogelijk moeten worden beschreven, zodat er daadwerkelijk sprake is van inkadering. Het kan echter voorkomen dat een maatschappelijke behoefte bestaat om persoonsgegevens, die zijn verzameld ten behoeve van een bepaald doel, verder te verwerken voor een ander doel. Dit belang van verdere verwerking dient te worden afgewogen tegen het belang van de betrokkene dat de gegevensverwerking over zijn persoon beperkt is tot het doel waarvoor de gegevens zijn verzameld. Als een persoon wordt veroordeeld voor een strafbaar feit, dan worden gegevens over de veroordeling geregistreerd ten behoeve van de strafrechtspleging. Bij latere strafzaken kan dan rekening worden gehouden met de eerdere

veroordeling. Deze gegevens kunnen echter ook nuttig zijn voor andere doelen, die samenhangen met het doel waarvoor de persoonsgegevens zijn verzameld, bijvoorbeeld het kunnen opstellen van een verklaring omtrent het gedrag. Het kaderbesluit schrijft voor dat de verdere verwerking van de gegevens voor een ander doel is toegestaan mits deze verwerking niet onverenigbaar is met het doel waarvoor de gegevens zijn verzameld. Hiermee wordt tot uitdrukking gebracht dat het doel van de verdere verwerking samenhang dient te vertonen met het doel waarvoor de gegevens zijn verzameld. Hierin schuilt uiteraard een zekere marge voor afweging in concrete gevallen. In zijn algemeenheid kan hierover echter worden opgemerkt dat het doel van de strafrechtspleging is gelegen in de bescherming van de maatschappij tegen criminaliteit. Met dat doel is verenigbaar dat de gegevens, die zijn verzameld voor de strafrechtspleging, verder worden verwerkt voor bijvoorbeeld de bewaking van de integriteit van de samenleving bij de toekenning van overheidsopdrachten, de selectie van personeel, de vervulling van belangrijke functies of de verlening van een militaire of Koninklijke onderscheiding. Met dat doel is niet verenigbaar dat de gegevens verder worden verwerkt voor doelen die geen samenhang hebben met het doel van de strafrechtspleging, zoals het aanspraak maken op gezondheidszorg of het volgen van onderwijs.

Het kaderbesluit regelt dat persoonsgegevens, die aan een andere lidstaat worden verstrekt ten behoeve van de preventie, het onderzoek of de vervolging van strafbare feiten of de tenuitvoerlegging van straffen, vervolgens verder kunnen worden verwerkt voor de in artikel 11 opgesomde doelen. De verdere verwerking voor een ander doel is slechts mogelijk na voorafgaande toestemming van de verstreckende lidstaat of met instemming van de betrokkene. Het vereiste van de instemming van de betrokkene is opgenomen op initiatief van enkele Scandinavische lidstaten, die in hun wettelijk systeem uitgaan van dit vereiste als voorwaarde voor de verdere verwerking van de persoonsgegevens. Voor Nederland is dit echter niet het geval, zoals hierboven reeds aan de orde is gekomen. Het ligt niet voor de hand om de verdere verwerking afhankelijk te doen zijn van de instemming van de betrokkene omdat dit voor de nationale situatie evenmin het geval is. De instemming van de verstreckende lidstaat is afhankelijk van de wettelijke mogelijkheden voor het verdere gebruik van de gegevens, die op grond van het nationale recht gelden. De samenwerking tussen de lidstaten bij de aanpak van gemeenschappelijke problemen, zou worden gehinderd als de toestemming van de betrokkene bepalend is voor de verdere verwerking van de gegevens voor bijvoorbeeld de screening van personen die in aanmerking willen komen voor een bepaalde maatschappelijke functie. Dit zou bovendien grote consequenties kunnen hebben voor de werklast van politie en justitie omdat de betrokkene niet altijd eenvoudig te vinden zal kunnen zijn.

#### *De verwerking van gevoelige persoonsgegevens*

De leden van de SP-fractie hebben geconstateerd dat de Wjsg nu nog geen bepaling kent over de verwerking van gevoelige persoonsgegevens maar dat deze nu wordt geïntroduceerd. Zij hebben gevraagd naar de reden waarom dat tot nu toe nog niet het geval was. Zij hebben gevraagd of daar geen behoefte aan was in de praktijk, of gevoelige persoonsgegevens niet werden verwerkt of dat er vooralsnog geen goede regels voor waren.

De Wet bescherming persoonsgegevens kent specifieke regels voor de verwerking van gevoelige persoonsgegevens (artikel 16 Wbp). Deze regels gelden evenwel niet voor de gegevensverwerking in strafzaken, omdat de Wet bescherming persoonsgegevens niet van toepassing is op de

verwerking van persoonsgegevens ten behoeve van de uitvoering van de Wet justitiële en strafvorderlijke gegevens (artikel 2, tweede lid, onderdeel e, Wbp). De Wet justitiële en strafvorderlijke gegevens geeft invulling aan het normenkader van de Wet bescherming persoonsgegevens, specifiek voor de gegevens die door het openbaar ministerie in een strafdossier worden verwerkt. Daarbij is er in het verleden niet voor gekozen specifieke regels op te nemen voor de verwerking van gevoelige persoonsgegevens. Dit hangt ermee samen dat – zoals hiervoor al aan de orde kwam – geen gevoelige justitiële gegevens worden verwerkt in de registers van de dienst Just-ID. Daarnaast bestaat het vertrouwen dat, indien gevoelige gegevens door het openbaar ministerie in een strafdossier zijn opgenomen, het openbaar ministerie zorgvuldig zal omgaan met eventuele verzoeken tot verstrekking van deze gegevens. Nu het kaderbesluit specifieke regels geeft over de verwerking van gevoelige persoonsgegevens, vormt dit aanleiding om de Wet justitie en strafvorderlijke gegevens op dit punt aan te vullen.

#### *De doorgifte van gegevens aan derde landen*

De leden van de PvdA-fractie hebben gevraagd of zij het goed hebben begrepen dat gegevens ook verstrekt kunnen worden aan een land dat gelegen is buiten de EU, en aan welke regels dit land moet voldoen alvorens de regering akkoord gaat met verstrekking van die persoonsgegevens. Verder hebben zij gevraagd of er controle plaatsvindt door de Nederlandse overheid als een ander EU-land gegevens die zijn verkregen van de Nederlandse autoriteiten, doorstuurt aan een derde, niet zijnde een EU-land.

Het kaderbesluit schrijft voor dat persoonsgegevens, die van een andere lidstaat zijn ontvangen, uitsluitend aan een derde land kunnen worden doorgegeven met instemming van de lidstaat waarvan de gegevens afkomstig zijn (artikel 13, eerste lid, onderdeel c). Dit instemmingvereiste is neergelegd in artikel 5:3, derde lid, van het ontwerpbesluit politiegegevens, dat als bijlage bij deze nota naar aanleiding van het verslag is gevoegd. Verder is vereist dat het derde land een toereikend beschermingsniveau voor de voorgenomen gegevensverwerking garandeert. Dit vereiste is hierboven toegelicht, bij de beantwoording van de vraag van de leden van de fracties van de SP en van D66. Het instemmingsvereiste brengt met zich mee dat de Nederlandse autoriteiten toetsen of er sprake is van een toereikend beschermingsniveau in het betreffende derde land, voordat de gegevens door een andere lidstaat wordt doorverstrekt. Deze toets is inhoudelijk gelijk aan de beoordeling van het toereikend beschermingsniveau in die gevallen waarin de persoonsgegevens door de Nederlandse autoriteiten rechtstreeks aan het derde land worden verstrekt. De wijze van toetsing is hierboven eveneens toegelicht, bij de beantwoording van de vraag van de leden van de fracties van de SP en van D66.

#### *Het recht op kennisneming*

De leden van de VVD-fractie hebben gevraagd hoe in dit wetsvoorstel invulling is gegeven aan het recht van de betrokkene geïnformeerd te worden over het verzamelen en verwerken van persoonsgegevens door de bevoegde autoriteiten, zoals verwoord in artikel 16 van het kaderbesluit en dit in samenhang met overweging 27.

Voor de beantwoording van deze vraag verwijs ik graag naar de eerdere beantwoording van een vergelijkbare vraag van de leden van de CDA-fractie. Daarbij merk ik nog op dat het kaderbesluit niet voorziet in een recht van de betrokkene geïnformeerd te worden over het verzamelen

en verwerken van persoonsgegevens. Het kaderbesluit verwijst hiervoor naar het nationale recht van de lidstaten zodat de lidstaten op de punt de nodige beleidsruimte houden.

De leden van de CDA-fractie wilden de wijziging van de onderhavige wetgeving aangrijpen om de problemen met de Wet openbaarheid van bestuur (Wob) aan te pakken. Zij hebben gesteld dat iedereen op grond van de Wob informatie of documenten kan opvragen. Door «creatief» gebruik te maken van de Wob kan men volgens deze leden het vereiste van het zwaarwegend algemeen belang, dat op grond van de Wpg en de Wjsg is vereist om aan informatie te komen, worden omzeild. Dat kan niet de bedoeling van de Wob zijn geweest, en is zeker niet in het belang van de veiligheid. Deze leden wilden zeker gesteld krijgen dat de voorliggende wijziging van de Wpg en de Wjsg, maar ook de documenten waarin die gegevens zijn vevat, gelden als *lex specialis* ten opzichte van de Wob. De leden van deze fractie hoorden graag of ik hier positief tegenover sta en zo ja, hoe de regering hier uitvoering aan gaat geven, en zo nee, waarom niet.

De Wet politiegegevens en de Wet justitiële en strafvorderlijke gegevens kennen een ieder het recht toe te vernemen of, en zo ja welke, deze persoon betreffende persoonsgegevens zijn vastgelegd (artikelen 25, eerste lid, Wpg en 18, eerste lid, Wjsg). Het recht op kennisneming is een essentieel recht binnen het systeem van de bescherming van persoonsgegevens. Het is echter geen absoluut recht, omdat bij wet beperkingen op dit recht kunnen worden aangebracht (artikel 10, derde lid, GW). In de Wpg en de Wjsg zijn weigeringsgronden opgenomen die samenhangen met de bescherming van het belang van opsporing en vervolging, het belang van de nationale veiligheid en de belangen van derden.

De Wet openbaarheid van bestuur (Wob) biedt eenieder de mogelijkheid een verzoek om informatie tot een bestuursorgaan te richten (artikel 3, eerste lid, Wob). Het gaat om informatie neergelegd in documenten over een bestuurlijke aangelegenheid. Een politiekorps is een bestuursorgaan in de zin van de Wet openbaarheid van bestuur. Een belanghebbende kan een dergelijk verzoek aan de korpsbeheerder richten. Een verzoek om informatie wordt ingewilligd met inachtneming van uitzonderingsgronden en beperkingen (artikel 3, vijfde lid, Wob). Het verstrekken van informatie blijft onder meer achterwege voor zover het belang daarvan niet opweegt tegen het belang van de opsporing en vervolging van strafbare feiten (artikel 10, tweede lid, onderdeel c, Wob). Dit betreft een zogenaamde relatieve weigeringsgrond, omdat het belang van de verstrekking moet worden tegen het belang van opsporing en vervolging.

Met de Wob is niet beoogd de bestaande wettelijke regelingen inzake openbaarheid en geheimhouding op speciale terreinen opzij te zetten dan wel daarnaast een aanvullende mogelijkheid te bieden om informatie te verkrijgen. Blijkens de wetsgeschiedenis derogerde de oude Wet politieregisters (Wpolr) destijds aan de Wob. In de rechtspraak is aanvaard dat de bepalingen over het recht op kennisneming in de oude WPolr dan als specialis gelden ten opzichte van de Wob. In deze lijn is later verandering gekomen, doordat de bestuursrechter onderscheid is gaan maken tussen gegevens die onder de reikwijdte van de oude Wet politieregisters vallen en overige informatie (zie RvS 11-02-2004, LJN: AO3393, RvS 28-02-2007, LJN: AZ9505 en RvS 29-11-2006, LJN: AZ3237). Sedertdien wordt in de bestuursrechtspraak de lijn aangehouden dat ook het verstrekkingenregime van de Wpg uitsluitend betrekking heeft op persoonsgegevens als bedoeld in artikel 1, aanhef en onder a, van de Wbp, en niet op de documenten waarin deze gegevens zijn vevat. In dit stelsel brengt de omstandigheid dat een document persoonsgegevens



bevat niet met zich dat het document als zodanig onder de werking van de Wpg valt (zie RvS 19-05-2010, LJN: BM 4969). Dit betekent dat er twee wettelijke openbaarheidsregimes van toepassing kunnen zijn op de gevraagde informatie. Deze jurisprudentie brengt met zich mee dat de korpsbeheerder nader zal moeten vaststellen welke gegevens uit de documenten als politiegegevens zijn aan te merken. Ten aanzien van de documenten zal hij, voor zover die geen politiegegevens behelzen, alsnog toepassing moeten geven aan de Wob. Ten aanzien van diezelfde documenten zal hij, voor zover die wel politiegegevens behelzen, toepassing geven aan het verstrekkingenregime van de Wpg.

Toetsing van informatie aan zowel de Wpg als de Wob kan een behoorlijke aanslag vormen op de beschikbare capaciteit van het betreffende bestuursorgaan. De Wob kent op dit moment geen mogelijkheid tot afweging van het belang van de openbaarheid ten opzichte van de capaciteit die het aanleveren van informatie kost (proportionaliteit). In het plan «Minder regels, meer op straat», dat 18 februari 2011 aan Uw Kamer is gezonden (Kamerstukken II, 2010/11, 29 628, nr. 238), heb ik aangegeven te streven naar opname van een proportionaliteitsafweging in de Wob, omdat de inzet van politiecapaciteit voor het afhandelen van omvangrijke Wob-verzoeken niet onbeperkt kan zijn. Voor het zomerreces zal mijn ambtgenoot van Binnenlandse Zaken en Koninkrijksrelaties een brief aan de Kamer verzenden met nadere voorstellen voor de Wob. Daarin zal ook op dit punt worden in gegaan.

#### *De positie van de toezichthoudende autoriteiten*

De leden van de PvdA-fractie hebben in de memorie van toelichting gelezen dat gegevens in het verzoekende land ook mogen worden doorgespeeld aan particuliere bedrijven en hebben gevraagd welk belang hiermee gediend wordt. Verder hebben zij gevraagd aan welke bedrijven deze gegevens mogen worden doorgespeeld en zo ja, waarom juist deze bedrijven, of het land dat de gegevens verstuurd eisen kan stellen aan het verwerken, opslaan, termijnen en dergelijke van de gegevens in het ontvangende land, of het doorgeven van politiegegevens of justitiële gegevens aan particuliere instanties niet een vergaande mogelijkheid is die eenvoudig misbruikt kan worden en hoe de regering in de toekomst omgaat met verzoeken om persoonsgegevens van andere EU-landen waarvan duidelijk is dat die doorgespeeld worden aan particuliere instanties aldaar, en zo nee, waarom niet. Voorts hebben deze leden opgemerkt dat de bevoegde autoriteiten maatregelen moeten treffen om persoonsgegevens te beveiligen tegen alle vormen van onrechtmatige verwerking. Zij hebben gevraagd hoe de autoriteiten voorkomen dat gegevens onrechtmatig worden verwerkt, terwijl gegevens ook aan particuliere organisaties en derde landen kunnen worden doorgespeeld. Tenslotte hebben zij gevraagd welke eisen de autoriteiten kunnen stellen aan deze particuliere instanties en derde landen.

Hierboven is, naar aanleiding van vragen van de leden van de fracties van het CDA en de SP, reeds ingegaan op de vraag om welke particuliere instanties het gaat bij de doorgifte van persoonsgegevens aan het buitenland. Daarbij zijn voorbeelden gegeven, zoals de verstrekking van persoonsgegevens aan luchtvaartmaatschappijen of aan buitenlandse voetbalorganisaties. De lidstaat van herkomst kan eisen stellen aan de doorgifte aan een particuliere instantie, omdat het kaderbesluit voorschrijft dat voor de doorgifte de toestemming van de bevoegde autoriteit van die lidstaat met inachtneming van het nationale recht vereist is. Verder is vereist dat afgewogen wordt of geen gerechtvaardigde specifieke belangen van de betrokkene zich tegen doorgifte verzetten en dat de doorgifte in bijzondere gevallen essentieel is voor de verstrekking

autoriteit ten behoeve van bepaalde doelen, zoals de uitvoering van haar wettelijke taak of de preventie, het onderzoek, de opsporing of de vervolging van strafbare feiten. De bevoegde autoriteit, die de gegevens doorgeeft, deelt de ontvangende particuliere instantie mee voor welk doel de gegevens uitsluitend gebruikt mogen worden. Daarbij geldt voor de ontvangers een wettelijke geheimhoudingsverplichting (artikel 7 Wpg). Uiteraard zullen de eventuele particuliere ontvangers op deze geheimhoudingsplicht worden gewezen. Of dit niet een vergaande mogelijkheid is die eenvoudig misbruikt kan worden, hangt af van de aard van de gegevens die worden verstrekt en de instantie aan wie de gegevens worden verstrekt. De regering zal in de toekomst verzoeken om persoonsgegevens van andere EU-landen, waarvan duidelijk is dat die doorgegeefd worden aan particuliere instanties, zorgvuldig toetsen, onder meer aan de in het kaderbesluit gespecificeerde doelen, en uitsluitend instemmen met de doorgifte indien een degelijke doorgifte in een vergelijkbare nationale situatie eveneens plaats zou hebben gevonden. Daarbij zal de voorgenomen doorgifte van de gegevens worden getoetst aan de eisen van noodzakelijkheid en proportionaliteit. Dit is bij de beantwoording van de eerdere vragen van de leden van de fracties van het CDA en de SP reeds aan de orde is gekomen. De leden van de SP-fractie hebben geconstateerd dat de wettelijke bevoegdheden van het Cbp worden aangevuld. Zij steunen deze aanvulling, maar hebben opgemerkt dat het Cbp toch in het algemeen meer bevoegdheden zou worden toebedeeld, bijvoorbeeld de mogelijkheid hogere boetes op te leggen. Zij hebben gevraagd wanneer die voorstellen de Kamer zullen bereiken.

Naar aanleiding van het rapport van de Adviescommissie Veiligheid en persoonlijke levenssfeer (commissie Brouwer-Korf) en het standpunt van het kabinet ten aanzien van de bevindingen van de commissie, wordt thans een wetsvoorstel voorbereid tot wijziging van de Wet bescherming persoonsgegevens. Naar verwachting zal het wetsvoorstel medio 2011 voor consultatie gereed zijn.

#### **X. Overige onderwerpen van dit wetsvoorstel**

De leden van de VVD-fractie wilden nog een opmerking maken over het Europolbesluit. Zij hebben opgemerkt dat gebleken is dat het Cbp vooralsnog niet formeel is aangewezen als nationaal controleorgaan. Bovendien bestaat er onduidelijkheid over het materieelrechtelijke kader voor verwerkingen in het Europees Informatie Systeem. Deze leden hebben de regering verzocht hierop in te gaan.

Het Besluit van de Raad van 6 april 2009, tot oprichting van de Europese politiedienst (2009/371/JBZ, PbEU L 121/37) schrijft voor dat iedere lidstaat een nationaal orgaan aanwijst dat, volgens het nationale recht onafhankelijk toeziet op de rechtmatigheid van de invoer, de opvraging en de verstrekking aan Europol van persoonsgegevens door de betrokken lidstaat, en dat toetst of de rechten van de betrokkene door deze invoer, opvraging of verstrekking niet worden geschaad (artikel 33, eerste lid, Besluit 2009/371/JBZ). Op grond van de Wet politiegegevens is het College bescherming persoonsgegevens belast met het toezicht op de verwerking van politiegegevens overeenkomstig het bij en krachtens deze wet bepaalde (artikel 35, eerste lid, Wpg). Hieruit volgt dat dit toezicht mede betrekking heeft op de invoer, opvraging en verstrekking van politiegegevens aan Europol. Een formele aanwijzing van het Cbp als nationaal controleorgaan voegt daaraan materieel niets toe, nu het toezicht van het Cbp reeds voortvloeit uit de wet.

Voor wat betreft het door de leden van de VVD-fractie aangehaalde materieelrechtelijke kader voor verwerkingen in het Europees Informatie Systeem neemt het kabinet aan dat deze leden hiermee doelen op het Europol-informatiesysteem. Het materieelrechtelijke kader voor deze verwerkingen is terug te vinden in het eerdergenoemde Besluit van de Raad van 6 april 2009 tot oprichting van de Europese politiedienst. Voorzien is in uitgebreide regels over het informatiesysteem van Europol, het gebruik van de gegevens en de rechten van betrokkenen. Het kabinet is verder overigens niet bekend met onduidelijkheid hierover.

## **XI. Adviezen**

De leden van de VVD-fractie hebben opgemerkt dat in het nader rapport, onder verwijzing naar de mogelijkheden die het Cbp op grond van de Awb heeft, wordt gesteld dat het Cbp voldoende bevoegdheden heeft om in rechte te kunnen optreden ingeval van inbreuken op de krachtens het kaderbesluit vastgestelde nationale bepalingen. Het is de leden van deze fractie echter opgevallen dat in de memorie van toelichting wordt aangegeven dat het kaderbesluit niet verplicht tot toedeling van de bevoegdheid aan de nationale toezichthoudende autoriteit om in rechte op te treden. Waar in het nader rapport wordt vermeld dat het Cbp voldoende bevoegdheden heeft om in rechte op te kunnen treden, blijkt evenwel uit de memorie van toelichting dat een toekenning van deze bevoegdheid geen verplichting is en dat volstaan kan worden met het onder de aandacht brengen van de inbreuk van de justitiële autoriteiten. Dit lijkt tegenstrijdig en onduidelijk en de leden van deze fractie zouden graag een reactie van de regering vernemen. Zij hebben de regering verzocht ook nader in te gaan op het bredere bereik van de term «justitiële autoriteiten» dan de term «bij de rechter», zoals de tekst van het kaderbesluit luidt.

In antwoord op de gestelde vragen moet erkend worden dat de woorden «in rechte optreden» tot verwarring aanleiding kunnen geven. Dit houdt ook verband met de Nederlandse vertaling van het kaderbesluit, die op dit punt afwijkt van de Engelse vertaling. In de Engelse vertaling wordt onderscheid gemaakt tussen «the power to engage in legal proceedings where the national provisions (–) have been infringed» en «to bring this infringement to the attention of the judicial authorities». Hiermee wordt bedoeld op het onderscheid tussen het zelfstandig in rechte optreden of het ter kennis brengen van een schending van de regels aan de justitiële autoriteiten. Met de term justitiële autoriteiten wordt bedoeld op officieren van justitie en rechters. In het nader rapport wordt met het in rechte optreden ten onrechte op de toepassing van bepaalde onderzoeksbevoegdheden bedoeld. De bevoegdheid tot het opleggen van een bestuurlijke boete kan echter wel worden aangemerkt als een bevoegdheid «to engage in legal proceedings». Het Cbp beschikt over de bevoegdheid tot het opleggen van een bestuurlijke boete, als de verplichting tot vastlegging van bepaalde verwerkingen van politiegegevens (protocolplicht) door de verantwoordelijke niet wordt nageleefd. Overigens is het Cbp bevoegd een schending van de Wbp of de Wjsg onder de aandacht van het openbaar ministerie te brengen, zodat met de toedeling van bevoegdheden aan het College wordt voldaan aan de eisen van artikel 25, tweede lid, onderdeel c, van het kaderbesluit. De afwijkende vertaling van de Nederlandse tekst op dit punt zal onder de aandacht van het Raadssecretariaat worden gebracht, met het verzoek de Nederlandse tekst beter af te stemmen op de Engelse tekst. Dit betekent dat de woorden «judicial authorities» worden vertaald met «justitiële autoriteiten» in plaats van «het gerecht».

De leden van de SP-fractie hebben de regering gevraagd te reageren op de constatering dat het Cbp er nu extra taken bij krijgt, zowel op het gebied van handhaving als advies. Zij hebben gevraagd of het budget en de personele mogelijkheden van het Cbp hiertoe eigenlijk wel toereikend zijn om zowel adviestaken als handhaving zorgvuldig en tijdig te kunnen uitvoeren.

Het Cbp is reeds belast met het toezicht op de naleving van het bij of krachtens de Wpg en de Wjsg gestelde. Op dit punt brengt het kaderbesluit nauwelijks een taakverzwaring met zich mee. Hoogstens kunnen de in dit wetsvoorstel opgenomen aanvullingen van het bestaande regelgevende kader, bijvoorbeeld de introductie van de mogelijkheid van het markeren van persoonsgegevens of het bewaren van gegevens over de verstrekking van persoonsgegevens aan derden, tot enige uitbreiding van de toezichtstaak leiden maar dit lijkt niet van die aard dat hiervoor aanvullende middelen nodig zijn. Voor wat betreft de adviestaak voorziet het kaderbesluit in de verplichting om het Cbp te consulteren voordat gevoelige persoonsgegevens in een nieuw bestand worden opgenomen of wanneer de aard van de verwerking specifieke risico's met zich meebrengt door de fundamentele rechten van de betrokkene, in het bijzonder het recht op bescherming van de persoonlijke levenssfeer. Deze bepaling wordt in de Nederlandse wetgeving geïmplementeerd, daarvoor kan worden gewezen op Artikel I, onderdeel J (artikel 35, vierde lid Wpg), en Artikel II, onderdeel H (artikel 27, derde lid, Wjsg), van het wetsvoorstel. Naar verwachting zal een dergelijk advies slechts sporadisch aan de orde zijn. Als de werklast van het Cbp door externe omstandigheden, zoals de invoering van het wetsvoorstel, zodanig wordt verzwaaard dat dit gevolgen heeft voor de taakuitvoering van dit orgaan, dan kan dit in het periodiek overleg met de Voorzitter van het College aan de orde komen.

De leden van de SP-fractie vonden dat de Nederlandse Orde van Advocaten (NOvA) terecht een klemmend beroep op de regering doet om ervoor te zorgen dat Nederland bij de geringste twijfel aan de toereikendheid van de bescherming van persoonsgegevens geen gegevens verstrekt. Ook heeft de NOvA erop aangedrongen uiterst terughoudend te zijn met de uitzonderingsmogelijkheid om, in die gevallen waarin geen sprake is van een toereikend niveau, toch tot gegevensverstrekking over te gaan. De leden van de SP-fractie zijn van mening dat de reactie van de regering niet erg helder is en hebben gevraagd om een duidelijk(er) antwoord op deze twee terechte vragen/verzoeken.

Voor de beantwoording van de vraag over de verstrekking van gegevens bij twijfel aan de toereikendheid van de bescherming verwijs ik de leden van de SP-fractie graag naar de hiervoor gegeven beantwoording van een soortgelijke vraag van de leden van deze fractie. Voor wat betreft de uitzonderingsmogelijkheid om, in die gevallen waarin geen sprake is van een toereikend niveau, toch tot gegevensverstrekking over te gaan herinner ik aan mijn eerdere opmerking, in reactie op een soortgelijke vraag van de leden van de fractie van de SP, dat de bronlanden van ernstige vormen van criminaliteit die de integriteit van de Nederlandse samenleving bedreigen en het veiligheidsgevoel van de burger aantasten, in andere werelddelen kunnen zijn gelegen waar andere normen gelden op het gebied van de gegevensbescherming. De Nederlandse opsporingsautoriteiten hebben groot belang bij een goede samenwerking met hun collega's in deze landen. Daarbij dient het belang van de betrokkene op een zorgvuldige verwerking van zijn persoonsgegevens te worden afgewogen tegen het belang bij de uitwisseling van persoonsgegevens ten behoeve van het betreffende opsporingsonderzoek of de betreffende strafzaak. Het spreekt vanzelf dat in die gevallen, waarin twijfel bestaat

over het niveau van gegevensbescherming in deze landen, terughoudendheid wordt betracht bij de verstrekking van persoonsgegevens. Dit behoeft echter niet te betekenen dat er in het geheel niet kan worden samengewerkt. In antwoord op een eerdergenoemde vraag van de leden van de fractie van de SP heb ik reeds aangegeven op welke wijze hiermee in de praktijk wordt omgegaan.

## **XII. De consequenties van het wetsvoorstel voor de praktijk, financiële gevolgen en administratieve lasten**

De leden van de PVV-fractie hebben in de memorie van toelichting gelezen dat de regering niet aanneemt dat, in tegenstelling tot wat het openbaar ministerie en de politie verwachten, de werklast voor de politie zal toenemen. Opgemerkt wordt dat de personele lasten gelet op de omvang van de politieorganisatie en het daarmee verbonden budget, niet onoverkomelijk lijken en dat dit volgens de regering binnen de bestaande budgettaire kaders kan worden opgevangen. Met de capaciteitsproblemen van de politie in het achterhoofd hebben deze leden gevraagd of de regering deze verwachting uitgebreider wil onderbouwen.

De leden van de CDA-fractie de regering hebben gevraagd nader toe te lichten waarom de gevolgen van het voorliggende wetsvoorstel voor de werklast van het OM niet goed te kwantificeren is en of de regering een poging kan doen om deze beter in kaart te brengen. Verder hebben zij gevraagd of de regering een nadere schatting kan maken van de kosten op het gebied van de personele lasten en de huishouding tengevolge van het onderhavige wetsvoorstel en ook van de werklast voor de politie.

In antwoord op de gestelde vragen over de gevolgen van het wetsvoorstel voor de werklast van politie en het openbaar ministerie kan het volgende worden opgemerkt. Het kaderbesluit geeft regels voor de verstrekking van persoonsgegevens in het kader van de politiere en justitiële samenwerking in strafzaken. Die regels geven aanleiding tot de aanpassing van de Nederlandse wetgeving op enkele aspecten. De voorgestelde aanpassingen houden geen verband met het aantal gevallen waarin tussen de lidstaten persoonsgegevens worden uitgewisseld in het kader van de politiere en de justitiële samenwerking. De intensiteit van de gegevensuitwisseling is afhankelijk van de ontwikkeling van de samenwerking op het gebied van de bestrijding van de grensoverschrijdende criminaliteit. Die ontwikkeling kan worden beïnvloed door Europese regels op dit terrein. Het kaderbesluit dataprotectie geeft slechts regels voor het geval dat gegevens worden uitgewisseld.

Voor wat betreft de Wet politiegegevens gaat het in de eerste plaats om de introductie van de mogelijkheid van het markeren van politiegegevens, als de juistheid van de gegevens niet kan worden vastgesteld. Dit impliceert, voor zover nodig, aanpassing van de ICT-systemen bij de politie zodat de gegevens kunnen worden voorzien van een kenmerk. Mede in het licht van het totale ICT-budget van de Nederlandse politie is het streven de ICT-consequenties van het kaderbesluit te minimaliseren. In de tweede plaats betreft dit de bewaartermijn van vier jaar voor de gegevens over de verstrekking van politiegegevens aan derden. In de Wet politiegegevens is thans reeds vastgelegd dat de verantwoordelijke schriftelijk gegevens vastlegt over de verstrekking van politiegegevens aan derden (artikel 32, eerste lid, onderdeel f, Wpg). Deze gegevens worden bewaard tenminste tot de datum waar de laatste audit is verricht. Als de audit binnen een jaar wordt verricht, dan worden de gegevens in ieder geval een jaar bewaard vanwege de verplichting om derden in kennis te stellen van de correctie van gegevens (artikel 32, derde lid, Wpg). In het Besluit politiegegevens is bepaald dat een audit iedere vier jaar wordt gehouden (art. 6:5, eerste lid, Bpg). Dit betekent dat de

maximale bewaartermijn vier jaar kan bedragen. Deze termijn is gelijk aan de bewaartermijn van vier jaar die, naar aanleiding van het Rijkeboer-arrest, in artikel 25, eerste lid, van de Wet politiegegevens wordt voorgesteld. In de derde plaats introduceert het kaderbesluit verplichtingen tot het controleren van gegevens voor of nadat deze zijn verstrekt, het informeren van andere lidstaten over het gebruik van gegevens en de vernietiging van gegevens. De aard van deze verplichtingen sluit aan bij de huidige werkwijze van de politie bij de verstrekking van politiegegevens aan het buitenland. De aard van deze verplichtingen sluit aan bij de huidige werkwijze van de politie in de verstrekking van politiegegevens aan het buitenland. Ook met betrekking tot de consequenties voor de werklast voor de politie is het streven deze minimaal te houden. Voor wat betreft de Wet justitiële en strafvorderlijke gegevens gaat het in de eerste plaats om verruiming van de mogelijkheden tot het verstrekken van justitiële en strafvorderlijke gegevens aan het buitenland. De verruiming vloeit voort uit de regels van het kaderbesluit, en staat los van de vraag in hoeverre deze verruiming daadwerkelijk zal leiden tot een stijging van het aantal verstrekkingen aan het buitenland. Zoals eerder opgemerkt, voorziet het kaderbesluit niet in een verplichting tot verstrekking van gegevens. Dergelijke verplichtingen kunnen voortvloeien uit internationale afspraken of bilaterale overeenkomsten met andere landen. De meerkosten, die aan een dergelijke intensivering verbonden zouden kunnen zijn, vloeien niet voort uit de implementatie van het kaderbesluit. In de tweede plaats wordt met dit wetsvoorstel de mogelijkheid van het markeren van justitiële en strafvorderlijke gegevens, als de juistheid van de gegevens niet kan worden vastgesteld, geïntroduceerd. Hiervoor geldt hetzelfde als voor het markeren van politiegegevens; mede in het licht van het totale ICT-budget voor de strafrechtspleging zijn de mogelijke meerkosten naar verwachting niet van een substantiële omvang. In de derde plaats betreft dit de bewaartermijn van vier jaar voor de gegevens over de verstrekking van politiegegevens aan derden. In de Wet justitiële en strafvorderlijke gegevens is thans reeds vastgelegd dat de verantwoordelijke schriftelijk gegevens vastlegt over de verstrekking van justitiële en strafvorderlijke gegevens aan derden (artikelen 19, eerste lid, en 39j, eerste lid, Wjsg). Ditzelfde geldt voor de verstrekking van afschriften van rapporten uit persoonsdossiers (artikel 44, eerste lid, Wjsg). Deze gegevens worden thans een jaar bewaard. Vanwege het Rijkeboer-arrest wordt voorgesteld deze bewaartermijn te verhogen naar vier jaar. Dit betekent dat extra geheugencapaciteit nodig is om meer gegevens te kunnen bewaren en dat hierdoor de omvang van de database zal toenemen. Dit lijkt echter geen substantiële verzwaring van de werklast op te gaan leveren, ook omdat het aantal verzoeken tot kennisneming van de gegevens naar verwachting niet zal stijgen. Dit aantal is betrekkelijk gering. Vanwege de verlenging van de periode waarover gegevens kunnen worden verstrekt zullen, naar aanleiding van een individueel verzoek, meer gegevens over de verstrekking van justitiële of strafvorderlijke gegevens aan derden verstrekt moeten worden. Dit lijkt evenmin een zodanig verzwaring van de werklast op te leveren, dat daarvoor aanvullende financiële middelen vereist zouden zijn. Ten slotte geldt voor wat betreft de verplichtingen tot het controleren van gegevens voor of nadat deze zijn verstrekt, het informeren van andere lidstaten over het gebruik van gegevens en de vernietiging van gegevens, hetzelfde als hetgeen hiervoor is opgemerkt voor de politiegegevens.

De leden van de SP-fractie hebben gevraagd of de zorgen over de toename van de werklast van de politie niet meer dan terecht zijn en dat hier wel degelijk financiële consequenties aan zullen zitten, zeker gelet op de financiële tekorten bij veel politiekorpsen. Zij hebben zich ook afgevraagd of het niet iets te gemakkelijk is om te zeggen dat deze kosten

«binnen de budgettaire ruimtes» zullen worden opgevangen, en zouden hierop graag een reactie ontvangen.

Voor de beantwoording van deze vraag kan worden verwezen naar het hiervoor gegeven antwoord op de vragen van de leden van de fracties van de PVV en het CDA.

## **ARTIKELSGEWIJS**

### **Artikel 25**

#### *Artikel I, onderdeel F*

De leden van de PvdA-fractie hebben opgemerkt dat in de tweede volzin van het voorgestelde artikel 25, eerste lid, Wpg een lidwoord teveel staat.

Naar aanleiding van de opmerking van de leden van de PvdA-fractie is de tekst van dit artikel opnieuw bekeken. Anders dan deze leden veronderstellen lijkt er geen sprake te zijn van een overbodig lidwoord. De tekst maakt duidelijk dat het gaat om de persoonsgegevens die de persoon betreffen die het verzoek tot kennisneming heeft gedaan.

#### Artikel I, onderdeel H

### **Artikel 28**

De leden van de VVD-fractie hebben opgemerkt dat in het kaderbesluit onderscheid wordt gemaakt tussen het corrigeren of het wissen van gegevens enerzijds, als de gegevens onjuist of overbodig zijn, en het markeren van gegevens anderzijds, indien de juistheid daarvan wordt betwist. Deze leden hebben verwezen naar het advies van het Cbp. Dit college adviseerde het wetsvoorstel nader te bezien op de gehanteerde terminologie, met als aandachtspunt dat het markeren kennelijk ook aangewezen was voor gegevens waarbij feitelijk vaststaat dat die feitelijk onjuist, onvolledig of niet ter zake dienend waren dan wel in strijd met een wettelijk voorschrift werden verwerkt. Dit in tegenstelling tot de situatie waarbij niet kan worden vastgesteld of het gegeven al dan niet juist is, waar markeren is aangewezen. Het ingediende wetsvoorstel bevat nog steeds de mogelijkheid gegevens die – kort gezegd – zeker niet juist zijn toch te markeren. Dit is nadelig voor de betrokkene, mede gelet op artikel 18, eerste lid, van het kaderbesluit, waarin de betrokkene het recht heeft op het nakomen van de voor de verwerking verantwoordelijke van zijn verplichtingen. De leden van de VVD-fractie hebben de regering verzocht hier op in te gaan en zo nodig de tekst van het wetsvoorstel aan te passen.

De tekst van artikel 18, tweede lid, van het kaderbesluit luidt als volgt: Indien de juistheid van de persoonsgegevens door de betrokkene wordt betwist en niet kan worden vastgesteld of het gegeven al dan niet juist is, kan dat gegeven worden gemarkeerd. Uit de tekst van de Engelse vertaling kan worden afgeleid dat het hier niet gaat om een verplichting voor de lidstaten («referencing of that item may take place»). Het markeren is in het kaderbesluit echter niet gedefinieerd. Het «kenmerken» van gegevens is wel gedefinieerd. Dit begrip wordt omschreven als het markeren van opgeslagen persoonsgegevens, zonder de bedoeling om hun toekomstige verwerking te beperken (artikel 2, onderdeel j). In het Besluit 2008/615/JBZ van de Raad van 23 juni 2008 inzake de intensivering van de grensoverschrijdende samenwerking, in het bijzonder ter bestrijding van terrorisme en grensoverschrijdende criminaliteit (Pb L 210/1) is overigens eenzelfde systematiek gevolgd (artikelen 24, eerste lid,

onderdeel c en 28, tweede lid), met dien verstande dat daar is gekozen voor een meer verplichtende tekst («moeten») in combinatie met een verwijzing naar het nationale recht, zodat betwijfeld kan worden of het om een verplichting voor de lidstaten gaat. De Nederlandse regering heeft gekozen voor een verplichting voor de verantwoordelijke om gegevens te markeren als de juistheid daarvan niet kan worden vastgesteld. Naar aanleiding van het advies van het Cbp is de tekst van artikel 28, eerste lid, van de Wpg en de artikelen 22, eerste lid, en 39m, eerste lid, van de Wjsg aangepast, zodat duidelijker tot uitdrukking wordt gebracht dat de mogelijkheid van het markeren aan de orde is indien de juistheid van de gegevens niet kan worden vastgesteld. In zijn advies heeft de Afdeling advisering van de Raad van State geadviseerd in de voorgestelde eerste leden van de artikelen 28 Wpg en 22 Wjsg en in de derde leden van deze artikelen eveneens een verwijzing naar markeren op te nemen. In de eerste leden van deze artikelen was die verwijzing echter reeds opgenomen. Naar aanleiding van het advies van de Raad van State is de tekst van artikel 28, eerste lid, van de Wet politiegegevens (artikel I, onderdeel H), en de artikelen 22, eerste lid en 39m, eerste lid van de Wet justitiële en strafvorderlijke gegevens (artikel II, onderdelen G en M) aangevuld met de mogelijkheid voor degene, aan wie kennis gegeven van hem betreffende politiegegevens, de verantwoordelijke te verzoeken – kort gezegd – de gegevens te verbeteren, te verwijderen, af te schermen of te markeren indien deze feitelijk onjuist zijn of in strijd met een wettelijk voorschrift worden verwerkt, dan wel te markeren als de juistheid van de gegevens niet kan worden vastgesteld. Daarbij is het woord markeren abusievelijk tweemaal gebruikt, eenmaal in relatie tot onjuiste of onvolledige gegevens en eenmaal in relatie tot gegevens waarvan de juistheid niet kan worden vastgesteld. Bij nota van wijziging zal worden voorgesteld de tekst van de artikelen 28 Wpg en 22 en 39m Wjsg aan te passen zodat het markeren uitsluitend mogelijk is als de juistheid van de gegevens niet kan worden vastgesteld. Verder zal in de nota van wijziging worden voorgesteld in plaats van «markeren» te spreken van «kenmerken», zodat de definitie van de richtlijn wordt gevolgd.

#### *Artikel II, onderdeel F*

De leden van de CDA-fractie hebben gevraagd waarom de regering voor de bewaring van gegevens heeft gekozen voor aansluiting bij de termijn voor de privacy-audits en aldus tot een bewaartermijn van vier jaar is gekomen, in plaats van de eerder beoogde drie jaar.

In het arrest Rijkeboer heeft het Europese Hof van Justitie geoordeeld dat een bewaartermijn van een jaar voor de verstrekking van persoonsgegevens uit de gemeentelijke basisadministratie persoonsgegevens (GBA) aan derden geen juist evenwicht vormt tussen het belang van de betrokkene om zijn rechten uit te oefenen en de verplichting voor de verantwoordelijke om gegevens te bewaren. In casu vroeg de betrokkene, Rijkeboer, om informatie over de verstrekking van persoonsgegevens aan derden in de twee jaren voorafgaand aan zijn verzoek.

Naar aanleiding van dit arrest is aanvankelijk een bewaartermijn van drie jaar voorgesteld voor de bewaring van gegevens over de verstrekking van persoonsgegevens aan derden. De Raad van State heeft opgemerkt dat in de memorie van toelichting onvoldoende aandacht werd besteed aan enkele overwegingen van dit arrest, met name die waarin parameters worden gegeven voor de vaststelling van dit evenwicht. Deze parameters betreffen de bewaartermijn van de gegevens, de gevoeligheid van de gegevens en het aantal ontvangers. Naar aanleiding van het advies van de Raad van State is de voorgestelde bewaartermijn van drie jaar nogmaals gezien. De door het Hof aangehaalde parameters bieden echter weinig



aanknopingspunten voor de vaststelling van een concrete bewaartermijn. Navraag bij de politie, de Koninklijke marechaussee en Just-ID heeft uitgewezen dat dergelijke verzoeken in de praktijk nauwelijks voorkomen, zeker niet over een termijn die langer is dan enkele jaren. De Wet politiegegevens verplicht de politie en de Koninklijke marechaussee om gegevens over de verstrekking van politiegegevens aan derden te bewaren, tenminste tot de datum waarop een audit is verricht (artikel 32, derde lid, Wpg). Op grond van het Besluit politiegegevens wordt eenmaal in de vier jaar een audit verricht (art. 6:5 Bpg). Dit brengt met zich mee dat de betreffende gegevens gedurende een termijn van ten hoogste vier jaar worden bewaard, afhankelijk van het tijdstip waarop de audit wordt verricht.

Gelet op het advies van de Raad van State en het evenwicht tussen de betrokken belangen, te weten het belang van de betrokkene om uitsluitend te kunnen verkrijgen over de vraag aan welke personen en instanties de hem betreffende politiegegevens zijn verstrekt en het belang van de rechtshandhavingsinstanties om de werklast niet nodeloos te verzwaren, stelt het kabinet voor om met de bewaartermijn aan te sluiten bij de maximale bewaarperiode van vier jaar voor gegevens over de verstrekking van politiegegevens. Voor de justitiële en strafvorderlijke gegevens betekent dit een verlenging van de bewaartermijn met drie jaar, omdat de huidige bewaartermijn een jaar is. Een bewaartermijn van vier jaar lijkt een alleszins redelijke termijn om de betrokkene in staat te stellen zijn recht op kennisneming uit te oefenen.

De minister van Veiligheid en Justitie,  
I. W. Opstelten