

AAN De Staatssecretaris van Binnenlandse Zaken en
Koninkrijksrelaties

DATUM 30 maart 2007

ONS KENMERK z2007-00010

CONTACTPERSOON

UW BRIEF VAN 20 december 2006

UW KENMERK

ONDERWERP Adviesaanvraag wijziging Paspoortwet i.v.m de
herinrichting van de
reisdocumentenadministratie

Bij brief van 20 december 2006 kreeg het College bescherming persoonsgegevens (CBP) van de Minister voor Bestuurlijke Vernieuwing en Koninkrijksrelaties het verzoek om ingevolge artikel 51, tweede lid, Wet bescherming persoonsgegevens (Wbp) te adviseren over het voorstel tot wijziging van de Paspoortwet in verband met het herinrichten van de reisdocumentenadministratie en het opnemen van vingerafdrukken daarin (hierna: het wetsvoorstel). Voorts maakt het wetsvoorstel het mogelijk dat de burger een reisdocument kan aanvragen in een Nederlandse gemeente naar keuze (plaatsonafhankelijke uitgifte). Daarnaast wordt het functioneel ontwerp aangeboden waarin wordt beschreven wat de gebruiksmogelijkheden van de reisdocumentenadministratie zijn en hoe deze worden vormgegeven. Een concept van dit functioneel ontwerp is met het CBP in een eerdere fase besproken.

Met het navolgende advies voldoet het CBP aan het verzoek. Het CBP verontschuldigt zich voor het feit dat de advisering vertraging heeft opgelopen.

Inhoud van het wetsvoorstel

De artikelen 4a en 4b van het wetsvoorstel vervangen het bestaande artikel 4a van de huidige wet.

Vastgelegde gegevens

Het eerste lid van artikel 4a van het wetsvoorstel bepaalt dat de Minister een centrale reisdocumentenadministratie voert waarin de gegevens worden bijgehouden met betrekking tot aangevraagde, vervaardigde, uitgereikte, ingehouden, ingeleverde, vervallen, ontvreemde of anderszins als vermist opgegeven en definitief aan het verkeer onttrokken reisdocumenten. Het bestaande basisregister dat uitsluitend gegevens bevat van reisdocumenten die zijn ontvreemd of anderszins als vermist zijn opgegeven dan wel van rechtswege zijn vervallen, wordt door het wetsvoorstel derhalve uitgebreid en van een 'negatief' register omgevormd tot een 'positief' register.

Artikel 4a, tweede lid, van het wetsvoorstel bepaalt welke persoonsgegevens worden vermeld in het centrale register. Naast de gegevens van artikel 3 van het wetsvoorstel – kort samengevat de

persoonsgegevens die zijn opgenomen in het reisdocument waaronder een gezichtsopname en twee vingerafdrukken – worden in het register opgenomen: twee andere vingerafdrukken van de aanvrager (artikel 4a, tweede lid onder b, van het wetsvoorstel), het A-nummer, het soort reisdocument en andere administratieve gegevens die noodzakelijk zijn voor de gegevensverwerking in de reisdocumentenadministratie (artikel 4a, tweede lid, onder c tot en met f).

Verstrekkingsregime

Artikel 4b regelt het verstrekkingsregime.

Het eerste lid bepaalt dat de reisdocumentenadministratie tot doel heeft het verstrekken van gegevens als bedoeld in artikel 4a, eerste lid, aan de daartoe ingevolge deze wet bevoegde instellingen en personen die betrokken zijn bij de uitvoering van deze wet.

Het tweede lid bepaalt dat buiten het in het eerste lid genoemde doel gegevens beschikbaar kunnen worden gesteld met het oog op:

- a. het voorkomen en bestrijden van fraude met en misbruik van reisdocumenten,
- b. de identificatie van slachtoffers van rampen en ongevallen,
- c. de opsporing en vervolging van strafbare feiten en
- d. het verrichten van onderzoek naar handelingen die een bedreiging vormen voor de veiligheid van de staat en andere gewichtige belangen van een of meerdere landen van het Koninkrijk dan wel de veiligheid van met het Koninkrijk bevriende mogendheden.

In het vierde lid wordt bepaald dat verstrekking ingevolge het tweede lid kan worden toegestaan aan bij algemene maatregel van rijksbestuur aangewezen:

- a. overheidsorganen (...) voor zover verstrekking van die gegevens noodzakelijk is voor de vervulling van hun taak;
- b. instellingen en personen die met het oog op de uitvoering van een wettelijke identificatieplicht een gerechtvaardigd belang hebben bij verstrekking van gegevens uit de reisdocumentenadministratie. Deze instellingen en personen krijgen ingevolge het zesde lid uitsluitend de mededeling of het documentnummer al dan niet in de reisdocumentenadministratie voorkomt en bij een bevestigend antwoord of het reisdocument in het maatschappelijk verkeer mag voorkomen.

Het vijfde lid regelt de verstrekking van de biometrische gegevens aan de officier van justitie in de in dat lid genoemde gevallen en voor de daar genoemde doeleinden (voorkomen en bestrijden van fraude met en misbruik van reisdocumenten en de opsporing en vervolging van strafbare feiten).

Toelichting en motivering van de wijzigingen

Het wetsvoorstel beoogt een nieuwe opzet van de reisdocumentenadministratie (die 24 uur per dag, zeven dagen per week, online raadpleegbaar is) met als voornaamste doel het creëren van een betrouwbaar aanvraag- en uitgifteproces van reisdocumenten met het oog op het voorkomen

van identiteitsfraude bij het aanvragen van een nieuw reisdocument en bij het gebruik van het reisdocument.

Ingevolge Verordening (EG) nr. 2252/2004 van de Raad van 13 december 2004, Pb EG L 385 is Nederland verplicht biometrische gegevens op te nemen in de reisdocumenten: eerst de gezichtsofopname en later twee vingerafdrukken.

Paragraaf 2 van de Memorie van Toelichting geeft een nadere beschouwing van de voorgeschiedenis rond de reisdocumentenadministratie en biometrie in reisdocumenten. Bij Rijkswet van 8 maart 2001, Stbl. 2001, 132 is het basisregister reisdocumenten met daarin opgenomen gegevens van reisdocumenten die zijn vermist, gestolen dan wel van rechtswege vervallen zijn verklaard, wettelijk verankerd. In 2004 uitte het toenmalige kabinet de wens om in het kader van terrorismebestrijding een informatiestructuur te ontwikkelen waarmee de mogelijkheid zou ontstaan de identiteit van personen online te verifiëren (TK 2004- 2005, 29754, 5). Daarbij werd verondersteld dat de oplossing daarvoor een centrale reisdocumentenadministratie met biometrische kenmerken zou zijn. In dit wetsvoorstel wordt deze gedachte uitgewerkt.

Paragraaf 3 van de Memorie van Toelichting beschouwt de centrale reisdocumentenadministratie nader. Daarin wordt beargumenteerd dat de huidige decentrale administraties van de uitgevende instanties, het basisregister reisdocumenten en het register paspoortsignaleringen niet meer voldoen aan de eisen van deze tijd. Door de gegevensuitwisseling op papier, de beperkte openstelling en het werken in verschillende tijdszones kunnen de beoogde doelstellingen (snelle bediening van de burger en het adequaat en snel voorzien in de informatiebehoefte van de uitgevende instanties en andere instellingen en personen die bij of krachtens de wet gerechtigd zijn persoonsgegevens te ontvangen) niet worden gerealiseerd.

De gegevens in de huidige reisdocumentenadministraties zijn niet actueel. Hierdoor ontstaat het risico dat bij uitgifte van reisdocumenten, ondanks een zorgvuldige controle bij de aanvraag toch in strijd met de wet meer dan één reisdocument onder dezelfde identiteit wordt verstrekt dan wel dat een persoon met gebruikmaking van persoonsgegevens van een ander een reisdocument verstrekt krijgt op diens naam. Met dit wetsvoorstel wordt beoogd dat te voorkomen.

Voorts wordt gesteld dat een plaatsonafhankelijke uitgifte van reisdocumenten vereist dat de gemeente waar de aanvraag wordt gedaan, toegang heeft tot een online bevroagbare centrale reisdocumentenadministratie waarin de documentgegevens van de aanvrager zijn opgeslagen en tot de benodigde persoonsgegevens uit de basisadministratie persoonsgegevens. De reden hiervan is dat de gemeente moet kunnen nagaan of er niet ook een aanvraag bij een andere gemeente is gedaan dan wel of er eerder een reisdocument is geweigerd. Ook kunnen de gegevens van de vorige verstrekking worden geraadpleegd.

In paragraaf 3.4 van de Memorie van Toelichting wordt nader ingegaan op de beveiliging van de reisdocumentenadministratie. Erkend wordt dat de vraag wat veiliger is (decentrale dan wel centrale opslag) niet eenduidig is te beantwoorden. Het gaat om een afweging van risico's en de maatregelen die daartegen mogelijk zijn. Na afweging van de risico's wordt geoordeeld dat het

voorkomen van fraude van en met reisdocumenten zwaarder moet wegen dan eventuele beveiligingsrisico's. Daarbij speelt mee dat de nieuwe administratie beter beveiligd – zo is de stelling - kan worden dan de huidige decentrale administraties door het nemen van passende maatregelen. De uitgangspunten voor de beveiliging (vertrouwelijkheid en integriteit, uitsluitend inzage binnen de wettelijke kaders, authenticatie van gebruikers en autorisaties) worden in de toelichting genoemd. Deze uitgangspunten worden in het technisch ontwerp van de administratie uitgewerkt in concrete beveiligingsmaatregelen.

Paragraaf 3.5 van de Memorie van Toelichting draagt de titel “privacybescherming”. Samengevat komt de daar gegeven redenering op het volgende neer.

Een meer effectief en betrouwbaar aanvraag- en uitgifteproces van reisdocumenten, de mogelijkheid om fraude met en misbruik van reisdocumenten te voorkomen en te bestrijden, het ter beschikking stellen van gegevens voor de identificatie van slachtoffers van rampen en ongevallen en bij de opsporing en vervolging van strafbare feiten en ten behoeve van de waarborgen van de staatsveiligheid en het tegengaan van identiteitsfraude in het kader van de uitvoering van de Wet op de identificatieplicht en de Wet financiële dienstverlening rechtvaardigen de met het aanleggen van een centrale reisdocumentenadministratie met biometrische gegevens, gepaard gaande inbreuken op de persoonlijke levenssfeer van de burger. Tevens wordt gesteld dat de beveiliging van de reisdocumentenadministratie met dit wetsvoorstel wordt verbeterd. Dit draagt bij aan een zorgvuldige verwerking van persoonsgegevens.

Beoordeling

In zijn beoordeling richt het CBP zich op de gevolgen van de beoogde wijzigingen van de Paspoortwet voor de persoonlijke levenssfeer van de burger, waarbij in het bijzonder aandacht wordt besteed aan de nieuwe opzet van de reisdocumentenadministratie (centraal), de opname daarin van de biometrische gegevens van de aanvrager van het reisdocument, de toegankelijkheid van de in de reisdocumentenadministratie opgenomen gegevens en de beveiliging.

Artikel 8 EVRM

Artikel 8 van het Europese verdrag tot bescherming van de rechten van de mens en de fundamentele vrijheden (EVRM) eist dat iedere beperking van het grondrecht op eerbiediging van de persoonlijke levenssfeer op een wettelijke grondslag berust. Artikel 10 van de Grondwet scherpt deze bepaling aan en verlangt voor elke beperking een grondslag in de formele wet.

Voor een wettelijke beperking van het voornoemde grondrecht gelden ook materiële eisen. Het voorschrift zal voldoende nauwkeurig moeten zijn en adequate en effectieve waarborgen moeten bevatten tegen ongeoorloofde inbreuken. Voorts is een beperking van het recht op privacy slechts toegestaan indien deze in een democratische samenleving noodzakelijk is in het belang van ‘national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or the protection of the rights and freedoms of others’.

Volgens de jurisprudentie van het Europese Hof voor de rechten van de mens betekent dit dat de beperking van de persoonlijke levenssfeer moet worden gerechtvaardigd door een 'pressing social need' en in overeenstemming moet zijn met de beginselen van proportionaliteit (de beperking mag niet onevenredig zijn in verhouding tot het nagestreefde doel) en de subsidiariteit (het nagestreefde doel moet niet op een voor de burger minder ingrijpende wijze kunnen worden bereikt). Deze vereisten moeten in hun onderlinge samenhang gelezen worden.

Proportionaliteit en subsidiariteit

Paragraaf 3.5 van de Memorie van Toelichting gaat in op artikel 8 EVRM. Er wordt echter naar het oordeel van het CBP onvoldoende ingegaan op de beginselen van proportionaliteit en subsidiariteit. Het CBP mist een concrete belangenafweging aan de hand van de uitgangspunten van het proportionaliteits- en subsidiariteitsbeginsel. De redenering en de daarbij naar voren gebrachte argumenten zijn erop gericht de centrale reisdocumentenadministratie te rechtvaardigen. De vraag is echter of voor een effectief en betrouwbaar aanvraag- en uitgifteproces van reisdocumenten niet kan worden volstaan met decentrale administraties die overigens ook deel blijven uitmaken van en een rol blijven spelen in het voorgestelde stelsel. Waarom is het niet mogelijk om een decentraal stelsel met een centrale verwijzindex in te richten dat 24 uur per dag en 7 dagen per week beschikbaar is om dezelfde doelstelling te halen? In welke reële behoefte wordt voorzien nu het aanvragen en verkrijgen van een reisdocument toch altijd enige dagen de tijd zal vergen vanwege het productieproces voordat deze aan betrokkene wordt overhandigd? Moet wat reeds decentraal is opgeslagen in een decentraal stelsel in dezelfde mate centraal worden opgeslagen? Is de toepassing van biometrie in het reisdocument zelf al niet een stap voorwaarts in het bestrijden van identiteitsfraude? Het CBP mist kortom een belangenafweging van de gevolgen van dit wetsvoorstel voor de persoonlijke levenssfeer van de burger in vergelijking met de huidige situatie.

Doelbinding

In zijn advies van 16 oktober 2001 (z2001-1368) heeft het CBP de nodige opmerkingen gemaakt over het toen voorliggende conceptwijzigingsvoorstel van de Paspoortwet. In dat advies heeft het CBP benadrukt dat - wanneer er al een centrale reisdocumentenadministratie noodzakelijk is - het essentieel is dat daarbij wordt uitgegaan van het strikt doelgebonden gebruik van de daarin opgenomen gegevens, in het bijzonder van de biometrische gegevens. Bij de parlementaire behandeling is dat advies van het CBP niet aan de orde gekomen omdat het toenmalige wetsvoorstel is ingetrokken. Ook is in de Memorie van Toelichting bij het voorliggende wetsvoorstel het eerder door het CBP uitgebrachte advies niet betrokken. De keuze voor een centrale reisdocumentenadministratie in dit wetsvoorstel lijkt mede te zijn gebaseerd op het realiseren van andere doeleinden dan een soepel verlopend aanvraag- en uitgifteproces. Eén van de veel genoemde doeleinden in dit verband is het opsporen van strafbare feiten, waaronder begrepen het bestrijden van terrorisme. Nog daargelaten de vraag of een centrale reisdocumentenadministratie hieraan een wezenlijke bijdrage kan leveren, wijst het CBP erop dat dit wetsvoorstel voor deze doeleinden weer één extra is bovenop alle andere maatregelen die al zijn genomen in de afgelopen periode. Het CBP denkt hier bijvoorbeeld aan de verplichting tot het bewaren van verkeersgegevens en uitbreidingen van bevoegdheden in het Wetboek van Strafvordering. Nu de officier van justitie de biometrische gegevens kan ontvangen bij bepaalde misdrijven, krijgt deze administratie in feite ook de functie van een opsporingsregister. Deze consequentie vormt een ernstige inbreuk op de persoonlijke levenssfeer omdat ook de gegevens van niet verdachte burgers zijn opgenomen in het register.

Het CBP mist in de Memorie van Toelichting een nadere beschouwing van de verenigbaarheid van dit doel met het doel van het aanvragen en uitgeven van reisdocumenten (zie artikel 9 Wbp).

Verstrekkingenregime

Artikel 4b van het wetsvoorstel bevat het nieuwe verstrekkingenregime van de wet. Het CBP leest artikel 4b, tweede lid, sub d, jo vierde lid, van het wetsvoorstel aldus dat daarin weliswaar de mogelijkheid wordt geschapen met het oog op het verrichten van het in sub d bedoelde onderzoek gegevens te verstrekken aan overheidsorganen, maar dat verstrekking aan bevriende mogendheden zelf niet mogelijk is.

In artikel 4b van het wetsvoorstel wordt de lijst van personen en organisaties genoemd waaraan persoonsgegevens kunnen worden verstrekt. Dat zijn er al veel. Wanneer deze centrale reisdocumentenadministratie eenmaal is gerealiseerd, dan zullen er – zo leert de praktijk - nieuwe soorten doeleinden en gebruikerswensen ontstaan. De gegevens die eens werden opgeslagen voor specifieke doeleinden, zullen de belangstelling krijgen van andere personen en organisaties ('function creep') waardoor de wettelijk verankerde doelbinding in gevaar komt. Ook overheidsvoornemens blijken in de loop der tijd veranderlijk. In de door het CBP georganiseerde expertmeeting op 20 februari 2006 zijn EU-systemen (VIS en SISII) waarin biometrisch gegevens zijn opgenomen, besproken. Ten aanzien van deze systemen bleek dat het bedoelde gebruik in de loop der tijd werd verruimd. Dit laat zien dat het risico van breder gebruik niet denkbeeldig is.

Biometrische gegevens

Ingevolge Verordening (EG) nr. 2252/2004 van de Raad van 13 december 2004, Pb EG L 385 is Nederland verplicht biometrische gegevens op te nemen in de reisdocumenten: eerst de gezichtsofopname en later twee vingerafdrukken. De verordening verplicht evenwel niet tot het opnemen van deze gegevens in een administratie, centraal of decentraal. Biometriegegevens voor identificatie- en verificatiedoeleinden zijn uitstekend bruikbaar door deze op te slaan in het document zelf zonder deze gegevens op te nemen in een (centrale) database.

Bij serieuze grootschalige toepassing en gebruik van biometrie zullen er alleen al door de intrinsieke fouten in biometrie veel personen serieuze nadelen ondervinden van valse meldingen van die toepassingen. Uit de in 2005 afgeronde biometrieproef en daarop volgende evaluatie, gedaan in opdracht van het ministerie van Binnenlandse Zaken en Koninkrijksrelaties, bleek dat in 3% van de gevallen er iets mis ging. Gesignaleerde tekortkomingen worden (mogelijk) deels opgelost door twee extra vingerafdrukken op te nemen. Welke correctiemaatregelen men ook neemt: intrinsieke fouten zullen blijven bestaan met alle gevolgen van dien. Het is dan ook de vraag of het grote vertrouwen dat in biometrie wordt gesteld met de huidige stand der techniek terecht is.

Beveiliging

Het CBP heeft waardering voor de beveiligingsmaatregelen die worden beschreven in de Memorie van Toelichting en hoe deze nader zijn uitgewerkt in het functioneel ontwerp. De voorgestelde maatregelen hebben een hoog niveau. Evenwel, bij elke vorm van beveiliging van grootschalige collecties zullen er onvoorzienbaar veel mogelijkheden tot onterechte toegang bestaan. De infrastructurele voorzieningen die nodig zijn om internationaal gegevens verantwoord uit te wisselen zijn alleen al om organisatorische redenen niet overal realiseerbaar. Erkend wordt in de toelichting dat de vraag wat veiliger is (decentrale dan wel centrale opslag)

niet eenduidig is te beantwoorden. Toch wordt er gekozen voor centraal. Grote collecties van gegevens van belang vormen echter een aantrekkelijk aanvalsobject voor hackers en/of criminelen (een centrale administratie zou het richtpunt kunnen worden voor manipulatie, zegt de toelichting op bladzijde 28). Als het bezit van oneerlijk verkregen gegevens tot voordelen kan leiden, terwijl er vertrouwd wordt op de feilloze werking van de systemen waarin die gegevens gebruikt worden, is het voor deze groep personen aantrekkelijk om gegevens te compromitteren, vooral naarmate er meer vertrouwd wordt op de unieke gegevensbron. Dit kan grote gevolgen hebben voor burgers die hun vertrouwen juist hebben gesteld in een zorgvuldige en betrouwbare overheid. Het CBP mist een nadere uitwerking van de maatregelen die er worden getroffen wanneer het systeem feitelijk gehacked wordt. Wat zijn de gevolgen in die situatie voor burgers? Worden zij ingelicht? Welke rechtsbescherming wordt hen geboden?

Maatschappelijk draagvlak

De permanente commissie van deskundigen in internationaal vreemdelingen-, vluchtelingen- en strafrecht (de commissie-Meijers) stelt in de brief van 13 april 2006, kenmerk CM0603, aan de leden van de Staten-Generaal het volgende: *“Een centrale administratie van biometrische gegevens houdt onmiskenbare risico’s van misbruik en onjuist gebruik in. Op deze risico’s is door vele deskundigen en nationale en internationale data protectie autoriteiten gewezen (zie adviezen van de Artikel 29 Data Protectie Groep, de Europese Data Protectie Toezichthouder en het College bescherming persoonsgegevens). Zo is aangetoond dat het gebruik van biometrische data voor persoonsherkenning nog steeds niet onfeilbaar is (en nooit zal worden). Identificatie of verificatie op basis van deze gegevens zal dus altijd een foutmarge inhouden. Centrale opslag van biometrische gegevens vergemakkelijkt de koppeling en gegevensuitwisseling met andere (Europese) bestanden. (...) Hierdoor wordt de controle die een individu kan uitoefenen op het gebruik van diens persoonsgegevens bemoeilijkt of zelfs onmogelijk gemaakt. Bovendien wijkt de bewindsman af van het algemene principe dat in Nederland personenadministraties van de overheid in beginsel decentraal worden opgezet (bijvoorbeeld in de GBA).”* Voorts betwijfelt de commissie of een centrale database wel effectief is in het kader van terrorismebestrijding. De praktijk leert, zo stelt de commissie, dat terroristen met legale, geldige reisdocumenten hun activiteiten ondernemen.

Burger@Overheid.nl, een door de overheid zelf opgerichte organisatie om kritisch naar de digitale overheid te kijken, spreekt in de brief van 18 augustus 2006 vergelijkbare zorgen uit.

“De introductie van het nieuwe paspoort is volgens sommigen een belangrijke stap die de veiligheid voor de burger vergroot. Volgens anderen is dit tegelijk een belangrijke stap die de vrijheid van de burger vermindert. Dit verschil in opvatting heeft te maken met de technologische onvolkomenheden van biometrie en het risico van misbruik van centraal opgeslagen persoonsgegevens.

De afgelopen jaren is door diverse deskundigen en belangengroeperingen gewezen op de nadelen die aan de toepassing van biometrie kleven. De betrouwbaarheid van unieke lichaamskenmerken (zoals vingerafdruk of gezichtsscan) is laag. De technische mankementen bij het verzamelen of gebruiken van biometrische gegevens zijn zo groot dat iemand ten onrechte kan worden geweigerd. Om diezelfde redenen kan iemand ten onrechte worden doorgelaten, wat ten koste gaat van de veiligheid. Aangezien het bij een paspoort gaat om grote aantallen personen en vele situaties, kunnen zelfs bij kleine foutenmarges relatief veel problemen ontstaan.

Naast deze bezwaren tegen de technologie is er kritiek op het voornemen om de paspoortgegevens centraal op te slaan in een landelijke of zelfs Europese database. Dit zou namelijk niet nodig zijn voor het doel van verificatie (vaststellen of het paspoort toebehoort aan de houder), maar wel het risico meebrengen dat de gegevens worden gebruikt voor een ander doel dan het bestrijden van paspoortfraude. Een voorbeeld is automatische identificatie met camera’s. Dat dit gevaar niet denkbeeldig is, mag blijken uit een recent

voorval waarbij de politie in Apeldoorn camera's die in het centrum zijn opgehangen om de veiligheid te verbeteren ook gebruikt om parkeerboetes uit te delen."

Ook de Europese toezichthouders hebben zich uitgesproken tegen een centrale reisdocumentenadministratie met biometrische gegevens. De voorzitter van de artikel 29 werkgroep heeft in zijn brief van 18 augustus 2004 dit standpunt kenbaar gemaakt aan de secretaris generaal van de Raad van Europa.

Het CBP merkt in dit verband op dat Nederland als eerste land in Europa daadwerkelijk stappen onderneemt om te komen tot een centrale reisdocumentenadministratie met biometrische gegevens met een breder doel dan alleen het aanvragen en uitgeven van reisdocumenten. De overheid moet plannen met een onomkeerbaar karakter alleen uitvoeren als er een evenwichtige analyse van voor- en nadelen heeft plaatsgevonden, met positief resultaat. Deze analyse heeft naar de mening van het CBP onvoldoende plaatsgevonden. In de Memorie van Toelichting is geen expliciete reactie gegeven op bovengenoemde bij de Minister bekende bezwaren. Het CBP is van oordeel dat hier sprake is van een ernstige omisatie.

Conclusie

Het CBP realiseert zich dat het aanleggen van een centrale reisdocumentenadministratie voor enkele van de genoemde doeleinden op aspecten zinvol kan zijn. Echter een centrale reisdocumentenadministratie met biometrische gegevens brengt voor de burgers ernstige en wellicht onnodige risico's voor de persoonlijke levenssfeer met zich, waartegen zij zich niet kunnen wapenen.

1. Het wetsvoorstel voldoet naar het oordeel van het CBP niet aan artikel 8 EVRM omdat een gedegen analyse van de voor- en nadelen van een centrale reisdocumentenadministratie ontbreekt. Alternatieven zoals een decentraal systeem met een centrale verwijzindex zijn niet besproken.
2. De hier beoogde centrale reisdocumentenadministratie is onomkeerbaar en zal de belangstelling krijgen van andere personen en organisaties vanwege de daarin opgeslagen persoonsgegevens. Het risico van 'function creep' is aanwezig en het wetsvoorstel sluit dit niet uit.
3. Grootschalige toepassing van biometrie heeft vanwege technische onvolkomenheden ernstige gevolgen voor grote aantallen burgers.
4. De infrastructurele voorzieningen die internationaal nodig zijn om gegevens verantwoord uit te wisselen, zijn zeer ingrijpend en brengen beveiligingsrisico's met zich. Er wordt onvoldoende stilgestaan bij de vraag wat de gevolgen zijn wanneer er wordt 'ingebroken' in het systeem.
5. Er worden zowel nationaal als internationaal bedenkingen geuit tegen een centrale reisdocumentenadministratie met biometrische gegevens. Gewezen wordt op de risico's van misbruik, onjuist en onvoorzien gebruik. In de toelichting wordt onvoldoende een analyse gemaakt die erop gericht is deze bezwaren weg te nemen.

DATUM 30 maart 2007
ONS KENMERK z2007-00010

Gelet op het voorgaande betekent het voorliggende wetsvoorstel naar het oordeel van het CBP een ernstige inbreuk op de persoonlijke levenssfeer die niet wordt gerechtvaardigd door de door het wetsvoorstel te realiseren doeleinden. Het CBP dringt erop aan het wetsvoorstel te heroverwegen mede in het licht van het in het coalitieakkoord van 7 februari 2007 (blz. 34, onder 9) genoemde uitgangspunt dat bij alle maatregelen de overheid de gevolgen voor de privacy van de burgers verantwoordt.

Graag verneemt het CBP van u een reactie op zijn advies waarin aandacht wordt besteed aan de gevolgen van dit wetsvoorstel voor de privacy van de burger.

Hoogachtend,

Het College bescherming persoonsgegevens,
Voor het College,

mw. mr. dr. J. Beuving
collegelid