DE EUROPESE TOEZICHTHOUDER VOOR GEGEVENSBESCHERMING

Advies van de Europese Toezichthouder voor gegevensbescherming over het voorstel voor een kaderbesluit van de Raad betreffende de uitwisseling van informatie volgens het beschikbaarheidsbeginsel (COM (2005) 490 def.)

(2006/C 116/04)

DE EUROPESE TOEZICHTHOUDER VOOR GEGEVENSBESCHERMING,

Gelet op het Verdrag tot oprichting van de Europese Gemeenschap, en met name op artikel 286,

Gelet op het Handvest van de grondrechten van de Europese Unie, en met name op artikel 8,

Gelet op Richtlijn 95/46/EG van het Europees Parlement en de Raad van 24 oktober 1995 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens;

Gelet op het verzoek om een advies overeenkomstig artikel 28, lid 2, van Verordening (EG) nr. 45/2001 van het Europees Parlement en de Raad van 18 december 2000 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens door de communautaire instellingen en organen en betreffende het vrije verkeer van die gegevens,

HEEFT HET VOLGENDE ADVIES AANGENOMEN:

I. INLEIDENDE OPMERKINGEN

1. Het voorstel voor een kaderbesluit van de Raad betreffende de uitwisseling van informatie volgens het beschikbaarheidsbeginsel is door de Commissie per brief van 12 oktober 2005 aan de EDPS toegezonden. De EDPS vat deze brief op als een verzoek om advies uit te brengen aan de communautaire instellingen en organen, overeenkomstig artikel 28, lid 2, van Verordening (EG) nr. 45/2001. Volgens de EDPS dient het onderhavige advies in de preambule van het kaderbesluit te worden vermeld.

2. De aard van dit advies moet worden gezien in de context zoals beschreven in punt II. Zoals in punt II wordt aangegeven is het allerminst vanzelfsprekend dat dit voorstel, of de daarin gevolgde aanpak van het begrip beschikbaarheid, er uiteindelijk toe zal leiden dat er een juridisch instrument zal worden aangenomen. Een aanzienlijk aantal lidstaten staat een andere aanpak voor.

3. Het spreekt echter vanzelf dat de beschikbaarheid van wetshandhavingsinformatie over de binnengrenzen heen, of, in ruimer opzicht, de uitwisseling ervan, een punt is dat hoog op de agenda van de lidstaten staat, zowel in de Raad als daarbuiten, en ook in het Parlement.

4. Ook spreekt het vanzelf dat dit onderwerp van groot belang is vanuit het oogpunt van de bescherming van persoonsgegevens, zoals uit dit advies naar voren zal komen. De EDPS memoreert dat dit voorstel van de Commissie nauw verbonden is met het voorstel voor een kaderbesluit van de Raad over de bescherming van persoonsgegevens die worden verwerkt in het kader van de politiële en justitiële samenwerking in strafzaken, waarover de EDPS op 19 december 2005 een advies heeft uitgebracht.

5. De EDPS zal van de gelegenheid gebruik maken om in dit advies algemene en meer fundamentele opvattingen naar voren te brengen over de uitwisseling van wetshandhavingsinformatie en over de wijzen waarop de regulering ervan kan worden aangepakt. Door dit advies uit te brengen beoogt de EDPS ervoor te zorgen dat in toekomstige debatten over het onderwerp terdege rekening zal worden gehouden met aspecten van gegevensbescherming.

6. De EDPS zal beschikbaar zijn voor verdere raadpleging in een later stadium, wanneer zich belangrijke ontwikkelingen voordoen in het wetgevingsproces met betrekking tot dit voorstel en andere eraan gerelateerde voorstellen.

II. HET VOORSTEL IN ZIJN CONTEXT

7. Het beschikbaarheidsbeginsel is in het Haags programma geïntroduceerd als een belangrijk nieuw rechtsbeginsel. Dit beginsel houdt in dat voor de misdaadbestrijding vereiste informatie onbelemmerd de binnengrenzen van de EU moet kunnen passeren. Doel van dit voorstel is dit beginsel in een bindend juridisch instrument praktisch uit te werken.

8. De uitwisseling van politiële informatie tussen de verschillende landen is een populair onderwerp voor wetgevers, zowel binnen als buiten de EU. Onderstaande initiatieven zijn de afgelopen tijd onder de aandacht gekomen van de EDPS.

9. Om te beginnen heeft Zweden op 4 juni 2004 een ontwerp-kaderbesluit voorgesteld betreffende de vereenvoudiging van de uitwisseling van informatie en inlichtingen tussen de wetshandhavingsautoriteiten van de lidstaten van de Europese Unie. De Raad heeft op 1 december 2005 overeenstemming bereikt over een algemene oriëntatie inzake dit voorstel.

10. Vervolgens hebben zeven lidstaten op 27 mei 2005 in Prüm (Duitsland) een Verdrag gesloten inzake de intensivering van de grensoverschrijdende samenwerking, in het bijzonder ter bestrijding van het terrorisme, de grensoverschrijdende criminaliteit en de illegale migratie. Het verdrag voorziet onder meer in maatregelen ter verbetering van de uitwisseling van informatie voor DNA en vingerafdrukken. Alle lidstaten van de Europese Unie mogen zich bij het verdrag aansluiten. De verdragsluitende partijen streven ernaar de bepalingen van het verdrag op te nemen in het juridisch raamwerk van de Europese Unie.

11. Ten slotte zal de beschikbaarheid van wetshandhavingsinformatie over de binnengrenzen van de Europese Unie heen ook nog worden bewerkstelligd door andere juridische instrumenten, zoals het voorstel voor een Schengeninformatiesysteem van de tweede generatie (SIS II), het voorstel voor toegang tot het visuminformatiesysteem (VIS) en het voorstel voor een kaderbesluit betreffende de organisatie en de inhoud van uitwisselingen van gegevens uit het strafregister tussen de lidstaten. Vermeld zij tevens de Mededeling over de verbetering van de doeltreffendheid, de interoperabiliteit en de synergie van de Europese gegevensbanken op het gebied van justitie en binnenlandse zaken, die de Commissie op 25 november 2005 het licht heeft doen zien.

12. Gezien al deze initiatieven moet dit voorstel voor een kaderbesluit inzake beschikbaarheid niet als enige worden besproken, maar moeten ook andere benaderingen van de uitwisseling van wetshandhavingsinformatie in overweging worden genomen. Dit is zelfs nog belangrijker gezien het feit dat de huidige tendens binnen de Raad erin bestaat de voorkeur te geven aan benaderingen van informatie-uitwisseling en van het concept van beschikbaarheid die afwijken van de algemene benadering in het onderhavige Commissievoorstel. De huidige tekst van het voorstel wordt misschien niet eens in de Raad besproken.

13. Voorts is dit voorstel nauw verbonden met het voorstel voor een kaderbesluit over de bescherming van persoonsgegevens. Dit advies moet worden gezien in samenhang met het dieper gaande advies over dat kaderbesluit.

14. In zijn advies over het voorstel voor een kaderbesluit over de bescherming van persoonsgegevens heeft de EDPS benadrukt dat adequate gegevensbescherming van belang is als noodzakelijk uitvloeisel van een juridisch instrument over beschikbaarheid. Volgens de EDPS moet een dergelijk juridisch instrument niet worden aangenomen zonder dat er essentiële garanties voor gegevensbescherming worden geboden.

15. De EDPS huldigt hetzelfde standpunt inzake het aannemen van andere juridische instrumenten die de stroom van wetshandhavingsinformatie over de binnengrenzen van de EU mogelijk maken. Daarom juicht de EDPS het toe dat zowel de Raad als het Europees Parlement eerdergenoemd voorstel voor een kaderbesluit over de bescherming van persoonsgegevens voorrang heeft gegeven.

III. HET BESCHIKBAARHEIDSBEGINSEL ALS ZODANIG

16. Het beschikbaarheidsbeginsel is op zich eenvoudig. De informatie die voor bepaalde instanties in een lidstaat beschikbaar is moet ook aan gelijkwaardige instanties in andere lidstaten worden verstrekt. De informatie moet zo snel en zo soepel mogelijk worden uitgewisseld tussen de instanties van de lidstaten en bij voorkeur middels het verlenen van rechtstreekse on line-toegang.

17. De problemen komen voort uit de omgeving waarin het beschikbaarheidsbeginsel in de praktijk moet worden gebracht:

— De politie en de rechterlijke macht zijn per lidstaat anders georganiseerd, met verschillende teugels en tegenwichten (checks and balances).

— Het gaat om verschillende soorten (gevoelige) informatie (zoals DNA of vingerafdrukken).

— Zelfs binnen de lidstaten zijn er voor de bevoegde instanties verschillende wegen om toegang te krijgen tot noodzakelijke informatie.

— Het is door de verschillende talen, technische systemen (interoperabiliteit) en rechtsstelsels moeilijk om te garanderen dat informatie uit een andere lidstaat correct wordt uitgelegd.

— Het beginsel moet worden opgenomen in de bestaande en uitgebreide lappendeken van juridische bepalingen over de uitwisseling van wetshandhavingsgegevens tussen landen.

18. Afgezien van deze complexe omgeving is men het erover eens dat het beginsel niet geïsoleerd kan functioneren. Aanvullende maatregelen moeten ervoor zorgen dat informatie inderdaad kan worden gevonden en ingezien. In ieder geval moeten deze maatregelen het voor de wetshandhavingsinstanties gemakkelijker maken uit te zoeken of wetshandhavingsinstanties in andere lidstaten beschikken over de noodzakelijke informatie, en waar deze informatie kan worden gevonden. Zulke bijkomende maatregelen zouden kunnen bestaan uit interfaces die rechtstreeks toegang bieden tot alle of tot specifieke gegevens waarover andere lidstaten beschikken. Daarom wordt in het voorstel voor een kaderbesluit over beschikbaarheid het begrip „indexgegevens" ingevoerd, waaronder specifieke gegevens worden verstaan die over de grenzen heen rechtstreeks toegankelijk zijn.

19. In algemene termen zou het beschikbaarheidsbeginsel de informatiestroom tussen de lidstaten moeten vergemakkelijken. De binnengrenzen zullen worden afgeschaft en de lidstaten moeten toestaan dat informatie die voor hun politie-instanties beschikbaar is, in toenemende mate toegankelijk wordt voor andere instanties. De lidstaten raken hun bevoegdheid om de informatiestroom te controleren kwijt en dat leidt er tevens toe dat zij niet langer kunnen vertrouwen op hun eigen wetgeving als een afdoend instrument voor een adequate bescherming van de informatie.

20. Daarom moet dit voorstel specifieke aandacht krijgen vanuit het oogpunt van de bescherming van persoonsgegevens. Ten eerste moet informatie, die normaliter vertrouwelijk en goed beveiligd is, worden verstrekt aan autoriteiten in andere lidstaten. Ten tweede moeten, wil men het systeem laten werken, indexgegevens worden gecreëerd en beschikbaar worden gesteld aan instanties in andere lidstaten. De toepassing van dit beginsel zal tot gevolg hebben dat er meer gegevens worden gegenereerd dan er thans beschikbaar zijn.

IV. **HOOFDELEMENTEN**

Toepassingsgebied van het beschikbaarheidsbeginsel

21. Allereerst is het van groot belang te omschrijven op wat voor soort informatie het beschikbaarheidsbeginsel van toepassing zal zijn. Het toepassingsgebied van dit beginsel wordt in algemene termen gedefinieerd in artikel 2 van het voorstel, in combinatie met artikel 1, lid 1 en artikel 3, onder a). Het beginsel is van toepassing op informatie die

    — bestaat,

    — genoemd wordt in bijlage II, waarin zes soorten informatie worden gedefinieerd,

    — beschikbaar is voor de bevoegde instanties.

    Dit zijn de drie hoofdelementen van het toepassingsgebied van het beginsel in het Commissievoorstel. Het toepassingsgebied wordt in artikel 2 verfijnd. In artikel 2, lid 1 wordt de toepassing van het beschikbaarheidsbeginsel beperkt tot de fase voorafgaand aan het instellen van een vervolging en in de leden 2, 3 en 4 worden specifiekere beperkingen uiteengezet.

22. Voor het begrip van de consequenties van het voorstel is een nadere analyse noodzakelijk vanmoeten de drie hierboven genoemde hoofdelementen. De eerste twee elementen van het toepassingsgebied zijn op zich al redelijk duidelijk. De definitie van „bestaande informatie" staat in lid 2 van artikel 2, dat zegt dat het kaderbesluit een verplichting inhoudt om informatie te verzamelen en op te slaan met als enig doel deze ter beschikking te stellen, en de lijst in Bijlage II kan niet op verschillende manieren worden uitgelegd. Het derde hoofdelement behoeft als zodanig, en in combinatie met de eerste twee elementen, nadere uitleg.

23. In het voorstel wordt niet nader omschreven of „beschikbare informatie" uitsluitend bestaat uit informatie die reeds door bevoegde instanties wordt beheerd of ook informatie omvat die deze instanties mogelijkerwijs kunnen verkrijgen. Volgens de EDPS kan het voorstel zodanig worden uitgelegd dat het beide omvat.

24. Artikel 2 lijkt te duiden op een enger toepassingsgebied omdat volgens lid 2 daarvan het kaderbesluit „geen verplichting inhoudt om […] informatie te verzamelen en op te slaan met als enig doel deze ter beschikking te stellen", terwijl artikel 3, een ruimere interpretatiemogelijkheid biedt omdat volgens a) onder „informatie" „bestaande informatie als vermeld in bijlage II" wordt verstaan.

25. In bijlage II staan op zijn minst twee categorieën gegevens die gewoonlijk door anderen dan de politie worden beheerd. De eerste categorie is informatie over voertuigregistratie. In veel lidstaten worden de gegevensbanken met deze informatie niet beheerd door de wetshandhavingsinstanties, hoewel ze regelmatig door deze instanties worden ingezien. Moet dit soort informatie vallen binnen het toepassingsgebied van „beschikbare informatie" die, volgens artikel 1, wordt verstrekt aan gelijkwaardige bevoegde instanties van andere lidstaten? De tweede categorie gegevens in de lijst in Bijlage II die moet worden genoemd omvat telefoonnummers en andere communicatiegegevens: moeten deze gegevens worden beschouwd als zijnde „beschikbaar", terwijl zij niet door bevoegde instanties, maar door particuliere bedrijven worden beheerd?

26. Voorts geven andere bepalingen van het voorstel, meer in het bijzonder in artikel 3, onder d) en artikel 4, lid 1, onder c) aan dat „aangewezen instanties" en ook „aangewezen partijen" informatie kunnen beheren die „beschikbaar" is voor „bevoegde instanties". Ook volgt uit de tekst van het voorstel dat „een bevoegde instantie" van een lidstaat een instantie is die valt onder het eerste streepje van artikel 29 van het EU-Verdrag, terwijl iedere nationale instantie een „aangewezen instantie" kan zijn.

27. Volgens de EDPS roept de toepassing van het beschikbaarheidsbeginsel op informatie die door aangewezen instanties en aangewezen partijen wordt beheerd, de volgende vragen op:

    — Biedt artikel 30, lid 1, onder b) een afdoende rechtsgrondslag, aangezien informatie beschikbaar moet worden gesteld door de aangewezen instanties en de aangewezen partijen en uit gegevensbanken die niet binnen het kader van de derde pijler vallen?

    — Is het kaderbesluit over de bescherming van persoonsgegevens van toepassing, zoals bijvoorbeeld in artikel 8 van het voorstel wordt verondersteld?

    — Zo niet, is de verwerking dan in overeenstemming met de verplichtingen uit hoofde van Richtlijn 95/46/EG?

28. De praktische uitwerking van een zo breed beginsel als het „beschikbaarheidsbeginsel" vereist een duidelijke en nauwkeurige definitie van de gegevens die zullen worden beschouwd als zijnde beschikbaar. De EDPS doet derhalve de volgende aanbevelingen:

— Verduidelijk het toepassingsgebied.

— Beperk als eerste optie het toepassingsgebied van het beschikbaarheidsbeginsel tot informatie die door bevoegde instanties wordt beheerd.

— Zorg als tweede optie, in het geval van een ruimer toepassingsgebied, voor voldoende waarborgen voor de bescherming van persoonsgegevens. Neem de in punt 27 aangestipte vragen in overweging.

Andere aspecten van het toepassingsgebied

29. Volgens artikel 2, lid 1, van het voorstel zal het kaderbesluit van toepassing zijn op de verwerking van informatie voorafgaand aan het instellen van een vervolging. Het toepassingsgebied ervan is beperkter dan het voorstel voor een kaderbesluit over de bescherming van persoonsgegevens, dat volledig van toepassing is op justitiële samenwerking in strafzaken.

30. Volgens de EDPS houdt deze beperking op zich echter niet in dat het toepassingsgebied van het voorstel wordt beperkt tot politiële samenwerking. Het zou ook justitiële samenwerking in strafzaken kunnen omvatten aangezien de justitiële autoriteiten in een aantal lidstaten ook bevoegd zijn voor onderzoek in strafzaken, voorafgaand aan het instellen van een vervolging. Het feit dat het voorstel uitsluitend gebaseerd is op artikel 30, lid 1, onder b) van het VEU lijkt er echter op te wijzen dat het alleen geldt voor politiële samenwerking. Een verduidelijking van dit aspect zou zeer welkom zijn.

31. Dit voorstel voorziet in het verstrekken van informatie aan Europol terwijl het voorstel voor een kaderbesluit over de bescherming van persoonsgegevens de verwerking van persoonsgegevens door Europol uitsluit. De EDPS adviseert de informatie-uitwisseling met Europol te beperken tot de doelstellingen van Europol zelf, zoals vermeld in artikel 2 van de Europol-overeenkomst en de bijlage erbij. Voorts moet rekening worden gehouden met de uitvoerige voorschriften voor de uitwisseling van gegevens met Europol, die reeds in een aantal besluiten van de Raad zijn vastgelegd.

Geen nieuwe gegevensbanken met persoonsgegevens

32. Uitgangspunt van het voorstel is dat het niet zal leiden tot het aanleggen van nieuwe gegevensbanken met persoonsgegevens. Artikel 2, lid 2, is hierover duidelijk: het houdt geen verplichting in om informatie te verzamelen en op te slaan met als enig doel deze ter beschikking te stellen. Dit is vanuit het oogpunt van gegevensbescherming een belangrijk en positief element van het voorstel. De EDPS herinnert aan zijn advies over het voorstel voor een richtlijn over de bewaring van gegevens die zijn verwerkt in verband met het aanbieden van openbare elektronischecommunicatiediensten [1], waarin hij benadrukte dat juridische verplichtingen die leiden tot omvangrijke gegevensbanken bijzondere risico's inhouden voor de betrokkenen, onder meer vanwege het gevaar van illegaal gebruik.

33. Echter:

— er dient voor te worden gezorgd dat het voorstel niet aanspoort tot een onvoorwaardelijke koppeling van gegevensbanken en zodoende tot een netwerk van gegevensbanken waarop moeilijk toezicht kan worden gehouden.

— er is een uitzondering op bovengenoemd uitgangspunt: artikel 10 van het voorstel waarin staat dat indexgegevens on line beschikbaar zijn. Indexgegevens kunnen persoonsgegevens bevatten of in elk geval het bestaan ervan onthullen.

Rechtstreekse en onrechtstreekse toegang tot informatie

34. Het voorstel biedt rechtstreekse en onrechtstreekse toegang tot informatie. Artikel 9 van het voorstel regelt rechtstreekse online toegang tot de in gegevensbanken opgeslagen informatie waartoe overeenkomstige bevoegde nationale instanties rechtstreeks online toegang hebben. Artikel 10 behelst onrechtstreekse toegang. Indexgegevens betreffende informatie die niet online toegankelijk is, kunnen online worden geraadpleegd door gelijkwaardige bevoegde instanties van andere lidstaten en door Europol. Wanneer bevraging van de indexgegevens een positief resultaat geeft, kan deze instantie een informatieaanvraag opstellen en toezenden aan de aangewezen instantie teneinde de aan de hand van de indexgegevens geïdentificeerde informatie te verkrijgen.

35. Rechtstreekse toegang leidt niet tot nieuwe gegevensbanken maar vereist interoperabiliteit van de gegevensbanken van gelijkwaardige bevoegde instanties binnen de lidstaten. Voorts zal er een nieuw gebruik van reeds bestaande gegevensbanken moeten worden ingevoerd, en wel door aan alle bevoegde instanties van de lidstaten een voorziening te bieden die tot nog toe alleen bestond voor nationale bevoegde instanties. Rechtstreekse toegang zal automatisch inhouden dat een groter aantal mensen toegang zal hebben tot een gegevensbank en dat leidt weer tot meer kans op misbruik.

[1] Advies van 26 september 2005 over het voorstel voor een Richtlijn van het Europees Parlement en de Raad over de bewaring van gegevens die zijn verwerkt in verband met het aanbieden van openbare elektronische-communicatiediensten en houdende wijziging van Richtlijn 2002/58/EG (COM (2005) 438 def.)

36. In het geval van rechtstreekse toegang voor een bevoegde instantie van een andere lidstaat, hebben de aangewezen instanties van de lidstaat van herkomst geen overzicht over de toegang tot en het verdere gebruik van de gegevens. Deze consequentie van rechtstreekse toegang, zoals in het voorstel wordt beoogd, moet op adequate wijze worden aangepakt, aangezien:

— de bevoegdheden van de aangewezen instanties om de informatieverstekking te weigeren (volgens artikel 14), erdoor ongedaan lijken te worden gemaakt.

— het vragen oproept over de verantwoordelijkheden voor de nauwkeurigheid en het bijhouden van de gegevens, nadat ze zijn ingezien. Hoe kan een aangewezen instantie van de lidstaat van herkomst garanderen dat de gegevens up to date worden gehouden?

— Niet alleen de aangewezen instantie is niet meer in staat al haar verplichtingen krachtens de wetgeving inzake gegevensbescherming na te komen, maar ook de nationale gegevensbeschermingsautoriteit van de lidstaat van herkomst kan geen toezicht meer uitoefenen op het nakomen van de verplichtingen, aangezien zij geen bevoegdheid heeft tegenover wetshandhavingsautoriteiten van andere lidstaten.

— Deze problemen zijn nog nadrukkelijker aanwezig indien aangewezen instanties en aangewezen partijen, die geen wetshandhavingsautoriteiten zijn, toegang hebben tot gegevensbanken (zie de punten 25-28 van dit advies).

Deze consequentie van rechtstreekse toegang is een belangrijke reden waarom de aanneming van dit voorstel moet afhangen van de aanneming van een kaderbesluit over de bescherming van persoonsgegevens. Eén probleem blijft: hoe kunnen aangewezen instanties de verstrekking van informatie weigeren krachtens artikel 14?

37. Wat betreft onrechtstreekse toegang via indexgegevens die informatie bieden volgens een systeem van hit/no hit: dit is geen nieuw verschijnsel. Het is de basis van de werking van Europese grootschalige informatiesystemen, zoals het Schengeninformatiesysteem. De instelling van een systeem van indexgegevens biedt het voordeel dat de lidstaten van herkomst toezicht kunnen uitoefenen op de uitwisseling van informatie uit hun politie-bestanden. Indien een raadpleging van indexgegevens leidt tot een treffer, kan de verzoekende instantie een informatieaanvraag in verband met de betrokkene doen uitgaan. Dit verzoek kan door de aangezochte instantie naar behoren worden beoordeeld.

38. Niettemin moet er een behoorlijke analyse worden gemaakt aangezien de instelling van een systeem van indexgegevens (in gebieden waar deze systemen tot nog toe niet bestonden, andere dan de Europese grootschalige informatiesystemen) nieuwe risico's kan creëren voor de betrokkene. De EDPS benadrukt dat indexgegevens weliswaar niet veel informatie over de betrokkene bevatten, maar dat raadpleging van indexgegevens een zeer gevoelig resultaat kan opleveren. Het kan onthullen dat een persoon in een politiebestand is opgenomen in verband met strafbare feiten.

39. Daarom is het van het allergrootste belang dat de Europese wetgever adequate voorschriften geeft, in elk geval voor het maken van indexgegevens, voor het beheer van de opbergsystemen ervan en voor een goede organisatie van de toegang tot de indexgegevens. De EDPS vindt het voorstel op deze punten niet bevredigend. In dit stadium maakt de EDPS drie opmerkingen:

— De definitie van indexgegevens is onduidelijk. Het is niet duidelijk of indexgegevens worden beschouwd als meta-gegevens, als belangrijkste sleutelvelden of als beide? Het begrip indexgegevens behoeft enige verduidelijking aangezien het een rechtstreekse invloed heeft op het niveau van gegevensbescherming en de vereiste waarborgen.

— Het voorstel moet de rol verduidelijken die de nationale contactpunten vervullen ten aanzien van indexgegevens. Betrokkenheid van de nationale contactpunten kan nodig zijn, in het bijzonder in gevallen waarin voor de interpretatie van indexgegevens specifieke kennis vereist is, bijvoorbeeld in het geval van een mogelijk positief resultaat van vingerafdrukken.

— In het voorstel wordt het aannemen van regels voor het maken van indexgegevens overgelaten aan uitvoeringsregelgeving overeenkomstig de comité-procedure in artikel 19. Ofschoon wellicht uitvoeringsregelgeving nodig is, moeten de basisregels voor het maken van indexgegevens in het kaderbesluit zelf worden opgenomen.

Voorafgaande toestemming van justitiële instanties

40. De informatie-uitwisseling zal de lidstaten niet beletten voorafgaande toestemming van de justitiële instanties te verlangen om de informatie naar de verzoekende instantie te sturen wanneer deze informatie in het aangezochte land onder justitieel beheer staat. Dit is belangrijk aangezien, volgens een onderzoek naar de bevoegdheden van de politie om persoonsgegevens uit te wisselen [1], de politie niet in alle lidstaten autonoom toegang heeft tot deze gegevens. Volgens de EDPS mag het beschikbaarheidsbeginsel de verplichting uit hoofde van de nationale wet om voorafgaande toestemming voor de informatie te krijgen, niet ondermijnen, of het moet op zijn minst uitmonden in specifieke, in alle lidstaten geldende regels inzake de categorieën gegevens waarvoor voorafgaande toestemming vereist is.

[1] Antwoorden op de vragenlijst over het ontwerp-kaderbesluit betreffende de vereenvoudiging van de uitwisseling van informatie en inlichtingen tussen de wetshandhavingsautoriteiten van de lidstaten van de EU, met name ten aanzien van zware misdrijven, zoals terroristische daden (document 5815/1/05 van de Raad).

41. Deze verplichting moet worden uitgelegd in samenhang met artikel 11, lid 2, van het voorstel voor een kaderbesluit over de bescherming van persoonsgegevens, waarin ook staat dat de verstrekkende lidstaat zeggenschap heeft over het verdere gebruik van de gegevens in de lidstaat waar de gegevens naartoe zijn gestuurd. De EDPS wijst op het belang van dit beginsel, dat nodig is om ervoor te zorgen dat beschikbaarheid niet zal leiden tot het omzeilen van restrictieve nationale wetgeving over het verdere gebruik van persoonsgegevens.

Slotopmerking

42. Deze elementen vereisen hoogstaande gegevensbeschermingsnormen. Er dient bijzondere aandacht te worden geschonken aan het waarborgen van de beginselen van doelbinding en verdere verwerking, evenals aan de nauwkeurigheid en betrouwbaarheid van de geraadpleegde informatie (zie het advies van de EDPS over het kaderbesluit inzake de bescherming van persoonsgegevens, IV.2 en IV.6).

V. ANDERE BENADERINGSWIJZEN

Zweeds voorstel

43. Het Zweedse voorstel blijft niet beperkt tot specifieke soorten informatie maar bestrijkt alle informatie *en inlichtingen*, zelfs informatie en inlichtingen die door anderen dan bevoegde wetshandhavingsinstanties worden beheerd. Het voorstel stimuleert samenwerking door het stellen van termijnen voor het beantwoorden van informatieverzoeken en door het afschaffen van het onderscheid tussen uitwisseling binnen één lidstaat en informatie-uitwisseling over de grenzen heen. Het biedt geen aanvullende garanties dat de informatie inderdaad kan worden ingezien. Daarom is het begrijpelijk dat de Commissie het Zweedse voorstel op zich geen adequaat instrument voor beschikbaarheid vond [1].

44. De benadering in het Zweedse voorstel heeft de volgende algemene implicaties wat betreft de gegevensbescherming:

— Het wordt toegejuicht dat het voorstel strikt beperkt blijft tot het verwerken van bestaande gegevens en niet leidt tot nieuwe gegevensbanken en zelfs niet tot indexgegevens.

— Het ontbreken van indexgegevens is echter niet per definitie een positief element. Indexgegevens kunnen, indien zij afdoende worden beveiligd, een doelgericht en daardoor minder indringend onderzoek van gevoelige gegevens mogelijk maken. Ook kunnen de verzoeken beter worden gefilterd en kan er beter toezicht worden gehouden.

— In ieder geval leidt het voorstel tot een toename van de uitwisseling van persoonsgegevens over de grenzen heen, met risico's voor de bescherming van persoonsgegevens, onder meer vanwege het feit dat de bevoegdheid van de lidstaten om de uitwisseling van gegevens te controleren, wordt aangetast. Het moet niet onafhankelijk van de aanneming van het kaderbesluit over de bescherming van persoonsgegevens worden aangenomen.

Het Verdrag van Prüm

45. Het Verdrag van Prüm volgt voor de toepassing van het beschikbaarheidsbeginsel een andere aanpak. Dit voorstel voor een kaderbesluit volgt een algemene aanpak (het biedt geen specifieke voorschriften voor de uitwisseling van specifieke soorten informatie maar geldt voor alle soorten informatie, voorzover genoemd in Bijlage II (zie de punten 21-28 van dit advies), terwijl de aanpak in het verdrag van Prüm geleidelijk van aard is.

46. Deze aanpak kan de „aanpak per gegevensveld" worden genoemd. De aanpak geldt voor specifieke soorten informatie (DNA, vingerafdrukgegevens en voertuigregistratiegegevens) en houdt de verplichting in om rekening te houden met de specifieke aard van de gegevens. Het Verdrag houdt de verplichting in om DNA-analysebestanden te openen en bij te houden ten behoeve van het onderzoek naar strafbare feiten. Voor vingerafdrukgegevens geldt een soortgelijke verplichting. De nationale contactpunten van andere lidstaten moeten rechtstreeks toegang krijgen tot voertuigregistratiegegevens.

47. De aanpak van het Verdrag van Prüm geeft aanleiding tot drie soorten opmerkingen.

48. Ten eerste spreekt het vanzelf dat de EDPS zich niet kan vinden in het proces dat tot dit verdrag heeft geleid: buiten het institutionele kader van de Europese Unie en dus zonder een noemenswaardige rol van de Commissie. Ook wordt er geen democratische controle uitgeoefend door het Europees Parlement en geen juridische controle door het Hof van Justitie, waardoor er minder garanties zijn dat alle (openbare) belangen in gelijke mate in aanmerking zijn genomen. Dit geldt ook voor de gegevensbescherming. Met andere woorden, de instellingen van de Europese Unie waren niet in de gelegenheid voorafgaand aan de invoering van het systeem het effect van de beleidskeuzes op de bescherming van persoonsgegevens in te schatten.

49. Ten tweede is het duidelijk dat sommige elementen van het Verdrag van Prüm veel indringender zijn voor de betrokkene dan het voorstel voor een kaderbesluit betreffende beschikbaarheid. Het Verdrag leidt noodzakelijkerwijs tot het aanleggen van nieuwe gegevensbanken, wat op zich al risico's inhoudt voor de bescherming van persoonsgegevens. De noodzaak en de evenredigheid van het aanleggen van nieuwe gegevensbanken moet worden aangetoond. Er dienen adequate garanties te worden geboden voor de bescherming van persoonsgegevens.

[1] Zie het werkdocument van de diensten van de Commissie, bijlage bij het voorstel voor een kaderbesluit van de Raad betreffende de uitwisseling van informatie volgens het beschikbaarheidsbeginsel, SEC 2005 (1207) van 12.10.2005.

Een „aanpak per gegevensveld"

50. Ten derde wordt in het Verdrag, zoals reeds is gezegd, een „aanpak per gegevensveld" gevolgd. De EDPS heeft eerder reeds melding gemaakt van de moeilijkheden en onzekerheden in verband met de omgeving waarin het beschikbaarheidsbeginsel in de praktijk moet worden gebracht. Daarom is het volgens de EDPS beter geen systeem op te zetten voor een hele reeks gegevens, maar te beginnen met een omzichtiger aanpak met maar één soort gegevens en te zien in welke mate het beschikbaarheidsbeginsel een daadwerkelijke steun kan zijn voor wetshandhaving, en welke specifieke risico's er zijn voor de bescherming van persoonsgegevens. Op basis van die ervaringen kan het systeem mogelijkerwijs worden uitgebreid tot andere soorten gegevens en/of worden gewijzigd zodat het beter werkt.

51. Deze „aanpak per gegevensveld" zou ook beter beantwoorden aan de vereisten van het evenredigheidsbeginsel. Volgens de EDPS kan de noodzaak van een betere gegevensuitwisseling over de grenzen heen ten behoeve van wetshandhaving een goede reden zijn om op EU-niveau een juridisch instrument aan te nemen. Echter, om evenredig te zijn dient het instrument geschikt voor zijn doel te zijn, hetgeen beter kan worden vastgesteld na een periode van praktijkervaring. Voorts mag het instrument de betrokkene niet onevenredig schaden. De uitwisseling mag geen betrekking hebben op meer soorten gegevens dan strikt noodzakelijk is, met de mogelijkheid van anonieme gegevensuitwisseling, en moet gebeuren onder strenge voorwaarden voor gegevensbescherming.

52. Voorts zou een omzichtiger aanpak, zoals door de EDPS wordt voorgestaan (eventueel naast de „aanpak per gegevensveld") kunnen inhouden dat alleen via onrechtstreekse toegang, via indexgegevens, met de praktische uitwerking van het beschikbaarheidsbeginsel wordt begonnen. De EDPS geeft dit mee als een punt van overweging in het verdere wetgevingsproces.

VI. **WELKE GEGEVENS?**

53. In Bijlage II staan de soorten informatie die krachtens het voorgestelde kaderbesluit kunnen worden verkregen. Alle zes soorten informatie die daar worden genoemd zijn meestal persoonsgegevens omdat het bij alle zes gaat om een band met een geïdentificeerde of identificeerbare persoon.

54. In artikel 3, onder g) van het voorstel worden onder indexgegevens verstaan: gegevens aan de hand waarvan gericht informatie kan worden geïdentificeerd en welke via een zoekroutine kunnen worden bevraagd om na te gaan of informatie al dan niet beschikbaar is. In de „Aanpak voor de toepassing van het beginsel van beschikbaarheid" [1] worden onderstaande gegevens gekwalificeerd als indexgegevens:

— de identificatie van de betrokkenen;

— een identificatienummer voor de betrokken voorwerpen (voertuigen, documenten);

— vingerafdrukken/digitale foto's

Andere soorten gegevens die als indexgegevens kunnen worden beschouwd zijn de DNA-profielen. Uit deze lijst van indexgegevens blijkt dat indexgegevens persoonsgegevens kunnen bevatten en dat derhalve adequate bescherming nodig is.

55. De EDPS besteedt specifiek aandacht aan het punt van de DNA-profielen. Het is bewezen dat DNA-analyse van beduidende waarde is voor het misdaadonderzoek en een goede uitwisseling van DNA-gegevens kan van wezenlijk belang zijn voor de bestrijding van de misdaad. Het is echter van wezenlijk belang dat het begrip DNA-gegevens duidelijk wordt gedefinieerd en dat terdege rekening wordt gehouden met de specifieke kenmerken van deze gegevens. Er is qua gegevensbescherming namelijk een groot verschil tussen DNA-monsters en DNA-profielen.

56. DNA-monsters (die vaak door wetshandhavingsinstanties worden verzameld en bewaard) moeten worden beschouwd als bijzonder gevoelig, aangezien er een grotere kans is dat zij het gehele DNA-„plaatje" bevatten. Zij kunnen informatie bieden over iemands genetische kenmerken en gezondheidstoestand die misschien nodig is voor geheel andere doeleinden zoals het geven van medisch advies aan personen of aan jonge stellen.

57. Daarentegen bevatten DNA-profielen slechts enige gedeeltelijke DNA-informatie uit het DNA-monster: zij kunnen worden gebruikt om de identiteit van een persoon na te gaan, maar onthullen in beginsel niet iemands genetische kenmerken. Niettemin kan de wetenschappelijke vooruitgang ertoe leiden dat de DNA-profielen meer informatie zullen kunnen onthullen: wat nu wordt beschouwd als een „onschuldig" DNA-profiel kan later veel meer informatie onthullen dan werd verwacht en noodzakelijk was, en in het bijzonder informatie over iemands genetische kenmerken. De informatie die door DNA-profielen kan worden onthuld moet dus worden beschouwd als dynamisch.

58. In dit verband tekent de EDPS aan dat zowel het Verdrag van Prüm als het Commissievoorstel de uitwisseling van DNA-gegevens tussen wetshandhavers stimuleert, maar dat zij dat op substantieel uiteenlopende wijzen doen.

[1] Document van het voorzitterschap aan de Raad van 5 april 2005 (doc. 7641/05).

59. De EDPS juicht het toe dat het Commissievoorstel geen verplichting oplegt om DNA-gegevens te verzamelen en dat het de uitwisseling van DNA-gegevens duidelijk beperkt tot DNA-profielen. In Bijlage II worden DNA-profielen gedefinieerd middels een eerste gemeenschappelijke lijst van DNA-merkers die in de lidstaten worden gebruikt bij forensische DNA-analyse. Deze lijst (die is gebaseerd op de zeven DNA-merkers van de Europese standaardset zoals beschreven in Bijlage I bij de Resolutie van de Raad van 25 juni 2001 inzake de uitwisseling van DNA-analyseresultaten) ([1]) garandeert dat DNA-profielen, wanneer zij worden geëxtraheerd, geen informatie over specifieke erfelijke eigenschappen bevatten.

60. De EDPS benadrukt dat deze resolutie van de Raad enkele zeer belangrijke waarborgen biedt die specifiek te maken hebben met de dynamische aard van DNA-profielen. In deel III van de Resolutie wordt de uitwisseling van DNA-analyseresultaten namelijk beperkt tot „chromosoomgebieden […] waarvan niet bekend is of zij informatie over specifieke erfelijke eigenschappen" bevatten en wordt de lidstaten vervolgens aanbevolen niet langer DNA-merkers te gebruiken die, als gevolg van het voortschrijden van de wetenschap, informatie over specifieke erfelijke eigenschappen kunnen bevatten.

61. Het Verdrag van Prüm volgt een andere aanpak en verplicht de verdragsluitende partijen om DNA-analysebestanden te openen en bij te houden ten behoeve van het onderzoek naar strafbare feiten. Het houdt dus in dat er nieuwe DNA-gegevensbanken worden opgericht en dat er meer DNA-gegevens worden verzameld. Verder is niet duidelijk wat voor soort gegevens er in de „DNA-analysebestanden" zitten en het Verdrag houdt geen rekening met de dynamische evolutie van DNA-profielen.

62. De EDPS wijst erop dat een juridisch instrument dat voorziet in uitwisseling van DNA-gegevens

— een duidelijke afbakening en definitie moet geven van het soort DNA-informatie dat mag worden uitgewisseld (ook gelet op het fundamentele verschil tussen DNA-monsters en DNA-profielen),

— gemeenschappelijk technische normen moet bieden om te vermijden dat verschillen tussen de methoden waarmee in de lidstaten met forensische DNA-gegevensbanken wordt gewerkt zouden kunnen leiden tot problemen en onnauwkeurige resultaten wanneer deze gegevens worden uitgewisseld,

— goede juridisch bindende waarborgen moet bieden om te voorkomen dat de wetenschappelijke ontwikkelingen ertoe zouden leiden dat uit DNA-profielen persoonsgegevens worden verkregen die niet alleen gevoelig zijn, maar ook niet nodig zijn voor het doel waarvoor de profielen zijn verzameld.

([1]) PB C 187, blz. 1.

63. In dit opzicht bevestigt en herhaalt de EDPS de opmerkingen die hij reeds heeft gemaakt in zijn advies over het kaderbesluit over de bescherming van persoonsgegevens (punt 80). In dat advies wees de EDPS er ten aanzien van DNA-gegevens op dat er specifieke waarborgen dienen te worden geboden om te garanderen dat de beschikbare informatie uitsluitend wordt gebruikt om personen te identificeren met als doel het voorkomen, onderzoeken, opsporen en vervolgen van strafbare feiten; dat de nauwkeurigheid van DNA-profielen zorgvuldig in overweging wordt genomen en door de betrokkene met gemakkelijk beschikbare middelen kan worden aangevochten; dat het respect voor de waardigheid van de persoon ten volle wordt gewaarborgd ([2]).

64. Deze overwegingen leiden voorts tot de slotsom dat wetgeving over het aanleggen van DNA-bestanden en de uitwisseling van gegevens uit deze bestanden alleen moet worden aangenomen na een effectbeoordeling waarin een grondige inschatting is gemaakt van de voordelen en de risico's. De EDPS beveelt aan in deze wetgeving verplichtingen op te nemen om de wetgeving, na haar inwerkingtreding, regelmatig te evalueren.

65. Tot slot bevat Bijlage II nog andere soorten informatie die mag worden uitgewisseld. Hierbij gaat het om informatie die afkomstig is van particuliere instanties, aangezien telefoonnummers en andere communicatiegegevens, evenals verkeersgegevens, normaliter afkomstig zijn van telefoonbedrijven. In de toelichting wordt bevestigd dat de lidstaten ervoor moeten zorgen dat voor de wetshandhaving relevante informatie, beheerd door autoriteiten of daartoe aangewezen particuliere instanties, wordt gedeeld met gelijkwaardige bevoegde instanties van andere lidstaten en Europol. Aangezien het voorstel geldt voor persoonsgegevens, afkomstig van particuliere instanties, moet het toepasselijk juridisch kader, volgens de EDPS, bijkomende waarborgen bieden ter bescherming van de betrokkene, zodat de nauwkeurigheid van de gegevens wordt verzekerd.

VII. **BEGINSELEN VAN DE GEGEVENSBESCHERMING**

66. Het voorgestelde kaderbesluit van de Raad bevat niet specifiek regels voor de bescherming van persoonsgegevens terwijl in andere instrumenten, zoals het Verdrag van Prüm of het Zweedse voorstel, een aantal specifieke bepalingen wel betrekking heeft op het beschermen van persoonsgegevens. Het ontbreken van specifieke regels voor het beschermen van persoonsgegevens in het voorgestelde kaderbesluit is slechts in zoverre aanvaardbaar dat de algemene regels in het voorstel voor een kaderbesluit over gegevensbescherming in de derde pijler volledig van toepassing zijn en voldoende bescherming bieden. Voorts mogen regels over de bescherming van persoonsgegevens in specifieke instrumenten, zoals het Zweedse voorstel en het Verdrag van Prüm, het niveau van de door het algemene kader geboden bescherming niet verlagen. De EDPS beveelt aan een specifieke bepaling over mogelijke conflicten tussen de verschillende regels inzake gegevensbescherming toe te voegen.

([2]) Zie ook van de Raad van Europa: „Progress Report on the Application of the Principles of Convention 108 to the Collection and Processing of personal biometric data" van februari 2005.

67. De EDPS wil er hier weer nadrukkelijk op wijzen, onder verwijzing naar zijn advies over het kaderbesluit over de bescherming van persoonsgegevens, dat het van belang is dat er consequente en alomvattende regels zijn voor gegevensbescherming ten aanzien de samenwerking van bij wetshandhaving, die voor alle verwerkingen gelden. Dientengevolge herhaalt de EDPS de overige in dat advies gemaakte opmerkingen. Hieronder worden enkele punten op het gebied van de gegevensbescherming benadrukt:

— Rechtmatige verwerking van persoonsgegevens. De EDPS steunt de opvatting dat informatie uitsluitend beschikbaar kan zijn indien zij op rechtmatige wijze is verzameld (zoals staat in artikel 2, lid 2, wat betreft informatie die door middel van dwangmaatregelen is verzameld). Rechtmatige verwerking van persoonsgegevens zal ook waarborgen dat beschikbaar gestelde en uitgewisselde informatie ook in een rechtszaak kan worden gebruikt. Hoewel informatie die na het instellen van een vervolging is verzameld buiten het toepassingsgebied van het voorgestelde instrument valt, is het nog steeds waarschijnlijk dat informatie die in een eerder stadium door wetshandhavingsinstanties is uitgewisseld, in een rechtszaak terechtkomt.

— De kwaliteit van persoonsgegevens is van specifiek belang aangezien het beschikbaarheidsbeginsel bevordert dat informatie wordt gebruikt door wetshandhavingsinstanties die werken buiten de context waarin de gegevens zijn verzameld. Deze instanties hebben zelfs rechtstreeks toegang tot gegevensbanken van andere lidstaten. De kwaliteit van de persoonsgegevens kan alleen worden gewaarborgd indien de nauwkeurigheid ervan regelmatig en grondig wordt gecontroleerd, indien onderscheid wordt gemaakt tussen de soorten informatie al naar gelang de verschillende categorieën betrokkenen (slachtoffers, verdachten, getuigen enz.) en indien, zo nodig, de mate van nauwkeurigheid is aangegeven (zie het advies van de EDPS over de bescherming van persoonsgegevens, IV.6).

Deze punten maken nogmaals duidelijk waarom gegevensbeschermingsregels, en in het bijzonder regels inzake de nauwkeurigheid, zouden moeten gelden voor alle soorten verwerking, ook binnenlandse. Anders zouden rechtstreeks geraadpleegde persoonsgegevens onjuist en achterhaald kunnen zijn, en zodoende de rechten van de betrokkene en de doeltreffendheid van de onderzoeken kunnen schaden.

— Doelbinding. Volgens het beschikbaarheidsbeginsel zijn persoonsgegevens toegankelijk voor gelijkwaardige bevoegde instanties van andere lidstaten. De bevoegdheden van wetshandhavingsinstanties kunnen per land echter aanzienlijk verschillen. Daarom is het van groot belang ervoor te zorgen dat het beginsel van doelbinding wordt gevolgd, ondanks de verschillende reikwijdten van de bevoegdheden van de diverse bevoegde instanties die gegevens uitwisselen. Informatie die door een bepaalde instantie met een specifiek doel wordt verzameld en verwerkt, kan dan niet voor een ander doel worden gebruikt alleen op grond van het feit dat de ontvangende instantie andere, wellicht ruimere bevoegdheden heeft.

Daarom is de EDPS ingenomen met artikel 7 van het voorgestelde kaderbesluit, dat moet worden gelezen als een specificatie van de algemene regels in het voorgestelde kaderbesluit over de bescherming van persoonsgegevens. Voorts tekent de EDPS aan dat de beoordeling van de gelijkwaardigheid van de verschillende instanties (die in dit voorstel wordt overgelaten aan een comité-procedure) zorgvuldig moet worden uitgevoerd, waarbij het beginsel van doelbinding precies moet worden gevolgd.

— Termijnen voor de opslag van uitgewisselde informatie moeten ook worden gezien in het licht van het beginsel van doelbinding: informatie die voor één doel is geraadpleegd of uitgewisseld dient te worden vernietigd zodra zij niet meer voor dat doel nodig is. Dit voorkomt een nodeloze verdubbeling van de gegevensbanken en tegelijkertijd kunnen de bevoegde instanties de beschikbare (en bijgewerkte) informatie nogmaals raadplegen indien dat voor een ander legitiem doel nodig is.

— Vastlegging van volgens het beschikbaarheidsbeginsel doorgestuurde informatie. Vastlegging dient aan twee kanten te gebeuren: zowel in de aangezochte als in de verzoekende lidstaat. Vastleggingen van toegang, en niet alleen van uitwisselingen, zijn noodzakelijk (zie het advies van de EDPS over de bescherming van persoonsgegevens, punt 133), ook om ervoor te zorgen dat nationale bevoegde instanties elkaar vertrouwen en niet geheel de controle over de beschikbare informatie kwijtraken. Het feit dat informatie traceerbaar moet zijn, houdt ook in dat het mogelijk moet zijn informatie te actualiseren en/of te corrigeren.

— Rechten van de betrokkenen Systemen voor de uitwisseling van informatie tussen wetshandhavingsinstanties van de EU leiden tot een toename van het aantal situaties waarin persoonsgegevens op hetzelfde tijdstip door bevoegde instanties in verschillende lidstaten (tijdelijk) worden verwerkt. Dit houdt enerzijds in dat er gemeenschappelijke EU-normen inzake de rechten van de betrokkene moeten worden vastgesteld en anderzijds dat de betrokkenen in staat moeten zijn hun rechten uit te oefenen in de mate die de regels inzake gegevensbescherming in de derde pijler toelaten, tegenover zowel de instanties die de gegevens beschikbaar stellen als de instanties die deze gegevens raadplegen en verwerken.

— Toezicht De EDPS wijst erop dat, afhankelijk van de zaak, meer dan één nationale toezichthoudende autoriteit bevoegd kan zijn om toezicht uit te oefenen op de verwerking van persoonsgegevens, uitgevoerd op basis van deze voorstellen. In dat opzicht maakt rechtstreekse on line toegang tot wetshandhavingsinformatie meer toezicht en betere coördinatie door de relevante nationale gegevensbeschermingsinstanties noodzakelijk.

VIII. CONCLUSIES

Algemene conclusies over het beschikbaarheidsbeginsel

68. De EDPS maakt van de gelegenheid gebruik om in dit advies een aantal algemene en meer fundamentele standpunten over de uitwisseling van wetshandhavingsinformatie en over de wijzen waarop de regulering ervan kan worden aangepakt, te presenteren. De EDPS zal beschikbaar zijn voor verdere raadpleging in een later stadium, wanneer zich belangrijke ontwikkelingen zullen hebben voorgedaan in het wetgevingsproces met betrekking tot dit voorstel of andere eraan gerelateerde voorstellen.

69. Volgens de EDPS moet het beschikbaarheidsbeginsel in een bindend juridisch instrument worden gegoten middels een omzichtiger, geleidelijke aanpak met maar één soort gegevens en moet worden bekeken in welke mate het beschikbaarheidsbeginsel een daadwerkelijke steun kan zijn voor wetshandhaving, en welke specifieke risico's er zijn voor de bescherming van persoonsgegevens. Deze omzichtiger aanpak zou kunnen inhouden dat alleen via onrechtstreekse toegang, via indexgegevens, met de toepassing van het beschikbaarheidsbeginsel wordt begonnen. Op basis van die ervaringen kan het systeem mogelijkerwijs worden uitgebreid tot andere soorten gegevens en/of worden gewijzigd zodat het beter werkt.

70. Er mag geen enkel juridisch instrument tot toepassing van het beschikbaarheidsbeginsel worden aangenomen zonder dat er eerst essentiële gegevensbeschermingsgaranties zoals vervat in het voorstel voor een kaderbesluit over de bescherming van persoonsgegevens zijn aangenomen.

Aanbevolen wijzigingen van het voorstel

71. De EDPS beveelt aan het toepassingsgebied van het beschikbaarheidsbeginsel als volgt te verduidelijken:

— Voeg een duidelijke en nauwkeurige definitie toe van de gegevens die zullen worden beschouwd als zijnde beschikbaar.

— Beperk als eerste optie het toepassingsgebied van het beschikbaarheidsbeginsel tot informatie die door bevoegde instanties wordt beheerd.

— Zorg als tweede optie, in het geval van een ruimer toepassingsgebied, voor voldoende waarborgen voor de bescherming van persoonsgegevens. Neem de in punt 27 aangestipte vragen in overweging.

72. De EDPS maakt onderstaande kanttekeningen bij rechtstreekse toegang tot gegevensbanken voor een bevoegde instantie van een andere lidstaat:

— Dit punt moet op adequate wijze worden geregeld aangezien de aangewezen instanties van de lidstaat van herkomst in het geval van rechtstreekse toegang geen controle hebben over de toegang tot en het gebruik van de gegevens.

— Het voorstel mag niet aanzetten tot onvoorwaardelijke koppeling van gegevensbanken en zodoende tot een netwerk van gegevensbanken waarop moeilijk toezicht kan worden gehouden.

73. Het kaderbesluit zou duidelijker moeten zijn over het instellen van een systeem van indexgegevens. Meer in het bijzonder:

— moet het voorstel adequate voorschriften geven, in elk geval voor het maken van indexgegevens, voor het beheer van de opbergsystemen ervan en voor een goede organisatie van de toegang tot de indexgegevens,

— moet het begrip indexgegevens duidelijker worden gedefinieerd,

— moet het voorstel de rol van die de nationale contactpunten ten aanzien van indexgegevens verduidelijken,

— moeten de basisregels voor het maken van indexgegevens in het kaderbesluit zelf worden opgenomen en niet worden overgelaten aan uitvoeringsregelgeving overeenkomstig de comité-procedure.

74. De EDPS stelt dat het voorstel, voorzover het de uitwisseling van DNA-gegevens betreft,

— een duidelijke afbakening en definitie moet geven van het soort DNA-informatie dat mag worden uitgewisseld (ook gelet op het fundamentele verschil tussen DNA-monsters en DNA-profielen),

— gemeenschappelijk technische normen moet bieden om te vermijden dat verschillen tussen de methoden waarmee in de lidstaten met forensische DNA-gegevensbanken wordt gewerkt zouden kunnen leiden tot problemen en onnauwkeurige resultaten wanneer deze gegevens worden uitgewisseld,

— goede juridisch bindende waarborgen moet bieden om te voorkomen dat de wetenschappelijke ontwikkelingen ertoe zouden leiden dat uit DNA-profielen persoonsgegevens worden verkregen die niet alleen gevoelig zijn, maar ook niet nodig voor het doel waarvoor de profielen zijn verzameld,

— alleen moet worden aangenomen na een effectbeoordeling.

75. De EDPS adviseert de informatie-uitwisseling met Europol te beperken tot de doelstellingen van Europol zelf, zoals vermeld in artikel 2 van de Europol-overeenkomst en de bijlage erbij.

Gedaan te Brussel, 28 februari 2006

Peter HUSTINX

Europese Toezichthouder voor gegevensbescherming