Advies van de Europese Toezichthouder voor gegevensbescherming over de Mededeling van de Commissie aan het Europees Parlement en de Raad — „De EU-interneveiligheidsstrategie in actie: vijf stappen voor een veiliger Europa"

(2011/C 101/02)

DE EUROPESE TOEZICHTHOUDER VOOR GEGEVENSBESCHERMING,

Gelet op het Verdrag betreffende de werking van de Europese Unie, en met name op artikel 16,

Gelet op het Handvest van de grondrechten van de Europese Unie, en met name op de artikelen 7 en 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 [1],

Gelet op het verzoek om een advies overeenkomstig Verordening (EG) nr. 45/2001 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 [2], met name op artikel 41,

BRENGT HET VOLGENDE ADVIES UIT:

I. INLEIDING

1. Op 22 november 2010 heeft de Commissie een Mededeling aangenomen met de titel „EU-interneveiligheidsstrategie in actie: vijf stappen voor een veiliger Europa" (hierna „Mededeling" genoemd) [3]. Deze Mededeling is naar de EDPS gestuurd voor raadpleging.

2. Het verheugt de EDPS dat de Commissie hem heeft geraadpleegd. Reeds voor de aanneming van de Mededeling heeft de EDPS informele opmerkingen gegeven over de ontwerptekst. Een deel van zijn opmerkingen zijn in acht genomen in de definitieve versie van de Mededeling.

Context van de Mededeling

3. De EU-interneveiligheidsstrategie, waarop de Mededeling betrekking heeft, is goedgekeurd op 23 februari 2010 onder het Spaanse voorzitterschap [4]. De strategie beschrijft een Europees veiligheidsmodel, dat onder andere maatregelen op het gebied van rechtshandhaving, justitiële samenwerking, grensbeheer en civiele bescherming omvat, met het nodige respect voor de gedeelde Europese waarden, zoals de fundamentele rechten. De belangrijkste doelstellingen zijn:

   — het publiek bewust maken van de EU-instrumenten die nu al worden ingezet om de veiligheid en vrijheid van de EU-burgers te waarborgen en de toegevoegde waarde die het optreden van de EU biedt op dit gebied;

   — de gemeenschappelijke instrumenten en beleidslijnen verder ontwikkelen en daarbij gebruik maken van een meer geïntegreerde benadering, die de oorzaken van de onveiligheid en niet alleen de gevolgen ervan aanpakt;

   — de rechtshandhaving en justitiële samenwerking, het grensbeheer, de civiele bescherming en de rampenbeheer versterken.

4. Het doel van de EU-interneveiligheidsstrategie is iets te doen aan de meest dringende bedreigingen en uitdagingen voor de veiligheid van de EU, zoals zware en georganiseerde misdaad, terrorisme en cybercriminaliteit, het beheer van de buitengrenzen van de EU, en te zorgen voor meer veerkracht bij natuurrampen en bij door de mens veroorzaakte calamiteiten. In de strategie zijn algemene richtsnoeren, beginselen en aanwijzingen in verband met de reactie van de EU op deze problemen vastgelegd en wordt de Commissie verzocht om tijdgebonden maatregelen voor te stellen voor de tenuitvoerlegging van de strategie.

5. Verder is het belangrijk in deze context te verwijzen naar de op 8-9 november 2010 aangenomen conclusies van de Raad Justitie en Binnenlandse Zaken over de totstandbrenging en uitvoering van een EU-beleidscyclus voor georganiseerde en zware internationale criminaliteit [5] (hierna „Conclusies van november 2010" genoemd). Dit document volgt de conclusie van de Raad over de architectuur van de interne veiligheid van 2006 [6], en verzoekt de Raad en de Commissie om een uitvoerige EU-interneveiligheidsstrategie te definiëren op basis van de gemeenschappelijke waarden en beginselen van de EU, zoals bevestigd in het Handvest van de grondrechten van de EU [7].

[1] PB L 281 van 23.11.1995, blz. 31.
[2] PB L 8 van 12.1.2001, blz. 1.
[3] COM(2010) 673 definitief.
[4] Doc. 5842/2/10.
[5] 3043e vergadering van de Raad Justitie en Binnenlandse Zaken, 8-10 november 2010, Brussel.
[6] Doc. 7039/2/06 JAI 86 CATS 34.
[7] De EU-beleidscyclus voor georganiseerde en zware internationale criminaliteit van de Conclusies van november 2010 bestaat uit vier stappen: 1) beleidsontwikkeling op basis van een EU-dreigingsevaluatie voor zware en georganiseerde criminaliteit (EU SOCTA), 2) beleids- en besluitvorming aan de hand van de vaststelling van een beperkt aantal prioriteiten, 3) uitvoering en monitoring van jaarlijkse operationele actieplannen (OAP) en 4) een grondige evaluatie aan het eind van de beleidscyclus die zal worden meegenomen in de volgende beleidscyclus.

6. Onder de aanwijzingen en doelstellingen die de tenuitvoerlegging van de EU-interneveiligheidsstrategie zouden moeten voortdrijven, wordt in de Conclusies van november 2010 verwezen naar de reflectie over een proactieve en op inlichtingen gebaseerde benadering, nauwe samenwerking tussen de organen van de Unie en een verdere verbetering van hun informatie-uitwisseling, de bewustmaking van de burgers van het belang van het werk van de Unie voor hun bescherming. In de Conclusies wordt de Commissie bovendien verzocht om samen met de deskundigen van de betrokken agentschappen/bureaus en lidstaten een strategisch meerjarenplan (MASP) voor elke prioriteit uit te werken, waarin de meest dienstige strategie voor de aanpak van het probleem wordt geformuleerd. De Commissie wordt verder verzocht om via overleg met de deskundigen van de lidstaten en de EU-agentschappen/bureaus een onafhankelijk mechanisme op poten te zetten dat de uitvoering van het MASP moet evalueren. De EDPS zal deze thema's later in dit advies behandelen, aangezien deze nauw verband houden met of een aanzienlijke invloed hebben op de bescherming van persoonsgegevens, de persoonlijke levenssfeer en andere gerelateerde fundamentele rechten en vrijheden.

Inhoud en doel van de Mededeling

7. In de Mededeling worden vijf strategische doelstellingen voorgesteld die allemaal verband houden met de persoonlijke levenssfeer en gegevensbescherming:

— ontwrichten van internationale criminele netwerken,

— voorkomen van terrorisme en aanpakken van radicalisering en werving,

— verbeteren van de internetveiligheid voor burgers en bedrijfsleven,

— veiligheid verbeteren door grensbeheer,

— de veerkracht van Europa bij crises en rampen vergroten.

8. De in de Mededeling voorgestelde *EU-interneveiligheidsstrategie in actie* omvat een gedeelde agenda voor de lidstaten, het Europees Parlement, de Commissie, de Raad, EU-organen en andere partijen, waaronder het maatschappelijk middenveld en lokale autoriteiten, en beschrijft hoe ze allemaal moeten samenwerken in de volgende vier jaar om de doelstellingen van de EU-interneveiligheidsstrategie te realiseren.

9. De Mededeling bouwt voort op het Verdrag van Lissabon en erkent de richtsnoeren van het programma van Stockholm (en het bijbehorende actieplan) waarin in hoofdstuk 4.1 de noodzaak van een uitvoerige EU-interneveiligheidsstrategie op basis van respect voor de fundamentele rechten, internationale bescherming en de rechtsstaat wordt benadrukt. Bovendien bepaalt het programma van Stockholm dat het ontwikkelen, monitoren en invoeren van de interneveiligheidsstrategie één van de prioritaire taken moet worden van het Permanent Comité binnenlandse veiligheid (COSI) dat is opgericht krachtens artikel 71 VWEU. Voor een doeltreffende handhaving van de EU-interneveiligheidsstrategie moet deze ook veiligheidsaspecten omvatten van een geïntegreerd grensbeheer en, waar nodig, justitiële samenwerking in strafzaken indien van belang voor de operationele samenwerking op het gebied inzake interne veiligheid. Het is in deze context ook belangrijk erop te wijzen dat het programma van Stockholm vraagt om een geïntegreerde benadering van de EU-interneveiligheidsstrategie, die ook rekening houdt met de door de EU ontwikkelde externeveiligheidsstrategie en andere EU-beleidsgebieden, met name degene die betrekking hebben op de interne markt.

Doel van het advies

10. De Mededeling heeft betrekking op verschillende beleidsterreinen die deel uitmaken van of invloed hebben op de „interne veiligheid" van de Europese Unie in ruime zin.

11. Het is niet de bedoeling in dit advies alle beleidsterreinen en specifieke thema's die aan bod komen in de Mededeling te analyseren, maar wel om:

— de werkelijke doelstellingen van de in de Mededeling voorgestelde EU-interneveiligheidsstrategie te bekijken vanuit het specifieke oogpunt van de persoonlijke levenssfeer en gegevensbescherming en — vanuit deze invalshoek — te wijzen op de noodzakelijke verbanden met andere strategieën die op dit moment worden besproken en goedgekeurd op EU-niveau;

— te wijzen op een aantal noties en concepten inzake gegevensbescherming waarmee rekening moet worden gehouden bij het ontwerpen, ontwikkelen en invoeren van de EU-interneveiligheidsstrategie op EU-niveau;

— waar nuttig en gepast voorstellen te formuleren over hoe aspecten van gegevensbescherming het best in aanmerking kunnen worden genomen bij de tenuitvoerlegging van de maatregelen die worden voorgesteld in de Mededeling.

12. De EDPS zal dat doen door met name de verbanden tussen de EU-interneveiligheids- en de informatiebeheerstrategie en het werk inzake het alomvattende kader voor gegevensbescherming te beklemtonen. Bovendien zal de EDPS verwijzen naar concepten als beste beschikbare technieken en „privacy by design", beoordeling van het effect op privacy- en gegevensbescherming en rechten van de betrokkenen, die een directe invloed hebben op het ontwerp en de tenuitvoerlegging van de EU-interneveiligheidsstrategie. Het advies bevat ook opmerkingen betreffende een aantal geselecteerde beleidsterreinen zoals geïntegreerd grensbeheer, waaronder EUROSUR en de verwerking van persoonsgegevens door FRONTEX, alsmede andere gebieden zoals cyberspace en TFTP.

II. ALGEMENE OPMERKINGEN

De nood aan een alomvattende, inclusieve en „strategische" benadering van EU-strategieën met betrekking tot de EU-interneveiligheidsstrategie

13. Momenteel worden er op basis van het Verdrag van Lissabon en het programma van Stockholm op EU-niveau verschillende EU-strategieën besproken en voorgesteld die de gegevensbescherming direct of indirect beïnvloeden. De EU-interneveiligheidsstrategie is hier één van en houdt nauw verband met andere strategieën (die al behandeld zijn in recente mededelingen van de Commissie of die gepland zijn voor de nabije toekomst) zoals de EU-informatiebeheersstrategie en het Europees model voor informatie-uitwisseling, de strategie voor de tenuitvoerlegging van het Handvest van de grondrechten van de Europese Unie, het alomvattend kader voor gegevensbescherming en het EU-beleid inzake terrorismebestrijding. In dit advies besteedt de EDPS bijzondere aandacht aan de verbanden met de informatiebeheersstrategie en het alomvattend kader voor gegevensbescherming op basis van artikel 16 VWEU, die de duidelijkste beleidsverbanden hebben met de EU-interneveiligheidsstrategie uit het oogpunt van de gegevensbescherming.

14. Al deze strategieën vormen een onoverzichtelijke „lappendeken" van onderling verweven beleidslijnen, programma's en actieplannen, zodat een alomvattende en geïntegreerde aanpak op EU-niveau noodzakelijk is.

15. Meer algemeen zou deze benadering van „verbanden leggen tussen de strategieën", indien toegepast bij toekomstige acties, laten zien dat er een visie is op EU-niveau wanneer het gaat om *EU-strategieën*. Ook zou het laten zien dat deze strategieën en de onlangs goedgekeurde mededelingen die daarop betrekking hebben, nauw op elkaar aansluiten, aangezien ze allemaal het programma van Stockholm als gemeenschappelijk referentiepunt hebben. Dit zou ook leiden tot positieve synergie-effecten tussen verschillende beleidsgebieden binnen de ruimte van vrijheid, veiligheid en rechtvaardigheid en zou eventueel dubbel werk en inspanningen op dit gebied voorkomen. Even belangrijk is dat deze benadering zou leiden tot een doeltreffendere en coherentere toepassing van gegevensbeschermingsregels in de context van alle onderling verbonden strategieën.

16. De EDPS beklemtoont dat een van de pijlers van de EU-interneveiligheidsstrategie een efficiënt informatiebeheer in de Europese Unie is, waarbij de informatie-uitwisseling gerechtvaardigd moet zijn op grond van de beginselen van noodzakelijkheid en evenredigheid.

17. Bovendien, zoals vermeld in het advies van de EDPS over de Mededeling over informatiebeheer ([8]), benadrukt de EDPS dat nieuwe wetgevingsmaatregelen die de opslag en uitwisseling van persoonsgegevens toestaan, alleen mogen worden voorgesteld als de noodzaak daarvan concreet is aangetoond ([9]). Deze wettelijke vereiste moet worden omgezet in een proactieve beleidsbenadering bij de tenuitvoerlegging van de EU-interneveiligheidsstrategie. De noodzaak van een alomvattende benadering van de EU-interneveiligheidsstrategie leidt onvermijdelijk ook tot de noodzaak alle bestaande middelen en instrumenten op het gebied van interne veiligheid te evalueren voordat er nieuwe worden voorgesteld.

18. In dit verband stelt de EDPS ook voor frequenter gebruik te maken van clausules die voorzien in een periodieke evaluatie van de bestaande instrumenten, zoals opgenomen in de richtlijn gegevensbewaring die op dit moment wordt beoordeeld. ([10])

Gegevensbescherming als een doel van de EU-interneveiligheidsstrategie

19. De Mededeling verwijst naar de bescherming van persoonsgegevens in de paragraaf „Veiligheidsbeleid op basis van gemeenschappelijke waarden", waar wordt gesteld dat de instrumenten en maatregelen ter uitvoering van de interneveiligheidsstrategie moeten worden gebaseerd op gemeenschappelijke waarden als de rechtsstaat en eerbiediging van de grondrechten zoals verankerd in het Handvest van de grondrechten van de Europese Unie. Verder stelt de Mededeling: „Waar informatie-uitwisseling doeltreffende rechtshandhaving in de EU mogelijk maakt, moeten we ook de persoonlijke levenssfeer beschermen en het grondrecht op bescherming van persoonsgegevens waarborgen".

20. Deze uitspraak verheugt de EDPS. Op zich volstaat ze echter niet om de kwestie van de gegevensbescherming in de EU-interneveiligheidsstrategie af te handelen. Ook in de Mededeling wordt niet dieper ingegaan op gegevensbescherming ([11]) of uitgelegd hoe de inachtneming van de persoonlijke levenssfeer en de bescherming van persoonsgegevens in de praktijk zal worden verzekerd in de acties voor de invoering van de EU-interneveiligheidsstrategie.

([8]) Advies van 30 september 2010 over de Mededeling van de Commissie aan het Europees Parlement en de Raad getiteld „Overzicht van het informatiebeheer op het gebied van vrijheid, veiligheid en recht".

([9]) Dit is een wettelijke vereiste; zie met name het vonnis van het Europees Hof van Justitie in gevoegde zaken C-92/09 en C-93/09 van 2 november 2010. Ook in meer specifieke contexten heeft de EDPS gepleit voor deze benadering in andere adviezen over wetgevingsvoorstellen met betrekking tot de ruimte van vrijheid, veiligheid en rechtvaardigheid: bijv. het advies van 19 oktober 2005 inzake drie voorstellen betreffende het Schengeninformatiesysteem van de tweede generatie (SIS II); het advies van 20 december 2007 betreffende het voorstel voor een kaderbesluit van de Raad over het gebruik van persoonsgegevens van passagiers (PNR-gegevens) voor wetshandhavingsdoeleinden; het advies van 18 februari 2009 over het voorstel voor een verordening betreffende de instelling van „Eurodac" voor de vergelijking van vingerafdrukken ten behoeve van een doeltreffende toepassing van Verordening (EG) nr. (…/…) (tot vaststelling van de criteria en instrumenten om te bepalen welke lidstaat verantwoordelijk is voor de behandeling van een verzoek om internationale bescherming dat door een onderdaan van een derde land of een staatloze bij een van de lidstaten wordt ingediend); het advies van 18 februari 2009 over het voorstel voor een verordening tot vaststelling van de criteria en instrumenten om te bepalen welke lidstaat verantwoordelijk is voor de behandeling van een verzoek om internationale bescherming dat door een onderdaan van een derde land of een staatloze bij een van de lidstaten wordt ingediend; en het advies van 7 oktober 2009 over de voorstellen inzake het verlenen van toegang aan rechtshandhavingsinstanties tot EURODAC.

([10]) Richtlijn 2006/24/EG van het Europees Parlement en de Raad van 15 maart 2006 betreffende de bewaring van gegevens die zijn gegenereerd of verwerkt in verband met het aanbieden van openbaar beschikbare elektronische communicatiediensten of van openbare communicatienetwerken en tot wijziging van Richtlijn 2002/58/EG, (PB L 105 van 13.4.2006, blz. 54).

([11]) Gegevensbescherming wordt alleen specifiek vermeld in de context van de verwerking van persoonsgegevens door FRONTEX.

21. De EDPS is van mening dat de EU-interneveiligheidsstrategie *in actie* minstens als één van haar doelstellingen een *bescherming* in ruime zin zou moeten hebben die zorgt voor het *juiste* evenwicht tussen enerzijds de bescherming van burgers tegen de bedreigingen en anderzijds de bescherming van de persoonlijke levenssfeer en het recht op de bescherming van persoonsgegevens. Met andere woorden: er moet evenveel belang worden gehecht aan veiligheid als aan privacy bij de ontwikkeling van de EU-interneveiligheidsstrategie die is afgestemd op het programma van Stockholm en de conclusies van de Raad.

22. Kortom, het scheppen van veiligheid en de eerbiediging van de privacy en gegevensbescherming zouden moeten worden vermeld als een doelstelling van de EU-interneveiligheidsstrategie. Dit moet tot uiting komen in alle maatregelen die de lidstaten en EU-instellingen nemen om de strategie ten uitvoer te leggen.

23. In deze context verwijst de EDPS naar Mededeling (2010) 609 over een integrale aanpak van de bescherming van persoonsgegevens in de Europese Unie. ([12]) De EDPS zal binnenkort een advies uitbrengen over deze Mededeling, maar benadrukt hier dat er geen efficiënte EU-interneveiligheidsstrategie kan worden ingevoerd zonder de aanvulling van een solide gegevensbeschermingsregeling die zorgt voor wederzijds vertrouwen en meer efficiëntie.

III. NOTIES EN CONCEPTEN MET BETREKKING TOT HET ONTWERP EN TENUITVOERLEGGING VAN DE EU-INTERNEVEILIGHEIDSSTRATEGIE

24. Het is duidelijk dat sommige acties die voortkomen uit de EU-interneveiligheidsstrategie, de risico's voor de privacy van individuen en de gegevensbescherming kunnen vergroten. Om deze risico's te compenseren, wil de EDPS de aandacht vestigen op concepten als „ingebouwde privacy" („privacy by design"), beoordeling van de gevolgen voor de persoonlijke levenssfeer en de gegevensbeveiliging, rechten van de betrokkenen en beste beschikbare technieken (BBT's). Met al deze concepten moet worden rekening gehouden bij de tenuitvoerlegging van de EU-interneveiligheidsstrategie. Ze kunnen een nuttige bijdrage leveren aan beleidsbeslissingen op dit gebied die de persoonlijke levenssfeer en de gegevensbeveiliging beter in acht nemen.

„Ingebouwde privacy"

25. De EDPS heeft op verschillende gelegenheden en in verschillende adviezen gepleit voor het concept van de „ingebouwde" („privacy by design" of „privacy by default"). Dit concept wordt momenteel zowel voor de particuliere als voor de overheidssector ontwikkeld en moet derhalve ook een belangrijke rol spelen in de interne veiligheid van de EU en op het gebied van politie en justitie ([13]).

26. Dit concept wordt niet vermeld in de Mededeling. De EDPS stelt voor naar dit concept te verwijzen in de acties die zullen worden voorgesteld en ondernomen om de EU-interneveiligheidsstrategie ten uitvoer te leggen, met name in de context van doelstelling 4 „Veiligheid verbeteren door grensbeheer", waar er duidelijk sprake is van een intensiever gebruik van nieuwe technologie voor grenscontroles en grensbewaking.

Beoordeling van de gevolgen voor de persoonlijke levenssfeer en de gegevensbeveiliging

27. De EDPS spoort de Commissie aan om — als deel van het toekomstige werk inzake het ontwerp en de invoering van de EU-interneveiligheidsstrategie op basis van de Mededeling — stil te staan bij de vraag wat werkelijk onder een „beoordeling van de gevolgen voor de persoonlijke levenssfeer en de gegevensbeveiliging" (PIA) moet worden verstaan op het gebied van vrijheid, veiligheid en rechtvaardigheid, en inzonderheid in de EU-interneveiligheidsstrategie.

28. De Mededeling verwijst naar dreigings- en risicoanalyses. Dit is verheugend. Er wordt echter — in geen enkel punt — iets gezegd over de beoordeling van de gevolgen voor de persoonlijke levenssfeer en de gegevensbeveiliging. De EDPS is van mening dat de werkzaamheden in het kader van de tenuitvoerlegging van de Mededeling over de EU-interneveiligheidsstrategie een goede gelegenheid bieden om zo'n beoordeling van de gevolgen voor de persoonlijke levenssfeer en de gegevensbeveiliging uit te werken in het kader van de interne veiligheid. De EDPS constateert dat dit aspect noch in de Mededeling beschreven algemene richtsnoeren noch in de richtsnoeren voor effectbeoordeling van de Commissie ([14]) nader wordt uitgewerkt of tot een beleidsbeginsel wordt verheven.

29. Derhalve beveelt de EDPS aan om bij de tenuitvoerlegging van toekomstige instrumenten een meer specifieke en grondige beoordeling van de gevolgen voor de persoonlijke levenssfeer en de gegevensbeveiliging uit te voeren, ofwel in de vorm van een aparte beoordeling of als onderdeel van de algemene effectbeoordeling inzake de grondrechten door de Commissie. Deze effectbeoordeling mag zich niet beperken tot het vermelden van algemene beginselen of het analyseren van beleidsopties, zoals momenteel het geval is, maar moet ook specifieke en concrete waarborgen aanbevelen.

30. Er moeten bijgevolg specifieke indicatoren en kenmerken worden geformuleerd om ervoor te zorgen dat elk voorstel dat een gevolg heeft voor de bescherming van de persoonlijke levenssfeer en persoonsgegevens op het gebied van de EU-interneveiligheidsstrategie aan een diepgaande beschouwing wordt onderworpen, met inbegrip van aspecten als evenredigheid, noodzakelijkheid en het beginsel van doelbinding.

31. Daarnaast zou het in dit verband van nut kunnen zijn om te verwijzen naar artikel 4 van de aanbeveling inzake RFID-toepassingen ([15]) waarin de Commissie de lidstaten aanspoort ervoor te zorgen dat de industrie, samen met de relevante belanghebbenden uit het maatschappelijke middenveld, een kader ontwikkelt voor effectbeoordeling op

([12]) Mededeling van de Commissie aan het Europees Parlement, de Raad, het Europees Economisch en Sociaal Comité en het Comité van de Regio's over een integrale aanpak van de bescherming van persoonsgegevens in de Europese Unie, COM(2010) 609.

([13]) De EDPS beval in zijn advies over de Mededeling van de Commissie over het programma van Stockholm aan een wettelijke verplichting in te voeren voor ontwerpers en gebruikers van informatiesystemen om systemen te ontwikkelen en te gebruiken die in overeenstemming zijn met het beginsel van ingebouwde privacy („privacy by design").

([14]) SEC(2009) 92 van 15.1.2009.

([15]) C(2009) 3200 definitief van 12.5.2009.

het gebied van persoonlijke levenssfeer en beveiliging. In de resolutie van Madrid, die in november 2009 werd aangenomen door de International Conference of Privacy and Data Protection Commissioners, werd er eveneens toe opgeroepen PIA's uit te voeren voorafgaand aan de invoering van nieuwe informatiesystemen en -technologieën voor de verwerking van persoonsgegevens en voorafgaand aan substantiële wijzigingen in bestaande verwerkingsprocessen.

Rechten van de betrokkenen

32. De EDPS stelt vast dat de Mededeling niet specifiek ingaat op de belangrijke kwestie van de rechten van de betrokkenen, die een essentieel element van de gegevensbescherming vormen en die een weerslag zouden moeten hebben op het ontwerp van de EU-interneveiligheidsstrategie. Het is van cruciaal belang ervoor te zorgen dat bij alle systemen en instrumenten die betrekking hebben op de EU-interneveiligheidsstrategie, de eraan onderworpen personen steeds dezelfde rechten genieten wat betreft de manier waarop hun persoonsgegevens worden verwerkt.

33. Voor vele systemen die in de Mededeling worden genoemd, zijn specifieke regels vastgesteld inzake de rechten van de betrokkenen (gericht op categorieën als slachtoffers, vermoedelijke criminelen of migranten) maar de verschillen tussen de systemen en instrumenten zijn op dit punt groot en lijken ongegrond.

34. Derhalve verzoekt de EDPS de Commissie in de nabije toekomst meer aandacht te besteden aan de harmonisatie van de rechten van de betrokkenen in de EU in de context van de EU-interneveiligheids- en informatiebeheersstrategie.

35. Daarbij zou bijzondere aandacht moeten worden besteed aan de rechtsmiddelen. De EU-interneveiligheidsstrategie moet garanderen dat telkens wanneer de rechten van een individu niet volledig zijn geëerbiedigd, de voor de gegevensverwerking verantwoordelijken instaan voor klachtenprocedures die gemakkelijk toegankelijk, efficiënt en betaalbaar zijn.

Beste beschikbare technieken

36. De tenuitvoerlegging van de EU-interneveiligheidsstrategie zal onvermijdelijk gebaseerd zijn op het gebruik van een IT-infrastructuur die de in de Mededeling geplande acties ondersteunt. Men zou kunnen stellen dat de beste beschikbare technieken (BBT's) het juiste evenwicht mogelijk maken tussen het verwezenlijken van de doelstellingen van de EU-interneveiligheidsstrategie en de eerbiediging van de rechten van individuen. In dit verband wil de EDPS de aanbeveling herhalen die hij heeft gedaan in eerdere adviezen ([16]) met betrekking tot de noodzaak voor de Commissie om samen met de belanghebbenden van de sector concrete maatregelen voor de toepassing van BBT's te bepalen en te bevorderen. Een dergelijke toepassing stemt overeen met het meest efficiënte en verst gevorderde stadium in de ontwikkeling van activiteiten en hun werkmethodes, die aangeven in hoeverre specifieke technieken de beoogde resultaten op een efficiënte manier kunnen opleveren in overeenstemming met het EU-kader voor privacy en gegevensbescherming. Deze benadering strookt volledig met de eerder vermelde benadering van „ingebouwde privacy".

37. Waar relevant en doenbaar moeten referentiedocumenten over BBT's worden opgesteld om te dienen als richtsnoeren en een grotere rechtszekerheid te bieden voor de eigenlijke tenuitvoerlegging van de maatregelen in het kader van de EU-interneveiligheidsstrategie. Dit zou ook bevorderlijk kunnen zijn voor de harmonisering van deze maatregelen in de verschillende lidstaten. Ten slotte zal het definiëren van BBT's die de persoonlijke levenssfeer en de gegevensbeveiliging eerbiedigen de toezichthoudende rol van gegevensbeschermingsautoriteiten vergemakkelijken doordat ze beschikken over technische referenties die stroken met de persoonlijke levenssfeer en de gegevensbeveiliging en die zijn goedgekeurd door de voor de gegevensverwerking verantwoordelijken.

38. De EDPS wijst ook op het belang van een correcte afstemming van de EU-interneveiligheidsstrategie op de activiteiten die al worden uitgevoerd op grond van het zevende kaderprogramma voor onderzoek en technologische ontwikkeling en het kaderprogramma Veiligheid en bescherming van de vrijheden. Een gemeenschappelijke visie die erop gericht is BBT's ter beschikking te stellen, zal vernieuwing mogelijk maken van de kennis en capaciteiten die vereist zijn om de burgers te beschermen en tegelijkertijd de fundamentele rechten in acht te nemen.

39. Ten slotte wijst de EDPS op de rol die het Europees Agentschap voor netwerk- en informatiebeveiliging (ENISA) kan spelen in het opstellen van richtsnoeren en de beoordeling van de veiligheidscapaciteiten die vereist zijn om in te staan voor de integriteit en beschikbaarheid van de IT-systemen en ook de bevordering van deze BBT's. Daarom verheugt het de EDPS dat dit agentschap een belangrijke rol heeft toebedeeld gekregen in de verbetering van de capaciteiten om cyberaanvallen aan te pakken en cybermisdaad te bestrijden ([17]).

Verduidelijking van de actoren en hun rol

40. In dit verband is er meer duidelijkheid nodig over de actoren die deel uitmaken van of bijdragen aan de architectuur van de EU-interneveiligheidsstrategie. De Mededeling verwijst naar de verschillende actoren en belanghebbenden,

([16]) Advies van de EDPS over intelligente vervoersystemen van juli 2009 en advies van de EDPS over RF/ID-Mededeling van december 2007, zie ook het jaarverslag van de EDPS van 2006, blz. 48.

([17]) De EDPS is van plan nog in december 2010 een advies over de kaderregeling van ENISA aan te nemen.

zoals burgers, rechterlijke macht, EU-agentschappen, nationale autoriteiten, politie en bedrijven. De specifieke rollen en bevoegdheden van deze actoren moeten beter worden beschreven in de specifieke acties die worden voorgesteld voor de tenuitvoerlegging van de EU-interneveiligheidsstrategie.

IV. SPECIFIEKE OPMERKINGEN BETREFFENDE DE BELEIDSTERREINEN MET BETREKKING TOT DE EU-INTERNEVEILIGHEIDSSTRATEGIE

Geïntegreerd grensbeheer

41. In de Mededeling wordt erop gewezen dat nu het Verdrag van Lissabon van kracht is, de EU de synergie tussen grensbeheersmaatregelen voor personen en goederen beter kan benutten: „Wat betreft personenverkeer kan de EU migratiebeheer en criminaliteitsbestrijding opvatten als twee complementaire doelstellingen van de strategie voor geïntegreerd grensbeheer". In het document wordt grensbeheer beschouwd als een mogelijk krachtig instrument om ernstige en georganiseerde misdaad te ontwrichten ([18]).

42. De EDPS stelt ook vast dat de Mededeling drie strategische elementen aanvoert: 1) intensiever gebruik van nieuwe technologie voor grenscontroles (SIS II, VIS, inreis-/uitreissysteem en programma voor geregistreerde reizigers); 2) intensiever gebruik van nieuwe technologie voor grensbewaking (Europees grensbewakingssysteem EUROSUR) en 3) intensievere coördinatie van de lidstaten via FRONTEX.

43. De EDPS wenst dit advies te benutten om te herinneren aan zijn in een aantal vroegere adviezen geformuleerde verzoek om een duidelijk beleid inzake grensbeheer — met volledige inachtneming van de regels inzake gegevensbescherming — in te voeren op EU-niveau. De EDPS is van mening dat de huidige werkzaamheden inzake de EU-interneveiligheidsstrategie en het informatiebeheer zeer goede gelegenheden zijn om concrete stappen te zetten in de richting van een coherent beleid op deze gebieden.

44. De EDPS wijst erop dat de Mededeling niet alleen betrekking heeft op grootschalige systemen die al bestaan of in de nabije toekomst in gebruik zullen worden genomen (zoals SIS, SIS II en VIS), maar — in het verlengde hiervan — ook op systemen die in de toekomst zouden kunnen worden voorgesteld door de Commissie en waarover op dit moment nog geen beslissing is genomen (zoals het programma voor geregistreerde reizigers en het inreis-/uitreissysteem). In deze context moet herinnerd worden aan het feit dat de doelstellingen en de legitimiteit van de invoering van deze systemen nog moeten worden gespecificeerd en aangetoond, ook in het licht van de resultaten van specifieke effectbeoordelingen door de Commissie. Indien dit niet gebeurt, zou men kunnen stellen dat de Mededeling vooruitloopt op het besluitvormingsproces, en bijgevolg geen rekening houdt met het feit dat de definitieve beslissing over de invoering van het programma voor geregistreerde reizigers en het inreis-/uitreissysteem in de Europese Unie nog niet is genomen.

45. De EDPS stelt daarom voor in de toekomstige werkzaamheden betreffende de tenuitvoerlegging van de EU-interneveiligheidsstrategie dergelijke anticipaties te vermijden. Zoals eerder vermeld mag er slechts na een gepaste evaluatie van alle bestaande systemen met de nodige aandacht voor de beginselen van noodzakelijkheid en evenredigheid een beslissing worden genomen over de invoering van nieuwe grootschalige systemen die de persoonlijke levenssfeer kunnen aantasten.

EUROSUR

46. In de Mededeling wordt gesteld dat de Commissie een wetgevingsvoorstel zal indienen voor de oprichting van EUROSUR in 2011 ten behoeve van de interne veiligheid en de criminaliteitsbestrijding. Er wordt ook gezegd dat EUROSUR zal gebruikmaken van de nieuwe technologieën die worden ontwikkeld dankzij door de EU gefinancierde onderzoeksprojecten en -activiteiten, zoals satellietbeelden om doelen aan de zeegrens op te sporen en te volgen, bijv. snelle vaartuigen waarmee drugs de EU worden binnengebracht.

47. In deze context wijst de EDPS erop dat het nog niet duidelijk is of en in hoeverre het wetgevingsvoorstel inzake EUROSUR dat zal worden ingediend door de Commissie in 2011, ook betrekking zal hebben op de verwerking van persoonsgegevens in het kader van EUROSUR. De Commissie heeft hieromtrent geen duidelijk standpunt ingenomen in de Mededeling. Deze kwestie is van nog groter belang daar de Mededeling een duidelijk verband legt tussen EUROSUR en FRONTEX op tactisch, operationeel en strategisch niveau (zie onderstaande opmerking met betrekking tot FRONTEX) en vraagt om nauwe samenwerking tussen de twee.

De verwerking van persoonsgegevens door FRONTEX

48. De EDPS heeft een advies uitgebracht over de herziening van de FRONTEX-Verordening van 17 mei 2010 ([19]) waarin hij oproept tot een echt debat en grondige reflectie over de gegevensbeschermingskwestie in de context van de versterking van de bestaande taken van FRONTEX en de toekenning van nieuwe verantwoordelijkheden.

49. De Mededeling verwijst naar de noodzaak de bijdrage van FRONTEX aan de buitengrenzen te vergroten onder doelstelling 4 „Veiligheid verbeteren door grensbeheer". Hieromtrent wordt in de Mededeling aangevoerd dat gelet op eerdere ervaringen en op de algemene benadering van de

([18]) Persbericht over de EU-interneveiligheidsstrategie in actie — vijf stappen voor een veiliger Europa. Memo 10/598.

([19]) Advies van de EDPS van 17 mei 2010 over het voorstel voor een verordening van het Europees Parlement en de Raad tot wijziging van Verordening (EG) nr. 2007/2004 tot oprichting van een Europees Agentschap voor het beheer van de operationele samenwerking aan de buitengrenzen van de lidstaten van de Europese Unie (FRONTEX).

EU op het gebied van informatiebeheer, de Commissie van mening is dat een belangrijke bijdrage kan worden geleverd tot de ontmanteling van criminele organisaties door FRONTEX deze informatie, in beperkte mate en overeenkomstig duidelijke regels inzake het beheer van persoonsgegevens, te laten verwerken en gebruiken. Dit is een nieuwe benadering in vergelijking met het voorstel van de Commissie over de herziening van de FRONTEX-Verordening, die momenteel besproken wordt in het Europees Parlement en de Raad, waarin niets werd gezegd over de verwerking van persoonsgegevens.

50. Tegen deze achtergrond is de EDPS verheugd over het feit dat de Mededeling een indicatie bevat omtrent de omstandigheden waarin een dergelijke verwerking noodzakelijk kan blijken (bijv. risicoanalyse, betere prestaties bij gezamenlijke operaties of informatie-uitwisseling met Europol). In de Mededeling wordt uitgelegd dat de informatie over criminelen die betrokken zijn bij smokkelnetwerken — die FRONTEX ontdekt — niet verder kan worden gebruikt voor risicoanalyses of om toekomstige gezamenlijke operaties beter te richten. Bovendien komen relevante gegevens voor verder onderzoek over verdachte criminelen niet aan bij de bevoegde nationale autoriteiten of Europol.

51. Toch stelt de EDPS vast dat de Mededeling niet verwijst naar het lopende debat over de herziening van het FRONTEX-wetgevingskader, waarin, zoals eerder vermeld, deze kwestie behandeld wordt om tot wetgevende oplossingen te komen. Bovendien kan de formulering in de Mededeling waarin de rol van FRONTEX in het kader van de ontmanteling van criminele organisaties wordt benadrukt, worden opgevat als een uitbreiding van de bevoegdheid van FRONTEX. De EDPS stelt voor dat er met dit punt rekening wordt gehouden in zowel de herziening van de FRONTEX-Verordening als de tenuitvoerlegging van de EU-interneveiligheidsstrategie.

52. De EDPS vestigt ook de aandacht op de noodzaak ervoor te zorgen dat er geen dubbel werk wordt verricht door Europol en FRONTEX. In dat verband verheugt het de EDPS dat de Mededeling vermeldt dat overlapping van taken tussen FRONTEX en Europol moet worden voorkomen. Deze kwestie moet echter duidelijker worden behandeld in zowel de herziene FRONTEX-Verordening als de acties voor de tenuitvoerlegging van de EU-interneveiligheidsstrategie die voorzien in een nauwe samenwerking tussen FRONTEX en EUROPOL. Dit is van bijzonder belang gelet op de beginselen van doelbeperking en gegevenskwaliteit. Deze opmerking geldt ook voor de toekomstige samenwerking met agentschappen als het Europees Agentschap voor netwerk- en informatiebeveiliging (ENISA) of het Europees Ondersteuningsbureau voor asielzaken.

Gebruik van biometrische gegevens

53. In de Mededeling wordt niet nader ingegaan op het actuele fenomeen van het toenemende gebruik van biometrische gegevens op het gebied van vrijheid, veiligheid en rechtvaardigheid, met name in grootschalige IT-systemen van de EU en andere instrumenten voor grensbeheer.

54. De EDPS neemt deze gelegenheid derhalve te baat om te herinneren aan zijn voorstel ([20]) om deze uit het oogpunt van de gegevensbescherming uiterst gevoelige aangelegenheid, ernstig in aanmerking te nemen bij de tenuitvoerlegging van de EU-interneveiligheidsstrategie, met name in de context van het grensbeheer.

55. De EDPS beveelt ook aan om inzake het gebruik van biometrische gegevens op het gebied van vrijheid, veiligheid en recht een duidelijk en strikt beleid te ontwikkelen dat is gebaseerd op een grondige evaluatie en beoordeling per geval van de noodzaak om dergelijke gegevens te gebruiken in de context van de EU-interneveiligheidsstrategie, en dat de fundamentele beginselen van gegevensbescherming zoals evenredigheid, noodzakelijkheid en doelbinding volledig in acht neemt.

TFTP

56. In de Mededeling wordt aangekondigd dat de Commissie in 2011 een EU-beleid wil ontwikkelen voor het opvragen en analyseren van gegevens betreffende het financiële berichtenverkeer op het eigen grondgebied. In deze context verwijst de EDPS naar zijn advies van 22 juni 2010 inzake de verwerking en doorgifte van gegevens betreffende het betalingsberichtenverkeer van de EU naar de VS ten behoeve van het Programma voor het traceren van financiering van terrorisme (TFTP II) ([21]). Alle kritische opmerkingen in dat advies zijn hier evenzeer van toepassing en gelden ook voor de geplande werkzaamheden voor de EU-kaderregeling inzake gegevens betreffende het betalingsberichtenverkeer. Daarom moeten ze ook in aanmerking worden genomen bij de bespreking van deze aangelegenheid. Er moet bijzondere aandacht worden besteed aan de evenredigheid van het opvragen en verwerken van grote hoeveelheden van gegevens van mensen die geen verdachten zijn, en aan de kwestie van een doeltreffend toezicht door onafhankelijke autoriteiten en door de rechterlijke macht.

Internetveiligheid voor burgers en bedrijfsleven

57. De EDPS is verheugd over het belang dat in de Mededeling gehecht wordt aan preventieve acties op EU-niveau en is van mening dat het versterken van de veiligheid van IT-netwerken een essentiële voorwaarde is voor een goed functionerende informatiemaatschappij. De EDPS is ook voorstander van de specifieke acties om de capaciteiten om cyberaanvallen te bestrijden op te voeren, de capaciteit van de rechtshandhavingsautoriteiten en de rechterlijke macht op te bouwen en samen te werken met de sector om bedrijven en burgers meer macht te geven. Ook de rol van ENISA als facilitator van talrijke acties in het kader van deze doelstelling is verheugend.

([20]) Zie met name het advies van de EDPS over de Mededeling getiteld, „Overzicht van het informatiebeheer op het gebied van vrijheid, veiligheid en recht", waarnaar wordt verwezen in voetnoot 8.

([21]) Advies van 22 juni 2010 van de EDPS over het voorstel voor een besluit van de Raad inzake de sluiting van de Overeenkomst tussen de Europese Unie en de Verenigde Staten van Amerika inzake de verwerking en doorgifte van gegevens betreffende het betalingsberichtenverkeer van de Europese Unie naar de Verenigde Staten ten behoeve van het Programma voor het traceren van financiering van terrorisme (TFTP II).

58. In de *EU-interneveiligheidsstrategie in actie* wordt echter niet verder ingegaan op de in cyberspace geplande rechtshandhavingsacties en hoe deze activiteiten een gevaar zouden kunnen vormen voor individuele rechten en welke maatregelen er nodig zijn als bescherming hiertegen. De EDPS verzoekt om een meer ambitieuze benadering inzake gepaste waarborgen. Deze benadering moet de fundamentele rechten beschermen van alle individuen, ook van degenen die getroffen kunnen worden door acties die zijn ontworpen om eventuele criminele activiteiten op dit gebied tegen te gaan.

V. **CONCLUSIE EN AANBEVELINGEN**

59. De EDPS vraagt om verbanden te leggen tussen de verschillende EU-strategieën en mededelingen die ontstaan in het proces van de tenuitvoerlegging van de EU-interneveiligheidsstrategie. Deze benadering moet worden gevolgd door een concreet actieplan op basis van een echte behoefteanalyse die moet resulteren in een alomvattend, geïntegreerd en goed gestructureerd EU-beleid inzake EU-interneveiligheidsstrategie.

60. De EDPS neemt deze gelegenheid ook te baat om het belang te benadrukken van de wettelijke verplichting om alle bestaande instrumenten die zullen worden gebruikt in het kader van de EU-interneveiligheidsstrategie en gegevensuitwisseling te evalueren alvorens nieuwe voor te stellen. In dat opzicht wordt de goedkeuring van bepalingen die regelmatige beoordelingen van de efficiëntie van de instrumenten vereisen, warm aanbevolen.

61. De EDPS stelt voor om bij de opstelling van het strategisch meerjarenplan, waarom wordt verzocht in de conclusies van de Raad van november 2010, rekening te houden met de lopende werkzaamheden ten behoeve van het alomvattende kader voor gegevensbescherming op basis van artikel 16 VWEU, met name Mededeling (2009) 609.

62. De EDPS doet een aantal voorstellen inzake noties en concepten die van belang zijn in de optiek van gegevensbescherming en waarmee rekening moet worden gehouden op het gebied van EU-interneveiligheidsstrategie, zoals ingebouwde privacy ("privacy by design"), beoordeling van het effect op de persoonlijke levenssfeer en de gegevensbeveiliging, beste beschikbare technieken.

63. De EDPS beveelt aan om bij de tenuitvoerlegging van toekomstige instrumenten een beoordeling van het effect op de persoonlijke levenssfeer en de gegevensbeveiliging uit te voeren, ofwel in de vorm van een aparte beoordeling ofwel als onderdeel van de algemene effectbeoordeling inzake de grondrechten door de Commissie.

64. Tevens verzoekt hij de Commissie een coherenter en consequenter beleid te ontwikkelen betreffende de voorwaarden voor het gebruik van biometrische gegevens op het gebied van de EU-interneveiligheidsstrategie, en op EU-niveau voor een grotere harmonisatie van de rechten van de betrokkenen te zorgen.

65. De EDPS maakt ten slotte nog enkele opmerkingen inzake de verwerking van persoonsgegevens in de context van grensbeheer en met name door FRONTEX en eventueel in de context van EUROSUR.

Gedaan te Brussel, 17 december 2010.

Peter HUSTINX

Europese Toezichthouder voor gegevensbescherming