Advies van de Europese Toezichthouder voor gegevensbescherming over het voorstel voor een verordening van het Europees Parlement en de Raad inzake het Europees Agentschap voor netwerk- en informatiebeveiliging (ENISA)

(2011/C 101/04)

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 in overeenstemming met artikel 28, lid 2, van Verordening (EG) nr. 45/2001 van het Europees Parlement en de Raad 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]),

BRENGT HET VOLGENDE ADVIES UIT:

I. INLEIDING

Beschrijving van het voorstel

1. De Commissie heeft op 30 september 2010 een voorstel aangenomen voor een verordening van het Europees Parlement en de Raad inzake ENISA, het Europees Agentschap voor netwerk- en informatiebeveiliging ([3]).

2. ENISA werd in maart 2004 bij Verordening (EG) nr. 460/2004 ([4]) voor een eerste periode van vijf jaar opgericht. In 2008 werd het mandaat bij Verordening (EG) nr. 1007/2008 ([5]) verlengd tot maart 2012.

3. Zoals voortvloeit uit artikel 1, lid 1, van Verordening (EG) nr. 460/2004 werd het Agentschap opgericht om te zorgen voor een hoog en doeltreffend niveau van netwerk- en informatiebeveiliging binnen de EU alsook om bij te dragen aan de goede werking van de interne markt.

4. Met het Commissievoorstel wordt beoogd het Agentschap te moderniseren, de bevoegdheden ervan te versterken, alsmede een nieuw mandaat te verstrekken van vijf jaar, opdat het Agentschap ook na maart 2012 haar werk kan voortzetten ([6]).

5. De rechtsgrond voor de voorgestelde verordening ligt in artikel 114 van het VWEU ([7]) dat de Unie de bevoegdheid verleent om maatregelen te treffen teneinde de goede werking van de interne markt tot stand te brengen of te waarborgen. Artikel 114 van het VWEU is de opvolger van artikel 95 van het voormalige EG-Verdrag waarop de voorgaande verordeningen ten aanzien van ENISA gegrondvest waren ([8]).

6. De memorie van toelichting bij het voorstel verwijst naar het feit dat met de inwerkingtreding van het Verdrag van Lissabon de preventie en bestrijding van de misdaad een gedeelde bevoegdheid is geworden. Dit biedt ENISA de gelegenheid zich op te werpen als platform voor de netwerk- en informatiebeveiligingsaspecten van de bestrijding van cybermisdaad, alsook om ideeën en goede praktijken uit te wisselen met overheidsinstellingen op het vlak van cyberverdediging, wetshandhaving en gegevensbeschermingsautoriteiten.

7. De Commissie heeft gekozen uit verschillende opties en stelt nu voor om het takenpakket van ENISA uit te breiden en om wetshandhavings- en gegevensbeschermingsautoriteiten aan de permanente groep van belanghebbenden toe te voegen als volwaardige leden. De nieuwe taakomschrijving omvat geen operationele taken, maar actualiseert en herformuleert de huidige taken.

Raadpleging EDPS

8. Het voorstel werd in overeenstemming met artikel 28, lid 2, van Verordening (EG) nr. 45/2001 op 1 oktober 2010 ter raadpleging naar de EDPS verstuurd. De EDPS is verheugd over deze kwestie te worden geraadpleegd en adviseert om in de overwegingen van het voorstel een verwijzing naar deze raadpleging op te nemen, zoals te doen gebruikelijk in wetsteksten waarover de EDPS in overeenstemming met Verordening (EG) nr. 45/2001 is geraadpleegd.

9. Voorafgaand aan de goedkeuring van het voorstel is de EDPS al informeel geraadpleegd, waarna deze een aantal informele op- en aanmerkingen bij het geheel heeft geplaatst. Deze zijn echter geen van alle meegenomen in de definitieve versie van het voorstel.

Algemene beoordeling

10. De EDPS benadrukt dat de beveiliging van gegevensverwerking een cruciaal onderdeel uitmaakt van gegevensbescherming ([9]). Om die reden is de EDPS ingenomen met het doel

([1]) PB L 281 van 23.11.1995, blz. 31.
([2]) PB L 8 van 12.1.2001, blz. 1.
([3]) COM(2010) 521 def.
([4]) PB L 77 van 13.3.2004, blz. 1.
([5]) PB L 293 van 31.10.2008, blz. 1.
([6]) Teneinde te voorkomen dat er een juridisch vacuüm ontstaat, indien de wetgevingsprocedure in het Europees Parlement en de Raad pas wordt afgerond na verstrijking van het huidige mandaat, heeft de Commissie op 30 september 2010 een tweede voorstel tot wijziging van Verordening (EG) nr. 460/2004 goedgekeurd met als enige doel het huidige mandaat met 18 maanden te verlengen. Zie COM(2010) 520 definitief.
([7]) Zie hierboven.
([8]) Het Hof van Justitie heeft op 2 mei 2006 een beroep tot nietigverklaring van de voorgaande Verordening (EG) nr. 460/2004 verworpen waarin de rechtsgrondslag van de verordening werd aangevochten (Zaak C-217/04).
([9]) In de artikelen 22 en 35 van Verordening (EG) nr. 45/2001, artikelen 16 en 17 van Richtlijn 95/46/EG en artikelen 4 en 5 van Richtlijn 2002/58/EG zijn al eisen ten aanzien van beveiliging opgenomen.

van het voorstel, namelijk uitbreiding van de bevoegdheden van het Agentschap, opdat het zijn huidige taken en verantwoordelijkheden doeltreffender invulling kan geven en tegelijkertijd zijn werkgebied kan uitbreiden. De EDPS is bovendien ingenomen met de toelating van wetshandhavings- en gegevensbeschermingsautoriteiten als volwaardige belanghebbenden en is van mening dat de uitbreiding van het mandaat van ENISA een manier is een professioneel en gestroomlijnd beheer van veiligheidsmaatregelen voor informatiesystemen op Europees niveau te bevorderen.

11. De algehele beoordeling van het voorstel is dan ook positief. Dat neemt niet weg dat de voorgestelde Verordening op een aantal punten onduidelijkheden laat bestaan of onvolledig is, wat vanuit gegevensbeschermingsperspectief aanleiding geeft tot zorg. In het volgende hoofdstuk wordt nader op deze kwesties ingegaan.

II. **OPMERKINGEN EN AANBEVELINGEN**

De nieuwe taken van ENISA zijn onvoldoende duidelijk

12. De nieuwe taken van het Agentschap ten aanzien van de betrokkenheid van wetshandhavingsautoriteiten zoals weergegeven in artikel 3 van het voorstel zijn in zeer algemene bewoordingen geformuleerd. De memorie van toelichting daarentegen is iets duidelijker. Daarin wordt ENISA neergezet als een agentschap dat samenwerkt met wetshandhavingsautoriteiten op het vlak van de cybermisdaad en geen operationele taken heeft ten aanzien van de bestrijding van die cybermisdaad. In artikel 3 worden deze taken echter niet of slechts in zeer algemene bewoordingen weergegeven.

13. Teneinde elke rechtsonzekerheid tegen te gaan, dient de voorgestelde verordening de taken van ENISA duidelijk en ondubbelzinnig te omschrijven. Zoals reeds gezegd, vormt de veiligheid van gegevensverwerking een cruciaal element van gegevensbescherming. ENISA zal een steeds belangrijkere rol spelen op dit vlak. Het dient de burgers, instellingen en organen duidelijk te zijn bij wat voor activiteiten ENISA betrokken kan zijn. Dit wordt des te belangrijker indien het nieuwe takenpakket tevens de verwerking van persoonsgegevens zal omvatten (zie de punten 17 t/m 20 hieronder).

14. In artikel 3, lid 1, onder k), van het voorstel staat dat het Agentschap gehouden is elke andere via een ander wetgevingsbesluit aan het Agentschap opgedragen taak uit te voeren. De EDPS stelt vraagtekens bij dit open einde, aangezien hiermee eventuele mazen worden gecreëerd, met alle mogelijke negatieve gevolgen voor de coherentie van het rechtsinstrument en alle risico's op functieverschuiving van het Agentschap van dien.

15. Een van de in artikel 3, lid 1, onder k), van het voorstel genoemde taken, maakt onderdeel uit van Richtlijn 2002/58/EG [1]. Daarin staat dat de Commissie gehouden is het Agentschap te raadplegen ten aanzien van technische uitvoeringsmaatregelen voortvloeiend uit kennisgevingen naar aanleiding van het uitlekken van vertrouwelijke gegevens. De EDPS adviseert deze activiteit van het Agentschap gedetailleerder te beschrijven en daarbij een beperking aan te brengen tot het beveiligingsdeel van het geheel. Gezien de potentiële impact van ENISA op de beleidsontwikkeling op dit gebied, dient er in de voorgestelde verordening voor deze activiteit een duidelijkere en prominentere positie te worden ingeruimd.

16. Bovendien adviseert de EDPS om gezien de specifieke taak van ENISA ten aanzien van de ondersteuning van de lidstaten en de Europese instellingen en organen bij hun inspanningen om gegevens te verzamelen, analyseren en verspreiden ten aanzien van netwerk- en informatiebeveiliging, zoals omschreven in artikel 3, lid 1, onder c), van onderhavig voorstel, een verwijzing naar Richtlijn 1999/5/EG [2] op te nemen in overweging 21. Dit dient de netwerk- en informatiebeveiligingsacties van ENISA ten aanzien van goede praktijken en technieken te bevorderen. Bovendien geeft het de mogelijkheden voor constructieve interacties tussen het Agentschap en de normalisatie-instellingen beter weer.

Er dient te worden aangegeven of het Agentschap al dan niet persoonsgegevens te verwerken krijgt

17. In het voorstel wordt niet aangegeven of het takenpakket van het Agentschap tevens de verwerking van persoonsgegevens omvat. Dat betekent dat er in het voorstel geen specifieke rechtsgrond in de betekenis van artikel 5 van Verordening (EG) nr. 45/2001 voor de verwerking van persoonsgegevens is opgenomen.

18. Een aantal taken van het Agentschap kan (althans tot op zekere hoogte) de verwerking van persoonsgegevens met zich meebrengen. Zo is het bijvoorbeeld niet uitgesloten dat er bij de analyse van beveiligingsincidenten en incidenten waarbij vertrouwelijke gegevens zijn uitgelekt, alsook bij de uitvoering van non-operationele functies in het kader van de bestrijding van cybermisdaad, tevens persoonsgegevens vergaard en geanalyseerd moeten worden.

19. In overweging 9 van het voorstel wordt verwezen naar de bepalingen van Richtlijn 2002/21/EG [3] waarin wordt bepaald dat waar aangewezen het Agentschap ingeval van het uitlekken van vertrouwelijke gegevens een melding krijgt van de nationale regelgevende instantie. De EDPS adviseert dan ook om gedetailleerder in het voorstel aan te geven wat voor een soort meldingen er naar ENISA toegestuurd zouden moeten worden en op welke wijze ENISA daarop zou moeten reageren. Bovendien dient in het voorstel aandacht te worden besteed aan de gevolgen van de verwerking van de analyse van eventuele dergelijke meldingen op het vlak van de verwerking van persoonsgegevens.

---

[1] Richtlijn 2002/58/EG van het Europees Parlement en de Raad van 12 juli 2002 betreffende de verwerking van persoonsgegevens en de bescherming van de persoonlijke levenssfeer in de sector elektronische communicatie (Richtlijn betreffende privacy en elektronische communicatie) PB L 201 van 31.7.2002, blz. 37.

[2] Richtlijn 1999/5/EG van het Europees Parlement en de Raad van 9 maart 1999 betreffende radioapparatuur en telecommunicatie-eindapparatuur en de wederzijdse erkenning van hun conformiteit, PB L 91 van 7.4.1999, blz. 10 en in het bijzonder artikel 3, lid 3, onder c) van deze richtlijn.

[3] Richtlijn 2002/21/EG van het Europees Parlement en de Raad van 7 maart 2002 inzake een gemeenschappelijk regelgevingskader voor elektronische-communicatienetwerken en -diensten (Kaderrichtlijn, PB L 108 van 24.4.2002, blz. 33).

20. De EDPS roept de wetgever dan ook op om opheldering te verschaffen over de vraag of, en zo ja, bij welke van de in artikel 3 opgesomde activiteiten van ENISA persoonsgegevens zullen worden verwerkt.

De interne beveiligingsregels van ENISA vragen om nadere uitwerking

21. Hoewel ENISA een belangrijke rol speelt in het debat over netwerk- en informatiebeveiliging in Europa, wordt er in het voorstel met nagenoeg geen woord gerept over mogelijke beveiligingsmaatregelen voor het Agentschap zelf (al dan niet verband houdend met de verwerking van persoonsgegevens).

22. De EDPS is van mening dat het Agentschap nog beter in staat zal zijn goede praktijken ten aanzien van de beveiliging van de verwerking van gegevens te verbreiden indien dergelijke beveiligingsmaatregelen uitgebreid toepassing vinden binnen ENISA zelf. Mede hierdoor zal het Agentschap niet alleen worden erkend als kenniscentrum, maar tevens als een referentie ten aanzien van de concrete toepassing van beste beschikbare technieken (BBT) op beveiligingsgebied. Het streven naar uitmuntendheid op het vlak van beveiligingsmaatregelen dient dan ook verankerd te worden in de Verordening tot vaststelling van de werkprocedures van het Agentschap. De EDPS stelt dan ook voor het voorstel uit te breiden met een bepaling in die richting, bijvoorbeeld door van het Agentschap te verlangen gebruik te maken van de beste beschikbare technieken, oftewel de meest doeltreffende en geavanceerde beveiligingsprocedures en bijbehorende werkmethoden.

23. Op deze manier kan het Agentschap advies verlenen ten aanzien van de praktische geschiktheid van specifieke technieken voor de beoogde beveiligingswaarborgen. Bovendien dient bij de tenuitvoerlegging van deze BBT's voorrang te worden gegeven aan die technieken waarmee aan de ene kant het beoogde beveiligingsniveau gewaarborgd is en anderzijds de mogelijke impact op de privacy wordt geminimaliseerd. Dat betekent dat er gekozen dient te worden voor technieken die zoveel mogelijk overeenstemmen met het „privacy by design"-concept.

24. De EDPS adviseert om zelfs wanneer de ambities iets lager worden gesteld, op zijn minst de volgende vereisten op te nemen in de Verordening: i) ontwikkeling van een intern beveiligingsbeleid na een uitgebreide risicobeoordeling, met inachtneming van de internationale normen en beste praktijken in de lidstaten, ii) de benoeming van een beveiligingsfunctionaris belast met de tenuitvoerlegging van het beleid met daarvoor toereikende middelen en bevoegdheden, iii) de goedkeuring van het beleid na nauwkeurige beoordeling van het residuele risico en de door de raad van bestuur voorgestelde maatregelen, en iv) een periodieke evaluatie van het beleid waarbij duidelijk wordt aangegeven hoe vaak deze dient plaats te vinden en wat de precieze doelstellingen ervan zijn.

De samenwerkingskanalen met gegevensbeschermingsautoriteiten (waaronder de EDPS) en de Groep gegevensbescherming artikel 29 dienen beter te worden gedefinieerd

25. Zoals reeds aangegeven, is de EDPS ingenomen met de uitbreiding van het mandaat van het Agentschap en is hij ervan overtuigd dat gegevensbeschermingsautoriteiten veel baat zullen hebben bij het bestaan van het Agentschap (en het Agentschap op zijn beurt bij de expertise van deze autoriteiten). Gezien de natuurlijke en logische samenhang tussen gegevensbeveiliging en gegevensbescherming worden het Agentschap en de gegevensbeschermingsautoriteiten dan ook opgeroepen nauw samen te werken.

26. In overwegingen 24 en 25 staat een verwijzing naar het voorstel voor een EU-richtlijn inzake cybermisdaad en wordt aangegeven dat het Agentschap in contact dient te treden met wetshandhavingsautoriteiten en ook gegevensbeschermingsautoriteiten als het gaat om de informatiebeveiligingsaspecten van de bestrijding van cybermisdaad [1].

27. Het voorstel dient tevens te voorzien in concrete kanalen en samenwerkingsmechanismen waarmee i) de *consistentie* van de activiteiten van het Agentschap met die van de gegevensbeschermingsautoriteiten gewaarborgd is en ii) *nauwe samenwerking* tussen het Agentschap en de gegevensbeschermingsautoriteiten mogelijk wordt.

28. Wat de *consistentie* betreft, wordt in overweging 27 expliciet verwezen naar het feit dat de taken van het Agentschap nooit en te nimmer in conflict mogen komen met de gegevensbeschermingsautoriteiten van de lidstaten. De EDPS is ingenomen met deze verwijzing, maar tekent aan dat er geen enkele verwijzing is naar de EDPS en de Groep gegevensbescherming artikel 29. De EDPS adviseert de wetgever om voor deze twee entiteiten een soortgelijke noninterferentiebepaling in het voorstel op te nemen, aangezien het speelveld van alle partijen er veel duidelijker door zou worden. Het dient dan ook het kader voor de samenwerkingskanalen en -mechanismen te vormen waarmee het Agentschap de uiteenlopende gegevensbeschermingsautoriteiten en de Groep gegevensbescherming artikel 29 kan ondersteunen.

29. Dienovereenkomstig is de EDPS voor wat *nauwe samenwerking* betreft, ingenomen met de opname van vertegenwoordigers van gegevensbeschermingsautoriteiten in de permanente groep van belanghebbenden dat het Agentschap zal bijstaan met advies ten aanzien van de tenuitvoerlegging van zijn activiteiten. De EDPS adviseert een expliciete bepaling op te nemen die stelt dat de benoeming van een dergelijke vertegenwoordiging van nationale gegevensbeschermingsautoriteiten door het Agentschap dient te geschieden op basis een voorstel van de Groep gegevensbescherming artikel 29. Tevens zou het op prijs worden gesteld indien er een verwijzing werd opgenomen uit hoofde waarvan EDPS aanwezig kan zijn bij bijeenkomsten waarin wordt beoogd kwesties te bespreken die relevant zijn voor de samenwerking met de EDPS. Bovendien adviseert de EDPS het Agentschap om (bijgestaan met advies door de permanente groep van belanghebbenden en na goedkeuring door de raad van bestuur) ad-hocwerkgroepen op te richten voor de onderwerpen waar een overlap bestaat tussen gegevensbescherming en gegevensbeveiliging, teneinde de beoogde nauwe samenwerking vorm te geven.

[1] Voorstel voor een Richtlijn van het Europees Parlement en de Raad over aanvallen op informatiesystemen en tot intrekking van Kaderbesluit 2005/222/JBZ van de Raad, COM(2010) 517 definitief.

30. Tot slot, teneinde elk mogelijk misverstand te vermijden, adviseert de EDPS om in plaats van de term „privacybeschermingsautoriteiten" de term „gegevensbeschermingsautoriteiten" te gebruiken en te verduidelijken wie deze autoriteiten zijn door een verwijzing op te nemen naar zowel artikel 28 van Richtlijn 95/46/EG als de EDPS, zoals bepaald in Hoofdstuk V van Verordening (EG) nr. 45/2001.

Het is onduidelijk welke partijen er bij ENISA voor hulp en ondersteuning terecht kunnen

31. De EDPS maakt melding van een inconsistentie in de voorgestelde Verordening met betrekking tot welke partijen ENISA om bijstand kunnen vragen. Uit overwegingen 7, 15, 16, 18 en 36 van het voorstel vloeit voort dat ENISA bevoegd is autoriteiten in de lidstaten en de Europese Unie als geheel assistentie te verlenen. In artikel 2, lid 1, daarentegen wordt uitsluitend naar de Commissie en de lidstaten verwezen, terwijl in artikel 14 de mogelijkheid om bijstand te vragen beperkt wordt tot i) het Europees Parlement, ii) de Raad, iii) de Commissie en iv) alle door een lidstaat aangewezen bevoegde organen, waardoor een aantal instellingen, organen, agentschappen en kantoren van de EU dus niet over dat recht zouden beschikken.

32. Artikel 3 van het voorstel is iets duidelijker en noemt verschillende soorten bijstand afhankelijk van het soort ontvangende partij: i) vergaring en analyse van informatiebeveiligingsgegevens (met betrekking tot de lidstaten en de Europese instellingen en organen), ii) analyse van de stand van zaken ten aanzien van de netwerk- en informatiebeveiliging in Europa (met betrekking tot de lidstaten en de Europese instellingen), iii) bevordering van het gebruik van risicomanagement en goede praktijken ten aanzien van beveiliging (in de gehele Europese Unie en de lidstaten), iv) de ontwikkeling van netwerk- en informatiebeveiligingsdetectie (binnen de Europese instellingen en organen) en v) deelname aan de dialoog en samenwerking met derde landen (als het gaat om de Europese Unie).

33. De EDPS roept de wetgever op deze inconsistentie uit de weg te ruimen en voornoemde bepalingen met elkaar in overeenstemming te brengen. Met betrekking daartoe adviseert de EDPS om artikel 14 dusdanig te wijzigen dat het op alle instellingen, organen, kantoren en agentschappen van de Europese Unie slaat en dat duidelijk is welk soort bijstand de verschillende entiteiten binnen de EU kunnen aanvragen (ingeval de wetgever een dergelijke differentiatie daadwerkelijk beoogt). Op soortgelijke wijze wordt geadviseerd eveneens publieke en private entiteiten de mogelijkheid te bieden zich door het Agentschap te laten assisteren indien een verzoek vanuit Europees perspectief een duidelijk potentieel bevat en het in overeenstemming is met de doelstellingen van het Agentschap.

Functies van de raad van bestuur

34. In de memorie van toelichting wordt voorzien in verdergaande bevoegdheden van de raad van bestuur als het gaat om haar toezichthoudende rol. De EDPS is ingenomen met deze taakverzwaring en adviseert een aantal aspecten met betrekking tot gegevensbescherming op te nemen in het functiepakket van de raad van bestuur. Bovendien adviseert de EDPS om in de Verordening ondubbelzinnig op te nemen wie bevoegd is: i) maatregelen vast te stellen voor de toepassing van Verordening (EG) nr. 45/2001 door het Agentschap, met inbegrip van de maatregelen met betrekking tot de benoeming van een functionaris voor gegevensbescherming, ii) het beveiligingsbeleid en de daaropvolgende periodieke herzieningen goed te keuren, en iii) het samenwerkingsprotocol met gegevensbeschermingsautoriteiten en wethandhavingsautoriteiten vast te stellen.

Toepasselijkheid van Verordening (EG) nr. 45/2001

35. Hoewel dit reeds krachtens Verordening (EG) nr. 45/2001 vereist is, stelt de EDPS voor om in artikel 27 een verwijzing op te nemen naar de benoeming van de functionaris voor gegevensbescherming, gezien het feit dat dit een buitengewoon belangrijk onderwerp is dat direct gepaard dient te gaan met de instelling van de uitvoeringsbepalingen ten aanzien van de reikwijdte van de aan de functionaris voor gegevensbescherming in overeenstemming met artikel 24, lid 8, van Verordening (EG) nr. 45/2001 toe te kennen bevoegdheden en op te dragen taken. Concreet zou artikel 27 er als volgt kunnen uitzien:

1. De door het Agentschap in overeenstemming met deze Verordening verwerkte informatie is onderhevig aan 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;

2. De raad van bestuur treft maatregelen voor de toepassing van Verordening (EG) nr. 45/2001 door het Agentschap, met inbegrip van maatregelen met betrekking tot de functionaris voor gegevensbescherming van het Agentschap.

36. Indien er een specifieke rechtsgrond nodig is voor de verwerking van persoonsgegevens, zoals besproken in de punten 17 t/m 20 hierboven, dient daarin te worden gespecificeerd welke waarborgen, beperkingen en voorwaarden er voor een dergelijke gegevensverwerking gelden moeten.

III. **CONCLUSIES**

37. De algehele beoordeling van het voorstel is positief en de EDPS is ingenomen met de verlenging van het mandaat van het Agentschap alsook de uitbreiding van de taken ervan door opname van gegevensbeschermingsautoriteiten en wethandhavingsautoriteiten als volwaardige belanghebbenden. De EDPS is van mening dat met de continuïteit van het Agentschap een professioneel en gestroomlijnd beheer van beveiligingsmaatregelen voor informatiesystemen op Europees niveau zal worden bevorderd.

38. De EDPS adviseert, teneinde alle rechtsonzekerheid te vermijden, het voorstel verder uit te werken ten aanzien van de uitbreiding van het takenpakket van het Agentschap, en dan met name ten aanzien van de taken met betrekking tot de betrokkenheid van wethandhavings- en gegevensbeschermingsautoriteiten. Verder wijst de EDPS op de eventuele mazen als gevolg van een van de bepalingen van het voorstel waarmee het Agentschap zonder enige nadere beperking middels andere wetgevingsbesluiten verdere taken toebedeeld kan krijgen.

39. De EDPS verzoekt de wetgever te verduidelijken of, en zo ja bij welke activiteiten er tevens persoonsgegevens verwerkt worden.

40. De EDPS adviseert bepalingen op te nemen met betrekking tot de totstandbrenging van een beveiligingsbeleid voor het Agentschap zelf, ter versterking van de rol van het Agentschap als drijvende kracht achter excellentie op het vlak van beveiliging, alsook als pleitbezorger van „privacy by design" door het gebruik van de best beschikbare beveiligingstechnieken die de rechten op het vlak van de bescherming van persoonsgegevens moeten waarborgen.

41. De samenwerkingskanalen met gegevensbeschermingsautoriteiten, waaronder de EDPS en de Groep gegevensbescherming artikel 29, dienen beter te worden gedefinieerd teneinde te zorgen voor consistentie en nauwe samenwerking.

42. De EDPS roept de wetgever op een aantal inconsistenties met betrekking tot de in artikel 14 genoemde beperkingen ten aanzien van de mogelijkheden het Agentschap om bijstand te vragen, op te lossen. De EDPS adviseert in concreto deze beperkingen te schrappen en alle instellingen, organen, agentschappen en kantoren van de Europese Unie de mogelijkheid te bieden het Agentschap om bijstand te vragen.

43. Tot slot adviseert de EDPS om de bevoegdheden van de raad van bestuur tevens uit te breiden met een aantal concrete elementen waarmee beter gegarandeerd kan worden dat goede praktijken ten aanzien van gegevensbeveiliging en gegevensbescherming binnen het Agentschap daadwerkelijk gevolgd worden. De EDPS stelt onder meer voor een verwijzing op te nemen naar de benoeming van een functionaris voor gegevensbescherming en de goedkeuring van de maatregelen ten behoeve van de correcte tenuitvoerlegging van Verordening (EG) nr. 45/2001.

Gedaan te Brussel, 20 december 2010.

Giovanni BUTTARELLI

Europese adjunct-toezichthouder voor gegevensbescherming