# Udtalelse fra Den Europæiske Tilsynsførende for Databeskyttelse om forslaget til Europa-Parlamentets og Rådets forordning om Det Europæiske Agentur for Net- og Informationssikkerhed (ENISA)

(2011/C 101/04)

DEN EUROPÆISKE TILSYNSFØRENDE FOR DATABESKYTTELSE,

som henviser til traktaten om Den Europæiske Unions funktionsmåde, særlig artikel 16,

som henviser til Den Europæiske Unions charter om grundlæggende rettigheder, særlig artikel 7 og 8,

som henviser til Europa-Parlamentets og Rådets direktiv 95/46/EF af 24. oktober 1995 om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger ([1]),

som henviser til anmodningen om en udtalelse i overensstemmelse med Europa-Parlamentets og Rådets forordning (EF) nr. 45/2001 om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger i fællesskabsinstitutionerne og -organerne og om fri udveksling af sådanne oplysninger ([2]),

HAR VEDTAGET FØLGENDE UDTALELSE:

## I. INDLEDNING

*Beskrivelse af forslaget*

1. Den 30. september 2010 vedtog Kommissionen et forslag til Europa-Parlamentets og Rådets forordning om Det Europæiske Agentur for Net- og Informationssikkerhed (ENISA) ([3]).

2. ENISA blev oprettet i marts 2004 for en første periode på fem år ved forordning (EF) nr. 460/2004 ([4]). I 2008 blev mandatet forlænget indtil marts 2012 ved forordning (EF) nr. 1007/2008 ([5]).

3. Som det fremgår af artikel 1, stk. 1, i forordning (EF) nr. 460/2004, blev agenturet oprettet for at sikre et højt og effektivt net- og informationssikkerhedsniveau i EU og for at bidrage til et velfungerende indre marked.

4. Kommissionens forslag sigter mod at modernisere agenturet, styrke dets kompetencer og etablere et nyt mandat for en femårig periode, som vil gøre det muligt for agenturet at fortsætte sit virke efter marts 2012 ([6]).

5. Retsgrundlaget for den foreslåede forordning er EUF-traktatens artikel 114 ([7]), der tillægger Unionen beføjelse til at vedtage foranstaltninger med henblik på at sikre det indre markeds funktion. EUF-traktatens artikel 114 efterfølger artikel 95 i den tidligere EF-traktat, som de tidligere forordninger om ENISA byggede på ([8]).

6. Det fremgår af begrundelsen til forslaget, at forebyggelse og bekæmpelse af internetkriminalitet er blevet et område, hvor der er delt kompetence, efter at Lissabontraktaten er trådt i kraft. Dette har givet ENISA mulighed for at fungere som en platform for net- og informationssikkerhedsaspekterne af bekæmpelsen af internetkriminalitet og for at udveksle synspunkter og bedste praksis med de myndigheder, der har ansvar for cyberforsvar, retshåndhævelse og databeskyttelse.

7. Ud af flere muligheder valgte Kommissionen at foreslå en udvidelse af ENISA's opgaver og at tilføje retshåndhævelses- og databeskyttelsesmyndighederne som fuldgyldige medlemmer af den stående gruppe af interessenter. Den nye liste over opgaver omfatter ikke operationelle opgaver, men ajourfører og omformulerer de nuværende opgaver.

*Høring af den tilsynsførende*

8. Den 1. oktober 2010 blev forslaget sendt til høring hos Den Europæiske Tilsynsførende for Databeskyttelse i overensstemmelse med artikel 28, stk. 2, i forordning (EF) nr. 45/2001. Den tilsynsførende glæder sig over, at han er blevet hørt om dette spørgsmål, og anbefaler, at der henvises til denne høring i betragtningerne til forslaget, sådan som det sædvanligvis gøres i lovgivningstekster, hvorom den tilsynsførende er blevet hørt i overensstemmelse med forordning (EF) nr. 45/2001.

9. Forud for vedtagelsen af forslaget blev den tilsynsførende hørt uformelt og fremsatte flere uformelle bemærkninger. Der er dog ikke taget hensyn til disse bemærkninger i den endelige udgave af forslaget.

*Generel vurdering*

10. Den tilsynsførende understreger, at sikkerhed i forbindelse med databehandling er et meget vigtigt element i databeskyttelsen ([9]). Han ser i den forbindelse med tilfredshed på forslagets mål om at styrke agenturets kompetencer, sådan at det kan udføre sine nuværende opgaver og hverv mere

([1]) EFT L 281 af 23.11.1995, s. 31.
([2]) EFT L 8 af 12.1.2001, s. 1.
([3]) KOM(2010) 521 endelig.
([4]) EUT L 77 af 13.3.2004, s. 1.
([5]) EUT L 293 af 31.10.2008, s. 1.
([6]) For at forhindre et retligt tomrum, såfremt lovgivningsproceduren i Europa-Parlamentet og Rådet strækker sig ud over det nuværende mandats gyldighedsperiode, vedtog Kommissionen den 30. september 2010 et andet forslag til ændring af forordning (EF) nr. 460/2004, der udelukkende har til formål at forlænge fristen for det nuværende mandat med 18 måneder. Jf. KOM(2010) 520 endelig.

([7]) Se ovenfor.
([8]) Den 2. maj 2006 afviste Domstolen et søgsmål om annullation af den tidligere forordning (EF) nr. 460/2004, der anfægtede forordningens retsgrundlag (sag C-217/04).
([9]) Sikkerhedskravene findes i artikel 22 og 35 i forordning (EF) nr. 45/2001, artikel 16 og 17 i direktiv 95/46/EF og artikel 4 og 5 i direktiv 2002/58/EF.

effektivt og samtidig udvide sit virkefelt. Den tilsynsførende ser endvidere med tilfredshed på medtagelsen af databeskyttelsesmyndighederne og retshåndhævelsesmyndighederne som fuldgyldige interessenter. Han betragter udvidelsen af ENISA's mandat som et middel til fremme af professionel og strømlinet forvaltning af informationssystemers sikkerhedsforanstaltninger på europæisk plan.

11. Den samlede vurdering af forslaget er positiv. Den foreslåede forordning er dog uklar eller ufuldstændig på flere punkter, hvilket giver anledning til bekymring set ud fra et databeskyttelsessynspunkt. Disse punkter vil blive forklaret og gennemgået i det næste kapitel af denne udtalelse.

## II. BEMÆRKNINGER OG ANBEFALINGER

*De udvidede opgaver, der skal udføres af ENISA, er ikke tilstrækkeligt klare*

12. Agenturets udvidede opgaver, der vedrører inddragelse af retshåndhævelsesmyndigheder og databeskyttelsesmyndigheder, er formuleret meget generelt i artikel 3 i forslaget. Begrundelsen er mere eksplicit i denne henseende. Det fremgår heraf, at ENISA fungerer som formidler i forhold til retshåndhævelsesmyndighederne inden for bekæmpelse af internetkriminalitet og udfører ikke-operationelle opgaver som led i bekæmpelsen af internetkriminalitet. Disse opgaver er dog ikke medtaget eller er kun nævnt i meget generelle vendinger i artikel 3.

13. For at undgå enhver form for retlig usikkerhed bør den foreslåede forordning være klar og utvetydig med hensyn til ENISA's opgaver. Sikkerhed i forbindelse med databehandling er som nævnt et meget vigtigt element i databeskyttelsen. ENISA vil spille en stadig vigtigere rolle på dette område. Det bør være klart for borgerne og de relevante institutioner og enheder, hvilken form for aktiviteter ENISA kan deltage i. Denne dimension er så meget desto vigtigere, hvis ENISA's udvidede opgaver kommer til at omfatte behandling af personoplysninger (jf. punkt 17-20).

14. Det fremgår af artikel 3, stk. 1, litra k), i forslaget, at agenturet udfører alle andre opgaver, som det pålægges ved en anden lovgivningsmæssig EU-retsakt. Den tilsynsførende er betænkelig ved denne åbne bestemmelse, da den skaber et muligt smuthul, som kan skade sammenhængen i retsakten og føre til »funktionsskred« i agenturet.

15. En af de opgaver, der er nævnt i artikel 3, stk. 1, litra k), i forslaget, findes i direktiv 2002/58/EF ([1]). Den bestemmer, at Kommissionen skal høre agenturet om alle tekniske gennemførelsesforanstaltninger, der gælder for indberetninger af databrud. Den tilsynsførende anbefaler, at denne aktivitet, som agenturet udfører, beskrives mere detaljeret, samtidig med at den begrænses til sikkerhedsområdet. På grund af den indvirkning, ENISA kan få på politikudviklingen på dette område, bør denne aktivitet spille en klarere og mere fremtrædende rolle i den foreslåede forordning.

16. Den tilsynsførende anbefaler endvidere, at der medtages en henvisning til direktiv 1999/5/EF ([2]) i betragtning 21 på grund af ENISA's specifikke opgave, der er nævnt i artikel 3, stk. 1, litra c) i det nuværende forslag, med at bistå medlemsstaterne og Unionens institutioner og organer i deres indsats for at indsamle, analysere og formidle oplysninger om net- og informationssikkerhed. Dette skulle give ENISA nogle redskaber, der kan fremme bedste praksis og teknikker inden for NIS (netinformationssikkerhed), da det bedre vil illustrere det mulige konstruktive samspil mellem agenturet og standardiseringsorganerne.

*Det bør afklares, om agenturet skal behandle personoplysninger*

17. Det fremgår ikke af forslaget, om de opgaver, som agenturet får tildelt, kan omfatte behandling af personoplysninger. Forslaget indeholder derfor ikke noget specifikt retsgrundlag for behandling af personoplysninger, jf. artikel 5 i forordning (EF) nr. 45/2001.

18. Nogle af de opgaver, der tildeles agenturet, kan dog (i hvert fald i en vis udstrækning) indebære behandling af personoplysninger. Det er f.eks. ikke udelukket, at analyse af sikkerhedshændelser og databrud eller udførelse af ikke-operationelle opgaver som led i bekæmpelsen af internetkriminalitet kan indebære indsamling og analyse af personoplysninger.

19. Betragtning 9 i forslaget henviser til bestemmelserne i direktiv 2002/21/EF ([3]), hvor det hedder, at de nationale tilsynsmyndigheder, hvor det er relevant, skal underrette agenturet i tilfælde af brud på sikkerheden. Den tilsynsførende anbefaler, at forslaget gøres mere detaljeret med hensyn til, hvilke indberetninger der skal sendes til ENISA, og hvordan ENISA skal reagere på disse. Forslaget bør ligeledes komme ind på de konsekvenser, som analysen af eventuelle indberetninger kan få for behandlingen af personoplysninger.

([1]) Europa-Parlamentets og Rådets direktiv 2002/58/EF af 12. juli 2002 om behandling af personoplysninger og beskyttelse af privatlivets fred i den elektroniske kommunikationssektor (Direktiv om databeskyttelse inden for elektronisk kommunikation) EFT L 201 af 31.7.2002, s. 37.

([2]) Europa-Parlamentets og Rådets direktiv 1999/5/EF af 9. marts 1999 om radio- og teleterminaludstyr samt gensidig anerkendelse af udstyrets overensstemmelse, EFT L 91 af 7.4.1999, s. 10, navnlig artikel 3, stk. 3, litra c).

([3]) Europa-Parlamentets og Rådets direktiv 2002/21/EF af 7. marts 2002 om fælles rammebestemmelser for elektroniske kommunikationsnet og -tjenester (rammedirektivet) EFT L 108 af 24.4.2002, s. 33.

20. Den tilsynsførende opfordrer lovgiveren til at præcisere, om nogle af ENISA's aktiviteter som anført i artikel 3 vil omfatte behandling af personoplysninger, og i bekræftende fald hvilke.

*De interne sikkerhedsregler for ENISA bør angives*

21. Selv om ENISA spiller en vigtig rolle i drøftelserne om net- og informationssikkerhed i Europa, nævner forslaget så godt som intet om udarbejdelse af sikkerhedsforanstaltninger for selve agenturet (uanset om de er knyttet til behandling af personoplysninger eller ej).

22. Den tilsynsførende er af den opfattelse, at agenturet i endnu højere grad vil kunne fremme god praksis for sikkerhed i forbindelse med databehandling, hvis disse sikkerhedsforanstaltninger finder udbredt anvendelse internt i selve agenturet. Dette vil medvirke til, at agenturet bliver anerkendt ikke blot som et ekspertisecenter, men også som et referencepunkt i forbindelse med den praktiske gennemførelse af bedste tilgængelige teknikker (BAT) på sikkerhedsområdet. Stræben efter topkvalitet i gennemførelsen af sikkerhedspraksis bør derfor fastsættes i forordningen om agenturets arbejdsprocedurer. Den tilsynsførende foreslår, at der tilføjes en bestemmelse herom i forslaget, f.eks. ved at kræve, at agenturet anvender de bedste tilgængelige teknikker, hvilket vil sige de mest effektive og avancerede sikkerhedsprocedurer og deres funktionsmåder.

23. Denne fremgangsmåde vil gøre det muligt for agenturet at rådgive om, hvorvidt særlige teknikker er praktisk egnede til at tilvejebringe de krævede sikkerhedsgarantier. Endvidere bør man ved gennemførelsen af disse BAT prioritere dem, der gør det muligt at garantere sikkerheden, samtidig med at indvirkningen på privatlivets fred begrænses til et minimum. Der bør vælges teknikker, som er bedre i overensstemmelse med begrebet »privacy by design« (privatlivsbeskyttelse i it-arkitekturen).

24. Selv med en mindre ambitiøs tilgang anbefaler den tilsynsførende, at forordningen som et minimum indeholder følgende krav: i) skabelse af en intern sikkerhedspolitik efter en samlet risikovurdering og under hensyn til internationale standarder og bedste praksis i medlemsstaterne, ii) udnævnelse af en sikkerhedsansvarlig, som skal stå for gennemførelsen af politikken, med passende ressourcer og myndighed, iii) godkendelse af denne politik efter en nøje undersøgelse af den resterende risiko og de kontrolforanstaltninger, der foreslås af bestyrelsen, og iv) en periodisk revision af politikken med en klar angivelse af den valgte tidsplan herfor og revisionens mål.

*Der bør i højere grad fastlægges kanaler for samarbejdet med databeskyttelsesmyndighederne (herunder den tilsynsførende) og Artikel 29-gruppen*

25. Som allerede nævnt bifalder den tilsynsførende udvidelsen af agenturets mandat og finder, at databeskyttelsesmyndighederne i vidt omfang kan få gavn af agenturets eksistens (og agenturet af disse myndigheders ekspertise). På grund af den naturlige og logiske konvergens mellem sikkerhed og databeskyttelse skal agenturet og databeskyttelsesmyndighederne virkelig arbejde tæt sammen.

26. Betragtning 24 og 25 indeholder en henvisning til det foreslåede EU-direktiv om internetkriminalitet og nævner, at agenturet etablerer kontakt med retshåndhævelsesmyndighederne og databeskyttelsesmyndighederne om informationssikkerhedsaspekterne af bekæmpelsen af internetkriminalitet ([1]).

27. Forslaget bør også indeholde bestemmelser om konkrete kanaler og samarbejdsmekanismer, der kan i) sikre *sammenhæng* mellem agenturets aktiviteter og databeskyttelsesmyndighedernes aktiviteter og ii) muliggøre et *tæt samarbejde* mellem agenturet og databeskyttelsesmyndighederne.

28. Med hensyn til *sammenhæng* fremgår det udtrykkeligt af betragtning 27, at agenturets opgaver ikke bør være i uoverensstemmelse med medlemsstaternes databeskyttelsesmyndigheder. Den tilsynsførende hilser denne henvisning velkommen, men bemærker, at der ikke henvises til den tilsynsførende eller Artikel 29-gruppen. Den tilsynsførende anbefaler, at lovgiveren medtager en tilsvarende bestemmelse om ikke-indblanding i forslaget vedrørende disse to enheder. Dette vil skabe klarere arbejdsbetingelser for alle parter og bør danne ramme om de samarbejdskanaler og -mekanismer, der skal gøre det muligt for agenturet at bistå de forskellige databeskyttelsesmyndigheder og Artikel 29-gruppen.

29. Med hensyn til *tæt samarbejde* noterer den tilsynsførende sig med glæde, at databeskyttelsesmyndighederne bliver repræsenteret i den stående gruppe af interessenter, der skal rådgive agenturet under udførelsen af dets aktiviteter. Han anbefaler, at det udtrykkeligt nævnes, at en sådan repræsentation af nationale databeskyttelsesmyndigheder skal udpeges af agenturet på grundlag af et forslag fra Artikel 29-gruppen. Det vil også blive påskønnet, hvis der indsættes en bestemmelse om, at den tilsynsførende som sådan skal deltage i møder, hvor der efter planen skal drøftes spørgsmål, som er relevante for samarbejdet med den tilsynsførende. Den tilsynsførende anbefaler endvidere, at agenturet (efter rådgivning fra den stående gruppe af interessenter og med bestyrelsens godkendelse) nedsætter ad hoc-arbejdsgrupper for forskellige emner, hvor databeskyttelse og sikkerhed overlapper hinanden, med henblik på at skabe en ramme for bestræbelserne på at etablere dette tætte samarbejde.

([1]) Forslag til Europa-Parlamentets og Rådets direktiv om angreb på informationssystemer og om ophævelse af Rådets rammeafgørelse 2005/222/RIA, KOM(2010) 517 endelig.

30. Endelig anbefaler den tilsynsførende for at undgå eventuelle misforståelser, at man anvender udtrykket »databeskyttelsesmyndigheder« i stedet for »myndigheder med ansvar for beskyttelse af privatlivets fred« og præciserer, hvem disse myndigheder er, ved at indsætte en henvisning til artikel 28 i direktiv 95/46/EF og den tilsynsførende, jf. kapitel V i forordning (EF) nr. 45/2001.

*Det er uklart, hvem der kan anmode om bistand fra ENISA*

31. Den tilsynsførende bemærker, at der er en uoverensstemmelse i den foreslåede forordning med hensyn til, hvem der kan anmode om bistand fra ENISA. Det fremgår af betragtning 7, 15, 16, 18 og 36 i forslaget, at ENISA har mulighed for at bistå medlemsstaternes organer og EU som helhed. Artikel 2, stk. 1, henviser dog kun til Kommissionen og medlemsstaterne, mens artikel 14 begrænser muligheden for at anmode om bistand til: i) Europa-Parlamentet, ii) Rådet, iii) Kommissionen og iv) ethvert kompetent organ udpeget af en medlemsstat med undtagelse af nogle af EU's organer, agenturer og kontorer.

32. Artikel 3 i forslaget er mere specifikt og foreslår forskellige former for bistand afhængigt af typen af modtagere: i) indsamling og analyse af oplysninger om informationssikkerhed (medlemsstaterne samt EU-institutionerne og -organerne), ii) analyse af net- og informationssikkerhedssituationen i Europa (medlemsstaterne og EU-institutionerne), iii) fremme af brugen af god praksis inden for risikostyring og sikkerhed (overalt i EU og medlemsstaterne), iv) udvikling af sporing af sikkerhedsproblemer i net og informationssystemer (i EU-institutionerne og -organerne) og v) samarbejde omkring dialogen og samarbejdet med tredjelande (EU).

33. Den tilsynsførende opfordrer lovgiveren til at afhjælpe denne uoverensstemmelse og tilpasse ovennævnte bestemmelser. I den forbindelse anbefaler den tilsynsførende, at artikel 14 ændres således, at den faktisk kommer til at omfatte alle EU's institutioner, organer, kontorer og agenturer, og så det bliver klart, hvilken form for bistand de forskellige enheder i EU kan anmode om (såfremt lovgiveren overvejer denne sondring). På samme måde anbefales det, at visse offentlige og private enheder kan anmode om bistand fra agenturet, hvis den støtte, der anmodes om, viser et klart potentiale set fra en europæisk synsvinkel, og hvis den afpasses efter agenturets mål.

*Bestyrelsens opgaver*

34. Det fremgår af begrundelsen, at bestyrelsen skal have styrkede beføjelser med hensyn til sin tilsynsrolle. Den tilsynsførende hilser denne styrkede rolle velkommen og anbefaler, at der medtages flere aspekter vedrørende databeskyttelse blandt bestyrelsens opgaver. Derudover anbefaler den tilsynsførende, at forordningen utvetydigt angiver, hvem der er berettiget til: i) at udarbejde foranstaltninger med henblik på agenturets anvendelse af forordning (EF) nr. 45/2001, herunder foranstaltninger vedrørende udnævnelsen af en databeskyttelsesansvarlig, ii) godkende sikkerhedspolitikken og de efterfølgende periodiske revisioner og iii) fastsætte samarbejdsprotokollen med databeskyttelsesmyndighederne og retshåndhævelsesmyndighederne.

*Anvendelsen af forordning (EF) nr. 45/2001*

35. Selv om det allerede kræves i forordning (EF) nr. 45/2001, foreslår den tilsynsførende, at udnævnelsen af den databeskyttelsesansvarlige medtages i artikel 27, eftersom dette er af særlig betydning, hvorefter der omgående bør udarbejdes gennemførelsesbestemmelser vedrørende omfanget af de beføjelser og opgaver, der skal tildeles den databeskyttelsesansvarlige i overensstemmelse med artikel 24, stk. 8, i forordning (EF) nr. 45/2001. Mere konkret kunne artikel 27 affattes således:

1) De oplysninger, der behandles af agenturet i overensstemmelse med denne forordning, er omfattet af Europa-Parlamentets og Rådets forordning (EF) nr. 45/2001 af 18. december 2000 om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger i fællesskabsinstitutionerne og -organerne og om fri udveksling af sådanne oplysninger.

2) Bestyrelsen udarbejder foranstaltninger med henblik på agenturets anvendelse af forordning (EF) nr. 45/2001, herunder foranstaltninger vedrørende agenturets databeskyttelsesansvarlige.

36. I tilfælde af, at der kræves et specifikt retsgrundlag for behandlingen af personoplysninger, jf. punkt 17-20 ovenfor, bør det også angive de nødvendige og relevante sikkerhedsgarantier, begrænsninger og betingelser, som gælder for denne behandling.

## III. **KONKLUSIONER**

37. Den samlede vurdering af forslaget er positiv, og den tilsynsførende ser med tilfredshed på forlængelsen af agenturets mandat og udvidelsen af dets opgaver i form af, at databeskyttelsesmyndighederne og retshåndhævelsesmyndighederne medtages som fuldgyldige interessenter. Den tilsynsførende finder, at agenturets fortsatte virke på europæisk plan vil tilskynde til at styrke professionel og strømlinet forvaltning af informationssystemers sikkerhedsforanstaltninger.

38. Den tilsynsførende anbefaler, at forslaget for at undgå enhver form for retlig usikkerhed præciseres med hensyn til udvidelsen af agenturets opgaver, navnlig de opgaver, der vedrører inddragelsen af retshåndhævelsesmyndighederne og databeskyttelsesmyndighederne. Den tilsynsførende gør også opmærksom på det potentielle smuthul, der kan opstå ved medtagelsen af en bestemmelse i forslaget, som gør det muligt at tildele agenturet nye opgaver ved enhver anden lovgivningsmæssig EU-retsakt uden yderligere begrænsning.

39. Den tilsynsførende opfordrer lovgiveren til at præcisere, om nogle af ENISA's aktiviteter vil omfatte behandling af personoplysninger, og i bekræftende fald hvilke.

40. Den tilsynsførende anbefaler, at der medtages bestemmelser om indførelse af en sikkerhedspolitik for agenturet selv med henblik på at styrke agenturets rolle som katalysator for topkvalitet i sikkerhedspraksis og som en faktor, der fremmer privatlivsbeskyttelse i it-arkitekturen ved at integrere anvendelsen af de bedste tilgængelige teknikker i sikkerheden for så vidt angår rettigheder til beskyttelse af personoplysninger.

41. Kanalerne for samarbejde med databeskyttelsesmyndighederne, herunder den tilsynsførende og Artikel 29-udvalget, bør defineres bedre med henblik på at sikre sammenhæng og tæt samarbejde.

42. Den tilsynsførende opfordrer lovgiveren til at løse nogle uoverensstemmelser med hensyn til begrænsningerne i artikel 14 vedrørende muligheden for at anmode om bistand fra agenturet. Den tilsynsførende anbefaler navnlig, at man giver afkald på disse begrænsninger, og at alle EU's institutioner, organer, agenturer og kontorer får mulighed for at anmode om bistand fra agenturet.

43. Endelig anbefaler den tilsynsførende, at bestyrelsens udvidede beføjelser kommer til at omfatte nogle konkrete aspekter, som kan give bedre garanti for, at agenturet følger god praksis med hensyn til sikkerhed og databeskyttelse. Det foreslås bl.a., at man medtager udnævnelsen af en databeskyttelsesansvarlig og godkendelsen af foranstaltninger, som sigter mod korrekt anvendelse af forordning (EF) nr. 45/2001.

Udfærdiget i Bruxelles, den 20. december 2010.

Giovanni BUTTARELLI

*Assisterende Europæisk Tilsynsførende for Databeskyttelse*