Yttrande från Europeiska datatillsynsmannenom förslaget till Europaparlamentets och rådets förordning om Europeiska byrån för nät- och informationssäkerhet (Enisa)

(2011/C 101/04)

EUROPEISKA DATATILLSYNSMANNEN HAR AVGETT DETTA YTTRANDE

med beaktande av fördraget om Europeiska unionens funktionssätt, särskilt artikel 16,

med beaktande av Europeiska unionens stadga om de grundläggande rättigheterna, särskilt artiklarna 7 och 8,

med beaktande av Europaparlamentets och rådets direktiv 95/46/EG av den 24 oktober 1995 om skydd för enskilda personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter ([1]),

med beaktande av begäran om ett yttrande i enlighet med Europaparlamentets och rådets förordning (EG) nr 45/2001 om skydd för enskilda då gemenskapsinstitutionerna och gemenskapsorganen behandlar personuppgifter och om den fria rörligheten för sådana uppgifter, särskilt artikel 28.2 ([2]).

HÄRIGENOM FRAMFÖRS FÖLJANDE.

I. INLEDNING

Beskrivning av förslaget

1. Den 30 september 2010 antog kommissionen ett förslag till Europaparlamentets och rådets förordning om Europeiska byrån för nät- och informationssäkerhet ([3]).

2. Europeiska byrån för nät- och informationssäkerhet inrättades i mars 2004 för en inledande period om fem år genom förordning (EG) nr 460/2004 ([4]). År 2008 utökades byråns mandattid genom förordning (EG) nr 1007/2008 ([5]) till mars 2012.

3. I enlighet med artikel 1.1 i förordning (EG) nr 460/2004 inrättades byrån för att säkerställa en hög och effektiv nivå av nät- och informationssäkerhet inom unionen och för att bidra till att den inre marknaden fungerar väl.

4. Syftet med kommissionens förslag är att modernisera byrån, stärka dess behörigheter och fastställa ett nytt mandat för en femårsperiod, så att byrån kan fortsätta efter mars 2012 ([6]).

5. Den rättsliga grunden till den föreslagna förordningen är artikel 114 i fördraget om Europeiska unionens funktionssätt ([7]), som ger unionen behörighet att besluta om åtgärder för att få den inre marknaden att fungera. Artikel 114 i EU-fördraget är efterföljaren till artikel 95 i det tidigare EG-fördraget som de tidigare förordningarna om Enisa grundades på ([8]).

6. I den motivering som åtföljer förslaget hänvisas till att förebyggandet och bekämpandet av brott har blivit en delad behörighet efter Lissabonfördragets ikraftträdande. Det har skapat möjligheten att låta Enisa fungera som plattform för nät- och informationssäkerhetsaspekter av kampen mot it-brottslighet och att utbyta synpunkter och bästa praxis med it-försvar, rättsvårdande myndigheter och dataskyddsmyndigheter.

7. Av flera alternativ valde kommissionen att föreslå en utökning av uppgifterna för Enisa och att lägga till rättsvårdande myndigheter och dataskyddsmyndigheter som fullvärdiga medlemmar av den ständiga intressentgruppen. I den nya förteckningen över uppgifter ingår inte operativa funktioner, utan de nuvarande uppgifterna aktualiseras och formuleras om.

Samråd med Europeiska datatillsynsmannen

8. Den 1 oktober 2010 översändes förslaget till Europeiska datatillsynsmannen för samråd i enlighet med artikel 28.2 i förordning (EG) nr 45/2001. Europeiska datatillsynsmannen välkomnar att ha hörts i ärendet och rekommenderar att en hänvisning till detta samråd görs i skälen till förslaget, så som är brukligt i de rättsakter där Europeiska datatillsynsmannen har hörts i enlighet med förordning (EG) nr 45/2001.

9. Innan förslaget antogs hördes Europeiska datatillsynsmannen informellt, och datatillsynsmannen lämnade flera informella kommentarer. Ingen av dessa synpunkter har dock beaktats i den slutliga versionen av förslaget.

Allmän bedömning

10. Europeiska datatillsynsmannen understryker att säkerheten i databehandlingen är en viktig faktor i dataskyddet ([9]). Därför välkomnar datatillsynsmannen att syftet med förslaget är att stärka byråns behörigheter så att den kan fullgöra sina nuvarande uppgifter och förpliktelser mer effektivt och

([1]) EGT L 281, 23.11.1995, s. 31.
([2]) EGT L 8, 12.1.2001, s. 1.
([3]) KOM(2010) 521 slutlig.
([4]) EUT L 77, 13.3.2004, s. 1.
([5]) EUT L 293, 31.10.2008, s. 1.
([6]) För att förhindra ett rättsligt vakuum om lagstiftningsförfarandet i Europaparlamentet och i rådet fortfarande pågår när det nuvarande mandatet löper ut antog kommissionen den 30 september 2010 ett andra förslag till ändring av förordning (EG) nr 460/2004 som bara förlänger det innevarande mandatet med 18 månader. Se KOM(2010) 520 slutlig.

([7]) Jfr ovan.
([8]) Den 2 maj 2006 ogillade domstolen en talan som väckts om ogiltigförklaring av den tidigare förordningen (EG) nr 460/2004, där dess rättsliga grund ifrågasattes (mål C-217/04).
([9]) Det finns säkerhetskrav i artiklarna 22 och 35 i förordning (EG) nr 45/2001, artiklarna 16 och 17 i direktiv 95/46/EG och artiklarna 4 och 5 i direktiv 2002/58/EG.

samtidigt bredda sitt verksamhetsområde. Datatillsynsmannen välkomnar även att dataskyddsmyndigheter och rättsvårdande myndigheter inbegrips som fullvärdiga intressenter. Datatillsynsmannen anser att breddningen av Enisas mandat är ett sätt att på EU-nivå främja en professionell och välfungerande förvaltning av säkerhetsåtgärder för informationssystem.

11. Den allmänna bedömningen av förslaget är positiv. På flera punkter är dock den föreslagna förordningen oklar eller ofullständig, vilket väcker farhågor utifrån ett dataskyddsperspektiv. Dessa punkter förklaras och diskuteras i nästa kapitel av yttrandet.

II. SYNPUNKTER OCH REKOMMENDATIONER

De utökade uppgifter som ska utföras av Enisa är inte tillräckligt tydligt definierade

12. Byråns utökade uppgifter, som gäller medverkan av rättsvårdande organ och dataskyddsmyndigheter, är mycket allmänt formulerade i artikel 3 i förslaget. Motiveringen är mer utförlig i detta avseende. Där sägs att Enisa är kontaktyta för rättsvårdande myndigheter i bekämpandet av it-brottslighet och utför icke-operativa uppgifter i kampen mot sådan brottslighet. Dessa uppgifter har dock inte tagits med och nämns endast i mycket allmänna ordalag i artikel 3.

13. För att undvika rättsosäkerhet bör den föreslagna förordningen vara klar och entydig om Enisas uppgifter. Som angetts är säker databehandling ett viktigt inslag i dataskyddet. Enisa kommer att spela en allt viktigare roll på detta område. Det bör göras klart för medborgare, institutioner och organ vilka slags verksamheter Enisa kan bedriva. En sådan dimension är ännu viktigare om behandling av personuppgifter (se punkterna 17–20 nedan) ska ingå i Enisas uppgifter.

14. I artikel 3.1 k i förslaget anges att byrån ska utföra varje annan uppgift som den tilldelas genom EU-lagstiftningen. Europeiska datatillsynsmannen är bekymrad över denna öppet formulerade bestämmelse, eftersom den skapar ett tänkbart kryphål som kan påverka rättsaktens konsekvens och leda till funktionsglidning för byrån.

15. En av de uppgifter som avses i artikel 3.1 k i förslaget återfinns i direktiv 2002/58/EG ([1]). I det direktivet föreskrivs att kommissionen ska samråda med byrån om tekniska genomförandebestämmelser för anmälan av överträdelser i fråga om personuppgifter. Datatillsynsmannen rekommenderar att byråns verksamhet i detta avseende beskrivs mer utförligt och begränsas till säkerhetsområdet. Med hänsyn till den påverkan som Enisa kan ha på den politiska utvecklingen på området bör denna verksamhet ha en tydligare och mer framträdande plats inom den föreslagna förordningen.

16. Datatillsynsmannen rekommenderar vidare att en hänvisning till direktiv 1999/5/EG ([2]) infogas i skäl 21 med hänsyn till den särskilda uppgift för Enisa som avses i artikel 3.1 c i det föreliggande förslaget om att bistå medlemsstaternas och EU:s institutioner och organ i deras insatser för att samla in, analysera och sprida data om nät- och informationssäkerhet. Detta bör understödja Enisas nät- och informationssäkerhetsaktiviteter för att främja bästa praxis och metoder eftersom det bättre skulle illustrera en tänkbar samverkan mellan byrån och standardiseringsorganen.

Det gör klargöras om personuppgifter kommer att behandlas av byrån

17. I förslaget anges inte om behandling av personuppgifter kan ingå bland de uppgifter som byrån tilldelas. Därför innehåller förslaget inte någon uttrycklig rättslig grund för behandling av personuppgifter i den mening som avses i artikel 5 i förordning (EG) nr 45/2001.

18. En del av de uppgifter som byrån tilldelats kan (åtminstone i viss utsträckning) medföra behandling av personuppgifter. Det är exempelvis inte uteslutet att analysen av säkerhetsincidenter och överträdelser i fråga om personuppgifter eller utförandet av icke-operativa funktioner i bekämpandet av it-brottslighet medför insamling och analys av personuppgifter.

19. I skäl 9 i förslagen hänvisas till bestämmelserna i direktiv 2002/21/EG ([3]) som föreskriver att de nationella tillsynsmyndigheterna när så är lämpligt ska informera byrån om överträdelser av säkerheten. Datatillsynsmannen rekommenderar att det i förslaget anges mer utförligt vilka underrättelser som det är meningen att myndigheterna ska skicka till Enisa och om hur Enisa ska svara på dem. I förslaget bör man också ta upp de konsekvenser i fråga om behandlingen av personuppgifter som kan uppkomma av analysen av dessa (eventuella) underrättelser.

([1]) Europaparlamentets och rådets direktiv 2002/58/EG av den 12 juli 2002 om behandling av personuppgifter och integritetsskydd inom sektorn för elektronisk kommunikation (direktiv om integritet och elektronisk kommunikation) EGT L 201, 31.7.2002, s. 37.

([2]) Europaparlamentets och rådets direktiv 1999/5/EG av den 9 mars 1999 om radioutrustning och teleterminalutrustning och om ömsesidigt erkännande av utrustningens överensstämmelse, EGT L 91, 7.4.1999, s. 10, och särskilt dess artikel 3.3 c.

([3]) Europaparlamentets och rådets direktiv 2002/21/EG av den 7 mars 2002 om ett gemensamt regelverk för elektroniska kommunikationsnät och kommunikationstjänster (ramdirektiv, EGT L 108, 24.4.2002, s. 33).

20. Datatillsynsmannen uppmanar lagstiftaren att klargöra om och i så fall hur de Enisaverksamheter som förtecknas i artikel 3 kommer att innefatta behandling av personuppgifter.

Interna säkerhetsregler för Enisa bör anges

21. Trots att Enisa har en viktig roll i diskussionen om nät- och informationssäkerhet i Europa, finns det praktiskt taget ingenting alls i förslaget om fastställande av säkerhetsåtgärder för byrån själv (oavsett om det gäller behandling av personuppgifter eller annat).

22. Europeiska datatillsynsmannen anser att byrån skulle ha bättre förutsättningar att främja god praxis i fråga om säker databehandling om byrån själv strikt tillämpade sådana säkerhetsåtgärder internt. Det skulle främja att byrån inte bara erkänns som ett kunskapscentrum utan även som en referenspunkt vid det praktiska genomförandet av bästa tillgängliga teknik på säkerhetsområdet. Att sträva efter högsta kvalitet i genomförandet av säkerhetspraxis bör därför ingå i byråns arbetsordning. Datatillsynsmannen föreslår därför att en bestämmelse om detta läggs till i förslaget, t.ex. genom att kräva att byrån tillämpar bästa tillgängliga teknik, vilket innebär de mest effektiva och avancerade säkerhetsförfarandena och deras tillämpningsmetoder.

23. Med en sådan uppläggning kan byrån ge råd om den praktiska lämpligheten av olika tekniker för att tillhandahålla de nödvändiga säkerhetsåtgärderna. Vidare bör man vid genomförandet av den bästa tillgängliga tekniken prioritera sådan teknik som gör det möjligt att garantera säkerheten samtidigt som man så långt möjligt minimerar inverkan på den personliga integriteten. Tekniker som bättre överensstämmer med begreppet ”inbyggda säkerhetsmekanismer” bör väljas.

24. Även med en mindre ambitiös uppläggning rekommenderar datatillsynsmannen att förordningen minst innehåller följande krav: i) upprättande av en intern säkerhetspolicy efter en heltäckande riskbedömning och beaktande av internationella standarder och bästa praxis i medlemsstaterna, ii) utnämning av ett uppgiftsskyddsombud som ska ansvara för genomförandet av policyn och ha tillräckliga resurser och befogenheter, iii) godkännande av policyn efter en ingående granskning av den resterande risken och de kontroller som föreslås av styrelsen samt iv) en regelbunden översyn av policyn med ett klart angivande av den valda periodiciteten och målen för översynen.

Kanaler för samarbete med dataskyddsmyndigheter (inklusive Europeiska datatillsynsmannen) och artikel 29-arbetsgruppen bör definieras bättre

25. Som redan nämnts välkomnar Europeiska datatillsynsmannen förlängningen av byråns mandat och anser att byråns existens är till stor nytta för dataskyddsmyndigheterna (och att byrån i sin tur kan dra nytta av sakkunskapen hos dessa myndigheter). Eftersom det finns ett naturligt och logiskt samband mellan säkerhet och dataskydd bör byrån och dataskyddsmyndigheterna verkligen samarbeta nära.

26. I skäl 24 och 25 hänvisas till det föreslagna EU-direktivet om it-brottslighet, och det sägs att byrån bör samarbeta med rättsvårdande organ och även med dataskyddsmyndigheter om informationssäkerhetsaspekterna av kampen mot it-brottslighet ([1]).

27. I förslaget borde man också ange konkreta kanaler och samarbetsmekanismer som i) säkerställer att byråns verksamheter *överensstämmer* med dataskyddsmyndigheternas och ii) möjliggör ett *nära samarbete* mellan byrån och dataskyddsmyndigheterna.

28. I fråga om *överensstämmelse* hänvisas det uttryckligen i skäl 27 till att byråns uppgifter inte bör inkräkta på de uppgifter som medlemsstaternas dataskyddsmyndigheter har. Europeiska datatillsynsmannen välkomnar denna hänvisning men konstaterar att ingen hänvisning görs till datatillsynsmannen och till artikel 29-arbetsgruppen. Datatillsynsmannen rekommenderar att lagstiftaren även tar med en liknande bestämmelse om icke-inblandning i fråga om dessa båda enheter i förslaget. Det skulle skapa en tydligare arbetsmiljö för alla parter och avgränsa de samarbetskanaler och mekanismer som ska göra det möjligt för byrån att bistå de olika dataskyddsmyndigheterna och artikel 29-arbetsgruppen.

29. I fråga om *nära samarbete* välkomnar Europeiska datatillsynsmannen införandet av en företrädare för dataskyddsmyndigheterna i byråns ständiga intressentgrupp, som ska ge byrån råd om genomförandet av dess verksamhet. Datatillsynsmyndigheten rekommenderar att det uttryckligen nämns att en sådan företrädare för de nationella dataskyddsmyndigheterna bör utses av byrån på förslag från artikel 29-arbetsgruppen. Det skulle också vara uppskattat om en hänvisning lades till som ger Europeiska datatillsynsmannen möjlighet att närvara i egen kapacitet vid de möten där frågor som är relevanta för samarbete med datatillsynsmannen ska diskuteras. Dessutom rekommenderar datatillsynsmannen att byrån (efter att ha hört den ständiga intressentgruppen och med styrelsens godkännande) inrättar ad hoc-arbetsgrupper för olika ämnesområden där dataskydd och säkerhet överlappar varandra som ram för denna insats för ett nära samarbete.

([1]) Förslag till Europaparlamentets och rådets direktiv om angrepp mot informationssystem och om upphävande av rådets rambeslut 2005/222/RIF, KOM(2010) 517 slutlig.

30. För att undvika eventuella missförstånd rekommenderar Europeiska datatillsynsmannen slutligen att ”dataskyddsmyndigheter” används i stället för ”myndigheter med ansvar för skydd av personlig integritet” och att man klargör vilka dessa myndigheter är genom att lägga till en hänvisning till artikel 28 i direktiv 95/46/EG och Europeiska datatillsynsmannen så som föreskrivs i kapitel V i förordning (EG) nr 45/2001.

Det är oklart vilka som kan begära bistånd från Enisa

31. Europeiska datatillsynsmannen konstaterar en inkonsekvens i den föreslagna förordningen i fråga om vem som kan begära bistånd från Enisa. Av skäl 7, 15, 16, 18 och 36 i förslaget följer att Enisa har behörighet att bistå medlemsstaternas organ och unionen som helhet. I artikel 2.1 hänvisas enbart till kommissionen och medlemsstaterna medan man i artikel 14 begränsar behörigheten att begära bistånd till i) Europaparlamentet, ii) rådet, iii) kommissionen samt iv) varje behörigt organ som utsetts av en medlemsstat, vilket innebär att vissa av EU:s institutioner, organ, byråer och kontor utesluts.

32. Artikel 3 i förslaget är mer specifikt, och där föreskrivs olika typer av bistånd beroende på typen av mottagare: i) insamling och analys av informationssäkerhetsdata (medlemsstaterna och EU:s institutioner och organ), ii) analys av läget för nät- och informationssäkerhet i EU (medlemsstaterna och EU-institutionerna), iii) främjandet av användning av god praxis för riskhantering och säkerhet (i hela unionen och medlemsstaterna), iv) utveckling av spårning inom nät- och informationssäkerhet (EU:s institutioner och organ) samt v) samarbete inom ramen för dialogen och samarbete med tredjeländer (unionen).

33. Europeiska datatillsynsmannen uppmanar lagstiftaren att avhjälpa denna inkonsekvens och se till att de ovannämnda bestämmelserna stämmer överens. I detta avseende rekommenderar datatillsynsmannen att artikel 14 ändras så att den verkligen inbegriper alla institutioner, organ, kontor och byråer i unionen och att det är klart vilken typ av bistånd som kan efterfrågas av de olika enheterna inom unionen (om det är denna differentiering som lagstiftaren avser). På samma sätt rekommenderas att vissa offentliga och privata enheter kan begära bistånd från byrån om det stöd som efterfrågas har en klar potential i EU-perspektiv och överensstämmer med byråns mål.

Styrelsens uppgifter

34. Enligt motiveringen eftersträvas utökade befogenheter för styrelsen i fråga om dess tillsynsroll. Europeiska datatillsynsmannen välkomnar denna utökade roll och rekommenderar att flera aspekter som gäller dataskyddet tas med bland styrelsens uppgifter. Dessutom rekommenderar datatillsynsmannen att man i förordningen klart anger vilka som har rätt att i) fastställa bestämmelser för byråns tillämpning av förordning (EG) nr 45/2001, bland annat dem som gäller utnämningen av ett uppgiftsskyddsombud, ii) godkänna säkerhetspolicyn och de följande regelbundna översynerna samt iii) fastställa protokollet för samarbete med dataskyddsmyndigheter och rättsvårdande organ.

Tillämpligheten av förordning (EG) nr 45/2001

35. Även om detta redan föreskrivs genom förordning (EG) nr 45/2001 föreslår Europeiska datatillsynsmannen att utnämningen av uppgiftsskyddsombud läggs till i artikel 27 eftersom detta är av särskilt stor betydelse och bör åtföljas av ett skyndsamt fastställande av genomförandebestämmelser för uppgiftsskyddsombudets befogenheter och uppgifter i enlighet med artikel 24.8 i förordning (EG) nr 45/2001. Artikel 27 borde lyda som följer:

1. Den information som behandlas av byrån i enlighet med denna förordning ska omfattas av Europaparlamentets och rådets förordning (EG) nr 45/2001 av den 18 december 2000 om skydd för enskilda då gemenskapsinstitutionerna och gemenskapsorganen behandlar personuppgifter och om den fria rörligheten för sådana uppgifter.

2. Styrelsen ska fastställa bestämmelser för byråns tillämpning av förordning (EG) nr 45/2001, även bestämmelser som rör byråns uppgiftsskyddsombud.

36. När det gäller en uttrycklig rättslig grund för behandlingen av personuppgifter krävs så som diskuterats i punkterna 17–20 ovan att det också specificeras vilka skyddsåtgärder, begränsningar och villkor som är nödvändiga och lämpliga för en sådan behandling av personuppgifter.

III. **SLUTSATSER**

37. Den allmänna bedömningen av förslaget är positiv, och Europeiska datatillsynsmannen välkomnar att byråns mandat förlängs och att dess uppgifter utökas genom att man inbegriper dataskyddsmyndigheter och rättsvårdande organ som fullvärdiga intressenter. Datatillsynsmannen anser att byråns fortsatta existens kommer att främja en professionell och välfungerande förvaltning av säkerhetsåtgärder för informationssystem.

38. För att undvika rättsosäkerhet rekommenderar Europeiska datatillsynsmannen att förslaget förtydligas i fråga om utökningen av byråns uppgifter och särskilt dem som gäller medverkan av rättsvårdande organ och dataskyddsmyndigheter. Datatillsynsmannen framhåller också det potentiella kryphål som skapas genom införandet av en bestämmelse i förslaget som utan några ytterligare inskränkningar gör det möjligt att tilldela byrån nya uppgifter genom annan EU-lagstiftning.

39. Europeiska datatillsynsmannen uppmanar lagstiftaren att klargöra om och i så fall hur de Enisaverksamheter som förtecknas i artikel 3 kommer att innefatta behandling av personuppgifter.

40. Europeiska datatillsynsmannen rekommenderar att man lägger till bestämmelser om fastställande av en säkerhetspolicy för byrån själv, för att förstärka byråns roll som främjare av kvalitet inom säkerhetspraxis och av ”inbyggda säkerhetsmekanismer” genom att användningen av bästa tillgängliga säkerhetsteknik integreras med respekt för rätten till skydd av personuppgifter.

41. Kanaler för samarbete med dataskyddsmyndigheter, inbegripet Europeiska datatillsynsmannen och artikel 29-arbetsgruppen, bör definieras bättre så att konsekvens och nära samarbete säkerställs.

42. Europeiska datatillsynsmannen uppmanar lagstiftaren att lösa vissa inkonsekvenser i fråga om inskränkningarna i artikel 14 av behörigheten att begära bistånd från byrån. Datatillsynsmannen rekommenderar särskilt att dessa inskränkningar stryks så att alla institutioner, organ, byråer och kontor i unionen får behörighet att begära bistånd från byrån.

43. Slutligen rekommenderar Europeiska datatillsynsmannen att det i styrelsens utökade befogenheter tillfogas vissa konkreta aspekter som skulle kunna garantera att en god praxis för säkerhet och dataskydd följs inom byrån. Bland annat föreslås att man lägger till utseendet av ett uppgiftsskyddsombud och godkännandet av genomförandeåtgärder för en korrekt tillämpning av förordning (EG) nr 45/2001.

Utfärdat i Bryssel den 20 december 2010.

Giovanni BUTTARELLI

Biträdande datatillsynsman