Yttrande från Europeiska datatillsynsmannenom meddelandet från kommissionen till Europaparlamentet och rådet – ”EU:s strategi för den inre säkerheten i praktiken: Fem steg mot ett säkrare Europa”

(2011/C 101/02)

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 yttrande i enlighet med förordning (EG) nr 45/2001 om skydd för enskilda då gemenskapsinstitutionerna och gemenskapsorganen behandlar personuppgifter och om den fria rörligheten för sådana uppgifter ([2]), särskilt artikel 41,

HÄRIGENOM FRAMFÖRS FÖLJANDE.

I. INLEDNING

1. Den 22 november 2010 antog kommissionen ett meddelande med titeln ”EU:s strategi för den inre säkerheten i praktiken: Fem steg mot ett säkrare Europa” (nedan kallat *meddelandet*) ([3]). Meddelandet sändes till Europeiska datatillsynsmannen för samråd.

2. Datatillsynsmannen uppskattar att kommissionen rådfrågade honom. Redan innan meddelandet antogs hade han lämnat informella synpunkter på utkastet till meddelandet, varav vissa har beaktats i slutversionen.

Meddelandets bakgrund

3. Den EU-strategi för den inre säkerheten (nedan kallad *strategin*) som behandlas i meddelandet antogs den 23 februari 2010 under det spanska ordförandeskapet ([4]). Strategin beskriver en europeisk säkerhetsmodell som bland annat innefattar åtgärder inom brottsbekämpning och straffrättsligt samarbete, gränsförvaltning och civilskydd, med vederbörlig respekt för gemensamma europeiska värderingar såsom grundläggande rättigheter. Strategins huvudsyfte är att

— presentera de befintliga EU-instrument som redan skyddar EU-medborgarnas säkerhet och frihet och det mervärde som EU tillhandahåller för allmänheten inom detta område,

— vidareutveckla gemensamma verktyg och policyer med en mer integrerande strategi som tar upp orsakerna till osäkerhet och inte bara följderna, och

— främja brottsbekämpning och straffrättsligt samarbete, gränsförvaltning, civilskydd och katastrofhantering.

4. Strategin har fokus på de mest överhängande hoten mot och problemen med säkerheten i EU, bland annat grov och organiserad brottslighet, terrorism och it-brottslighet, förvaltningen av EU:s yttre gränser och att bygga upp förmågan att klara katastrofer. Strategin innehåller allmänna riktlinjer, principer och anvisningar om hur EU bör reagera inom dessa områden och uppmanar kommissionen att föreslå åtgärder med tidsgränser för att genomföra strategin.

5. Vidare är det viktigt att i detta sammanhang hänvisa till de slutsatser om inrättande och genomförande av en policycykel för EU avseende organiserad och grov internationell brottslighet som rådet (rättsliga och inrikes frågor) antog den 8–9 november 2010 ([5]) (nedan kallade *slutsatserna från november 2010*). Detta dokument följer rådets slutsatser om den inre säkerhetens arkitektur 2006 ([6]) och uppmanar rådet och kommissionen att definiera en heltäckande strategi för den inre säkerheten som bygger på EU:s gemensamma värderingar och principer såsom dessa bekräftas i EU-stadgan om de grundläggande rättigheterna ([7]).

([1]) EGT L 281, 23.11.1995, s. 31..
([2]) EGT L 8, 12.1.2001, s. 1.
([3]) KOM(2010) 673 slutlig.
([4]) Dok. 5842/2/10.
([5]) 3043:e mötet i rådet (rättsliga och inrikes frågor), 8–10 november 2010, Bryssel.
([6]) Dok. 7039/2/06 RIF 86 CATS 34.
([7]) Policycykeln för EU avseende organiserad och grov internationell brottslighet utgörs av fyra steg: 1) policyutveckling på grundval av Europeiska unionens hotbildsbedömning avseende den grova och organiserade brottsligheten (EU Socta), 2) fastställande av policy och beslutsfattande som bygger på ett begränsat antal prioriteringar, 3) genomförande och övervakning av årliga operativa handlingsplaner och 4) vid slutet av policycykeln kommer man att göra en ingående utvärdering som kommer att tjäna som input för nästa cykel.

6. Bland de anvisningar och mål som bör vara vägledande för genomförandet av strategin tar slutsatserna från november 2010 upp att dessa bör hänvisa till en framåtsyftande och underrättelseledd strategi, bindande samarbete mellan EU-organen, inklusive ytterligare förbättring av deras informationsutbyte, samt att göra medborgarna medvetna om vikten av EU:s arbete för att skydda dem. Rådet uppmanar dessutom i sina slutsatser kommissionen att tillsammans med experter vid relevanta organ och i medlemsstaterna utveckla en flerårig strategisk plan för varje prioritering, där den lämpligaste strategin för att tackla problemet beskrivs. Rådet uppmanar också kommissionen att genom samråd med experter från medlemsstaterna och EU:s organ utveckla en oberoende mekanism för att utvärdera genomförandet av den fleråriga strategiska planen. Europeiska datatillsynsmannen tar upp dessa aspekter längre fram i yttrandet, eftersom de har nära anknytning till eller betydande konsekvenser för skyddet av personuppgifter och andra relaterade grundläggande rättigheter och friheter.

Meddelandets innehåll och syfte

7. I meddelandet föreslås fem strategiska mål som alla har kopplingar till integritet och uppgiftsskydd:

— Störa den verksamhet som bedrivs av kriminella nätverk på internationell nivå.

— Förebygga terrorism och hantera radikalisering och rekrytering.

— Förbättra säkerheten för medborgare och företag på Internet.

— Stärka säkerheten genom gränsförvaltning.

— Öka EU:s förmåga att stå emot kriser och katastrofer.

8. Den strategi för den inre säkerheten i praktiken som föreslås i meddelandet omfattar en gemensam dagordning för medlemsstaterna, Europaparlamentet, kommissionen, rådet samt byråer och andra organ, inklusive det civila samhället och lokala myndigheter. Meddelandet beskriver även hur alla dessa parter bör samarbeta under de kommande fyra åren för att nå målen för strategin.

9. Meddelandet bygger på Lissabonfördraget och tar hänsyn till den vägledning som ges i Stockholmsprogrammet (och dess handlingsplan), som i kapitel 4.1 belyser behovet av en övergripande strategi för den inre säkerheten som bygger på respekt för de grundläggande rättigheterna, internationella skyddsregler och rättstatsprincipen. I enlighet med Stockholmsprogrammet bör det vidare bli en av de prioriterade uppgifterna för kommittén för den inre säkerheten (Cosi), som inrättats enligt artikel 71 i EUF-fördraget, att utveckla, kontrollera och genomföra strategin för den inre säkerheten. För att säkerställa ett effektivt genomförande av strategin bör även säkerhetsaspekter av en integrerad gränsförvaltning täckas in, och i tillämpliga fall, dessutom straffrättsligt samarbete som är relevant för det operativa samarbetet inom området inre säkerhet. I detta sammanhang är det också viktigt att nämna att Stockholmsprogrammet tar upp att den inre säkerheten bör ta hänsyn till den yttre strategi som EU har utvecklat och till annan EU-politik, särskilt sådan som rör den inre marknaden.

Yttrandets syfte

10. Meddelandet hänvisar till olika politikområden som utgör en del av eller inverkar på begreppet *inre säkerhet* i vid bemärkelse i Europeiska unionen.

11. Syftet med det här yttrandet är inte att analysera alla politikområden och specifika ämnen som tas upp i meddelandet utan att

— granska själva målen för den strategi för den inre säkerheten som föreslås i meddelandet när det gäller det specifika perspektivet integritet och uppgiftsskydd, och – ur den synvinkeln – betona de nödvändiga kopplingarna till andra strategier som i dagsläget diskuteras och antas på EU-nivå,

— ta upp ett antal uppgiftsskyddsbegrepp som man bör ta hänsyn till vid utformning, utveckling och genomförande av strategin för den inre säkerheten på EU-nivå,

— där det är användbart och ändamålsenligt ge förslag på lämpliga sätt att ta hänsyn till uppgiftsskyddsaspekter vid genomförande av de åtgärder som föreslås i meddelandet.

12. Europeiska datatillsynsmannen kommer att göra detta genom att belysa särskilt kopplingarna mellan å ena sidan strategin för den inre säkerheten och strategin för informationshantering och å andra sidan arbetet med en heltäckande rättslig ram för uppgiftsskydd. Vidare kommer datatillsynsmannen att hänvisa till begrepp som *bästa tillgängliga tekniker* och *inbyggda säkerhetsmekanismer, konsekvensanalys av inverkan på integritets- och uppgiftsskydd* och *rättigheter för registrerade personer,* vilka har direkta konsekvenser för utformningen och genomförandet av strategin för den inre säkerheten. I yttrandet kommenteras dessutom ett antal utvalda politikområden, t.ex. integrerad gränsförvaltning, inklusive Eurosur och behandling av personuppgifter inom Frontex, samt andra områden, bland annat Internet och programmet för att spåra finansiering av terrorism (TFTP).

II. ALLMÄNNA SYNPUNKTER

Behovet av ett mer övergripande, inkluderande och ”strategiskt” tillvägagångssätt i samband med strategin för den inre säkerheten

13. För närvarande diskuteras och föreslås på EU-nivå olika EU-strategier som bygger på Lissabonfördraget och Stockholmsprogrammet och som har direkta eller indirekta konsekvenser för uppgiftsskyddet. Strategin för den inre säkerheten är en av dessa, och den har nära anknytning till andra strategier (som antingen har tagits upp i meddelanden från kommissionen under den senaste tiden eller kommer att tas upp inom den närmaste framtiden), bland annat en EU-strategi för informationshantering och en europeisk modell för informationsutbyte, en strategi för tillämpning av EU-stadgan om de grundläggande rättigheterna, en övergripande strategi för uppgiftsskydd och EU:s strategi för terrorismbekämpning. I yttrandet fäster Europeiska datatillsynsmannen särskild uppmärksamhet vid kopplingarna till strategin för informationshantering och den övergripande ram för uppgiftsskydd som bygger på artikel 16 i EUF-fördraget, eftersom dessa har det mest uppenbara politiska sambandet med strategin för den inre säkerheten ur ett uppgiftsskyddsperspektiv.

14. Alla dessa strategier utgör ett komplext lappverk av inbördes relaterade politiska riktlinjer, program och handlingsplaner som kräver ett övergripande och integrerat tillvägagångssätt på EU-nivå.

15. Mer generellt skulle detta tillvägagångssätt med ”koppling av strategier” om det tillämpas för framtida åtgärder dels visa att det finns en vision på EU-nivå när det gäller EU-strategier, dels visa att dessa strategier och de nyligen antagna meddelandena med förslag till utformning av dem är nära sammankopplade, vilket faktiskt är fallet, samt att Stockholmsprogrammet är den gemensamma referenspunkten för dem alla. Det skulle också leda till positiva synergieffekter mellan olika politiker som omfattas av området med frihet, säkerhet och rättvisa och göra det möjligt att undvika dubbelarbete inom området. Lika viktigt är att ett sådant tillvägagångssätt dessutom skulle innebära en effektivare och mer samordnad tillämpning av reglerna för uppgiftsskydd inom ramen för alla sammankopplade strategier.

16. Europeiska datatillsynsmannen understryker att en av pelarna inom strategin för den inre säkerheten är en effektiv informationshantering inom EU, som skulle bygga på nödvändighets- och proportionalitetsprinciperna för att motivera behovet av utbyte av information.

17. Såsom nämns i Europeiska datatillsynsmannens yttrande om meddelandet om informationshantering ([8]) betonar datatillsynsmannen dessutom att nya lagstiftningsåtgärder som kan underlätta lagring och utbyte av personuppgifter endast ska föreslås om det finns konkreta bevis på att de behövs ([9]). Detta rättsliga krav bör överföras till ett framåtsyftande politiskt tillvägagångssätt vid genomförandet av strategin för den inre säkerheten. Behovet av ett övergripande tillvägagångssätt för strategin för den inre säkerheten medför också att alla instrument och verktyg som redan finns inom området inre säkerhet bör utvärderas innan nya föreslås.

18. I detta sammanhang föreslår datatillsynsmannen att klausuler om regelbunden utvärdering av befintliga instrument används oftare, såsom de som ingår i direktivet om lagring av uppgifter, som ses över för närvarande ([10]).

Uppgiftsskydd som ett mål för strategin för den inre säkerheten

19. Meddelandet hänvisar till skyddet av personuppgifter i stycket ”Säkerhetsstrategier baserade på gemensamma värderingar”, där det nämns att de verktyg och åtgärder som krävs för att genomföra strategin måste vila på gemensamma värderingar, bland annat rättstatsprincipen och respekten för de grundläggande rättigheterna enligt EU:s stadga om de grundläggande rättigheterna. I detta sammanhang anges det att ”I de fall en effektiv brottsbekämpning i EU underlättas av informationsutbyte, är det också av största vikt att skydda människors privatliv och deras grundläggande rätt till skydd för sina personuppgifter”.

20. Detta är ett välkommet påpekande. Det kan dock inte i sig anses räcka för att täcka in uppgiftsskyddet i strategin för den inre säkerheten. Meddelandet innehåller inte någon närmare diskussion av uppgiftsskyddet ([11]) och förklarar inte heller hur respekten för integriteten och skyddet av personuppgifter kommer att garanteras i praktiken i samband med åtgärderna för att genomföra strategin för den inre säkerheten.

([8]) Europeiska datatillsynsmannens yttrande av den 30 september 2010 om kommissionens meddelande till Europaparlamentet och rådet – ”Översikt av informationshanteringen inom området med frihet, säkerhet och rättvisa”.

([9]) Detta är ett rättsligt krav, se särskilt domstolens dom i de förenade målen C-92/09 och C-93/09 av den 2 november 2010. I mer specifika sammanhang har Europeiska datatillsynsmannen också förespråkat denna strategi i andra yttranden om lagförslag med anknytning till området med frihet, säkerhet och rättvisa: t.ex. yttrandet av den 19 oktober 2005 om tre förslag om andra generationen av Schengens informationssystem (SIS II), yttrandet av den 20 december 2007 om utkastet till förslag till rådets rambeslut om användande av passageraruppgifter (PNR-uppgifter) i brottsbekämpningssyfte, yttrandet av den 18 februari 2009 om förslaget till en förordning om inrättande av Eurodac för jämförelse av fingeravtryck för en effektiv tillämpning av förordning (EG) nr […/…](om kriterier och mekanismer för att avgöra vilken medlemsstat som har ansvaret för att pröva en ansökan om internationellt skydd som en tredjelandsmedborgare eller en statslös person har gett in i någon medlemsstat), yttrandet av den 18 februari 2009 om förslag till en förordning om inrättande av kriterier och mekanismer för att avgöra vilken medlemsstat som har ansvaret för att pröva en ansökan om internationellt skydd som en tredjelandsmedborgare eller en statslös person har gett in i någon medlemsstat och yttrandet av den 7 oktober 2009 förslag gällande tillgång till Eurodac i brottsförebyggande syfte.

([10]) Europaparlamentets och rådets direktiv 2006/24/EG av den 15 mars 2006 om lagring av uppgifter som genererats eller behandlats i samband med tillhandahållande av allmänt tillgängliga elektroniska kommunikationstjänster eller allmänna kommunikationsnät och om ändring av direktiv 2002/58/EG, (EUT L 105, 13.4.2006, s. 54).

([11]) Uppgiftsskydd nämns bara närmare när det gäller behandling av personuppgifter inom Frontex.

21. Enligt Europeiska datatillsynsmannens bör ett mål för *strategin för den inre säkerheten i praktiken* vara en vid tolkning av skyddet som bör säkra *rätt* balans mellan å ena sidan skyddet av medborgarna mot befintliga hot och å andra sidan skyddet av deras integritet och rätten till skydd av personuppgifter. Med andra ord måste man ta lika allvarligt på säkerhets- som på integritetsfrågor vid utveckling av strategin för den inre säkerheten, vilket skulle vara i linje med Stockholmsprogrammet och rådets slutsatser.

22. Sammanfattningsvis bör tillhandahållande av säkerhet med full respekt för integritet och uppgiftsskydd nämnas som ett specifikt mål för EU:s strategi för den inre säkerheten. Detta bör avspeglas i samband med alla åtgärder som vidtas av medlemsstaterna och EU:s institutioner när strategin genomförs.

23. I detta sammanhang hänvisar Europeiska datatillsynsmannen till meddelandet 2010(609) om ett samlat grepp på skyddet av personuppgifter i Europeiska unionen ([12]). Datatillsynsmannen kommer snart att utfärda ett yttrande om detta meddelande men betonar här att en effektiv strategi för den inre säkerheten inte kan införas utan stöd av ett pålitligt system för uppgiftsskydd som komplement till strategin som ger ömsesidigt förtroende och förbättrar strategins effekt.

III. BEGREPP SOM ÄR TILLÄMPLIGA PÅ UTFORMNING OCH GENOMFÖRANDE AV STRATEGIN FÖR DEN INRE SÄKERHETEN

24. Det står klart att vissa av de åtgärder som kan härledas från målen för strategin för den inre säkerheten kan äventyra enskildas integritet och skyddet av personuppgifter. För att motverka dessa risker vill datatillsynsmannen särskilt fästa uppmärksamheten på begrepp som *inbyggda säkerhetsmekanismer, konsekvensanalys av inverkan på integritets- och uppgiftsskydd, de registrerades rättigheter* och *bästa tillgängliga tekniker*. Hänsyn bör tas till alla dessa begrepp vid genomförandet av strategin för den inre säkerheten och de kan bidra till en mer integritetsvänlig och uppgiftsskyddsorienterad politik inom detta område.

Inbyggda säkerhetsmekanismer

25. Europeiska datatillsynsmannen har vid olika tillfällen och i olika yttranden förespråkat inbyggda säkerhetsmekanismer (eller förvalda inställningar för sekretess). Begreppet utvecklas för närvarande både för den privata den offentliga sektorn och måste därför spela en viktig roll i samband med EU:s inre säkerhet och det polisära och rättsliga området ([13]).

26. Begreppet nämns inte i meddelandet. Datatillsynsmannen föreslår att man hänvisar till detta begrepp i samband med de åtgärder som ska förelås och vidtas i samband med att strategin för den inre säkerheten genomförs, särskilt när det gäller mål 4, ”Stärka säkerheten genom gränsförvaltning”, där ökad användning av ny teknik för gränskontroller och gränsövervakning uttryckligen tas upp.

Konsekvensanalys av inverkan på integritets- och uppgiftsskydd

27. Europeiska datatillsynsmannen uppmuntrar kommissionen att som en del av det framtida arbetet med utformning och genomförande av strategin för den inre säkerheten utifrån meddelandet reflektera över vad en *konsekvensanalys av inverkan på integritets- och uppgiftsskydd* verkligen innebär i området med frihet, säkerhet och rättvisa, särskilt när det gäller strategin för den inre säkerheten.

28. Meddelandet hänvisar till hot- och riskbedömning. Detta är välkommet. Men meddelandet hänvisar inte i någon punkt till en konsekvensanalys av inverkan på integritets- och uppgiftsskydd. Europeiska datatillsynsmannen tror att arbetet med meddelandet om strategin för den inre säkerheten är ett lämpligt tillfälle att göra sådana konsekvensanalyser av inverkan på integritets- och uppgiftsskyddet inom ramen för den inre säkerheten. Datatillsynsmannen noterar att varken meddelandet eller kommissionens riktlinjer för konsekvensanalyser ([14]) tar upp denna aspekt och utvecklar den till ett policykrav.

29. Datatillsynsmannen rekommenderar att framtida instrument genomför en mer specifik och noggrann konsekvensanalys av inverkan på integritet och uppgiftsskydd, antingen som en separat bedömning eller som en del av den allmänna konsekvensbedömning som kommissionen genomför när det gäller de grundläggande rättigheterna. Denna konsekvensanalys bör inte bara ta upp allmänna principer eller analysera policyalternativ, såsom fallet är i dagsläget, utan bör också rekommendera specifika och konkreta uppgiftsskyddsgarantier.

30. Därför bör särskilda indikatorer och funktioner utvecklas för att se till att varje förslag som inverkar på integritets- och uppgiftsskyddet inom området EU:s inre säkerhet blir föremål för noggrant övervägande, bland annat när det gäller aspekter som proportionalitetsprincipen, nödvändighetsprincipen och principen om ändamålsbegränsning.

31. Det skulle dessutom vara till hjälp i sammanhanget att hänvisa till artikel 4 i RFID-rekommendationen ([15]), där kommissionen uppmanade medlemsstaterna att se till att branschen, i samarbete med lämpliga aktörer från det civila

([12]) Kommissionens meddelande till Europaparlamentet, rådet, Europeiska ekonomiska och sociala kommittén och Regionkommittén om ett samlat grepp på skyddet av personuppgifter i Europeiska unionen, KOM (2010) 609 slutlig.

([13]) I sitt yttrande om kommissionens meddelande om Stockholmsprogrammet rekommenderar Europeiska datatillsynsmannen att det ska finnas en juridisk skyldighet för dem som bygger upp och använder informationssystem att utveckla och använda system som överensstämmer med principen *Inbyggda säkerhetsmekanismer.*

([14]) SEK(2009) 92, 15.1.2009.

([15]) C(2009) 3200 slutlig, 12.5.2009.

samhället, utarbetar en ram för konsekvensanalyser av inverkan på integritets- och uppgiftsskydd. Vidare uppmuntrade Madridresolutionen, som antogs i november 2009 av den internationella konferensen för dataskyddskommissionärer, genomförandet av PIA innan nya informationssystem och -tekniker för behandling av personuppgifter eller omfattande ändringar av befintliga behandlingar införs.

Rättigheter för registrerade personer

32. Europeiska datatillsynsmannen noterar att meddelandet inte specifikt tar upp frågan om rättigheter för registrerade personer, som utgör ett mycket viktigt inslag i uppgiftsskyddet och bör inverka på utformningen av strategin för den inre säkerheten. Det är mycket viktigt att se till att medborgarna inom alla olika system och instrument som hanterar EU:s inre säkerhet omfattas av liknande rättigheter när det gäller hur deras personuppgifter hanteras.

33. Många av de system som meddelandet hänvisar till fastställer särskilda regler för rättigheterna för registrerade personer (som även omfattar kategorier som brottsoffer, misstänkta brottslingar eller migranter), men det finns många variationer mellan system och instrument, utan att det finns goda skäl till detta.

34. Europeiska datatillsynsmannen uppmanar därför kommissionen att under den närmaste framtiden titta mer noggrant på frågan om att anpassa rättigheterna för registrerade personer när det gäller EU:s strategi för den inre säkerheten och strategi för informationshantering.

35. Särskild uppmärksamhet bör ägnas åt mekanismer för rättslig prövning. Strategin för den inre säkerheten bör garantera att registeransvariga alltid tillhandahåller lättillgängliga och effektiva förfaranden för klagomål till överkomlig kostnad i de fall då enskildas rättigheter inte har respekterats fullt ut.

Bästa tillgängliga tekniker

36. Genomförandet av strategin för den inre säkerheten kommer oundvikligen att bygga på användning av en it-infrastruktur som stödjer de åtgärder som beskrivs i meddelandet. Bästa tillgängliga tekniker kan ses som förutsättningar för en lämplig balans mellan uppnående av målen för strategin för den inre säkerheten och respekten för enskildas rättigheter. I det aktuella sammanhanget vill Europeiska datatillsynsmannen upprepa sin rekommendation från tidigare yttranden ([16]) om att kommissionen tillsammans med intressenterna inom industrin bör definiera och främja åtgärder för tillämpning av bästa tillgängliga tekniker. En sådan tillämpning innebär det mest effektiva och mest avancerade skedet i utvecklingen av åtgärder och deras funktionssätt, som anger en viss tekniks praktiska lämplighet att i princip ligga till grund för att tillämpningar och system för informationsteknik och datasäkerhet och iakttar kraven på personlig integritet, dataskydd och säkerhet i EU:s regelverk. Detta tillvägagångssätt är helt i linje med begreppet *inbyggda säkerhetsmekanismer*, som tas upp ovan.

37. Där det är relevant och genomförbart bör referensdokument om bästa tillgängliga tekniker utarbetas för att ge vägledning och bättre rättslig förutsebarhet för det praktiska genomförandet av åtgärder inom ramen för strategin för den inre säkerheten. Detta kan dessutom främja harmonisering av sådana åtgärder mellan olika medlemsstater. Sist men inte minst kommer definition av bästa tillgängliga tekniker som ger hög integritet och säkerhet att underlätta datatillsynsmyndigheternas övervakande roll genom att ge dem tillgång till tekniska referenser som uppfyller integritets- och uppgiftsskyddskraven och som kan antas av registeransvariga.

38. Europeiska datatillsynsmannen noterar även vikten av en korrekt anpassning av strategin för den inre säkerheten till åtgärder som redan genomförs inom sjunde ramprogrammet för forskning och teknisk utveckling och programmet om säkerhet och skydd av friheter. En gemensam vision för att tillhandahålla bästa tillgängliga tekniker kan ligga till grund för ett innovativt tillvägagångssätt när det gäller kunskaper och kapaciteter som krävs för att skydda medborgarna och samtidigt respektera deras grundläggande rättigheter.

39. Slutligen pekar datatillsynsmannen på den roll som Europeiska byrån för nät- och informationssäkerhet (Enisa) kan spela när det gäller att utarbeta riktlinjer och bedöma vilken säkerhetskompetens som krävs för att säkra it-systems integritet och tillgänglighet och även när det gäller att främja bästa tillgängliga tekniker. Här välkomnar datatillsynsmannen att byrån inkluderas som en nyckelaktör vid förbättringen av kompetensen för att hantera Internetangrepp och bekämpa it-brottslighet ([17]).

Förtydligande när det gäller aktörerna och deras roller

40. I detta sammanhang krävs dessutom ett ytterligare förtydligande när det gäller vilka aktörer som utgör en del av eller bidrar till arkitekturen för strategin för den inre säkerheten. Meddelandet hänvisar till olika aktörer och intressenter

([16]) Datatillsynsmannens yttrande om intelligenta transportsystem, juli 2009; Datatillsynsmannens yttrande om RFID-kommunikation, december 2007; Datatillsynsmannens årsrapport 2006, s. 48.

([17]) Europeiska datatillsynsmannen planerar fortfarande att anta ett yttrande om den rättsliga ramen för Enisa i december 2010.

såsom medborgare, domstolar, EU-byråer, nationella myndigheter, polisväsende och företag. Dessa aktörers olika roller och kompetenser bör behandlas mer ingående när det gäller de särskilda åtgärder som föreslås för genomförandet av strategin för den inre säkerheten.

IV. SÄRSKILDA SYNPUNKTER NÄR DET GÄLLER POLITIKOMRÅDEN MED ANKNYTNING TILL STRATEGIN FÖR DEN INRE SÄKERHETEN

Integrerad gränsförvaltning

41. Meddelandet hänvisar till att EU sedan Lissabonfördraget trädde i kraft står bättre rustat att utnyttja synergier mellan gränsförvaltningsstrategier för personer och varor. När det gäller rörlighet för personer nämns det i meddelandet att ”EU kan behandla migrationshantering och brottsbekämpning som två parallella mål i den integrerade strategin för gränsförvaltning”. Gränsförvaltningen beskrivs i meddelandet som en potentiellt kraftfull metod för att störa grov och organiserad brottslighet ([18]).

42. Europeiska datatillsynsmannen noterar också att meddelande identifierar tre strategiska förutsättningar: 1) en förbättrad användning av ny teknik för gränskontroller (den andra generationen av Schengens informationssystem (SIS II), informationssystemet för viseringar (VIS), systemet för inresa och utresa samt programmet för registrerade resenärer), 2) en förbättrad användning av ny teknik för gränsövervakning (Europeiska gränsövervakningssystemet, Eurosur) och 3) en förbättrad samordning mellan medlemsstaterna genom Frontex.

43. Europeiska datatillsynsmannen vill i detta yttrande ta tillfället i akt att påminna om sina önskemål från ett antal tidigare yttranden om att en tydlig policy för gränsförvaltning – som fullt ut respekterar bestämmelserna för uppgiftsskydd – fastställs på EU-nivå. Datatillsynsmannen tror att det nuvarande arbetet med strategin för den inre säkerheten och för informationshantering innebär mycket goda möjligheter att ta mer konkreta steg mot en samordnad politisk strategi inom dessa områden.

44. Europeiska datatillsynsmannen noterar att meddelandet inte bara hänvisar till befintliga stora system och dem som kan tas i drift inom den närmaste framtiden (såsom SIS, SIS II och VIS) utan – i samma textavsnitt – även tar upp system som kan komma att föreslås av kommissionen i framtiden men om vilka beslut ännu inte har fattats (dvs. programmet för registrerade resenärer (RTP) och systemet för inresa och utresa). Man bör i detta sammanhang komma ihåg att målen och legitimiteten för att införa dessa system fortfarande behöver klargöras och visas, även i ljuset av särskilda konsekvensbedömningar som genomförs av kommissionen. Om detta inte sker kan meddelandet tolkas som att det föregriper beslutsprocessen och därmed att ingen hänsyn tas till att det slutliga beslutet om huruvida RTP och systemet för inresa och utresa ska införas i EU ännu inte har fattats.

45. Europeiska datatillsynsmannen föreslår därför att sådana föregripanden undviks vid det framtida arbetet med att genomföra strategin för den inre säkerheten. Såsom nämnts tidigare bör inga beslut om införande av nya stora system som angriper privatlivet fattas förrän en rimlig utvärdering av alla befintliga system har genomförts, med vederbörlig hänsyn till nödvändighet och proportionalitet.

EUROSUR

46. I meddelandet nämns det att kommissionen kommer att lägga fram ett lagförslag om inrättande av Eurosur under 2011, i syfte att bidra till den inre säkerheten och brottsbekämpningen. Det nämns också att Eurosur kommer att dra nytta av ny teknik som utvecklats genom EU-finansierade forskningsprojekt och forskningsverksamheter, såsom satellitbilder som gör det möjligt att upptäcka och följa mål vid sjögränsen.

47. I detta sammanhang noterar Europeiska datatillsynsmannen att det inte är klart huruvida och i så fall i vilken omfattning det lagstiftningsförslag om Eurosur som kommer att presenteras av kommissionen 2011 även kommer att innefatta behandling av personuppgifter inom ramen för Eurosur. Kommissionen tar inte klar ställning till detta i meddelandet. Frågan är desto mer relevant med tanke på att det i meddelandet görs tydliga kopplingar mellan Eurosur och Frontex på taktisk, operativ och strategisk nivå (se synpunkterna nedan om Frontex) och att ett nära samarbete mellan de båda efterfrågas.

Behandling av personuppgifter inom FRONTEX

48. Den 17 maj 2010 utfärdade Europeiska datatillsynsmannen ett yttrande om Frontexförordningen ([19]). I yttrandet efterfrågade datatillsynsmannen en verklig debatt och en djupgående reflektion om uppgiftsskyddet i samband med att befintliga arbetsuppgifter för Frontex utökas och nya arbetsuppgifter tillkommer.

49. Meddelandet hänvisar till behovet av att öka Frontex bidrag vid de yttre gränserna i samband med Mål 4, ”Stärka säkerheten genom gränsförvaltning”. I detta sammanhang nämns det i meddelandet att kommissionen utifrån tidigare erfarenheter och mot bakgrund av EU:s övergripande strategi för informationshantering anser att åtgärder som gör

([18]) Press release on the EU Internal Security Strategy in Action – five steps towards a more secure Europe Memo 10/598 (på engelska).

([19]) Yttrande från Europeiska datatillsynsmannen av den 17 maj 2010 över förslaget till Europaparlamentets och rådets förordning om ändring av rådets förordning (EG) nr 2007/2004 om inrättande av en europeisk byrå för förvaltningen av det operativa samarbetet vid Europeiska unionens medlemsstaters yttre gränser (Frontex).

det möjligt för Frontex att behandla och använda denna information för vissa begränsade ändamål och i enlighet med tydligt fastställda regler för behandling av personuppgifter skulle vara till stor hjälp för att spränga kriminella organisationer. Detta är ett nytt tillvägagångssätt jämfört med kommissionens förslag om en översyn av Frontexförordningen, som för närvarande är föremål för diskussion i Europaparlamentet och rådet, där inget nämns om behandling av personuppgifter.

50. Mot denna bakgrund välkomnar Europeiska datatillsynsmannen att meddelandet ger en viss indikation om under vilka omständigheter sådan behandling kan visa sig vara nödvändig (t.ex. riskanalys, effektivare genomförande av gemensamma insatser eller utbyte av information med Europol). Närmare bestämt förklarar meddelandet att information om kriminella som är involverade i nätverk för människohandel som Frontex kommer i kontakt med i sin verksamhet för närvarande inte kan användas för riskanalyser eller för att utforma framtida gemensamma insatser på ett bättre sätt. Vidare når uppgifterna om misstänkta brottslingar aldrig fram till de behöriga nationella myndigheterna eller Europol för vidare utredning.

51. Europeiska datatillsynsmannen noterar dock att meddelandet inte hänvisar till den pågående diskussionen om översyn av den rättsliga ramen för Frontex, som såsom nämnts tidigare tar upp denna fråga för att hitta lagstiftningslösningar. Vidare kan meddelandets ordalydelse om Frontex roll när det gäller målet att bryta ner kriminella nätverk tolkas så att Frontex mandat utökas. Europeiska datatillsynsmannen föreslår att hänsyn tas till denna punkt både vid översynen av Frontexförordningen och vid genomförandet av strategin för den inre säkerheten.

52. Europeiska datatillsynsmannen vill dessutom fästa uppmärksamheten på att man bör se till att undvika dubblering av arbetsuppgifter mellan Europol och Frontex. I detta sammanhang välkomnar Datatillsynsmannen att meddelandet tar upp att dubbelarbete mellan Frontex och Europol ska undvikas. Denna fråga skulle dock även kunna behandlas mer utförligt både i den ändrade Frontexförordningen och i samband med de åtgärder för att genomföra strategin för den inre säkerheten som innebär ett nära samarbete mellan Frontex och Europol. Detta är särskilt viktigt när det gäller principen om ändamålsbegränsning och principen om uppgifters kvalitet. Denna anmärkning gäller även det framtida samarbetet med sådana organ som Europeiska byrån för nät- och informationssäkerhet (Enisa) eller Europeiska byrån för samarbete i asylfrågor (EASO).

Användning av biometriska kännetecken

53. Meddelandet tar inte särskilt upp det aktuella fenomenet med ökad användning av biometriska kännetecken inom området med frihet, säkerhet och rättvisa, inklusive stora it-system i EU och andra verktyg för gränsförvaltning.

54. Därför tar Europeiska datatillsynsmannen tillfället i akt att påminna om sitt förslag ([20]) att denna fråga, som är mycket känslig ur uppgiftsskyddsperspektiv, behandlas med stort allvar vid genomförandet av strategin för den inre säkerheten, särskilt i samband med gränsförvaltningen.

55. Europeiska datatillsynsmannen rekommenderar också en tydlig och strikt politik för användning av biometriska kännetecken inom området med frihet, säkerhet och rättvisa, baserad på en seriös utvärdering och en bedömning från fall till fall av behovet av att använda biometriska kännetecken inom ramen för strategin för den inre säkerheten, med full respekt för sådana grundläggande principer för uppgiftsskydd som proportionalitet, nödvändighet och begränsning av ändamålet.

TFTP

56. Det anges i meddelandet att kommissionen 2011 kommer att utarbeta en strategi som gör det möjligt för EU att ta fram och analysera uppgifter om finansiella meddelanden som lagras inom EU:s eget territorium. I detta sammanhang hänvisar Europeiska datatillsynsmannen till sitt yttrande av den 22 juni 2010 om behandling och överföring av uppgifter om finansiella betalningsmeddelanden från Europeiska unionen till Förenta staterna i enlighet med programmet för att spåra finansiering av terrorism (TFTP II) ([21]). Alla kritiska synpunkter i det yttrandet är i lika måtto giltiga för och tillämpliga på det planerade arbetet med en EU-ram för finansiella betalningsmeddelanden. Därför bör hänsyn tas till synpunkterna vid diskussioner om denna fråga. Särskild uppmärksamhet bör ägnas åt proportionaliteten i att ta fram och behandla stora mängder uppgifter om personer som inte är misstänkta, och om frågan om effektiv rättslig tillsyn från oberoende myndigheters och rättsväsendets sida.

It-säkerhet för medborgare och företag

57. Europeiska datatillsynsmannen välkomnar den vikt meddelandet fäster vid förebyggande åtgärder på EU-nivå och anser att en förstärkt säkerhet för it-nätverk är en nödvändig faktor för att bidra till ett välfungerande informationssamhälle. Datatillsynsmannen stödjer också de särskilda åtgärderna för att förbättra förmågan att möta it-attacker, bygga upp kapaciteten hos organ inom brottsbekämpning och rättsväsende samt skapa samarbeten med industrin för att stödja medborgare och företag. Dessutom är det välkommet med Enisas stödjande roll för de åtgärder som föreskrivs för att uppnå detta mål.

([20]) Se särskilt Europeiska datatillsynsmannens yttrande om meddelandet om översikt av informationshanteringen inom området med frihet, säkerhet och rättvisa som nämns i fotnot 8.

([21]) Europeiska datatillsynsmannens yttrande av den 22 juni 2010 om förslag till rådets beslut om ingående av avtalet mellan Europeiska unionen och Amerikans förenta stater om behandling och överföring av uppgifter om finansiella betalningsmeddelanden från Europeiska unionen till Förenta staterna i enlighet med programmet för att spåra finansiering av terrorism (TFTP II).

58. Däremot beskriver meddelandet om strategin för den inre säkerheten i EU i praktiken inte vilka brottsbekämpningsåtgärder som ska sättas in mot it-brottslighet, hur dessa åtgärder kan äventyra enskildas rättigheter och vilka uppgiftsskyddsgarantier som skulle krävas. Europeiska datatillsynsmannen efterfrågar en mer ambitiös strategi för tillräckliga garantier. Denna strategi bör utarbetas för att skydda alla enskildas grundläggande rättigheter, inklusive de som kan påverkas av åtgärder som är avsedda att motverka eventuell brottslig verksamhet inom detta område.

V. **SLUTSATSER OCH REKOMMENDATIONER**

59. Europeiska datatillsynsmannen efterfrågar en koppling mellan olika EU-strategier och meddelanden i samband med genomförandet av strategin för den inre säkerheten. Detta tillvägagångssätt bör följas av en konkret handlingsplan som stöds av en konkret bedömning av behoven och vars resultat bör vara en övergripande, integrerad och välstrukturerad EU-policy för strategin för den inre säkerheten.

60. Europeiska datatillsynsmannen tar också detta tillfälle i akt att betona vikten av ett rättsligt krav på en konkret bedömning av alla befintliga instrument som ska användas inom ramen för strategin för den inre säkerheten och informationsutbytet innan nya instrument föreslås. I detta sammanhang rekommenderar datatillsynsmannen starkt bestämmelser som kräver regelbundna bedömningar av relevanta instruments effektivitet.

61. Europeiska datatillsynsmannen föreslår att man vid utarbetande av den fleråriga strategiska plan som efterfrågas i rådets slutsatser från den 10 november 2010 tar hänsyn till det pågående arbetet med en övergripande ram för uppgiftsskydd utifrån artikel 16 i EUF-fördraget, särskilt meddelande 2009 (609).

62. Europeiska datatillsynsmannen kommer med ett antal förslag om begrepp som är relevanta ur ett uppgiftsskyddsperspektiv och till vilka hänsyn bör tas när det gäller strategin för den inre säkerheten, t.ex. inbyggda säkerhetsmekanismer, konsekvensanalys av inverkan på integritet och uppgiftsskydd och bästa tillgängliga tekniker.

63. Europeiska datatillsynsmannen rekommenderar att framtida instrument genomför en konsekvensanalys av inverkan på integritet och uppgiftsskydd, antingen som en separat bedömning eller som en del av den allmänna konsekvensbedömning som kommissionen genomför när det gäller de grundläggande rättigheterna.

64. Han uppmanar också kommissionen att utarbeta en mer enhetlig och konsekvent politik när det gäller kraven för användning av biometriska kännetecken samt större likriktning på EU-nivå när det gäller rättigheter för registrerade personer.

65. Slutligen lägger Europeiska datatillsynsmannen fram ett antal synpunkter på behandlingen av personuppgifter inom ramen för gränsförvaltning, särskilt när det gäller Frontex och eventuellt i samband med Eurosur.

Utfärdat i Bryssel den 17 december 2010.

Peter HUSTINX

Europeiska datatillsynsmannen