Yttrande från Europeiska datatillsynsmannen om kommissionens meddelande till Europaparlamentet och rådet om ett område med frihet, säkerhet och rättvisa i allmänhetens tjänst

(2009/C 276/02)

EUROPEISKA DATATILLSYNSMANNEN HAR ANTAGIT DETTA YTTRANDE

med beaktande av fördraget om upprättandet av Europeiska gemenskapen, särskilt artikel 286,

med beaktande av Europeiska unionens stadga om de mänskliga rättigheterna, särskilt artikel 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,

med beaktande 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, särskilt artikel 41.

HÄRIGENOM FRAMFÖRS FÖLJANDE.

I. INLEDNING

1. Den 10 juni 2009 antog kommissionen meddelandet till Europaparlamentet och rådet om ett område med frihet, säkerhet och rättvisa i allmänhetens tjänst ([1]). Datatillsynsmannen lämnar detta yttrande i enlighet med artikel 41 i förordning (EG) nr 45/2001.

2. Genom en skrivelse av den 19 maj 2009 hörde kommissionen informellt datatillsynsmannen om meddelandet innan det antogs. Därefter skickade datatillsynsmannen den 20 maj 2009 några informella synpunkter för att ytterligare förbättra texten till meddelandet. Datatillsynsmannen har dessutom aktivt bidragit till en skrivelse av den 14 januari 2009 från arbetsgruppen för polisiära och rättsliga frågor om det fleråriga programmet på området frihet, säkerhet och rättvisa ([2]).

3. I meddelandet (punkt 1) betonas det att unionen behöver ett nytt fleårigt program som bygger på de framsteg som hittills gjorts och erfarenheterna av de kvarstående bristerna för att ambitiöst kunna gå vidare. I det nya programmet bör prioriteringarna för de kommande fem åren fastställas. Detta fleråriga program (redan är känt som ”Stockholmsprogrammet”) kommer att utgöra uppföljningen av Tammerfors- och Haagprogrammen som gav viktiga politiska impulser till området med frihet, säkerhet och rättvisa.

4. Meddelandet är avsett att utgöra grunden för detta nya fleråriga program. Datatillsynsmannen noterar i detta sammanhang att även om fleråriga program i sig inte är några bindande instrument har de en betydande inverkan på den politik som institutioner kommer att utveckla på det berörda området, eftersom många av de konkreta, lagstiftande och icke lagstiftande åtgärderna kommer att grundas på programmet.

5. Även själva meddelandet måste betraktas ur detta perspektiv. Det utgör nästa steg i en debatt som i stort sett inleddes genom två rapporter som lades fram i juni 2008 av de ”framtidsgrupper” som rådets ordförandeskap inrättade i syfte att tillhandahålla idéer: Frihet, säkerhet och personlig integritet – europeiska inrikes frågor i en öppen värld ([3]) och Förslag till lösningar för EU:s framtida program för rättsliga frågor ([4]).

II. HUVUDDRAGEN I YTTRANDET

6. Detta yttrande är inte bara en reaktion på meddelandet utan är också ett bidrag från datatillsynsmannen till diskussionerna i allmänhet om framtiden för området med frihet, säkerhet och rättvisa, vilka måste leda fram till ett nytt strategiskt arbetsprogram (Stockholmsprogrammet) i enlighet med vad det svenska ordförandeskapet för EU meddelat ([5]). I det här yttrande kommer också några av konsekvenserna av ett eventuellt ikraftträdande av Lissabonfördraget att tas upp.

7. I del III anges de viktigaste aspekterna i yttrandet och i del IV görs en allmän bedömning av meddelandet.

8. I del V behandlas frågan hur man ska bemöta behovet av att upprätthålla respekt för skyddet av personlig integritet och personuppgifter i samband med ett allt större utbyte av personuppgifter. Tonvikten kommer att ligga på punkt 2.3 i meddelandet, *Skydd av* personuppgifter och privatliv, och mer allmänt, behovet av ytterligare lagstiftande åtgärder och andra åtgärder för att förbättra ramen för dataskydd.

([1]) KOM(2009) 262 slutlig (”meddelandet”).

([2]) Ej offentliggjord. Arbetsgruppen för polisiära och rättsliga frågor inrättades av de europeiska dataskyddskommissionärernas konferens för att utarbeta konferensens ståndpunkter på brottsbekämpningsområdet och för att agera på konferensens vägnar i brådskande ärenden.

([3]) Rådets dokument nr 11657/08. Nedan kallad *rapporten om inrikes frågor*.

([4]) Rådets dokument nr 11549/08 (rapporten om rättsliga frågor).

([5]) Regeringens arbetsprogram för EU, http://www.regeringen.se

9. I del VI diskuteras behovet av och möjligheterna till lagring, åtkomst och utbyte av uppgifter som instrument för brottsbekämpning eller, som det uttrycks i meddelandet, ”Ett EU som erbjuder skydd”. Punkt 4 i meddelandet innehåller ett antal mål när det gäller informationsflödet och de tekniska verktygen, särskilt punkterna 4.1.2 (Hantering av information), 4.1.3 (Införande av nödvändiga tekniska verktyg) och 4.2.3.2 (Informationssystem). Framtagandet av en europeisk informationsmodell (punkt 4.1.2) kan betraktas som det mest utmanande förslaget i detta sammanhang. Datatillsynsmannen kommer att göra en ingående analys av detta förslag.

10. Del VII berör i korthet en särskild fråga på området med frihet, säkerhet och rättvisa och som har anknytning till dataskydd, nämligen, möjligheten att få rättslig prövning och e-juridik.

III. **ASPEKTERNA I YTTRANDET**

11. Utgångspunkten för att analysera meddelandet i detta yttrande är behovet av skydd av de grundläggande rättigheterna och, mer allmänt, framtiden för området med frihet, säkerhet och rättvisa, i enlighet med det nya fleråriga programmet. Yttrandet bygger också vidare på datatillsynsmannens bidrag för att utveckla EU:s politik på detta område, huvudsakligen i rollen som rådgivare. Hittills har datatillsynsmannen antagit mer än trettio yttranden och kommentarer när det gäller initiativ som har sitt ursprung i Haagprogrammet. Samtliga yttranden återfinns på datatillsynsmannens webbplats.

12. I bedömningen av detta meddelande kommer datatillsynsmannen särskilt att beakta följande fyra aspekter som är relevanta för framtiden för området med frihet, säkerhet och rättvisa. Alla dessa aspekter har även en framträdande plats i meddelandet.

13. Den första aspekten gäller den exponentiella ökning av digital information som medborgarna kommer i kontakt med till följd av informations- och kommunikationsteknikens snabba utveckling ([6]). Samhället är på väg mot vad som ofta kallas ”övervakningssamhället” där varje transaktion och nästan varje rörelse av medborgarna kan förväntas skapa en digital notering. De så kallade ”sakernas Internet” och ”intelligent miljö” utvecklas redan snabbt med hjälp av RFID-etiketter. Digitaliserade uppgifter om människokroppen (biometri) används allt oftare. Detta leder till en allt mer sammankopplad värld där organisationer för allmän säkerhet kan få tillgång till stora mängder potentiellt användbara uppgifter som direkt kan påverka de berörda personernas liv.

14. Den andra aspekten är internationaliseringen. Dels är datautbytet i den digitala tidsåldern inte begränsat av Europeiska unionens yttre gränser, dels finns det ett ökat behov av internationellt samarbete när det gäller alla gemenskapsinsatser på området med frihet, säkerhet och rättvisa. Kampen mot terrorism, polisiärt och rättsligt samarbete, civilrätt och gränskontroll är bara några exempel.

15. Den tredje aspekten är användningen av uppgifter för brottsbekämpande ändamål. Hoten mot samhället på senare tid har, oavsett om de har anknytning till terrorism eller inte, lett till (krav på) utökade möjligheter för brottsbekämpande myndigheter att samla in, lagra och utbyta personuppgifter. I många fall deltar privata aktörer aktivt, vilket bland annat framgår av direktivet om lagring av uppgifter ([7]) och olika instrument som gäller passageraruppgifter ([8]).

16. Den fjärde aspekten är den fria rörligheten. En utveckling steg-för-steg av ett område med frihet, säkerhet och rättvisa kräver att de inre gränserna och eventuella hinder för den fria rörligheten inom området avskaffas i ännu högre grad. Under inga omständigheter bör hindren på detta område återinföras genom nya instrument. Fri rörlighet omfattar i detta sammanhang dels fri rörlighet för personer, dels fri rörlighet för (person-) uppgifter.

17. Dessa fyra aspekter visar att det sammanhang i vilket uppgifterna används förändras snabbt. I ett sådant sammanhang kan det inte råda några tvivel om vikten av en stark mekanism för att skydda medborgarnas grundläggande rättigheter, särskilt när det gäller personlig integritet och dataskydd. Det är av dessa skäl som datatillsynsmannen väljer behovet av skydd som utgångspunkt för sin analys, vilket nämns i punkt 11.

([6]) I rapporten om inrikes frågor talas det i detta sammanhang t.o.m. om en ”digital störtflod”.

([7]) 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.

([8]) Se t.ex. avtalet mellan Europeiska unionen och Amerikas förenta stater om lufttrafikföretags behandling av passageraruppgifter (PNR) och överföring av dessa till Förenta staternas Department of Homeland Security (DHS) (2007 års PNR-avtal), EUT L 204, 4.8.2007, s. 18 och förslaget till rådets rambeslut om användande av passageraruppgifter (PNR-uppgifter) i brottsbekämpningssyfte, KOM(2007) 654 slutlig.

IV. **ALLMÄN BEDÖMNING**

18. Meddelandet och Stockholmsprogrammet syftar till att ange EU:s avsikter för de kommande fem åren, med möjliga effekter på ännu längre sikt. Datatillsynsmannen noterar att meddelandet är avfattat på ett ”Lissabonneutralt” sätt. Datatillsynsmannen inser till fullo anledningen till att kommissionen valt detta tillvägagångssätt, men beklagar samtidigt att meddelandet inte till fullo utnyttjar de extra möjligheter som erbjuds genom Lissabonfördraget. Lissabonfördragets aspekter kommer att ges ökad uppmärksamhet i detta yttrande.

19. Meddelandet bygger vidare på resultaten av EU:s åtgärder på området med frihet, säkerhet och rättvisa de senaste åren. Dessa resultat kan betecknas som händelsestyrda, med betoning på åtgärder som utvidgar de brottsbekämpande myndigheternas befogenheter och som har en inkräktande verkan för medborgarna. Detta är tveklöst fallet på de områden där personuppgifter intensivt utnyttjas och utbyts och som därför har stor betydelse i fråga om dataskydd. Resultaten är händelsestyrda efter det att yttre händelser såsom 9/11 och bombdåden i Madrid och London gav starka impulser till lagstiftningsarbetet. Överföringen av passageraruppgifter till Förenta staterna kan t.ex. ses som en följd av 9/11, ([9]) medan bombdåden i London ledde till direktiv 2006/24/EG ([10]) om lagring av uppgifter. Tyngdpunkten låg på mer inkräktande åtgärder eftersom EU:s lagstiftare inriktade sig på åtgärder för att underlätta användning och utbyte av uppgifter, medan diskussionerna om åtgärder för att garantera skyddet av personuppgifter gavs lägre prioritering. De viktigaste skyddsåtgärder som antogs, efter tre års diskussioner i rådet, var rådets rambeslut 2008/977/RIF om skydd av personuppgifter som behandlas inom ramen för polissamarbete och straffrättsligt samarbete ([11]). Resultatet var ett rambeslut från rådet som inte är helt tillfredsställande (se punkterna 29–30).

20. De senaste årens erfarenheter har visat att det, innan nya instrument antas, finns ett behov av att överväga konsekvenserna för de brottsbekämpande myndigheterna och för de europeiska medborgarna. När dessa övervägs bör vederbörlig hänsyn tas till kostnaderna för den personliga integriteten och brottsbekämpningens effektivitet, i första hand när nya instrument föreslås och diskuteras men även efter det att de har genomförts genom regelbundna översyner. Det är också mycket viktigt att göra dessa överväganden innan större initiativ för den närmaste framtiden fastställs i det nya fleråriga programmet.

21. Datatillsynsmannen välkomnar att skyddet av de grundläggande rättigheterna, särskilt skyddet av personuppgifter, erkänns i meddelandet som en av de viktigaste frågorna i framtiden för området med frihet, säkerhet och rättvisa. I punkt 2 i meddelandet beskrivs EU som ett unikt område för skyddet av grundläggande rättigheter grundade på gemensamma värderingar. Det är också positivt att anslutningen till den europeiska konventionen om de mänskliga rättigheterna omnämns som en prioriterad fråga – t.o.m. den högst prioriterade frågan i meddelandet. Anslutningen är ett viktigt steg framåt för att säkerställa ett harmoniskt och sammanhängande system för skyddet av de grundläggande rättigheterna. Sist men inte minst har dataskydd fått en framträdande plats i meddelandet.

22. Att meddelandet fått denna inriktning visar på en stark vilja att säkerställa skyddet av medborgarnas rättigheter och – genom att göra detta – inta ett mer balanserat förhållningssätt. Regeringarna behöver lämpliga instrument för att garantera medborgarnas säkerhet, men måste i våra europeiska samhällen även till fullo respektera medborgarnas grundläggande rättigheter. För att kunna vara i allmänhetens tjänst ([12]), krävs det att Europeiska unionen upprätthåller denna jämvikt.

23. Datatillsynsmannen anser att behovet av jämvikt mycket väl beaktas i meddelandet, inbegripet behovet av skydd av personuppgifter. Det erkänns att det är nödvändigt att tyngdpunkten förskjuts. Detta är viktigt eftersom politiken på området med frihet, säkerhet och rättvisa inte bör främja utvecklingen mot ett övervakningssamhälle. Datatillsynsmannen förväntar sig att rådet intar samma förhållningssätt när det gäller Stockholmsprogrammet, däribland genom att erkänna riktlinjerna i punkt 25 nedan.

24. Detta är desto viktigare eftersom området med frihet, säkerhet och rättvisa är ett område som inverkar på medborgarnas situation i livet, särskilt den privata sfären av eget ansvar och personlig och social trygghet vilka skyddas genom de grundläggande rättigheterna, något som helt nyligen betonades av den tyska författningsdomstolen i domen av den 30 juni 2009 om Lissabonfördraget ([13]).

([9]) Avtalet från 2007 om passageraruppgifter omnämns i föregående och tidigare fotnoter.

([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. Även om den rättsliga grunden är artikel 95 i EG-fördraget var direktivet en omedelbar reaktion på bombdåden i London.

([11]) Rådets rambeslut 2008/977/RIF av den 27 november 2008 om skydd av personuppgifter som behandlas inom ramen för polissamarbete och straffrättsligt samarbete, EUT L 350, 30.12.2008, s. 60.

([12]) Se meddelandets titel.

([13]) Se den tyska federala författningsdomstolens pressmeddelande nr 72/2009 av den 30 juni 2009, punkt 2 c.

25. Datatillsynsmannen understryker att på ett sådant område

— bör utbytet av uppgifter mellan medlemsstaternas myndigheter, däribland, när så är lämpligt, europeiska organ eller databaser, genomförs med hjälp av lämpliga och effektiva mekanismer som till fullo respekterar de grundläggande rättigheterna för medborgarna och skapar ömsesidigt förtroende.

— Detta kräver inte bara tillgång till uppgifter i kombination med ömsesidigt erkännande av rättssystemen i medlemsstaterna (och EU), utan även en harmonisering av dataskyddsnormer till exempel, men inte uteslutande, genom en gemensam ram för dataskydd.

— Dessa gemensamma normer bör inte endast vara tillämpliga på situationer med gränsöverskridande dimensioner. Ömsesidigt förtroende kan endast existera när det finns solida normer som alltid respekteras, utan någon risk för att de inte längre kommer att tillämpas när den gränsöverskridande dimensionen inte är självklar. Bortsett från detta, särskilt när det gäller hur uppgifterna utnyttjas, fungerar skillnaderna mellan ”interna” och ”gränsöverskridande” uppgifter inte i praktiken ([14]).

V. **DATASKYDDSINSTRUMENT**

V.1 **Mot ett övergripande system för uppgiftsskydd**

26. Datatillsynsmannen stöder strategin att ge dataskydd en framträdande plats i meddelandet. Många initiativ på området med frihet, säkerhet och rättvisa är beroende av att personuppgifter används och ett bra dataskydd är avgörande för att dessa initiativ ska kunna bli framgångsrika. Respekt för personlig integritet och dataskydd är inte bara en rättsligt förpliktelse som i allt större utsträckning erkänns på gemenskapsnivå utan också en fråga som är mycket viktig för medborgarna, vilket framgår av resultaten av Eurobarometer ([15]). Att begränsa tillgången till personuppgifter är dessutom viktigt i syfte att skapa förtroende för de brottsbekämpande organen.

27. Enligt punkt 2.3 i meddelandet finns det ett behov av att inrätta ett heltäckande dataskyddssystem som omfattar alla EU:s behörighetsområden ([16]). Datatillsynsmannen stöder till fullo detta mål, oberoende av ikraftträdandet av Lissabonfördraget. Datatillsynsmannen noterar också att ett sådant system inte nödvändigtvis innebär ett enda regelverk som omfattar all behandling. Enligt de gällande fördragen är möjligheterna att anta ett enda övergripande regelverk för all behandling begränsade på grund av pelarstrukturen och på grund av att skyddet av de uppgifter som behandlas av EU:s institutioner – åtminstone inom den första pelaren – omfattas av en särskild rättslig grund (artikel 286 EG). Datatillsynsmannen påpekar dock att man kan göra vissa förbättringar genom att till fullo utnyttja de möjligheter som erbjuds i de nuvarande fördragen, vilket kommissionen redan framhävde i sitt meddelande om ”Genomförandet av Haagprogrammet: framtida utveckling” ([17]). Efter ikraftträdandet av Lissabonfördraget kommer artikel 16 i EUF-fördraget att ge den nödvändiga rättsliga grunden för ett övergripande regelverk som omfattar all behandling.

28. Datatillsynsmannen noterar att det – under alla omständigheter – är avgörande att säkerställa överensstämmelse inom den rättsliga ramen för dataskydd, när så är lämpligt genom att harmonisera och konsolidera de olika rättsliga instrument som gäller på området med frihet, säkerhet och rättvisa.

Under de gällande fördragen

29. Ett första steg togs nyligen genom antagandet av rådets rambeslut 2008/977/RIF ([18]). Detta rättsliga instrument kan dock inte betraktas som någon övergripande ram, främst på grund av att dess bestämmelser inte har allmän giltighet. De gäller inte interna situationer när personuppgifterna kommer från den medlemsstat som utnyttjar dem. En sådan begränsning kommer att minska mervärdet av rådets rambeslut, såvida inte alla medlemsstater beslutar att låta den interna situationen omfattas av den nationella genomförandelagstiftningen vilket är föga sannolikt.

30. Det andra skälet till varför datatillsynsmannen anser att rådets rambeslut 2008/977/RIF i det långa loppet inte kommer att utgöra någon tillfredsställande dataskyddsram på området med frihet, säkerhet och rättvisa, är att flera viktiga bestämmelser inte överensstämmer med direktiv 95/46/EG. Ett andra steg skulle kunna tas enligt de gällande fördragen genom att utöka räckvidden och anpassa rådets rambeslut till direktiv 95/46/EG.

31. Förverkligandet av ett omfattande dataskyddssystem skulle kunna stimuleras genom att man skapar en tydlig vision på lång sikt. Denna vision skulle kunna innehålla en övergripande och konsekvent strategi för att definiera insamling och utbyte av uppgifter, utnyttjande av befintliga databaser

([14]) Datatillsynsmannen behandlar utförligt denna sista punkt i yttrandet av den 19 december 2005 om förslaget till rådets rambeslut om skydd av personuppgifter som behandlas inom ramen för polissamarbete och straffrättsligt samarbete (KOM(2005)475 slutlig), EUT C 47, 25.2.2006, s. 27, punkterna 30–32.

([15]) Dataskydd i Europeiska unionen. Medborgarnas uppfattning. Analytisk rapport, Flash Eurobarometer serie 225, januari 2008, http://www.ec.europa.eu/public_opinion/flash/fl_225_en.pdf

([16]) Se även de prioriterade frågorna i meddelandet.

([17]) KOM(2006) 331 slutlig av den 28 juni 2006.

([18]) Se fotnot 11.

och dataskyddsgarantier. I denna vision bör onödigt dubbelarbete och dubblering av instrument (och därmed behandling av personuppgifter) undvikas. Visionen bör främja en sammanhängande EU-politik på detta område samt förtroende för myndigheternas hantering av uppgifter om medborgarna. Datatillsynsmannen rekommenderar rådet att fastställa att det finns behov av en tydlig vision på lång sikt i Stockholmsprogrammet.

32. Datatillsynsmannen rekommenderar också att de åtgärder som redan har antagits på detta område liksom deras konkreta genomförande och effektivitet bör utvärderas och sättas in i sitt rätta perspektiv. I denna utvärdering bör vederbörlig hänsyn tas till kostnaderna för den personliga integriteten och brottsbekämpningens effektivitet. Om utvärderingen visar att vissa åtgärder inte leder till avsett resultat eller inte står i proportion till de ändamål som eftersträvas, bör följande åtgärder övervägas:

— I första hand, ändra eller upphäva åtgärderna om dessa inte verkar vara tillräckligt motiverade för att skapa ett konkret mervärde för de brottsbekämpande myndigheterna och för de europeiska medborgarna.

— I andra hand, utvärdera möjligheterna att förbättra tillämpningen av de befintliga åtgärderna.

— Endast i tredje hand bör nya lagstiftningsåtgärder föreslås, om det är troligt att de behövs för de planerade ändamålen. Nya instrument bör endast antas om de har ett tydligt och konkret mervärde för de brottsbekämpande myndigheterna och för de europeiska medborgarna.

Datatillsynsmannen rekommenderar att det görs en hänvisning till ett utvärderingssystem för befintliga åtgärder i Stockholmsprogrammet.

33. Sist men inte minst bör särskild tonvikt läggas på ett bättre genomförande av befintliga skyddsåtgärder, i linje med kommissionens meddelande om uppföljningen av arbetsprogrammet för ett bättre genomförande av dataskyddsdirektivet ([19]) och de förslag som lades fram av datatillsynsmannen i yttrandet om detta meddelande ([20]). Tyvärr saknar kommissionen möjlighet att inleda överträdelseförfaranden i tredje pelaren.

Enligt Lissabonfördraget

34. Lissabonfördraget ger möjlighet till en verkligt övergripande ram för dataskydd. Enligt artikel 16.2 i fördraget om Europeiska unionens funktionssätt ska rådet och Europaparlamentet fastställa bestämmelser om skydd för enskilda personer när det gäller behandling av personuppgifter hos unionens institutioner, organ och byråer och i medlemsstaterna, när dessa utövar verksamhet som omfattas av unionsrättens tillämpningsområde, samt hos privata aktörer.

35. Datatillsynsmannen har förståelse för att tyngdpunkten i meddelandet ligger på ett övergripande dataskyddssystem och att kommissionen avser att föreslå en rättslig ram som ska gälla för all behandling. Datatillsynsmannen stöder till fullo dessa avsikter som skulle öka samstämmigheten i systemet, säkerställa rättssäkerhet och därigenom förbättra skyddet. Framför allt skulle svårigheter kunna undvikas i framtiden för att dra gränsen mellan pelarna när uppgifter som samlas in inom den privata sektorn för kommersiella ändamål senare används för brottsbekämpande ändamål. Gränsen mellan pelarna återspeglar dock inte till fullo verkligheten, vilket framgår av betydelsefulla domar från domstolen när det gäller passageraruppgifter ([21]) och uppgiftslagring ([22]).

36. Datatillsynsmannen föreslår att motiveringen för ett övergripande dataskyddssystem ska ges en framträdande plats i Stockholmsprogrammet. Det skulle visa att ett sådant system inte bara är något önskvärt utan också en nödvändighet på grund av ändrad praxis i användningen av uppgifterna. Datatillsynsmannen rekommenderar även att behovet av en ny rättslig ram, för att bland annat ersätta rådets rambeslut 2008/977/RIF, prioriteras i Stockholmsprogrammet.

37. Datatillsynsmannen betonar att ett övergripande dataskyddssystem på grundval av en allmän rättslig ram inte utesluter att det antas ytterligare dataskyddsbestämmelser för polisen och rättsväsendet. I dessa tilläggsbestämmelser skulle man kunna ta hänsyn till brottsbekämpningens särskilda behov, i enlighet med förklaring 21 som bifogas Lissabonfördraget ([23]).

V.2 **Åminnelse om dataskyddsprinciperna**

38. I meddelandet noteras de tekniska förändringar som inverkar på kommunikationen mellan enskilda och offentliga och privata organisationer. Enligt kommissionen föranleder detta en omformulering ett antal grundläggande dataskyddsprinciper.

([19]) KOM(2007) 87 slutlig av den 7 mars 2007.

([20]) Yttrande av den 25 juli 2007, EUT C 255, 27.10.2007, s. 1, särskilt punkt 30.

([21]) Domstolens dom av den 30 maj 2006 i de förenade målen C-317/04 och C-318/04, Europaparlamentet mot Europeiska unionens råd (C-317/04) och Europeiska gemenskapernas kommission (C-318/04), Reg. [2006], s. I-4721.

([22]) Domstolens dom av den 10 februari 2009 i mål C-301/06, Irland mot Europaparlamentet och Europeiska unionens råd.

([23]) Se förklaring 21 om skydd av personuppgifter på området för straffrättsligt samarbete och polissamarbete, fogad till slutakten från den regeringskonferens som antagit Lissabonfördraget, EUT C 115, 9.5.2008, s. 345.

39. Datatillsynsmannen välkomnar dessa avsikter i meddelandet. En utvärdering av principernas effektivitet mot bakgrund av de tekniska förändringarna är mycket användbar. För det första är det viktigt att notera att en omformulering och upprepning av dataskyddsprinciperna inte alltid måste ha direkt koppling till den tekniska utvecklingen. Detta kan också behövas på grund av någon annan aspekt som nämns i del III ovan, dvs. internationaliseringen, den ökade användningen av uppgifter för brottsbekämpande ändamål och den fria rörligheten.

40. Enligt datatillsynsmannen skulle denna utvärdering dessutom kunna omfattas av det offentliga samråd som kommissionen kungjorde vid konferensen ”Personuppgifter – ökad användning, bättre skydd?” den 19–20 maj 2009. Detta offentliga samråd skulle kunna ge ett värdefullt bidrag ([24]). Datatillsynsmannen föreslår att sambandet mellan avsikterna i punkt 2.3 i meddelandet och det offentliga samrådet om dataskyddet i framtiden, betonas av rådet i texten till Stockholmsprogrammet och av kommissionen i dess offentliga uttalanden om samrådet.

41. För att åskådliggöra vad som skulle kunna ingå i sådan utvärdering, nämns följande punkter:

— Personuppgifter på området med frihet, säkerhet och rättvisa kommer sannolikt att vara en särskilt känslig fråga, t.ex. uppgifter om brottmålsdomar, polisuppgifter och biometriska uppgifter såsom fingeravtryck och DNA-profiler.

— Behandlingen av dessa kan medföra negativa konsekvenser för de registrerade, särskilt när man beaktar de brottsbekämpande myndigheternas rätt att tillgripa tvångsmedel. Dataövervakningen och -analyserna blir dessutom alltmer automatiserade, ofta utan någon mänsklig inblandning. Tekniken gör det möjligt att utnyttja databaser med personuppgifter för allmänna sökningar (datautvinning, profilering etc.). De rättsliga skyldigheterna i samband med behandlingen bör tydligt fastställas.

— En hörnsten i dataskyddslagstiftningen är att personuppgifter ska samlas in för särskilda ändamål och inte får användas på ett sätt som är oförenligt med dessa ändamål. Användning för oförenliga ändamål bör endast tillåtas i den mån detta föreskrivs i lag och är nödvändigt för att uppnå specifika allmänna intressen, såsom de som fastställs i artikel 8.2 i den europeiska konventionen om skydd för de mänskliga rättigheterna och de grundläggande friheterna.

— Kravet att respektera principen om ändamålsbegränsning kan få konsekvenser för nuvarande praxis när det gäller uppgifternas användning. Uppgifter som samlats in av privata företag för kommersiella ändamål inom telekommunikations-, transport- och finanssektorn används för brottsbekämpningsändamål. Dessutom inrättas storskaliga informationssystem, till exempel i fråga om invandring och gränskontroll. Dessutom tillåts sammankopplingar mellan och åtkomst till databaser, varvid de ändamål för vilka personuppgifterna ursprungligen samlades in utvidgas. Det behövs en diskussion om de nuvarande tendenserna, däribland justeringar och/eller ytterligare skyddsåtgärder, när så krävs.

— Utöver de dataskyddsprinciper som nämns i meddelandet bör man vid utvärderingen uppmärksamma behovet av öppenhet i behandlingen, och möjligheterna för de registrerade att utöva sina rättigheter. Öppenhet är en speciellt svår fråga på brottsbekämpningsområdet, särskilt eftersom öppenhet bör vägas mot risker vid utredningar.

— Man bör finna lösningar för utbyten med tredjeland.

42. Denna utvärdering bör dessutom inriktas på möjligheterna att förbättra effektiviteten vid tillämpningen av dataskyddsprinciper. I detta sammanhang kan det vara bra att koncentrera sig på instrument som kan stärka de registeransvarigas ansvar. Instrumenten måste innebära fullständig ansvarsutkrävning av de registeransvariga för datahanteringen. ”Uppgiftsförvaltning” är ett användbart begrepp i detta sammanhang. Det omfattar alla rättsliga, tekniska och organisatoriska medel genom vilka organisationer säkerställer fullständigt ansvar för hur uppgifterna hanteras, såsom planering och kontroll, användning av sund teknik, lämplig utbildning av personal, granskning av regelefterlevnad, etc.

V.3 **Integritetsbeaktande teknik**

43. Datatillsynsmannen välkomnar att certifiering av respekt för privatlivet omnämns i punkt 2.3 i meddelandet. Utöver detta skulle man kunna hänvisa till inbyggda skyddsmekanismer för personlig integritet (”privacy by design”) och behovet av att identifiera ”bästa tillgängliga teknik” som överensstämmer med EU:s ram för dataskydd.

44. Datatillsynsmannen anser att ”privacy by design” och integritetsbeaktande teknik skulle kunna vara användbara verktyg för att uppnå ett bättre skydd och en effektivare användning av uppgifter. Datatillsynsmannen föreslår två vägar framåt, som inte utesluter varandra:

— Ett certifieringssystem för personlig integritet och dataskydd ([25]) som ett alternativ för konstruktörer och användare av informationssystem, med eller utan stöd av EU-medel eller EU-lagstiftning.

([24]) Artikel 29-gruppen, i vilken datatillsynsmannen deltar, har beslutat att arbeta intensivt med sitt bidrag till detta offentliga samråd.

([25]) Ett exempel på ett sådant system är European Privacy Seal (EuroPriSe – en europeisk integritetsmärkning).

— En lagfäst skyldighet för konstruktörer och användare av informationssystem att använda system som iakttar principen med ”privacy by design”. Detta kan komma att kräva att den nuvarande räckvidden för dataskyddslagstiftningen utvidgas för att konstruktörerna ska ta ansvar för de informationssystem de utvecklar ([26]).

Datatillsynsmannen föreslår att dessa tänkbara vägar framåt omnämns i Stockholmsprogrammet.

V.4 **Yttre aspekter**

45. En annan fråga som nämns i meddelandet är utveckling och främjande av internationella dataskyddsnormer. Det vidtas för närvarande många åtgärder för att fastställa normer som är möjliga att tillämpa internationellt, t. ex. av den internationella konferensen för ombudsmän för dataskydd och integritet. Detta kan inom kort leda till ett internationellt avtal. Datatillsynsmannen föreslår att dessa åtgärder får stöd i Stockholmsprogrammet.

46. I meddelandet nämns även ingående, på grundval av de framsteg som redan gjorts tillsammans med USA, av bilaterala avtal. Datatillsynsmannen håller med om att det behövs en tydlig rättslig ram för överföring av uppgifter till tredje land och välkomnar därför det gemensamma arbete som gjorts av myndigheterna i gemenskapen och i USA, inom kontaktgruppen på hög nivå, om ett eventuellt transatlantiskt instrument för dataskydd, men begär samtidigt ökad tydlighet och större uppmärksamhet åt specifika frågor ([27]). I detta perspektiv är det också intressant att notera idéerna i rapporten om inrikes frågor om ett euroatlantiskt samarbetsområde när det gäller frihet, säkerhet och rättvisa om vilket EU, enligt denna rapport, bör fatta beslut senast 2014. Ett sådant område skulle inte vara möjligt utan tillräckliga dataskyddsgarantier.

47. Enligt datatillsynsmannen bör de europeiska dataskyddsnormer som bygger på Europarådets konvention 108 om skydd för enskilda vid automatisk databehandling av personuppgifter ([28]) samt rättspraxis vid Europeiska gemenskapernas domstol och Europeiska domstolen för de mänskliga rättigheterna, avgöra nivån för skyddet i ett allmänt avtal med USA om dataskydd och utbyte av uppgifter. Ett sådant allmänt avtal skulle kunna utgöra grunden för särskilda arrangemang för utbyte av personuppgifter. Detta är desto viktigare med tanke på att Europeiska unionen ska ingå avtal om polissamarbete där så behövs, i enlighet med punkt 4.2.1 i meddelandet.

48. Datatillsynsmannen förstår till fullo behovet av att öka det internationella samarbetet, i vissa fall även med länder där skydd av de grundläggande rättigheterna saknas. Det är emellertid ([29]) mycket viktigt att beakta att detta internationella samarbete troligen kommer att föranleda en stor ökning av antalet insamlade och internationellt överförda uppgifter. Det är därför väsentligt att principerna om en rättvis och laglig behandling – samt principerna om ett korrekt rättsligt förfarande i allmänhet – gäller för insamling och överföring av personuppgifter över Europeiska unionens gränser, och att personuppgifter endast överförs till tredje länder eller internationella organisationer om en adekvat skyddsnivå eller lämpliga skyddsåtgärder garanteras av de berörda tredje parterna.

49. Avslutningsvis rekommenderar datatillsynsmannen att det betonas i Stockholmsprogrammet att det är viktigt att allmänna avtal med Förenta staterna och andra tredje länder om dataskydd och utbyte av uppgifter grundar sig på den skyddsnivå som garanteras inom EU:s territorium. I ett bredare perspektiv pekar datatillsynsmannen på vikten av att aktivt främja respekt för de grundläggande rättigheterna, särskilt dataskydd, i förbindelserna med tredjeländer och internationella organisationer ([30]). Den allmänna uppfattningen att utbyte av personuppgifter med tredjeländer kräver en tillräcklig skyddsnivå eller lämpliga skyddsåtgärder i dessa tredjeländer skulle också kunna nämnas i Stockholmsprogrammet.

VI. **ANVÄNDNING AV UPPGIFTER**

VI.1 **Mot en europeisk informationsmodell**

50. Bättre utbyte av uppgifter är ett viktigt politiskt mål för Europeiska unionen på området med frihet, säkerhet och rättvisa. I punkt 4.1.2 i meddelandet betonas det att säkerheten i Europeiska unionen förutsätter effektiva mekanismer för utbyte av uppgifter mellan nationella myndigheter och andra europeiska aktörer. Denna betoning av uppgiftsutbyte är logisk, i avsaknad av en europeisk polisstyrka, ett

([26]) Användare av uppgifter, liksom registeransvariga eller registerförare, omfattas av dataskyddslagstiftningen.

([27]) Se datatillsynsmannens yttrande av den 11 november 2008 om slutrapporten från EU–USA-kontaktgruppen på hög nivå för informationsutbyte, integritetsskydd och skydd av personuppgifter, EUT C 128, 6.6.2009, s. 1.

([28]) ETS nr 108, 28.1.1981.

([29]) Se datatillsynsmannens yttrande av den 28 november 2005 om kommissionens meddelande om den yttre dimensionen av området med frihet, säkerhet och rättvisa som finns tillgängligt på datatillsynsmannens webbplats.

([30]) Aktuell rättspraxis i fråga om terroristlistor bekräftar att det behövs garantier – även i förbindelserna med Förenta nationerna – för att säkerställa att åtgärderna för att bekämpa terrorism överensstämmer med EU:s normer om grundläggande rättigheter (förenade målen C-402/05 P och C-415/05 P, Kadi and Al Barakaat Foundation mot rådet, dom den 3 september 2008, ännu ej offentliggjord).

europeiskt straffrättsligt system och en europeisk gränskontroll. Åtgärder när det gäller uppgifter utgör därför viktiga bidrag från Europeiska unionen som gör det möjligt för myndigheterna i medlemsstaterna att ta itu med gränsöverskridande brottslighet på ett effektivt sätt och att effektivt skydda de yttre gränserna. De bidrar dock inte bara till medborgarnas säkerhet utan även till deras frihet – den fria rörligheten för personer nämndes tidigare som en av aspekterna av detta yttrande – och till rättvisa.

51. Det är just av dessa skäl som principen om tillgänglighet infördes i Haagprogrammet. Det medför att uppgifter som behövs för brottsbekämpningsändamål bör förmedlas över EU:s inre gränser utan hinder. De senaste erfarenheterna visar att det har varit svårt att införliva denna princip i de rättsliga åtgärderna. Kommissionens förslag till rådets rambeslut om utbyte av uppgifter enligt principen om tillgänglighet av den 12 oktober 2005 ([31]) godkändes inte av rådet. Medlemsstaterna var inte redo att acceptera konsekvenserna av principen om tillgänglighet i full utsträckning. I stället antogs mer begränsade instrument ([32]) såsom rådets beslut 2008/615/RIF av den 23 juni 2008 om ett fördjupat gränsöverskridande samarbete, särskilt för bekämpning av terrorism och gränsöverskridande brottslighet (Prümbeslutet) ([33]).

52. Även om principen om tillgänglighet utgjorde kärnan i Haagprogrammet förefaller kommissionen nu inta ett måttfullare tillvägagångssätt. Kommissionen avser att ytterligare stimulera utbytet av uppgifter mellan myndigheter i medlemsstaterna genom att införa den europeiska informationsmodellen. Det svenska ordförandeskapet för EU är inne på samma spår ([34]). Det kommer att lägga fram ett förslag till en strategi för utbyte av uppgifter. Rådet har redan inlett arbetet med detta ambitiösa projekt för en informationshanteringsstrategi för Europeiska unionen som är nära knuten till den europeiska informationsmodellen. Datatillsynsmannen noterar utvecklingen med stort intresse och understryker den vikt som dataskyddsaspekter bör ges i dessa projekt.

Den europeiska informationsmodellen och dataskydd

53. Det bör inledningsvis betonas att framtiden för området med frihet, säkerhet och rättvisa inte bör vara ”teknikdriven”, vilket innebär att de näst intill obegränsade möjligheter som erbjuds genom ny teknik alltid bör kontrolleras mot gällande dataskyddsprinciper och endast utnyttjas i den mån de överensstämmer med dessa principer.

54. Datatillsynsmannen noterar att informationsmodellen enligt meddelandet inte bara är en teknisk modell, utan dessutom har stor kapacitet till strategiska analyser och möjliggör förbättrad insamling och behandling av operativa uppgifter. Det erkänns också att politiska aspekter – som kriterier för insamling, utbyte och behandling av uppgifter – bör beaktas samtidigt som dataskyddsprinciperna iakttas.

55. Informationsteknik och rättsliga villkor är – och kommer att fortsätta att vara – väsentliga. Datatillsynsmannen välkomnar att man i meddelandet utgår från antagandet att en europeisk informationsmodell inte ska förstås på grundval av tekniska överväganden. Det är mycket viktigt att uppgifter endast samlas in, utbyts och behandlas på grundval av konkreta säkerhetsbehov och med beaktande av principerna om dataskydd. Datatillsynsmannen håller också helt med om att det måste definieras en uppföljningsmekanism för att bedöma hur utbytet av uppgifter fungerar. Han föreslår att rådet vidareutvecklar dessa inslag i Stockholmsprogrammet.

56. I detta sammanhang understryker datatillsynsmannen att dataskydd i syfte att skydda medborgarna inte bör ses som ett hinder för en effektiv datahantering. Dataskyddet tillhandahåller viktiga verktyg för att förbättra lagring, åtkomst och utbyte av information. De registrerades rättighet att informeras om vilka uppgifter om dem som har behandlats och att korrigera felaktiga uppgifter, kan också stärka uppgifternas korrekthet i systemen för datahantering.

57. Dataskyddslagstiftningen har i huvudsak följande konsekvenser: Om uppgifterna behövs för specifika och legitima ändamål får de utnyttjas. Om de inte behövs för ett väl definierat ändamål får personuppgifter inte användas. I det första fallet kan särskilda åtgärder mycket väl vidtas för att tillhandahålla lämpligt skydd.

58. Datatillsynsmannen är dock kritisk mot den utsträckning i vilken ”fastställandet av framtida behov” omnämns i meddelandet som en del av informationsmodellen. Datatillsynsmannen betonar också att principen om ändamålsbegränsning även i framtiden bör vara vägledande när informationssystem utarbetas ([35]). Den utgör en av de viktigaste garantier som dataskyddssystemet erbjuder medborgaren: Han måste i förväg veta för vilket ändamål uppgifterna om honom samlas in och att de endast kommer att utnyttjas för detta ändamål, särskilt i framtiden. Denna garanti föreskrivs t.o.m. i artikel 8 i Europeiska unionens stadga om de grundläggande rättigheterna. Principen om ändamålsbegränsning tillåter undantag – som är av särskild relevans på området med frihet, säkerhet och rättvisa – men dessa undantag bör inte vara avgörande för utformningen av ett system.

([31]) KOM(2005) 490 slutlig.

([32]) När det gäller tillgänglighetsaspekten innehåller Prümbeslutet långtgående beslut om användning av biometriska uppgifter (DNA och fingeravtryck).

([33]) EUT L 210, 6.8.2008, s. 1.

([34]) Se regeringens arbetsprogram för EU som omnämns i fotnot 5, s. 23.

([35]) Se även ovan, punkt 41.

Att välja rätt struktur

59. Att välja rätt struktur för uppgiftsutbytet är utgångspunkten för det hela. Vikten av en lämplig informationsstruktur erkänns i meddelandet (punkt 4.1.3) men tyvärr endast i samband med driftskompatibilitet.

60. Datatillsynsmannen framhåller en annan aspekt: I den europeiska informationsmodellen bör dataskyddskraven ingå i all systemutveckling och inte enbart ses som en nödvändig förutsättning för att ett system ska vara lagligt ([36]). Man bör utnyttja begreppet ”privacy by design” och fastställa ”bästa tillgängliga teknik” ([37]), vilket omnämns i punkt 43 ovan. Den europeiska informationsmodellen bör bygga på dessa begrepp. Mer konkret innebär detta att informationssystem som utformas för att tillgodose allmänna säkerhetsbehov alltid ska utformas i enlighet med principen om ”privacy by design”. Datatillsynsmannen rekommenderar rådet att ta med dessa inslag i Stockholmsprogrammet.

Systemens driftskompatibilitet

61. Datatillsynsmannen betonar att driftskompatibilitet inte enbart är en teknisk fråga utan även har konsekvenser för skyddet av medborgarna, särskilt dataskyddet. När det gäller dataskydd innebär driftskompatibilitet mellan systemen, om denna är rätt utformad, klara fördelar i och med att man undviker dubbellagring av uppgifterna. Men det är även uppenbart att det faktum att man gör tillgång till och utbyte av uppgifter tekniskt möjligt i många fall blir en stark drivkraft för att faktiskt ta del av eller utbyta dessa uppgifter. Med andra ord innebär driftskompabilitet särskilda risker i fråga om samtrafik mellan databaser som har olika ändamål ([38]). Detta kan ha konsekvenser för databasernas strikta ändamålsbegränsningar.

62. Kort sagt motiverar det faktum att det är tekniskt möjligt att utbyta digitala uppgifter mellan kompatibla databaser eller att slå samman dessa databaser inte något undantag från principen om ändamålsbegränsning. Driftskompatibilitet måste i det konkreta fallet grundas på tydliga och noggranna politiska val. Datatillsynsmannen föreslår att detta preciseras i Stockholmsprogrammet.

([36]) Se de riktlinjer och kriterier för utveckling, genomförande och användning av integritetsfrämjande säkerhetsteknik som utarbetats inom Priseprojektet (http://www.prise.oeaw.ac.at).

([37]) Med bästa tillgängliga teknik avses det mest effektiva och avancerade skedet i utvecklingen av åtgärder och deras funktionssätt och som anger en viss tekniks praktiska lämplighet att i princip ligga till grund för att tillämpningar och system för informationsteknik och datasäkerhet iakttar kraven på personlig integritet, dataskydd och säkerhet i EU:s regelverk.

([38]) Se datatillsynsmannens yttrande om kommissionens meddelande om kommissionens meddelande om interoperabilitet mellan de europeiska databaserna av den 10 mars 2006 som är tillgängligt på http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Comments/2006/06-03-10_Interoperability_EN.pdf

VI.2 **Användning av uppgifter som samlats in för andra ändamål**

63. En av de viktigaste tendenserna under de senaste åren, nämligen användning för polisiära ändamål av uppgifter som samlats in i den privata sektorn för kommersiella ändamål, tas inte uttryckligen upp i meddelandet. Denna tendens berör inte bara uppgifter om elektronisk kommunikation och passageraruppgifter om enskilda som flyger till (vissa) tredjeländer ([39]), utan gäller även den finansiella sektorn. Ett exempel är Europaparlamentets och rådets direktiv 2005/60/EG av den 26 oktober 2005 om åtgärder för att förhindra att det finansiella systemet används för penningtvätt och finansiering av terrorism ([40]). Ett annat välkänt och omdiskuterat exempel är behandlingen vid Society for Worldwide Interbank Financial Telecommunication (SWIFT) ([41]) av personuppgifter som det amerikanska finansministeriet behöver för sitt program för att spåra finansiering av terrorism.

64. Datatillsynsmannen anser att dessa tendenser bör ägnas särskild uppmärksamhet i Stockholmsprogrammet. De kan ses som undantag från principen om ändamålsbegränsning och inkräktar i stor utsträckning ofta på privatlivet, eftersom användningen av dessa uppgifter kan avslöja mycket om de enskildas beteende. Varje gång sådana åtgärder föreslås måste det föreligga mycket starka bevis för att en sådan inkräktande åtgärd är nödvändig. Om detta kan bevisas måste man säkerställa att den enskildes rättigheter skyddas fullt ut.

65. Datatillsynsmannen anser att personuppgifter som samlats in för kommersiella ändamål endast bör få användas för brottsbekämpande ändamål på strikta villkor, såsom de följande:

— Uppgifterna ska enbart användas för särskilda, i varje enskilt fall fastställda ändamål såsom kampen mot terrorism eller grov brottslighet.

— Uppgifterna ska överföras genom ett direktåtkomstsystem (”pull system”) snarare än genom ett sändsystem (”push system”) ([42]).

([39]) Se punkt 15 ovan.

([40]) EUT L 309, 25.11.2005, s. 15.

([41]) Se yttrande 10/2006 från artikel 29-gruppen om behandlingen av personuppgifter vid Society for Worldwide Interbank Financial Telecommunication (SWIFT).

([42]) Enligt sändsystemet skickar den registeransvarige uppgifterna på begäran till det brottsbekämpande organet. Enligt direktåtkomstsystemet har det brottsbekämpande organet tillgång till den registeransvariges databas och hämtar uppgifterna från denna databas. Enligt direktåtkomstsystemet är det svårare för den registeransvarige att återta ansvaret för uppgifterna.

— En begäran om uppgifter ska vara proportionell, specifikt riktad och i princip bygga på misstankar mot särskilda personer.

— Rutinsökningar, datautvinning och profilering bör undvikas.

— All användning av uppgifterna för brottsbekämpande ändamål bör registreras för att den registrerade vid utövandet av sina rättigheter, dataskyddsmyndigheterna och rättsväsendet effektivt ska kunna kontrollera användningen.

VI.3 **Informationssystem och EU-organ**

Informationssystem med eller utan central lagring ([43])

66. Under de senaste åren har antalet informationssystem baserade på gemenskapslagstiftningen avsevärt ökat på området med frihet, säkerhet och rättvisa. I bland fattats beslut om att etablera ett system med central lagring av uppgifter på europeisk nivå, i andra fall föreskrivs det i lagstiftningen endast ett utbyte av uppgifter mellan nationella databaser. Schengens informationssystem är förmodligen det bästa exemplet på ett system med central lagring. Rådets beslut 2008/615/RIF (Prümbeslutet) ([44]) är i dataskyddshänseende det mest belysande exemplet på ett system utan central lagring, eftersom det i detta föreskrivs ett omfattande utbyte av biometriska uppgifter mellan myndigheterna i medlemsstaterna.

67. I meddelandet ges exempel som illustrerar att tendensen att skapa nya system kommer att fortsätta. Det första exemplet, i punkt 4.2.2, gäller ett informationssystem genom vilket det europeiska informationssystemet för utbyte av uppgifter ur kriminalregister (Ecris) utvidgas till att omfatta tredjelandsmedborgare. Kommissionen har redan beställt en studie om ett europeiskt index över dömda tredjelandsmedborgare vilket skulle kunna leda fram till en central databas. Ett annat exempel är utbyte av personuppgifter i konkursregister i andra medlemsstater, inom ramen för e-juridik (punkt 3.4.1 i meddelandet) utan någon central lagring.

68. Ett decentraliserat system skulle ha vissa fördelar i dataskyddshänseende. Man undviker dubbel lagring av uppgifter i medlemsstatens myndighet och i det centraliserade systemet, och ansvaret för uppgifterna är tydligt eftersom det är medlemsstatens myndighet som är registeransvarig och rättsväsendets och dataskyddsmyndigheternas kontroll kan äga rum på medlemsstatsnivå. Men vid utbyte av uppgifter med andra jurisdiktioner finns det också brister i systemet, t.ex. när man vill säkerställa att uppgifterna är uppdaterade såväl i ursprungslandet som i bestämmelselandet och att det finns en effektiv kontroll på båda sidor. Att säkerställa ansvaret för det tekniska systemet för utbytet är än mer komplicerat. Bristerna kan lösas genom att man väljer ett centraliserat system där EU-organen har ansvar för åtminstone delar av systemet (t.ex. den tekniska infrastrukturen).

69. I detta sammanhang skulle det vara värdefullt om det utarbetades konkreta kriterier för valet mellan centrala och decentraliserade system, vilket skulle säkerställa klara och genomtänkta politiska beslut i de konkreta fallen. Dessa kriterier kan bidra till driften av själva systemen, liksom till skyddet av medborgarnas uppgifter. Datatillsynsmannen föreslår att avsikten att utveckla sådana kriterier tas med i Stockholmsprogrammet.

Storskaliga informationssystem

70. I punkt 4.2.3.2 i meddelandet diskuteras i korthet framtiden för storskaliga informationssystem med tonvikt på Schengens informationssystem (SIS) och Informationssystemet för viseringar (VIS).

71. I punkt 4.2.3.2 nämns även inrättande av ett system för elektronisk registrering av inresor till och utresor från medlemsstaternas territorium vid sidan av program för registrerade resenärer. Detta system tillkännagavs tidigare av kommissionen som en del av det ”gränspaket” som kommissionens vice ordförande Franco Frattini har tagit initiativet till ([45]). I sina inledande kommentarer ([46]) var datatillsynsmannen relativt kritisk mot detta förslag, eftersom behovet av ett sådant inkräktande system, utöver de befintliga storskaliga systemen, inte kunde påvisas tillräckligt. Datatillsynsmannen kan inte se några andra belägg för att ett sådant system skulle behövas och föreslår därför att rådet inte tar upp denna idé i Stockholmsprogrammet.

72. I detta sammanhang hänvisar datatillsynsmannen till sina yttranden om olika initiativ när det gäller EU:s informationsutbyte ([47]) i vilka han lagt fram flera förslag och synpunkter i fråga om konsekvenserna av användningen av stora databaser på gemenskapsnivå för dataskyddet. Bland annat uppmärksammade datatillsynsmannen särskilt behovet av kraftfulla, skräddarsydda skyddsåtgärder och

([43]) Med central lagring avses i detta sammanhang lagring på central europeisk nivå medan decentraliserad lagring avser lagring på medlemsstatsnivå.

([44]) Se fotnot 33.

([45]) Meddelande från kommissionen – *Att förbereda nästa steg i utvecklingen av Europeiska unionens gränsförvaltning*, av den 13 februari 2008, KOM(2008) 69 slutlig.

([46]) Datatillsynsmannens inledande kommentarer om tre meddelanden från kommissionen om gränsförvaltning (KOM(2008) 69, KOM(2008) 68 och KOM(2008) 67), av den 3 mars 2008. http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Comments/2008/08-03-03_Comments_border_package_EN.pdf

([47]) I synnerhet bör följande nämnas: Yttrande av den 23 mars 2005 om förslaget till Europaparlamentets och rådets förordning om informationssystemet för viseringar (VIS) och utbytet mellan medlemsstaterna av uppgifter om viseringar för kortare vistelse, EUT C 181, 23.7.2005, s. 13 samt yttrande av den 19 oktober 2005 om tre förslag om andra generationen av Schengens informationssystem (SIS II), EUT C 91, 19.4.2006, s. 38.

proportionalitet, liksom behovet av konsekvensanalyser innan det föreslås eller vidtas några åtgärder på detta område. Datatillsynsmannen har alltid förespråkat system där skyddet av rättigheter och uppgifter respekteras och där det råder jämvikt mellan säkerhetskraven och integritetsskyddet för de enskilda som omfattas av systemen. Datatillsynsmannen har intagit samma förhållningssätt i rollen som tillsynsansvarig för de centrala delarna i systemen.

73. Vidare tar datatillsynsmannen tillfället i akt att betona att det krävs en konsekvent strategi för EU:s uppgiftsutbyte i sin helhet när det gäller den rättsliga och tekniska överensstämmelsen samt tillsynsöverensstämmelsen mellan de system som redan finns och de som håller på att utvecklas. Faktum är att det i dag, mer än någonsin, finns ett klart behov av en modig och övergripande syn på hur EU:s uppgiftsutbyte och de framtida storskaliga informationssystemen bör se ut. Endast på grundval av en sådan vision skulle ett system för elektronisk registrering av inresor till och utresor från medlemsstaternas territorium eventuellt kunna omprövas.

74. Datatillsynsmannen föreslår att Stockholmsprogrammet innehåller en hänvisning till avsikten att utveckla en sådan vision och en diskussion om ett tänkbart ikraftträdande av Lissabonfördraget och konsekvenserna därav för system med en rättslig grund för den första respektive den tredje pelaren.

75. Slutligen omnämns i meddelandet inrättandet av ett nytt organ som enligt meddelandet även bör bli behörigt för systemet för elektronisk registrering av inresor och utresor. Under tiden har kommissionen antagit ett förslag om inrättande av ett sådant organ ([48]). Datatillsynsmannen stöder i princip detta förslag eftersom det kan göra att dessa system fungerar mer effektivt, däribland att göra dataskyddet mer effektivt. Datatillsynsmannen kommer i god tid att avge ett yttrande om förslaget.

Europol och Eurojust

76. Europols roll nämns på flera ställen i meddelandet där det betonas, som en prioriterad fråga, att Europol måste spela en central roll för samordning, utbyte av uppgifter och fortbildning. Likaså hänvisas det i punkt 4.2.2 i meddelandet till de senaste ändringarna i den rättsliga ramen för samarbetet mellan Eurojust och Europol, och det anges att arbetet med att stärka Eurojust kommer att fortsätta, särskilt vad gäller utredningar på områden med gränsöverskridande organiserad brottslighet. Datatillsynsmannen stöder till fullo dessa mål förutsatt att åtgärderna för dataskydd iakttas på lämpligt sätt.

77. I detta sammanhang välkomnar datatillsynsmannen det nya utkast till avtal som Europol och Eurojust nyligen enats om ([49]) och som syftar till ett förbättrat och stärkt samarbete mellan de båda organen och till ett effektivt utbyte av uppgifter mellan dem. Detta är ett arbete där ett effektivt och ändamålsenligt dataskydd spelar en avgörande roll.

VI.4 **Användning av biometriska uppgifter**

78. Datatillsynsmannen noterar att meddelandet inte tar upp frågan om den ökade användningen av biometriska uppgifter i Europeiska unionens olika rättsliga instrument om användning av informationsutbyte, inklusive rättsakterna om inrättande av storskaliga informationssystem. Detta är beklagligt eftersom det är en fråga som är särskilt känslig i dataskydds- och integritetshänseende.

79. Datatillsynsmannen inser de generella fördelarna med att utnyttja biometriska kännetecken, men har vid upprepade tillfällen betonat de viktigaste konsekvenserna för enskildas rättigheter av att sådana uppgifter används och har föreslagit att det ska införas strikta skyddsåtgärder för användning av biometriska kännetecken i varje enskilt system. Den nyligen avkunnade domen från Europeiska domstolen för de mänskliga rättigheterna i målet *S. och Marper mot Förenade kungariket* ([50]) ger goda insikter i detta sammanhang, särskilt när det gäller berättigandet av och begränsningarna för användningen av biometriska uppgifter. Särskilt användningen av DNA-uppgifter kan avslöja känslig information om enskilda personer, också med beaktande av att de tekniska möjligheterna att utvinna information från DNA fortfarande ökar. När det gäller användning i stor skala av biometriska uppgifter i informationssystem finns det också problem på grund av en inneboende osäkerhet i insamlingen och jämförelsen av de biometriska uppgifterna. Av dessa skäl bör EU:s lagstiftare utnyttja dessa uppgifter med återhållsamhet.

80. En annan återkommande fråga under de senaste åren har varit användningen av fingeravtryck från barn och äldre, på grund av den inneboende osäkerheten i de biometriska systemen när det gäller dessa åldersgrupper. Datatillsynsmannen har begärt en djupgående undersökning för att korrekt fastställa systemens exakthet ([51]). Han föreslog en åldersgräns på 14 år för barn såvida inte studien visade på något annat. Datatillsynsmannen föreslår att denna fråga omnämns i Stockholmsprogrammet.

([48]) Kommissionens förslag av den 24 juni 2009 till Europaparlamentets och rådets förordning om inrättande av en byrå för den operativa förvaltningen av Schengens informationssystem (SIS II), Informationssystemet för viseringar (VIS), Eurodac och andra stora IT-system inom området med frihet, säkerhet och rättvisa (KOM(2009) 293/2).

([49]) Utkast till avtal, godkänt av rådet, som fortfarande måste undertecknas av båda parter. Se rådets register:
http://register.consilium.europa.eu/pdf/en/09/st10/st10019.en09.pdf
http://register.consilium.europa.eu/pdf/en/09/st10/st10107.en09.pdf

([50]) Gemensamma ansökningar 30562/04 och 30566/04, S. och Marper mot Förenade kungariket, dom den 4 december 2008 från Europadomstolen, ännu inte offentliggjord.

([51]) Yttrande av den 26 mars 2008 om förslaget till förordning om ändring av rådets förordning 2252/2004 om standarder för säkerhetsdetaljer och biometriska kännetecken i pass och resehandlingar som utfärdas av medlemsstaterna, EUT C 200, 6.8.2008, s. 1.

81. Datatillsynsmannen anser dock att det vore värdefullt att utveckla konkreta kriterier för användningen av biometriska uppgifter. Dessa kriterier bör säkerställa att uppgifterna endast används när så är nödvändigt, lämpligt och proportionellt och när ett uttryckligt, särskilt och berättigat ändamål har påvisats av lagstiftaren. Närmare bestämt bör biometriska uppgifter och i synnerhet DNA-uppgifter inte användas om samma resultat kan uppnås med hjälp av andra, mindre känsliga uppgifter.

VII. **TILLGÅNG TILL RÄTTSLIG PRÖVNING OCH E-JURIDIK**

82. Även tekniken kommer att utnyttjas som ett instrument för att förbättra det rättsliga samarbetet. Enligt punkt 3.4.1 i meddelandet kommer e-juridiken att underlätta tillgången till rättslig prövning för medborgarna. Den består av en portal med uppgifter och videokonferenser som en del av det rättsliga förfarandet. Det möjliggör dessutom rättsliga förfaranden online och förutser en sammankoppling av nationella register såsom konkursregister. Datatillsynsmannen noterar att meddelandet inte tar upp några nya initiativ om e-juridik men däremot befäster de åtgärder som redan är i gång. Datatillsynsmannen deltar i några av dessa åtgärder, som en uppföljning av det yttrande han avgav den 19 december 2008 om meddelandet från kommissionen – *Mot en europeisk strategi för e-juridik* ([52]).

83. e-juridik är ett ambitiöst projekt som måste stödjas fullt ut. Det kan effektivt förbättra rättsväsendet i Europa och det rättsliga skyddet för medborgarna. Det är ett viktigt steg framåt mot ett europeiskt område med rättvisa. Med detta positiva omdöme i åtanke kan dock några kommentarer göras:

— De tekniska systemen för e-juridik bör byggas i enlighet med principen ”privacy by design”. Att välja rätt struktur är, som tidigare nämnts, utgångspunkten när det gäller den europeiska informationsmodellen.

— Samtrafiken och driftskompatibiliteten mellan systemen bör respektera principen om ändamålsbegränsning.

— Ansvarsfördelningen mellan de olika aktörerna bör fastställas exakt.

— Konsekvenserna för enskilda av sammankopplingen av nationella register med känsliga personuppgifter, såsom konkursregister, bör analyseras i förväg.

VIII. **SLUTSATSER**

84. Datatillsynsmannen välkomnar att skyddet av de grundläggande rättigheterna, särskilt skyddet av personuppgifter, framhävs i meddelandet som en av de viktigaste frågorna i framtiden för området med frihet, säkerhet och rättvisa. Datatillsynsmannen anser att meddelandet på ett korrekt sätt främjar jämvikt mellan behoven av lämpliga instrument för att säkerställa säkerhet för medborgarna och skydda deras grundläggande rättigheter. Det erkänns i meddelandet att skyddet av personuppgifter bör uppmärksammas i större utsträckning.

85. Datatillsynsmannen ger sitt fulla stöd till punkt 2.3 i meddelandet där man konstaterar behovet av att det inrättas ett övergripande dataskyddssystem som omfattar alla EU:s behörighetsområden, oberoende av ikraftträdandet av Lissabonfördraget. Han rekommenderar i detta sammanhang att

— behovet av en tydlig vision på lång sikt när det gäller ett sådant övergripande system fastställs i Stockholmsprogrammet,

— de åtgärder som redan har antagits på detta område, liksom deras konkreta genomförande och effektivitet, utvärderas med beaktande av kostnaderna för den personliga integriteten och brottsbekämpningens effektivitet,

— behovet av en ny rättslig ram, för att bland annat ersätta rådets rambeslut 2008/977/RIF, prioriteras i Stockholmsprogrammet.

86. Datatillsynsmannen välkomnar kommissionens avsikt att upprepa dataskyddsprinciperna vilka måste kopplas till det offentliga samråd som kommissionen kungjorde vid konferensen ”Personuppgifter – ökad användning, bättre skydd?” den 19–20 maj 2009. När det gäller själva sakfrågan betonar datatillsynsmannen vikten av principen om ändamålsbegränsning som en hörnsten i dataskyddslagstiftningen samt inriktningen på möjligheterna att förbättra effektiviteten vid tillämpningen av dataskyddsprinciperna genom instrument som stärker de registeransvarigas ansvar.

87. ”Privacy by design” och integritetsbeaktande teknik skulle kunna främjas genom

— ett certifieringssystem för personlig integritet och dataskydd som ett alternativ för konstruktörer och användare av informationssystem,

— en lagfäst skyldighet för konstruktörer och användare av informationssystem att använda system som iakttar principen med ”privacy by design”.

88. När det gäller dataskyddets yttre aspekter rekommenderar datatillsynsmannen att

— vikten av allmänna avtal med Förenta staterna och andra tredje länder om dataskydd och utbyte av uppgifter betonas i Stockholmsprogrammet,

([52]) Datatillsynsmannens yttrande av den 19 december 2008 om meddelandet från kommissionen – *Mot en europeisk strategi för e-juridik*. EUT C 128, 6.6.2009, s. 13.

— respekten för de grundläggande rättigheterna, särskilt dataskyddet, aktivt främjas i förbindelserna med tredjeländer och internationella organisationer,

— det nämns i Stockholmsprogrammet att utbyte av personuppgifter med tredjeländer kräver en tillräcklig skyddsnivå eller lämpliga skyddsåtgärder i dessa tredjeländer.

89. Datatillsynsmannen noterar med stort intresse utvecklingen mot en informationshanteringsstrategi för Europeiska unionen liksom en europeisk informationsmodell, och understryker att dataskyddsinslagen i dessa projekt närmare bör utarbetas i Stockholmsprogrammet. Strukturen för uppgiftsutbytet bör grundas på ”privacy by design” och ”bästa tillgängliga teknik”.

90. Det faktum att det är tekniskt möjligt att utbyta digitala uppgifter mellan kompatibla databaser eller att slå samman dessa databaser motiverar inte något undantag från principen om ändamålsbegränsning. Driftskompatibilitet måste i det konkreta fallet grundas på tydliga och genomtänkta politiska val. Datatillsynsmannen föreslår att detta preciseras i Stockholmsprogrammet.

91. Datatillsynsmannen anser att personuppgifter som samlats in för kommersiella ändamål endast bör få användas för brottsbekämpande ändamål på strikta villkor, vilka anges i punkt 65 i detta yttrande.

92. Bland de övriga förslagen när det gäller användning av personuppgifter ingår följande:

— Att utarbeta materiella kriterier för valet mellan centrala och decentraliserade system och nämna avsikterna att utarbeta dessa kriterier i Stockholmsprogrammet.

— Att inte omnämna inrättandet av ett system för elektronisk registrering av inresor till och utresor från medlemsstaternas territorium vid sidan av program för registrerade resenärer i Stockholmsprogrammet.

— Att stödja förstärkningen av Europol och Eurojust samt det nya avtal mellan dem som nyligen utarbetats.

— Utarbeta konkreta kriterier för användningen av biometriska uppgifter för att säkerställa att uppgifterna endast används när så är nödvändigt, lämpligt och proportionellt och när ett uttryckligt, särskilt och berättigat ändamål har påvisats av lagstiftaren. DNA-uppgifter bör inte användas om samma resultat kan uppnås med hjälp av andra, mindre känsliga uppgifter.

93. Datatillsynsmannen stöder e-juridik och har lämnat några synpunkter på hur projektet kan förbättras (se punkt 83).

Utfärdat i Bryssel den 10 juli 2009.

Peter HUSTINX

Europeiska datatillsynsmannen