I

(Resolutioner, rekommendationer och yttranden)

YTTRANDEN

EUROPEISKA DATATILLSYNSMANNEN

Yttrande från Europeiska datatillsynsmannen om slutrapporten från EU–USA-kontaktgruppen på hög nivå för informationsutbyte, integritetsskydd och skydd av personuppgifter

(2009/C 128/01)

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 grundläggande 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 – BAKGRUND TILL YTTRANDET

1. Inför EU-toppmötet den 12 juni 2008 meddelade ordförandeskapet för Europeiska unionens råd den 28 maj 2008 Coreper att EU–USA-kontaktgruppen på hög nivå (nedan kallad *kontaktgruppen*) för informationsutbyte, integritetsskydd och skydd av personuppgifter hade färdigställt sin rapport. Rapporten offentliggjordes den 26 juni 2008. [1]

2. Rapporten syftar till att fastställa gemensamma principer för integritetsskydd och uppgiftsskydd som ett första steg mot informationsutbyte med Förenta staterna för att bekämpa terrorism och allvarlig gränsöverskridande brottslighet.

3. I meddelandet förklarar rådets ordförandeskap att det välkomnar alla synpunkter som rör uppföljningen av rapporten, särskilt reaktioner på de rekommendationer för det fortsatta arbetet som anges i rapporten. Europeiska datatillsynsmannen svarar på denna uppmaning genom att avge följande yttrande som bygger på den lägesbeskrivning som offentliggjorts och som inte föregriper någon ståndpunkt som han eventuellt kommer att inta senare när det gäller frågans utveckling.

4. Datatillsynsmannen noterar att kontaktgruppen har utfört sitt arbete mot bakgrund av att utbytet av uppgifter mellan USA och EU har förändrats, särskilt sedan den 11 september 2001, genom internationella avtal eller andra typer av instrument. Bland dessa finns Europols och Eurojusts avtal med Förenta staterna samt PNR-avtalet och Swift-fallet som ledde till en skriftväxling mellan tjänstemän i EU och USA för att fastställa minimigarantier för uppgiftsskydd [2].

[1] Rådets dokument 9831/08 finns tillgängligt på http://ec.europa.eu/justice_home/fsj/privacy/news/index_en.htm.

[2] — Avtal mellan Amerikas förenta stater och Europeiska polisbyrån av den 6 december 2001 samt tilläggsavtal mellan Europol och USA om utbyte av personuppgifter och relaterade upplysningar, offentliggjorda på Europols webbplats.
— Avtal mellan Amerikas förenta stater och Eurojust om rättsligt samarbete av den 6 november 2006, offentliggjort på Eurojusts webbplats.
— Avtal 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), undertecknat i Bryssel den 23 juli 2007 och i Washington den 26 juli 2007, EUT L 204, 4.8.2007, s. 18.
— Skriftväxling mellan myndigheter i USA och EU om programmet för att spåra finansiering av terrorism, den 28 juni 2007.

5. Dessutom förhandlar EU också om och godkänner liknande instrument för utbyte av personuppgifter med andra tredjeländer. Ett exempel nyligen är avtalet mellan Europeiska unionen och Australien om lufttrafikföretags behandling av passageraruppgifter (PNR) från Europeiska unionen och överföring av dessa till Australiens tullmyndighet ([3]).

6. Det framgår i detta sammanhang att framställningar om personuppgifter från brottsbekämpande myndigheter i tredjeländer ständigt ökar, och att de också utvidgats från traditionella statliga databaser till andra typer av register, särskilt dataregister i den privata sektorn.

7. Som en viktig bakgrundsfaktor erinrar datatillsynsmannen också om att frågan om överföring av personuppgifter till tredjeländer inom ramen för polissamarbete och straffrättsligt samarbete omfattas av rådets rambeslut om skydd av personuppgifter som behandlas inom ramen för polissamarbete och straffrättsligt samarbete ([4]), vilket sannolikt kommer att antas före utgången av 2008.

8. Det transatlantiska informationsutbytet kan endast förväntas öka och beröra ytterligare sektorer där personuppgifter behandlas. I detta sammanhang är en dialog om ”transatlantisk brottsbekämpning” välkommen men samtidigt känslig. Den är välkommen i den meningen att den kan ge en tydligare ram för det uppgiftsutbyte som äger rum eller som kommer att äga rum. Den är också känslig, eftersom en sådan ram kan legitimera omfattande överföringar av uppgifter på ett område, brottsbekämpning, där konsekvenserna för enskilda personer är särskilt allvarliga och där det är särskilt nödvändigt med strikta och tillförlitliga säkerhetsåtgärder och garantier. ([5])

9. Det följande kapitlet i detta yttrande behandlar det nuvarande läget och det tänkbara framtida arbetet. Kapitel III inriktas på omfattningen och arten av ett instrument som möjliggör informationsutbyte. I kapitel IV i yttrandet analyseras ur ett allmänt perspektiv de rättsliga frågor som har anknytning till innehållet i ett eventuellt avtal. Det behandlar frågor som villkoren för bedömning av den skyddsnivå som erbjuds i Förenta staterna och diskuterar frågan om användningen av EU:s regelverk som riktmärke för att bedöma denna skyddsnivå. I det kapitlet förtecknas också de grundläggande krav som ska ingå i ett sådant avtal. Slutligen innehåller kapitel V i yttrandet en analys av de principer för integritetsskydd som bifogas rapporten.

II. DET NUVARANDE LÄGET OCH DET TÄNKBARA FRAMTIDA ARBETET

10. Datatillsynsmannen bedömer det nuvarande läget på följande sätt. Vissa framsteg har gjorts för att fastställa gemensamma standarder för informationsutbyte, integritetsskydd och skydd av personuppgifter.

11. Förberedelsearbetet för någon typ av avtal mellan EU och USA har emellertid ännu inte slutförts. Det behövs ytterligare arbete. I kontaktgruppens rapport nämns också flera kvarstående frågor, varav frågan om ”möjlighet till rättslig prövning” är den mest framträdande. Det råder fortfarande oenighet om vilken omfattning som krävs för möjligheten till rättslig prövning ([6]). Fem andra kvarstående frågor fastställs i kapitel 3 i rapporten. Det framgår dessutom av detta yttrande att många andra frågor ännu inte har lösts, till exempel omfattningen och arten av ett instrument om informationsutbyte.

12. Eftersom det alternativ som förordas i rapporten är ett bindande avtal, vilket också datatillsynsmannen föredrar, är det särskilt nödvändigt med försiktighet. Ytterligare noggranna och ingående förberedelser behövs innan ett avtal kan uppnås.

13. Enligt datatillsynsmannen skulle det slutligen vara bäst att ett avtal ingås enligt Lissabonfördraget, givetvis under förutsättning att detta träder i kraft. Enligt Lissabonfördraget skulle det nämligen inte råda någon rättslig osäkerhet om avgränsningen mellan EU:s olika pelare. Dessutom skulle det garanteras att Europaparlamentet deltar fullt ut samt att domstolen utövar rättslig kontroll.

14. Under dessa förhållanden skulle det framtida arbetet bäst kunna bestå i utarbetandet av en färdplan mot ett eventuellt senare avtal. En sådan färdplan kan innehålla följande delar:

— Riktlinjer för det fortsatta arbetet i kontaktgruppen (eller någon annan grupp) samt en tidsplan.

— I ett tidigt skede, diskussion och eventuell överenskommelse om grundläggande frågor, till exempel avtalets omfattning och art.

— På grundval av en gemensam uppfattning av dessa grundläggande frågor, vidareutveckling av principerna för uppgiftsskydd.

— De berörda parternas medverkan i olika skeden i förfarandet.

— På den europeiska sidan, behandling av de institutionella begränsningarna.

([3]) EUT L 213, 8.8.2008, s. 49.

([4]) Rådets rambeslut om skydd av personuppgifter som behandlas inom ramen för polissamarbete och straffrättsligt samarbete, versionen av den 24 juni 2008 är tillgänglig på http://ec.europa.eu/prelex/detail_dossier_real.cfm?CL=sv&DosId=193371.

([5]) När det gäller behovet av en tydlig rättslig ram, se kapitlen III och IV i detta yttrande.

([6]) Sidan 5 i rapporten, avsnitt C.

III. **OMFATTNINGEN OCH ARTEN AV ETT INSTRUMENT OM INFORMATIONSUTBYTE**

15. Datatillsynsmannen anser att det är av avgörande betydelse att omfattningen och arten av ett eventuellt instrument, inklusive principer för uppgiftsskydd, fastställs tydligt, som ett första steg i vidareutvecklingen av ett sådant instrument.

16. När det gäller omfattningen är det viktigt att följande frågor besvaras:

— Vilka aktörer som berörs, inom och utanför brottsbekämpningsområdet.

— Vad som avses med ”brottsbekämpningssyfte” och dess förhållande till andra syften som nationell säkerhet, och mer specifikt gränskontroll och folkhälsa.

— Hur instrumentet passar in i ett övergripande transatlantiskt säkerhetsområde.

17. När det gäller fastställandet av arten bör följande frågor klargöras:

— Om det är tillämpligt, inom vilken pelare förhandlingarna om instrumentet ska föras.

— Huruvida instrumentet ska vara bindande för EU och USA.

— Huruvida det ska få direkt effekt i den meningen att det innehåller rättigheter och skyldigheter för enskilda personer vilka kan göras gällande inför en rättslig myndighet.

— Huruvida instrumentet i sig ska möjliggöra informationsutbyte eller om det ska fastställa minimistandarder för informationsutbyte, vilka ska kompletteras genom särskilda avtal.

— Instrumentets förhållande till befintliga instrument, huruvida det ska respektera, ersätta eller komplettera dem.

III.1 **Instrumentets omfattning**

Berörda aktörer

18. Även om den exakta omfattningen av det framtida instrumentet inte anges klart i kontaktgruppens rapport kan man av de principer som nämns i den dra slutsatsen att avsikten är att det ska omfatta överföringar såväl mellan privata och offentliga aktörer ([7]) som mellan offentliga myndigheter.

— Mellan privata och offentliga aktörer

19. Datatillsynsmannen anser att det är logiskt att ett framtida instrument ska vara tillämpligt på överföringar mellan privata och offentliga aktörer. Ett sådant instrument utarbetas mot bakgrund av USA:s framställningar om information från privata parter under de senaste åren. Datatillsynsmannen noterar att privata aktörer håller på att bli en systematisk informationskälla i brottsbekämpningssammanhang, såväl på EU-nivå som på internationell nivå ([8]). Swift-fallet är ett viktigt tidigare exempel där ett privat företag anmodades att systematiskt överföra stora mängder uppgifter till brottsbekämpande myndigheter i en tredjestat ([9]). Insamlingen av PNR-uppgifter från flygbolag följer samma logik. Redan i sitt yttrande om utkastet till rambeslut om ett europeiskt PNR-system ifrågasatte datatillsynsmannen lagenligheten av denna tendens ([10]).

20. Det finns ytterligare två skäl till att hysa betänkligheter mot att överföringar mellan privata och offentliga aktörer införs i tillämpningsområdet för ett framtida instrument.

21. För det första kan införandet få en oönskad effekt inom EU:s eget territorium. Om uppgifter från privata företag (till exempel finansinstitut) i princip kan överföras till tredjeländer, hyser datatillsynsmannen allvarliga farhågor om att detta kan ge upphov till starka påtryckningar för att samma typ av uppgifter ska bli tillgängliga för de brottsbekämpande myndigheterna också inom EU. PNR-systemet är ett exempel på en sådan oönskad utveckling som startade med USA:s insamling av stora mängder passageraruppgifter och därefter överfördes också till ett internt europeiskt sammanhang ([11]), utan att systemets nödvändighet och rimlighet visats på ett tydligt sätt.

22. För det andra tar datatillsynsmannen i sitt yttrande om kommissionens förslag till EU:s PNR-system också

([7]) Se särskilt kapitel 3 i rapporten, ”Kvarstående frågor rörande transatlantiska förbindelser”, punkt 1: ”Enhetlighet i privata enheters skyldigheter i samband med överföring av uppgifter”.

([8]) När det gäller denna fråga, se yttrandet från Europeiska datatillsynsmannen av den 20 december 2007 om förslaget till rådets rambeslut om användande av passageraruppgifter (PNR-uppgifter) i brottsbekämpningssyfte, EUT C 110, 1.5.2008, s. 1. ”Av tradition har det funnits en tydlig åtskillnad mellan brottsbekämpning och verksamhet inom den privata sektorn, varvid brottsbekämpningsuppgifter har utförts av särskilt avdelade myndigheter, särskilt polisen, medan privata aktörer från fall till fall anmodas överföra personuppgifter till dessa brottsbekämpande myndigheter. Det finns nu en tendens att systematiskt kräva samarbete av privata aktörer i brottsbekämpningssyfte.”

([9]) Se yttrande 10/2006 av den 22 november 2006 från arbetsgruppen för skydd av enskilda med avseende på behandlingen av personuppgifter (artikel 29-gruppen) om behandling av personuppgifter av Society for Worldwide Interbank Financial Telecommunication (Swift), WP 128.

([10]) Yttrande av den 20 december 2007, op.cit.

([11]) Se förslaget till rådets rambeslut om användande av passageraruppgifter (PNR-uppgifter) i brottsbekämpningssyfte, se fotnot 8, som för närvarande diskuteras i rådet.

upp frågan om vilket regelverk för uppgiftsskydd (den första eller den tredje pelaren) som är tillämpligt på villkoren för samarbetet mellan offentliga och privata aktörer: Bör reglerna bygga på kategorin av registeransvarig (privat sektor) eller på det eftersträvade målet (brottsbekämpning)? Avgränsningen mellan den första och den tredje pelaren är långt ifrån tydlig i situationer där privata aktörer åläggs skyldigheter att behandla personuppgifter för brottsbekämpningssyften. I detta sammanhang är det signifikativt att generaladvokat Bot nyligen i sitt förslag till avgörande i målet om lagring av uppgifter ([12]) föreslår en avgränsning för dessa situationer, men gör följande tillägg: ”Visserligen kan denna avgränsning kritiseras och i vissa avseenden förefalla konstgjord.” Datatillsynsmannen konstaterar också att domstolen i sin dom i PNR-målet ([13]) inte fullständigt besvarar frågan om det tillämpliga regelverket. Det faktum att vissa verksamheter inte omfattas av direktiv 95/46/EG innebär till exempel inte automatiskt att dessa verksamheter kan regleras inom den tredje pelaren. Detta kan därför lämna ett kryphål när det gäller tillämplig lag och leder under alla omständigheter till rättslig osäkerhet när det gäller de rättsliga garantier som de registrerade personerna omfattas av.

23. Mot bakgrund av detta betonar datatillsynsmannen att det måste säkerställas att ett framtida instrument med allmänna principer för uppgiftsskydd inte kan legitimera den transatlantiska överföringen av personuppgifter mellan privata och offentliga parter som sådan. Denna överföring kan endast införas i ett framtida instrument under förutsättning att

— det fastställs i det framtida instrument att överföringen endast är tillåten om den har visats vara absolut nödvändig för ett specifikt syfte, vilket ska beslutas från fall till fall,

— själva överföringen omfattas av strikta garantier för uppgiftsskydd (vilka beskrivs i detta yttrande).

Datatillsynsmannen konstaterar dessutom att det råder osäkerhet om vilket regelverk som ska tillämpas på uppgiftsskydd och vädjar därför under alla omständigheter om att överföringen av personuppgifter mellan privata och offentliga parter inte ska införas enligt den nu gällande EU-lagstiftningen.

— Mellan offentliga myndigheter

24. Den exakta omfattningen av informationsutbytet är oklar. Som ett första steg i det framtida arbetet mot ett gemensamt instrument bör den planerade omfattningen av ett sådant instrument klargöras. I synnerhet följande frågor kvarstår:

— När det gäller databaser i EU, huruvida instrumentet ska omfatta centraliserade databaser som (delvis) förvaltas av EU, till exempel Europols och Eurojusts databaser, eller decentraliserade databaser som förvaltas av medlemsstaterna, eller båda.

— Huruvida instrumentet också ska omfatta sammanlänkade nät, dvs. huruvida de planerade garantierna ska omfatta uppgifter som utbyts mellan medlemsstater eller myndigheter, såväl i EU som i USA.

— Huruvida instrumentet endast ska omfatta utbyte mellan databaser på brottsbekämpningsområdet (polis, rättsväsende, eventuellt tullen) eller också andra databaser som skattedatabaser.

— Huruvida instrumentet också ska gälla nationella säkerhetsorgans databaser eller ge dessa organ tillgång till databaser för brottsbekämpning på den andra avtalsslutande partens territorium (EU till USA och omvänt).

— Huruvida instrumentet ska omfatta överföring av information från fall till fall eller ständig tillgång till befintliga databaser. Det sistnämnda alternativet skulle givetvis väcka frågor om proportionalitet, vilka diskuteras närmare i kapitel V punkt 3.

Brottsbekämpningssyfte

25. Fastställandet av syftet med ett eventuellt avtal ger också utrymme för osäkerhet. Brottsbekämpningssyften anges klart såväl i inledningen som i den första principen som bifogas rapporten, och kommer att analyseras närmare i kapitel IV i detta yttrande. Datatillsynsmannen noterar redan att det av dessa förklaringar framgår att utbytet av uppgifter ska inriktas på frågor inom den tredje pelaren, men man kan fråga sig om detta endast är ett första steg mot ett mer omfattande informationsutbyte. Det förefaller klart att de syften avseende ”allmän säkerhet” som anges i rapporten omfattar kampen mot terrorism, organiserad brottslighet och andra typer av brott. Är avsikten emellertid att utbyte av uppgifter också ska vara möjligt för andra allmänintressen, exempelvis risker för folkhälsan?

26. Datatillsynsmannen rekommenderar att syftet ska begränsas till exakt identifierad behandling av uppgifter och att de policyval som leder till detta fastställande av syftet ska motiveras.

([12]) Generaladvokat Bots förslag till avgörande av den 14 oktober 2008, Irland mot Europaparlamentet och rådet (mål C-301/06), punkt 108.

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

Ett övergripande transatlantiskt säkerhetsområde

27. Rapportens breda räckvidd bör sättas i förhållande till det övergripande transatlantiska säkerhetsområde som diskuteras av den s.k. framtidsgruppen ([14]). Rapporten från denna grupp, som lämnades i juni 2008, inriktas i viss utsträckning på den yttre dimensionen i politiken för inrikes frågor. I rapporten förespråkas följande: *"Senast 2014 bör Europeiska unionen fatta beslut om det politiska målet att förverkliga ett Euroatlantiskt samarbetsområde när det gäller frihet, säkerhet och rättvisa med Förenta staterna."* Ett sådant samarbete skulle gå utöver säkerhet i strikt mening och åtminstone omfatta de frågor som behandlas i nuvarande avdelning IV i EG-fördraget, till exempel invandring, visering och asyl samt civilrättsligt samarbete. Det måste ifrågasättas i vilken utsträckning ett avtal om grundläggande principer för uppgiftsskydd, som de principer som nämns i kontaktgruppens rapport, kan och bör ligga till grund för ett informationsutbyte på ett så brett område.

28. Normalt kommer pelarstrukturen att ha upphört att existera 2014 och det kommer att finnas en enda rättslig grund för uppgiftsskydd inom själva EU (enligt Lissabonfördraget, artikel 16 i fördraget om Europeiska unionens funktionssätt). Det faktum att *lagstiftningen* om uppgiftsskydd är harmoniserad på EU-nivå innebär dock inte att *överföringen* av personuppgifter kan tillåtas enligt ett avtal med ett tredjeland, oavsett syfte. Beroende på sammanhanget och villkoren för behandling kan det krävas anpassade garantier för uppgiftsskydd för särskilda områden, till exempel brottsbekämpning. Datatillsynsmannen rekommenderar att konsekvenserna av dessa olika perspektiv ska beaktas i samband med utarbetandet av ett framtida avtal.

III.2 **Avtalets art**

Den europeiska institutionella ramen

29. Åtminstone på kort sikt är det väsentligt att avgöra inom vilken pelare förhandlingarna om avtalet ska föras. Detta är nödvändigt särskilt på grund av det interna regelverket för uppgiftsskydd som kommer att påverkas av ett sådant avtal. Ska förhandlingarna föras inom ramen för den första pelaren, huvudsakligen direktiv 95/46/EG med sitt specifika system för överföring av uppgifter till tredjeländer, eller inom ramen för den tredje pelaren med ett mindre strikt system för överföringar till tredjeländer? ([15])

30. Som redan sagts överväger brottsbekämpningssyftena, men i kontaktgruppens rapport nämns ändå insamling av uppgifter från privata aktörer, och syftena kan också tolkas så brett att de går utöver ren säkerhet, inklusive till exempel invandrings- och gränskontrollfrågor, men också eventuellt folkhälsa. Med hänsyn till denna osäkerhet skulle det i hög grad vara att föredra att invänta harmoniseringen av pelarna enligt EU-lagstiftningen, vilket föreskrivs i Lissabonfördraget, för att klart fastställa den rättsliga grunden för förhandlingarna och den exakta rollen för de europeiska institutionerna, särskilt Europaparlamentet och kommissionen.

Instrumentets bindande karaktär

31. Det bör klargöras om de avslutade diskussionerna ska leda till ett samförståndsavtal eller något annat icke bindande instrument eller till ett bindande internationellt avtal.

32. Datatillsynsmannen stöder rapportens preferens för ett bindande avtal. Datatillsynsmannen anser att ett officiellt bindande avtal är en nödvändig förutsättning för all överföring av uppgifter utanför EU, oavsett för vilket syfte uppgifterna överförs. Ingen överföring av uppgifter till ett tredjeland kan ske utan adekvata villkor och garantier som ingår i ett specifikt (och bindande) regelverk. Ett samförståndsavtal eller något annat icke bindande instrument kan med andra ord vara användbart för att ge riktlinjer för förhandlingar om ytterligare bindande avtal, men kan aldrig ersätta behovet av ett bindande avtal.

Direkt effekt

33. Bestämmelserna i instrumentet bör vara bindande såväl för USA som för EU och dess medlemsstater.

34. Det bör dessutom säkerställas att enskilda personer får utöva sina rättigheter, och särskilt få möjlighet till rättslig prövning, på grundval av överenskomna principer. Datatillsynsmannen anser att detta resultat bäst kan uppnås om de materiella bestämmelserna i instrumentet utformas så att de har direkt effekt gentemot invånarna i Europeiska unionen och kan åberopas inför en domstol. Den direkta effekten av bestämmelserna i det internationella avtalet, samt villkoren för införlivandet i intern europeisk och nationell lagstiftning för att säkerställa bestämmelsernas verkningsfullhet, måste därför klargöras i instrumentet.

Förhållandet till andra instrument

35. Det är också en grundläggande fråga i vilken utsträckning avtalet står ensamt eller om det från fall till fall måste kompletteras med ytterligare avtal om specifika utbyten av uppgifter. Det kan verkligen ifrågasättas om ett enda avtal, med en enda uppsättning standarder, på ett tillfredsställande sätt kan täcka mångfalden av särdrag när det gäller behandlingen av uppgifter inom den tredje pelaren.

([14]) Rapport från den informella rådgivande högnivågruppen avseende framtiden för den europeiska politiken för inrikes frågor, "Frihet, säkerhet och personlig integritet – europeiska inrikes frågor i en öppen värld", juni 2008, tillgänglig på register.consilium.europa.eu.

([15]) Se artiklarna 11 och 13 i det rambeslut som nämns i punkt 7 i detta yttrande.

Det är ändå mera tveksamt om det kan *tillåta*, utan ytterligare diskussioner och garantier, ett allmänt godkännande av alla överföringar av uppgifter, oavsett de berörda uppgifternas syfte och art. Dessutom är avtal med tredjeländer inte nödvändigtvis permanenta, eftersom de kan kopplas till specifika hot, bli föremål för översyn eller omfattas av klausuler om automatiskt upphörande. Å andra sidan kan gemensamma minimistandarder som erkänns i ett bindande avtal underlätta eventuella senare diskussioner om överföring av personuppgifter i förhållande till en specifik databas eller uppgiftsbehandling.

36. Datatillsynsmannen vill därför förespråka att en miniuppsättning kriterier för uppgiftsskydd utarbetas vilka från fall till fall kompletteras med specifika tilläggsbestämmelser, så som nämns i kontaktgruppens rapport, i stället för alternativet med ett enda avtal. Dessa specifika tilläggsbestämmelser är en förutsättning för att överföringen av uppgifter ska vara tillåten i ett specifikt fall. Detta skulle främja en harmoniserad strategi för uppgiftsskydd.

Tillämpning på befintliga instrument

37. Det bör också undersökas hur ett eventuellt allmänt avtal skulle samverka med redan befintliga avtal som ingåtts mellan EU och USA. Det bör noteras att dessa befintliga avtal inte har samma bindande karaktär; särskilt bör nämnas PNR-avtalet (det avtal som erbjuder störst rättslig säkerhet), Europol- och Eurojustavtalen samt Swift-skriftväxlingen ([16]). Kommer ett nytt allmänt regelverk att komplettera dessa befintliga instrument eller kommer de att förbli opåverkade och det nya regelverket endast vara tillämpligt på andra framtida utbyten av personuppgifter? Datatillsynsmannen anser att det för rättslig enhetlighet krävs en harmoniserad uppsättning bestämmelser som är tillämpliga på och kompletterar både befintliga och framtida bindande avtal om överföring av uppgifter.

38. Tillämpningen av det allmänna avtalet på befintliga instrument skulle medföra fördelen att den stärker deras bindande karaktär. Detta skulle vara särskilt välkommet när det gäller instrument som inte är rättsligt bindande, till exempel Swift-skriftväxlingen, eftersom det åtminstone skulle föreskrivas att en uppsättning allmänna principer för integritetsskydd ska följas.

IV. **ALLMÄN RÄTTSLIG BEDÖMNING**

39. I detta kapitel kommer det att diskuteras hur skyddsnivån inom ett specifikt regelverk eller i ett specifikt instrument ska bedömas, inklusive frågan om vilka riktmärken som ska användas och de nödvändiga grundläggande kraven.

([16]) Se fotnot 2.

Adekvat skyddsnivå

40. Datatillsynsmannen anser att det bör stå klart att ett av de viktigaste resultaten av ett framtida instrument ska vara att överföring av personuppgifter till Förenta staterna endast får ske om myndigheterna i Förenta staterna garanterar en adekvat skyddsnivå (och vice versa).

41. Datatillsynsmannen anser att endast en verklig prövning av att skyddsnivån är adekvat skulle säkerställa tillräckliga garantier när det gäller skyddsnivån för personuppgifter. Han anser att ett allmänt ramavtal med en så bred räckvidd som i kontaktgruppens rapport skulle ha svårt att som sådant klara en verklig prövning av att skyddsnivån är adekvat. Det allmänna avtalet kan endast erkännas ha en adekvat skyddsnivå om det kombineras med en adekvat skyddsnivå i särskilda avtal som ingås från fall till fall.

42. Det är inte ovanligt att den skyddsnivå som erbjuds av tredjeländer bedöms, särskilt av Europeiska kommissionen: inom den första pelaren är adekvat skyddsnivå ett krav för överföring. Den har mätts vid flera tillfällen enligt artikel 25 i direktiv 95/46/EG på grundval av specifika kriterier och bekräftats genom beslut av Europeiska kommissionen ([17]). Inom den tredje pelaren fastställs inte uttryckligen något sådant system: mätning av adekvat skyddsnivå föreskrivs endast i den specifika situation som behandlas i artiklarna 11 och 13 i det ännu inte antagna ramdirektivet om uppgiftsskydd ([18]) och överlåts till medlemsstaterna.

43. I det aktuella fallet omfattar bedömningen brottsbekämpningssyften och diskussionerna förs av kommissionen under rådets överinseende. Sammanhanget skiljer sig från bedömningen av principerna om integritetsskydd (Safe Harbour Principles) eller bedömningen av om den kanadensiska lagstiftningen föreskriver en adekvat skyddsnivå, och har ett närmare samband med de PNR-förhandlingar som nyligen fördes med USA och Australien, vilka ägde rum inom den tredje pelarens regelverk. Kontaktgruppens principer har emellertid också nämnts i samband med programmet för viseringsundantag som gäller gränser och invandring och därmed frågor inom den första pelaren.

44. Datatillsynsmannen rekommenderar att alla konstateranden av adekvat skyddsnivå enligt ett framtida instrument bör bygga på erfarenheterna inom dessa olika områden.

([17]) Kommissionens beslut om adekvat skydd för personuppgifter i tredjeländer, bland annat Argentina, Kanada, Schweiz, Förenta staterna, Guernsey, Isle of Man och Jersey, finns tillgängliga på http://ec.europa.eu/justice_home/fsj/privacy/thirdcountries/index_sv.htm.

([18]) Begränsat till en medlemsstats överföring till ett tredjeland eller ett internationellt organ av uppgifter som erhållits från en behörig myndighet i en annan medlemsstat.

Han rekommenderar en vidareutveckling av begreppet ”adekvat skyddsnivå” i samband med ett framtida instrument, på grundval av liknande kriterier som de som använts i tidigare bedömningar av adekvat skyddsnivå.

Ömsesidigt erkännande – ömsesidighet

45. Ett andra inslag i skyddsnivån gäller det ömsesidiga erkännandet av EU:s och USA:s system. I kontaktgruppens rapport nämns i detta sammanhang att målet kommer att vara att ”erhålla erkännande att motpartens system för integritets- och uppgiftsskydd är verkningsfullt på de områden som omfattas av dessa principer” ([19]) och att uppnå ”likvärdig och ömsesidig tillämpning av lagstiftningen om integritetsskydd och skydd av personuppgifter”.

46. För datatillsynsmannen är det uppenbart att ömsesidigt erkännande (eller ömsesidighet) endast är möjligt om en adekvat skyddsnivå garanteras. Med andra ord bör det framtida instrumentet harmonisera en minimiskyddsnivå (genom ett konstaterande av adekvat skyddsnivå, med beaktande av behovet av särskilda avtal från fall till fall). Endast under denna förutsättning kan ömsesidighet erkännas.

47. Den första faktorn som ska beaktas är ömsesidigheten i materiella bestämmelser om uppgiftsskydd. Datatillsynsmannen anser att ett avtal bör behandla begreppet ömsesidighet i materiella bestämmelser om uppgiftsskydd på ett sätt som säkerställer dels att behandling av uppgifter inom EU:s (och USA:s) territorium fullt ut följer de inhemska lagarna om uppgiftsskydd, dels att sådan behandling utanför det land varifrån uppgifter kommer vilken omfattas av avtalet följer de principer om uppgiftsskydd som fastställs i avtalet.

48. Den andra faktorn är ömsesidighet när det gäller systemen för tillgång till rättslig prövning. Det bör säkerställas att europeiska medborgare har tillfredsställande möjligheter till rättslig prövning när uppgifter som rör dem behandlas i Förenta staterna (oberoende av den lag som är tillämplig på den behandlingen), men också att Europeiska unionen och dess medlemsstater ger likvärdiga rättigheter till USA-medborgare.

49. Den tredje faktorn är ömsesidighet när det gäller de brottsbekämpande myndigheternas tillgång till personuppgifter. Om något instrument tillåter myndigheterna i Förenta staterna att få tillgång till uppgifter från Europeiska unionen skulle ömsesidigheten medföra att myndigheterna i EU ges samma tillgång när det gäller uppgifter från USA. Ömsesidigheten får inte skada ett verkningsfullt skydd av de registrerade personerna. Detta är en nödvändig förutsättning för att de brottsbekämpande myndigheterna ska tillåtas få ”transatlantisk” tillgång. Detta innebär konkret följande:

— Direkt tillgång för myndigheter i Förenta staterna till uppgifter inom EU:s territorium (och vice versa) bör inte tillåtas. Tillgång bör endast ges indirekt enligt ett ”pushsystem”.

— Denna tillgång bör ske under kontroll av datatskyddsmyndigheterna och de rättsliga myndigheterna i det land där uppgifterna behandlas.

— Tillgång för myndigheterna i Förenta staterna till databaser inom EU bör följa de materiella bestämmelserna om uppgiftsskydd (se ovan) och garantera fullständiga möjligheter till rättslig prövning för de registrerade personerna.

Instrumentets exakthet

50. Specificeringen av villkoren för bedömningen (adekvat skyddsnivå, likvärdighet, ömsesidigt erkännande) är viktig eftersom den bestämmer innehållet, när det gäller exakthet, rättslig säkerhet och skyddets verkningsfullhet. Innehållet i ett framtida instrument måste vara exakt och noggrant.

51. Dessutom bör det stå klart att alla särskilda avtal som ingås i ett senare skede fortfarande måste innehålla detaljerade och fullständiga garantier för uppgiftsskydd i förhållande till de registrerade personer som berörs av det planerade uppgiftsutbytet. Endast en sådan dubbel nivå av konkreta principer för uppgiftsskydd kommer att säkerställa den nödvändiga ”nära anpassningen” mellan det allmänna avtalet och särskilda avtal, vilket redan noteras i punkterna 35 och 36 i detta yttrande.

Utarbetande av en modell för andra tredjeländer

52. Det förtjänar att särskilt uppmärksammas i vilken utsträckning ett avtal med USA kan stå som modell för andra tredjeländer. Datatillsynsmannen noterar att i den ovannämnda rapporten från framtidsgruppen anges utöver USA också Ryssland som en strategisk partner för EU. I den mån principerna är neutrala och överensstämmer med grundläggande EU-garantier kan de utgöra ett användbart prejudikat. Särskilda egenskaper som är knutna till exempelvis mottagarlandets regelverk eller syftet med överföringen kommer dock att hindra en ren överföring av avtalet. Lika avgörande kommer den demokratiska situationen i tredjeländerna att vara: det bör säkerställas att de överenskomna principerna kommer att garanteras och genomföras på ett verkningsfullt sätt i mottagarlandet.

Vilka riktmärken ska användas för att bedöma skyddsnivån?

53. En underförstådd eller uttrycklig adekvat skyddsnivå bör under alla omständigheter överensstämma med det internationella och europeiska regelverket och särskilt de gemensamt överenskomna garantierna för uppgiftsskydd.

([19]) Kapitel A, Bindande internationella avtal, s. 8.

Dessa fastställs i Förenta nationernas riktlinjer, Europarådets konvention 108 och tilläggsprotokollet till denna, OECD-riktlinjerna och utkastet till rambeslut om uppgiftsskydd samt, när det gäller aspekter inom den första pelaren, direktiv 95/46/EG ([20]). Alla dessa instrument innehåller likartade principer som är mer allmänt erkända som kärnan i skyddet för personuppgifter.

54. Med hänsyn till effekterna av ett potentiellt avtal som det som avses i kontaktgruppens rapport är det särskilt viktigt att de ovannämnda principerna beaktas. Ett instrument som omfattar hela den *brottsbekämpande* sektorn i ett tredjeland skulle verkligen vara en situation som saknar motstycke. Befintliga beslut om adekvat skyddsnivå inom den första pelaren och avtal som ingåtts med tredjeländer inom EU:s tredje pelare (Europol, Eurojust) har alltid varit knutna till en specifik överföring av uppgifter, medan överföring av mycket bredare omfattning kan bli möjlig här, med hänsyn till det breda syftet (brottsbekämpning, nationell och allmän säkerhet, hävdande av gränser) och det okända antal databaser som berörs.

Grundläggande krav

55. De villkor som ska uppfyllas i samband med överföring av personuppgifter till tredjeländer har utformats i ett arbetsdokument från arbetsgruppen för skydd av enskilda med avseende på behandlingen av personuppgifter ([21]). Alla avtal om minimiprinciper för integritetsskydd bör klara en prövning för att säkerställa överensstämmelsen med verkningsfulla garantier för uppgiftsskydd.

— Avseende sakinnehåll: Principerna för uppgiftsskydd bör medge en hög skyddsnivå och uppfylla standarder som överensstämmer med EU:s principer. De tolv principerna i kontaktgruppens rapport kommer att analyseras mer ingående ur denna synvinkel i kapitel V i detta yttrande.

— Avseende exakthet: Beroende på avtalets karaktär, och särskilt om det utgör ett officiellt internationellt avtal, bör bestämmelserna och förfarandena vara så detaljerade att en verkningsfull tillämpning blir möjlig.

— Avseende tillsyn: För att säkerställa att de överenskomna bestämmelserna följs bör särskilda kontrollmekanismer införas, både internt (revisioner) och externt (översyner). Båda parter i avtalet måste få lika tillgång till dessa mekanismer. Tillsyn omfattar mekanismer för att säkerställa efterlevnad på makronivå, till exempel gemensamma mekanismer för översyn, och på mikronivå, till exempel individuell möjlighet till rättslig prövning.

56. Utöver dessa tre grundläggande krav bör särskild uppmärksamhet ägnas åt de särdrag som är knutna till behandlingen av personuppgifter i brottsbekämpningssammanhang. Detta är verkligen ett område där de grundläggande rättigheterna kan drabbas av vissa restriktioner. Garantier för att kompensera restriktionerna av de enskilda personernas rättigheter bör därför införas, särskilt med avseende på följande aspekter, med hänsyn till effekterna på de enskilda personerna:

— Öppenhet: Information och tillgång till personuppgifter kan begränsas i ett brottsbekämpningssammanhang, till exempel på grund av att det är nödvändigt med diskreta utredningar. Inom EU har traditionsenligt kompletterande mekanismer införts för att kompensera denna begränsning av de grundläggande rättigheterna (ofta med hjälp av oberoende dataskyddsmyndigheter), men det måste säkerställas att liknande kompensationsmekanismer finns tillgängliga när information har överförts till ett tredjeland.

— Möjlighet till rättslig prövning: Av de ovannämnda skälen bör enskilda personer kunna utnyttja alternativa möjligheter för att försvara sina rättigheter, särskilt genom en oberoende tillsynsmyndighet och inför en domstol.

— Bevarande av uppgifter: Motiveringen till den period under vilken uppgifterna bevaras är eventuellt inte klar och tydlig. Åtgärder måste vidtas så att detta inte hindrar de registrerade personerna eller tillsynsmyndigheterna från att faktiskt utöva sina rättigheter.

([20]) — Förenta nationernas riktlinjer avseende datoriserade personuppgiftsregister, som antogs av generalförsamlingen den 14 december 1990, tillgängliga på www.unhchr.ch/html/menu3/b/71.htm.
— Europarådets konvention om skydd för enskilda vid automatisk databehandling av personuppgifter av den 28 januari 1981, tillgänglig på www.conventions.coe.int/treaty/en/Treaties/html/108.htm.
— OECD:s riktlinjer för integritetsskydd och gränsöverskridande flöden av personuppgifter, som antogs den 23 september 1980, tillgängliga på www.oecd.org/document/20/0,3343.en_2649_34255_15589524_1_1_1_1,00.html.
— Utkast till rådets rambeslut om skydd av personuppgifter som behandlas inom ramen för polissamarbete och straffrättsligt samarbete, tillgängligt på http://ec.europa.eu/prelex/detail_dossier_real.cfm?CL=sv&DosId=193371.
— 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, EGT L 281, 23.11.1995, s. 31.

([21]) Arbetsdokument av den 24 juli 1998 om överföring av personuppgifter till tredjeländer: tillämpning av artiklarna 25 och 26 i EU:s direktiv om uppgiftsskydd, WP12.

— De brottsbekämpande myndigheternas redovisningsskyldighet: I avsaknad av faktisk öppenhet kan kontrollmekanismerna inte på något sätt vara heltäckande, vare sig för de enskilda eller de institutionella berörda parterna. Det kommer ändå att vara av avgörande betydelse att sådana kontroller fastställs strikt, med hänsyn till uppgifternas känslighet och de tvångsåtgärder som kan vidtas mot enskilda personer på grundval av behandlingen av uppgifterna. Redovisningsskyldighet är en avgörande fråga i förhållande till nationella kontrollmekanismer i mottagarlandet, men också i förhållande till översynsmöjligheterna för det land eller den region varifrån uppgifter kommer. Sådana översynsmekanismer föreskrivs i särskilda avtal som PNR-avtalet och datatillsynsmannen rekommenderar starkt att de ska införas också i det allmänna instrumentet.

V. **ANALYS AV PRINCIPERNA**

Inledning

57. I detta kapitel analyseras de tolv principerna i kontaktgruppens dokument med utgångspunkt i följande:

— Dessa principer visar att USA:s och EU:s synsätt när det gäller principernas nivå i viss mån sammanfaller, eftersom likheter kan noteras med principerna i konvention 108.

— Enighet om principernas nivå är dock inte tillräckligt. Ett rättsligt instrument måste vara så starkt att efterlevnaden säkerställs.

— Datatillsynsmannen beklagar att principerna inte åtföljs av en motivering.

— Innan beskrivningen av principerna diskuteras bör det klargöras att båda parter har samma tolkning av den formulering som används, till exempel när det gäller begreppen personuppgifter och enskilda personer som skyddas. Det skulle vara välkommet med definitioner i detta avseende.

1. Specificering av syftet

58. I den första principen som förtecknas i bilagan till kontaktgruppens rapport anges att personuppgifter ska behandlas för lagenliga brottsbekämpningssyften. Som nämns ovan gäller detta för Europeiska unionens del förebyggande, upptäckt, utredning eller lagföring av brott. För USA:s del går dock tolkningen av brottsbekämpning utöver straffbara gärningar och omfattar ”hävdande av gränser, allmän säkerhet och nationell säkerhet”. Konsekvenserna av sådana skillnader mellan EU:s och USA:s angivna syften är inte tydliga. I rapporten anges att syftena i stor utsträckning kan sammanfalla i praktiken, men det är avgörande att veta exakt i vilken utsträckning de *inte* sammanfaller. Med tanke på konsekvenserna av de åtgärder som vidtas mot enskilda personer måste principen om begränsning av syftet följas strikt på brottsbekämpningsområdet och de angivna syftena måste vara tydliga och begränsade. Med hänsyn till den ömsesidighet som avses i rapporten förefaller det också vara väsentligt med en tillnärmning av dessa syften. Kort sagt måste tolkningen av denna princip klargöras.

2. Integritetsskydd/uppgiftskvalitet

59. Datatillsynsmannen välkomnar bestämmelsen om att det för lagenlig behandling är nödvändigt med krav på korrekta, relevanta och fullständiga personuppgifter i rätt tid. En sådan princip är ett grundläggande villkor för all effektiv behandling av uppgifter.

3. Nödvändighet/proportionalitet

60. Principen innebär en nära koppling mellan den insamlade informationen och denna informations nödvändighet för att uppfylla ett brottsbekämpningssyfte som fastställs enligt lag. Detta krav på en rättslig grund är en positiv faktor när det gäller att garantera behandlingens lagenlighet. Trots att detta stärker behandlingens rättsliga säkerhet noterar dock datatillsynsmannen att den rättsliga grunden för denna behandling utgörs av en lag i ett tredjeland. En lag i ett tredjeland kan inte i sig utgöra en legitim grund för en överföring av personuppgifter ([22]). I kontaktgruppens rapport förefaller det förutsättas att legitimiteten av lagen i ett tredjeland, till exempel Förenta staterna, i princip erkänns. Det bör hållas i åtanke att om ett sådant resonemang kan vara berättigat här, med hänsyn till att Förenta staterna är en demokratisk stat, skulle samma system inte vara giltigt för och kunna överföras till förbindelserna med något annat tredjeland.

61. Enligt bilagan till kontaktgruppens rapport måste alla överföringar av personuppgifter vara relevanta, nödvändiga och lämpliga. Datatillsynsmannen betonar att om behandlingen ska vara proportionell får den inte vara onödigt inkräktande och förfarandena för behandlingen måste vara väl avvägda, med beaktande av de registrerade personernas rättigheter och intressen.

62. Av detta skäl bör tillgång ges till information från fall till fall, beroende på de praktiska behoven i samband med en specifik utredning. Permanent tillgång för brottsbekämpande myndigheter i ett tredjeland till databaser i EU bör betraktas som oproportionell och otillräckligt motiverad.

([22]) Se särskilt artikel 7 c och e i direktiv 95/46/EG. I sitt yttrande 6/2002 av den 24 oktober 2002 om överföring av passagerarlistor och andra uppgifter från flygbolag till Förenta staterna förklarade arbetsgruppen för skydd av enskilda med avseende på behandlingen av personuppgifter att ”det inte förefaller godtagbart att ett ensidigt beslut som fattats av ett tredjeland av skäl som hänför sig till dess eget allmänintresse ska leda till rutinmässig och omfattande överföring av uppgifter som skyddas enligt det direktivet”.

Datatillsynsmannen erinrar om att även i samband med befintliga avtal om utbyte av uppgifter, till exempel när det gäller PNR-avtalet, baseras utbytet av uppgifter på särskilda omständigheter och avtal har ingåtts för en begränsad tidsperiod ([23]).

63. Enligt samma logik bör tidsperioden för bevarandet av uppgifter regleras: uppgifterna bör bevaras endast så länge de behövs med hänsyn till det specifika syftet. Om de inte längre är relevanta i förhållande till det fastställda syftet bör de raderas. Datatillsynsmannen motsätter sig starkt upprättandet av datalager där information om icke misstänkta personer skulle lagras med tanke på ett eventuellt kommande behov.

4. Informationssäkerhet

64. Åtgärder och förfaranden för att skydda uppgifter från missbruk, ändring och andra risker utvecklas i principerna, liksom en bestämmelse om att endast behöriga personer ska få tillgång till uppgifterna. Datatillsynsmannen anser att detta är tillfredsställande.

65. Principen kan också kompletteras med en bestämmelse om att register ska föras över de personer som konsulterar uppgifterna. Detta skulle stärka verkningsfullheten av garantierna för att begränsa tillgången och förhindra missbruk av uppgifterna.

66. Dessutom bör det föreskrivas ömsesidig information vid fall av säkerhetsöverträdelser: mottagare såväl i USA som i EU skulle vara ansvariga för att informera sina motparter i det fall att uppgifter som de har erhållit lämnats ut olagligen. Detta kommer att bidra till ökat ansvar för en säker behandling av uppgifterna.

5. Särskilda kategorier av personuppgifter

67. Datatillsynsmannen anser att principen om förbud mot behandling av känsliga uppgifter försvagas avsevärt genom det undantag som tillåter behandling av känsliga uppgifter om den inhemska lagen föreskriver ”lämpliga garantier” i samband med detta. Just på grund av uppgifternas känsliga karaktär måste alla undantag från principen om förbud motiveras tillfredsställande och exakt, och det bör finnas en förteckning över vilka syften och omständigheter som medför att det är tillåtet att behandla en fastställd typ av känsliga uppgifter, samt uppgift om vilka kategorier av registeransvariga som har rätt att behandla dessa typer av uppgifter. Bland de garantier som ska införas anser datatillsynsmannen att det bör ingå att känsliga uppgifter som sådana inte bör utgöra en utlösande faktor för en utredning. Uppgifterna kan göras tillgängliga under särskilda omständigheter, men endast som kompletterande information om en registrerad person som redan är föremål för utredning. Dessa garantier och villkor måste förtecknas på ett begränsande sätt i texten till principen.

6. Redovisningsskyldighet

68. Enligt diskussionen i punkterna 55–56 i detta yttrande måste redovisningsskyldigheten för de offentliga myndigheter som behandlar personuppgifter säkerställas på ett verkningsfullt sätt, och garantier måste ges i avtalet för hur denna redovisningsskyldighet ska ombesörjas. Detta är alldeles särskilt viktigt med tanke på den brist på öppenhet som traditionellt är förknippad med behandlingen av personuppgifter i brottsbekämpningssammanhang. Med hänsyn till detta är ett omnämnande, som nu är fallet i bilagan, av att de offentliga myndigheterna ska vara redovisningsskyldiga, men utan att någon ytterligare förklaring ges av förfarandena för och konsekvenserna av denna redovisningsskyldighet, ingen tillfredsställande garanti. Datatillsynsmannen rekommenderar att en sådan förklaring ska ges i texten till instrumentet.

7. Oberoende och verkningsfull tillsyn

69. Datatillsynsmannen stöder fullt ut att det införs en bestämmelse som föreskriver oberoende och verkningsfull tillsyn av en eller flera offentliga tillsynsmyndigheter. Han anser att tolkningen av oberoende bör klargöras, särskilt vem dessa myndigheter är oberoende av och vem de ska rapportera till. Det behövs kriterier i detta avseende, vilka bör beakta institutionellt och funktionellt oberoende i förhållande till de verkställande och lagstiftande organen. Datatillsynsmannen erinrar om att detta är en väsentlig faktor för att säkerställa att de överenskomna principerna följs på ett verkningsfullt sätt. Dessa myndigheters befogenheter när det gäller intervention och säkerställande av efterlevnad är också avgörande i samband med frågan om redovisningsskyldigheten för de offentliga myndigheter som behandlar personuppgifter, vilket nämns ovan. Deras existens och behörighet bör göras tydligt synbara för de registrerade personerna, så att det blir möjligt för dessa att utöva sina rättigheter, särskilt om flera myndigheter är behöriga beroende på i vilket sammanhang behandlingen sker.

70. Datatillsynsmannen rekommenderar dessutom att det i ett framtida avtal också ska fastställas samarbetsmekanismer mellan tillsynsmyndigheterna.

8. Individuell tillgång och rättelse

71. Specifika garantier krävs när det gäller tillgång och rättelse i brottsbekämpningssammanhang. Datatillsynsmannen välkomnar därför den princip i vilken det konstateras att enskilda personer ska/bör få tillgång till och möjligheter att söka ”rättelse och/eller radering av sina personuppgifter”. Viss osäkerhet kvarstår dock när det gäller definitionen av enskilda personer (alla registrerade personer bör skyddas och inte endast medborgare i det berörda landet)

([23]) Avtalet ska upphöra att gälla sju år efter den dag då det undertecknades, om inte parterna ömsesidigt beslutar att ersätta det.

samt de villkor som gäller för att enskilda personer ska kunna göra invändningar mot behandlingen av uppgifter som rör dem. Det bör preciseras i vilka ”lämpliga fall” en invändning kan eller inte kan göras. Det bör stå klart för de registrerade personerna under vilka omständigheter, beroende till exempel på typen av myndighet, typen av utredning eller andra kriterier, som de kommer att kunna utöva sina rättigheter.

72. Om det av berättigade skäl inte finns någon direkt möjlighet att invända mot en behandling bör vidare en indirekt kontroll finnas tillgänglig, genom den oberoende myndighet som ansvarar för tillsynen av behandlingen.

9. Öppenhet och meddelande

73. Datatillsynsmannen betonar ännu en gång vikten av faktisk öppenhet, för att de enskilda personerna ska kunna utöva sina rättigheter och för att bidra till den allmänna redovisningsskyldigheten för offentliga myndigheter som behandlar personuppgifter. Han stöder principerna, så som de utformats, och insisterar särskilt på behovet av allmänt *och* individuellt meddelande till den enskilda personen. Detta återspeglas i den princip som utformas i punkt 9 i bilagan.

74. I kapitel 2 punkt A.B i rapporten (”Överenskomna principer”) anges emellertid att i USA kan öppenhet omfatta ”enbart eller i kombination med varandra, offentliggörande i det federala registret, personligt meddelande och avslöjande vid en rättegång”. Det måste stå klart att ett offentliggörande i en officiell tidning inte i sig är tillräckligt för att garantera lämplig information till den registrerade personen. Utöver behovet av personligt meddelande erinrar datatillsynsmannen om att informationen måste lämnas i en form och på ett språk som är lätt att förstå för den registrerade personen.

10. Möjlighet till rättslig prövning

75. För att garantera att enskilda personer faktiskt ska kunna utöva sina rättigheter måste dessa personer ha möjlighet att lämna in ett klagomål till en oberoende dataskyddsmyndighet samt ha tillgång till ett rättsmedel inför en oberoende och opartisk domstol. Båda möjligheterna till rättslig prövning bör vara tillgängliga i lika stor utsträckning.

76. Det är nödvändigt med tillgång till en oberoende dataskyddsmyndighet, eftersom detta erbjuder en flexibel och mindre kostsam hjälp i ett sammanhang, brottsbekämpning, som kan vara ganska ogenomskinligt för enskilda personer. Dataskyddsmyndigheterna kan också ge bistånd när det gäller att utöva rättigheten till tillgång på de registrerade personernas vägnar, när undantag hindrar dessa från att få direkt tillgång till de personuppgifter som rör dem.

77. Tillgång till det rättsliga systemet är en ytterligare och oundgänglig garanti för att de registrerade personerna ska kunna få tillgång till rättslig prövning inför en myndighet som tillhör en gren av det demokratiska systemet som är skild från de offentliga institutioner som faktiskt behandlar deras uppgifter. EG-domstolen ([24]) har fastställt att ett sådant verkningsfullt rättsmedel inför en domstol är viktigt ”så att den enskildes rättigheter kan ges ett effektivt skydd. (…) [Det] utgör en allmän gemenskapsrättslig princip som härrör från de konstitutionella traditioner som är gemensamma för medlemsstaterna och som fastställs i artiklarna 6 och 13 i Europeiska konventionen angående skydd för de mänskliga rättigheterna och de grundläggande friheterna.” Förekomsten av ett rättsmedel anges också uttryckligen i artikel 47 i Europeiska unionens stadga om de grundläggande rättigheterna och i artikel 22 i direktiv 95/46/EG, utan att det påverkar möjligheten att utnyttja något administrativt förfarande.

11. Databehandlade enskilda beslut

78. Datatillsynsmannen välkomnar bestämmelsen om lämpliga garantier vid databehandling av personuppgifter. Han noterar att en gemensam tolkning av vad som betraktas som en ”betydande skadlig åtgärd som rör den enskilda personens relevanta intressen” skulle klargöra villkoren för tillämpningen av denna princip.

12. Vidareöverföringar

79. Villkoren för vissa vidareöverföringar är oklara. Särskilt när vidareöverföringen ska överensstämma med internationella avtal och avtal mellan de sändande och mottagande länderna bör det anges huruvida det gäller avtal mellan de båda länder som har tagit initiativ till den första överföringen eller mellan de båda länder som är inblandade i vidareöverföringen. Datatillsynsmannen anser att det under alla omständigheter krävs avtal mellan de båda länder som har tagit initiativ till den första överföringen.

80. Datatillsynsmannen noterar också en mycket bred definition av de ”legitima allmänna intressen” som medger en vidareöverföring. Räckvidden för allmän säkerhet förblir oklar och utvidgningen till överföringar vid fall av brott mot etiska regler eller reglerade yrken förefaller oberättigad och alltför omfattande i ett brottsbekämpningssammanhang.

VI. **SLUTSATS**

81. Datatillsynsmannen välkomnar EU- och USA-myndigheternas gemensamma arbete på området för brottsbekämpning, där uppgiftsskydd är av avgörande betydelse. Han vill dock framhålla att frågan är komplicerad, särskilt

([24]) Mål 222/84, Johnston, REG 1986, s. 1651, mål 222/86, Heylens, REG 1987, s. 4097, och mål C-97/91, Borelli, REG 1992, s. I-6313.

när det gäller dess exakta omfattning och art, och att den därför förtjänar noggrann och ingående analys. Ett transatlantiskt instruments effekter på uppgiftsskyddet bör övervägas noggrant i förhållande till det befintliga regelverket och konsekvenserna för medborgarna.

82. Datatillsynsmannen uppmanar till större tydlighet och konkreta bestämmelser, särskilt när det gäller följande aspekter:

— Förtydligande när det gäller instrumentets karaktär, som bör vara rättsligt bindande för att erbjuda tillräcklig rättslig säkerhet.

— Ett noggrant konstaterande av adekvat skyddsnivå, på grundval av väsentliga krav rörande systemets innehåll, särdrag och tillsyn. Datatillsynsmannen anser att det allmänna instrumentets adekvata skyddsnivå kan erkännas endast om det kombineras med adekvata särskilda avtal från fall till fall.

— Ett begränsat tillämpningsområde, med en tydlig och gemensam definition av de brottsbekämpningssyften som berörs.

— Preciseringar av villkoren för att privata enheter ska kunna medverka i system för uppgiftsöverföring.

— Överensstämmelse med proportionalitetsprincipen, vilket innebär utbyte av uppgifter från fall till fall när det finns ett konkret behov.

— Kraftfulla tillsynssystem samt system för rättslig prövning som är tillgängliga för registrerade personer, inklusive administrativa förfaranden och rättsmedel.

— Verkningsfulla åtgärder som garanterar att alla registrerade personer kan utöva sina rättigheter, oberoende av deras medborgarskap.

— Medverkan av oberoende dataskyddsmyndigheter, särskilt i samband med tillsyn och bistånd till registrerade personer.

83. Datatillsynsmannen insisterar på att all brådska bör undvikas när principerna utarbetas, eftersom detta endast kan leda till otillfredsställande lösningar, med effekter som är motsatta dem som avses i fråga om uppgiftsskydd. Den bästa vägen framåt skulle därför i detta skede vara utarbetandet av en färdplan mot ett eventuellt avtal vid en senare tidpunkt.

84. Datatillsynsmannen uppmanar också till större öppenhet när det gäller utarbetandet av principerna för uppgiftsskydd. Endast om samtliga berörda parter, inklusive Europaparlamentet, medverkar kan instrumentet dra fördel av en demokratisk debatt och få det nödvändiga stödet och erkännandet.

Utfärdat i Bryssel den 11 november 2008

Peter HUSTINX

Europeisk datatillsynsman