

## EUROPEISKA DATATILLSYNSMANNEN

### Europeiska datatillsynsmannens yttrande om förslaget till rådets rambeslut om skydd av personuppgifter som behandlas inom ramen för polissamarbete och straffrättsligt samarbete (KOM(2005) 475 slutlig)

(2006/C 47/12)

EUROPEISKA DATATILLSYNSMANNEN har,

Förslagets betydelse

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 begäran om ett yttrande i enlighet med artikel 28.2 i 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.

ANTAGIT FÖLJANDE YTTRANDE:

#### I. INLEDANDE ANMÄRKNINGAR

Samråd med datatillsynsmannen

1. Kommissionen skickade förslaget till rådets rambeslut om skydd av personuppgifter som behandlas inom ramen för polissamarbete och straffrättsligt samarbete till datatillsynsmannen i ett brev av den 4 oktober 2005. Datatillsynsmannen ser brevet som en begäran om samråd från gemenskapens institutioner och organ i enlighet med artikel 28.2 i förordning nr 45/2001/EG. Enligt datatillsynsmannen bör detta yttrande nämnas i ingressen till rambeslutet.

2. Datatillsynsmannen betonar förslagets betydelse med tanke på fysiska personers grundläggande rättigheter och friheter att få sina personuppgifter skyddade. Om förslaget antas, skulle det innebära ett betydande steg framåt i skyddet av personuppgifter på ett viktigt område, som framför allt kräver en enhetlig och effektiv mekanism för skyddet av personuppgifter inom Europeiska unionen.

3. I detta sammanhang betonar datatillsynsmannen att polis-samarbete och rättsligt samarbete mellan medlemsstaterna, som ett inslag i det gradvisa upprättandet av ett område med frihet, säkerhet och rättvisa, får allt större betydelse. Haagprogrammet har infört principen om tillgänglighet för att förbättra det gränsöverskridande utbytet av information om brottsbekämpning. Enligt Haagprogrammet <sup>(1)</sup> bör bara det faktum att information är gränsöverskridande inte längre vara tillräckligt. Införandet av principen om tillgänglighet återspeglar en mer allmän tendens att underlätta utbytet av information om brottsbekämpning (se t.ex. den s.k. Prümkonventionen <sup>(2)</sup>, som undertecknats av sju medlemsstater, samt det svenska förslaget till rambeslut om förenklat informations- och underrättelseutbyte mellan de brottsbekämpande myndigheterna <sup>(3)</sup>). Europaparlamentets godkännande helt nyligen av Europaparlamentets och rådets direktiv om lagring av kommunikationsuppgifter <sup>(4)</sup> kan ses i samma perspektiv. Denna utveckling kräver att ett rättsligt instrument antas för att garantera ett effektivt skydd för personuppgifter inom alla medlemsstater i Europeiska unionen, baserat på gemensamma normer.

<sup>(1)</sup> Punkt 18 i programmet.

<sup>(2)</sup> Konvention mellan Konungariket Belgien, Förbundsrepubliken Tyskland, Konungariket Spanien, Republiken Frankrike, Storhertigdömet Luxemburg, Konungariket Nederländerna och Republiken Österrike om utökad gränsöverskridande samarbete, särskilt för att bekämpa terrorism, gränsöverskridande brottslighet och olaglig invandring. Prüm (Tyskland) den 27 maj 2005.

<sup>(3)</sup> Konungariket Sveriges initiativ inför antagandet av ett rambeslut om förenklat uppgifts- och underrättelseutbyte mellan de brottsbekämpande myndigheterna i Europeiska unionens medlemsstater, särskilt i fråga om grova brott, inbegripet terroristdåd (EUT C 281, 18.11.2005).

<sup>(4)</sup> På grundval av förslaget till Europaparlamentets och rådets direktiv om lagring av uppgifter som behandlas i samband med tillhandahållande av allmänt tillgängliga elektroniska kommunikationstjänster och om ändring av direktiv 2002/58/EG (KOM(2005) 438 slutlig).

4. Datatillsynsmannen påpekar att den nuvarande allmänna ramen för uppgiftsskydd på detta område är otillräcklig. För det första gäller inte direktiv 95/46/EG för sådan behandling av personuppgifter som utgör ett led i en verksamhet som inte omfattas av gemenskapsrätten, exempelvis sådan verksamhet som avses i avdelning VI i fördraget om Europeiska unionen (artikel 3.2 i direktivet). Även om tillämpningsområdet för genomförandebestämmelserna i flertalet medlemsstater är vidare än vad själva direktivet kräver och inte utesluter behandling av uppgifter för brottsbekämpning, finns det betydande skillnader i nationell rätt. För det andra innehåller Europarådets konvention nr 108 <sup>(1)</sup>, av vilken alla medlemsstater är bundna, inte tillräckligt precisa bestämmelser om skydd, vilket erkändes redan när direktiv 95/46/EG antogs. För det tredje beaktar ingen av dessa två rättsakter det som är särskilt utmärkande för polismyndigheternas och de rättsliga myndigheternas utbyte av uppgifter <sup>(2)</sup>.

*Ett bidrag till att samarbetet i sig skall bli framgångsrikt*

5. Ett effektivt skydd av personuppgifter är inte bara viktigt för de registrerade utan bidrar också till att polis-samarbetet och det rättsliga samarbetet i sig blir framgångsrika. På många sätt går båda de allmänna intressena hand i hand.
6. Man måste komma ihåg att personuppgifterna i fråga ganska ofta är av känslig natur och har erhållits av polisen och de rättsliga myndigheterna som ett resultat av en utredning om personer. Villigheten att utbyta dessa uppgifter med myndigheter i andra medlemsstater kommer att öka om en myndighet försäkras om skyddsnivån i den andra medlemsstaten. Datatillsynsmannen nämner datakonfidentialitet och datasäkerhet samt begränsning av tillgång och vidare användning som relevanta inslag i uppgiftsskydd.
7. Dessutom kan personuppgifternas korrekthet och tillförlitlighet garanteras genom en hög nivå på uppgiftsskyddet. Vid utbyte av uppgifter mellan polisen och/eller de rättsliga myndigheterna blir det ännu viktigare att dessa uppgifter är korrekta och tillförlitliga, särskilt som uppgifter efter på varandra följande utbyten och nya översändanden av uppgifter mellan de brottsbekämpande myndigheterna i slutändan behandlas långt från källan och utanför det sammanhang där de ursprungligen samlades in och användes. Normalt känner de mottagande myndigheterna inte till de ytterligare omständigheterna och måste lita helt på själva uppgifterna.
8. Harmoniseringen av de nationella reglerna om personuppgifter inom polisen och rättsväsendet, inklusive lämpliga säkerhetsåtgärder för skyddet av dessa uppgifter, kan således öka det ömsesidiga förtroendet och effektiviteten i själva utbytet.

<sup>(1)</sup> Europarådets konvention om skydd för enskilda vid automatisk databehandling av personuppgifter av den 28 januari 1981.

<sup>(2)</sup> 1987 utfärdade Europarådet rekommendation nr R (87) 15 om polisens användning av personuppgifter, men denna rekommendation är inte bindande för medlemsstaterna.

*Iakttagande av principerna om uppgiftsskydd, kombinerat med ytterligare en rad regler*

9. Behovet och betydelsen av detta förslag har betonats vid flera tillfällen. Under vårkonferensen i Krakow i april 2005 antog de europeiska dataskyddsmyndigheterna ett uttalande och ett sammanfattande dokument, där de efterlyste antagandet av en ny rättslig ram för uppgiftsskydd vilken kan tillämpas på verksamhet under tredje pelaren. I denna nya ram bör man inte endast iaktta principerna för dataskydd enligt direktiv 95/46/EG – det är viktigt att garantera ett enhetligt uppgiftsskydd inom Europeiska unionen – utan där bör även fastställas ytterligare en rad regler med beaktande av brottsbekämpningens särskilda natur <sup>(3)</sup>. Datatillsynsmannen välkomnar att förslaget som utgångspunkt beaktar principerna om uppgiftsskydd enligt direktiv 95/46/EG och att ytterligare ett antal regler fastställs.

10. I detta yttrande kommer det att analyseras i vilken utsträckning resultatet kan godtas ur ett dataskyddsperspektiv, med vederbörlig hänsyn till det specifika sammanhang som dataskydd på brottsbekämpningsområdet utgör. Dels är de berörda uppgifterna ganska ofta av mycket känslig natur (se punkt 6 i detta yttrande), dels är trycket på att få tillgång till dessa uppgifter starkt, så att de brottsbekämpande organen skall kunna utföra ett effektivt arbete, vilket kan omfatta skydd av personers liv och fysiska säkerhet. Enligt datatillsynsmannen bör dataskyddsregler motsvara de brottsbekämpande organens berättigade behov, men även skydda den registrerade mot oberättigad behandling och tillgång. För att överensstämma med proportionalitetsprincipen bör resultatet av den europeiska lagstiftarens överväganden avspegla respekten för de två potentiellt motsatta allmänna intressena. I detta sammanhang nämner datatillsynsmannen återigen att båda dessa intressen ofta går hand i hand.

*Avdelning VI i fördraget om Europeiska unionen*

11. Slutligen skall det nämnas att förslaget omfattas av avdelning VI i fördraget om Europeiska unionen, den s.k. tredje pelaren. Den europeiska lagstiftarens ingripande omfattas av tydliga begränsningar: begränsningar av unionens lagstiftande befogenheter till de områden som avses i artiklarna 30 och 31, begränsningar när det gäller lagstiftningsförfarandet som inte omfattar fullt deltagande av Europaparlamentet, och begränsningar när det gäller den rättsliga kontrollen, eftersom EG-domstolens behörighet enligt artikel 35 i EU-fördraget är ofullständig. Dessa begränsningar kräver en ännu mer noggrann analys av förslagstexten.

<sup>(3)</sup> Se i detta sammanhang "Den europeiska datatillsynsmannen som rådgivare till gemenskapens institutioner när det gäller förslag till lagstiftning och därtill hörande dokument", 18 mars 2005, offentliggjort på [www.edps.eu.int](http://www.edps.eu.int).

## II. KONTEXT: INFORMATIONsutBYTE ENLIGT PRINCIPEN OM TILLGÄNGLIGHET, LAGRING AV UPPGIFTER OCH DE SPECIFIKA RAMARNA SIS II OCH VIS

### II.1 Principen om tillgänglighet

12. Förslaget är nära kopplat till förslaget till rådets rambeslut om utbyte av uppgifter enligt principen om tillgänglighet (KOM(2005) 490 slutlig). Syftet med det sistnämnda förslaget är att genomföra principen om tillgänglighet och därigenom se till att uppgifter som är tillgängliga för behöriga myndigheter i en medlemsstat för kampen mot brottslighet lämnas till motsvarande myndigheter i andra medlemsstater. Det bör leda till att de inre gränserna för utbytet av dessa uppgifter avskaffas genom att utbytet av uppgifter underkastas enhetliga villkor i hela unionen.

13. Den nära kopplingen mellan de två förslagen beror på att uppgifter om brottsbekämpning i stor utsträckning omfattar personuppgifter. Lagstiftning om utbyte av uppgifter om brottsbekämpning kan inte antas utan att tillräckligt skydd för personuppgifter garanteras. Om ett ingripande på unionsnivå leder till att de inre gränserna för utbytet av dessa uppgifter avskaffas kan skyddet av personuppgifter inte längre endast vara en fråga för nationell rätt. Det har blivit de europeiska institutionernas uppgift att garantera skyddet av personuppgifter inom hela unionens territorium utan inre gränser. Denna uppgift anges klart och tydligt i artikel 30.1 b i EU-fördraget och är en följd av unionens skyldighet att respektera grundläggande rättigheter (artikel 6 i EU-fördraget). Dessutom gäller följande:

— I artikel 1.2 i det aktuella förslaget anges uttryckligen att medlemsstaterna inte längre får begränsa eller förbjuda det gränsöverskridande informationsflödet av skäl som grundar sig på skyddet av personuppgifter.

— Förslaget till rambeslut om utbyte av uppgifter enligt principen om tillgänglighet innehåller flera hänvisningar till det aktuella förslaget.

14. Datatillsynsmannen påpekar att rådets rambeslut om utbyte av uppgifter enligt principen om tillgänglighet endast bör antas under förutsättning att ett rambeslut om skydd av personuppgifter också antas. Det aktuella förslaget till rådets rambeslut om skydd av uppgifter har dock sina egna förtjänster och behövs även om en rättsakt om tillgänglighet saknas. Detta har framhållits i avsnitt I i detta yttrande.

15. Datatillsynsmannen kommer därför att analysera de båda förslagen i två separata yttranden. Det finns också ett praktiskt skäl till detta. Det finns ingen garanti för att förslagen kommer att behandlas gemensamt och lika snabbt av rådet och Europaparlamentet.

### II.2 Datalagring

16. Den 26 september 2005 lade datatillsynsmannen fram sitt yttrande om förslaget till direktiv om lagring av kommunikationsuppgifter<sup>(1)</sup>. I detta yttrande pekade han på några viktiga brister i förslaget och föreslog att man till direktivet fogar specifika bestämmelser om de behöriga myndigheternas tillgång till trafik- och lokaliseringssuppgifter och om den vidare användningen av uppgifterna samt ytterligare extra skyddsåtgärder för uppgiftsskydd. Den text till direktivet som antagits av Europaparlamentet och rådet innehåller en begränsad, men på inget sätt tillräcklig, bestämmelse om uppgiftsskydd och datasäkerhet och en ännu mer otillräcklig bestämmelse om tillgång, där utfärdandet av bestämmelser om tillgången till lagrade uppgifter skjuts till nationell rätt, med förbehåll för tillämpliga bestämmelser i Europeiska unionens lagstiftning eller folkrätten.

17. Godkännandet av direktivet om lagring av kommunikationsutgifter gör det ännu mer brådskande att fastställa en rättslig ram för uppgiftsskydd inom tredje pelaren. Genom att anta direktivet förpliktar gemenskapens lagstiftare leverantörerna av telekommunikations- och Internettjänster att lagra uppgifter för brottsbekämpningsändamål utan de nödvändiga och lämpliga mekanismerna för skydd av den registrerade. Det finns fortfarande en lucka i skyddet, eftersom direktivet inte (i tillräcklig utsträckning) tar upp tillgången till uppgifter eller deras vidare användning, när behöriga myndigheter på brottsbekämpningsområdet har fått tillgång till uppgifter.

18. Det aktuella förslaget fyller igen en betydande del av denna lucka, eftersom det gäller den vidare användningen av uppgifterna efter det att de brottsbekämpande myndigheterna har fått tillgång till dem. Datatillsynsmannen beklagar dock att förslaget inte heller tar upp tillgången till dessa uppgifter. I motsats till vad som anges för systemen SIS II och VIS (se II.3 i detta yttrande) överläts det åt den nationella lagstiftaren att avgöra denna fråga.

### II.3 Behandling inom ramen för SIS II och VIS

19. Europeiska unionen använder eller utvecklar för närvarande flera storskaliga informationssystem (Eurodac, SIS II, VIS) och strävar efter synergier mellan dessa system. Det finns också en ökande tendens att bevilja en mer omfattande tillgång till dessa system för brottsbekämpningsändamål. Denna långtgående utveckling måste enligt Haagprogrammet ta hänsyn till "nödvändigheten av att uppnå rätt balans mellan brottsförebyggande syften och skyddet av enskildas grundläggande rättigheter".

<sup>(1)</sup> Europeiska datatillsynsmannens yttrande om förslaget till Europaparlamentets och rådets direktiv om lagring av uppgifter som behandlats i samband med tillhandahållande av allmänt tillgängliga elektroniska kommunikationstjänster och om ändring av direktiv 2002/58/EG (KOM(2005) 438 slutlig), offentliggjort på [www.edp-s.eu.int](http://www.edp-s.eu.int).

20. I sitt yttrande av den 19 oktober 2005 om förslagen till en andra generation av Schengens informationssystem (SIS II) <sup>(1)</sup> betonade datatillsynsmannen de delar som rör samtidig tillämpning av generella regler (*lex generalis*) och mer specifika regler (*lex specialis*) om uppgiftsskydd. Det aktuella förslaget kan ses som en *lex generalis* som ersätter konvention nr 108 inom ramen för tredje pelaren <sup>(2)</sup>.
21. Datatillsynsmannen understryker i detta sammanhang att förslaget även innehåller bestämmelser om en allmän ram för uppgiftsskydd för specifika instrument såsom tredje pelarens del av SIS II och de brottsbekämpande organens tillgång till informationssystemet för viseringar <sup>(3)</sup>.

### III. FÖRSLAGETS KÄRNA

#### III.1 Gemensamma normer för all behandling

##### Utgångspunkt

22. Enligt artikel 1.1. i förslaget är dess syfte att fastställa gemensamma normer för skyddet av personuppgifter i samband med verksamhet inom ramen för polissamarbete och straffrättsligt samarbete. Artikel 1.1. bör läsas tillsammans med artikel 3.1, enligt vilken förslaget skall gälla behandling av personuppgifter (...) av en behörig myndighet för att förebygga, utreda, avslöja och lagföra brott.
23. Av dessa bestämmelser följer att det föreslagna rambeslutet har två viktiga särdrag: Det innehåller gemensamma normer och det gäller all behandling för brottsbekämpningsändamål, även om de berörda uppgifterna inte har översänts eller gjorts tillgängliga av behöriga myndigheter i andra medlemsstater.
24. Datatillsynsmannen betonar dessa två särdrags betydelse. Det aktuella förslaget bör sträva efter att fastställa en ram för uppgiftsskydd vilken fullt ut kompletterar den redan befintliga rättsliga ramen inom första pelaren. Endast om detta villkor uppfylls, fullgör Europeiska unionen fullt ut sin skyldighet enligt artikel 6.2 i EU-fördraget att respektera de grundläggande rättigheterna, såsom de garanteras i Europakonventionen om skydd för de mänskliga rättigheterna och de grundläggande friheterna.

<sup>(1)</sup> Punkt 2.2.4 i yttrandet.

<sup>(2)</sup> Europarådets konvention om skydd för enskilda vid automatisk databehandling av personuppgifter av den 28 januari 1981.

<sup>(3)</sup> Förslag till rådets beslut om möjlighet till sökningar i informationssystemet för viseringar (VIS) för medlemsstatsmyndigheter med ansvar för intern säkerhet och för Europol för att förhindra, upptäcka och utreda terroristbrott och andra grova brott som lades fram den 24 november 2005. Datatillsynsmannen har för avsikt att yttra sig om förslaget i början av 2006.

##### Gemensamma normer

25. Vad beträffar det första särdraget är syftet med förslaget att se till att de befintliga principerna om uppgiftsskydd kommer att tillämpas inom tredje pelarens område. Dessutom innehåller det bestämmelser om gemensamma normer där dessa principer specificeras med tanke på deras tillämpning på detta område. Datatillsynsmannen understryker betydelsen av dessa aspekter av förslaget. De återspeglar den specifika och känsliga karaktär som behandlingen av personuppgifter på detta område har. Datatillsynsmannen uppskattar särskilt införandet av principen om åtskillnad mellan personuppgifter om olika kategorier av personer som en specifik princip för uppgiftsskydd inom området polissamarbete och straffrättsligt samarbete, utöver befintliga principer om uppgiftsskydd (artikel 4.4). Enligt datatillsynsmannen bör själva principen och dess rättsliga följder för den registrerade till och med specificeras *ytterligare* (se punkterna 88-92 i detta yttrande).
26. Reglerna måste gälla för olika situationer och kan därför inte vara alltför detaljerade. Å andra sidan behöver de ge medborgaren nödvändig rättssäkerhet samt adekvat skydd av dennes personuppgifter. Datatillsynsmannen anser att balansen mellan dessa två potentiellt motstridiga rättsliga krav på det hela taget har uppnåtts i förslaget. Bestämmelserna lämnar flexibilitet när det behövs men är på de flesta områden tillräckligt precisa för att skydda medborgaren.
27. På några punkter är dock förslaget alltför flexibelt och föreskriver inte de nödvändiga skyddsåtgärderna. Exempelvis föreskrivs i artikel 7.1 i förslaget generellt undantag från skyddsåtgärderna på det enda villkoret att "annat föreskrivs i den nationella lagstiftningen". Att lämna ett sådant omfattande utrymme för fri bedömning när det gäller att behålla uppgifter längre än vad som är nödvändigt för det planerade syftet skulle inte endast vara oförenligt med den grundläggande rättigheten till uppgiftsskydd utan också skada det grundläggande behovet av harmonisering av skyddet av personuppgifter som behandlas inom ramen för polissamarbete och straffrättsligt samarbete.
28. Undantag bör, om de behövs, begränsas till nationella eller europeiska rättsliga bestämmelser, utfärdade för att skydda specifika allmänna intressen. Dessa allmänna intressen bör anges i artikel 7.1.
29. Detta leder fram till en annan punkt. Om ett annat specifikt rättsligt instrument enligt avdelning VI i EU-fördraget fastställer mer exakta villkor eller begränsningar för behandling av eller tillgång till uppgifter, bör denna mer specifika lagstiftning gälla som en *lex specialis*. I artikel 17 i förslaget föreskrivs undantag från artiklarna 12, 13, 14 och 15, om särskild lagstiftning enligt avdelning VI i EU-fördraget innehåller specifika villkor för överlämnande av uppgifter. Detta är en illustration av förslagets allmänna natur (se ovan), men det täcker inte alla hypoteser. Den

europiska datatillsynsmannen anser att följande skall gälla för artikel 17:

- Den bör få en mer generell utformning. Om det finns en mer specifik lagstiftning som styr någon som helst aspekt av uppgiftsbehandling (inte endast överlämnande av uppgifter), gäller den specifika lagstiftningen.
- Den bör innehålla säkerhetsåtgärden att undantag inte får sänka skyddsnivån.

#### Tillämpliga på all behandling

30. Vad beträffar det andra särdraget skulle det ideala resultatet vara att all insamling och behandling av personuppgifter inom ramen för tredje pelaren omfattas.
31. För att rambeslutets mål skall uppnås är det väsentligt att beslutet omfattar alla polisuppgifter och rättsliga uppgifter, även om de inte överlämnas eller görs tillgängliga av de behöriga myndigheterna i andra medlemsstater.
32. Detta är så mycket viktigare, eftersom varje begränsning av de uppgifter som överlämnas till eller görs tillgängliga för de behöriga myndigheterna i andra medlemsstater skulle göra rambeslutets tillämpningsområde synnerligen osäkert eller vagt, vilket skulle motverka mot dess huvudsakliga syfte<sup>(1)</sup>. Individens rättssäkerhet skulle skadas. Under normala omständigheter vet man aldrig i förväg – vid tidpunkten för insamling och behandling av personuppgifter – om dessa uppgifter kommer att komma i fråga för ett utbyte med behöriga myndigheter i andra medlemsstater. Datatillsynsmannen hänvisar härvid till principen om tillgänglighet och avskaffandet av de inre gränserna för utbytet av uppgifter om brottsbekämpning.
33. Slutligen noterar datatillsynsmannen att förslaget inte gäller:
- behandling inom ramen för EU-fördragets andra pelare (gemensam utrikes- och säkerhetspolitik),
  - underrättelsetjänsters behandling av uppgifter och deras tillgång till sådana uppgifter när de behandlas av behöriga myndigheter eller andra parter (detta följer av artikel 33 i EU-fördraget).

På dessa områden skall nationell rätt ge registrerade personer adekvat skydd. Denna lucka i skyddet på EU-nivå måste beaktas vid bedömningen av förslaget<sup>(2)</sup>. Eftersom all behandling på brottsbekämpningsområdet inte kan omfattas måste lagstiftaren sörja för ett ännu effektivare skydd på de områden som faktiskt omfattas av förslaget.

<sup>(1)</sup> Datatillsynsmannen hänvisar till samma resonemang av domstolen i (bl.a.) domen Österreichischer Rundfunk m.fl., de förenade målen C-465/00, C-138/01 och C-139/01 REG [2003], s. I-4989.

<sup>(2)</sup> Se i detta sammanhang Europeiska datatillsynsmannens yttrande av den 26 september 2005 om förslaget till Europaparlamentets och rådets direktiv om bevarande av uppgifter som behandlats i samband med tillhandahållande av allmänna elektroniska kommunikationstjänster och om ändring av direktiv 2002/58/EG, punkt 33.

### III.2 Rättslig grund

34. I ingressen till förslaget till rådets rambeslut om utbyte av uppgifter enligt principen om tillgänglighet anges en särskild rättslig grund, nämligen artikel 30.1 b. I det aktuella förslaget specificeras däremot inte vilka bestämmelser i artikel 30 eller artikel 31 som utgör den rättsliga grunden.

35. Även om det inte är datatillsynsmannens uppgift som rådgivare om Europeiska unionens lagstiftning att välja rättslig grund för ett förslag, är det lämpligt att anta att även det aktuella förslaget kan grundas på artikel 30.1 b. Dessutom kan det grundas på artikel 31.1 c i EU-fördraget och bör även i sin helhet tillämpas på inhemska situationer, förutsatt att detta är nödvändigt för att förbättra polissamarbetet och det straffrättsliga samarbetet mellan medlemsstaterna. I detta sammanhang betonar datatillsynsmannen återigen att alla personuppgifter som har samlats in, lagrats, behandlats eller analyserats i brottsbekämpande syfte, i synnerhet enligt principen om tillgänglighet, bör kunna utbytas med behöriga myndigheter i en annan medlemsstat.

36. Datatillsynsmannen delar uppfattningen att artiklarna 30.1 b och 31.1 c i EU-fördraget utgör en rättslig grund för regler om uppgiftsskydd vilka inte är begränsade till skydd av personuppgifter som faktiskt utbyts mellan de behöriga myndigheterna i medlemsstaterna, utan också är tillämpliga på inhemska situationer. I synnerhet gäller följande:

— Artikel 30.1 b, som kan tjäna som rättslig grund för regler om insamling, lagring, behandling, analys och utbyte av relevant information, är inte begränsad till information som har gjorts tillgänglig för eller överlämnats till andra medlemsstater. Den enda begränsning som åläggs genom artikel 30.1 b är att informationen skall vara relevant för polissamarbetet.

— För rättsligt samarbete är artikel 31.1 c ännu tydligare, eftersom de gemensamma insatserna skall omfatta "säkerställande av förenlighet mellan tillämpliga regler i medlemsstaterna, när detta är nödvändigt för att förbättra samarbetet".

— Det följer av Pupino-målet<sup>(3)</sup> att domstolen tillämpar principer i gemenskapsrätten på frågor som omfattas av tredje pelaren. Denna rättspraxis återspeglar utvecklingen från rent samarbete mellan medlemsstaternas myndigheter inom tredje pelaren till ett område med frihet, säkerhet och rättvisa, jämförbart med den inre marknaden så som den upprättats inom EG-fördraget.

<sup>(3)</sup> Domstolens dom av den 16 juni 2005, Pupino, mål C-105/03.

- Enligt datatillsynsmannen innebär principen om effektivitet att fördraget inte får tolkas på ett sätt som hindrar Europeiska unionens institutioner från att utföra sina uppgifter effektivt. Här ingår deras uppgift att skydda grundläggande rättigheter.
  - En begränsning till gränsöverskridande situationer skulle som tidigare nämnts innebära att konsekvenserna av principen om tillgänglighet inte respekteras och dessutom skada enskilda personers rättssäkerhet.
37. Datatillsynsmannen fäster separat uppmärksamhet på *utbytet av uppgifter med tredjeländer*. Medlemsstaternas använder personuppgifter som samlats in och behandlats i tredjeländer och översänts till dem i brottsbekämpande syfte och överlämnar personuppgifter som de själva har samlat in och/eller behandlat till behöriga myndigheter i tredjeländer och till internationella organ.
38. Artiklarna 30 och 31 i EU-fördraget kräver inte att personuppgifter som samlats in av myndigheter i tredjeländer behandlas på ett annat sätt än de som ursprungligen har samlats in av behöriga myndigheter inom medlemsstaterna. När uppgifter från tredjeländer har mottagits, måste de uppfylla samma normer som uppgifter som samlats in om en medlemsstat. Det är dock inte alltid lätt att säkerställa uppgifternas kvalitet (detta kommer att diskuteras i nästa kapitel i detta yttrande).
39. Översändande av personuppgifter av behöriga myndigheter i medlemsstaterna till tredjeländer faller strängt taget utanför tillämpningsområdet för avdelning VI i EU-fördraget. Om uppgifter kan översändas till tredjeländer utan att skydd för den registrerade garanteras, skulle detta dock allvarligt skada det skydd som fastställs i det aktuella förslaget inom Europeiska unionens territorium av de skäl som nämns i avdelning III.4 i detta yttrande. Kort sagt gäller följande:
- Registrerades rättigheter, så som de garanteras i detta förslag, påverkas direkt, om överlämnandet till tredjeländer inte omfattas av regler för uppgiftsskydd.
  - Det skulle finnas en risk för att behöriga myndigheter i medlemsstaterna skulle kunna kringgå de strikta normerna för uppgiftsskydd.
40. Att kunna tillämpa gemensamma regler för uppgiftsskydd på personuppgifter som behöriga myndigheter i medlemsstaterna utbyter med myndigheter i tredjeländer och internationella organisationer är sammanfattningsvis nödvändigt för att de gemensamma reglerna för skydd av personuppgifter mellan de behöriga myndigheterna i medlemsstaterna skall vara effektiva och således nödvändigt för att förbättra samarbetet mellan medlemsstaterna.

Artiklarna 30 och 31 i EU-fördraget utgör den nödvändiga rättsliga grunden.

### III.3 Särskilda anmärkningar om förslaget tillämpningsområde

#### *Personuppgifter som behandlas av rättsliga myndigheter*

41. Personuppgifter behandlas och utbyts både av polisen och de rättsliga myndigheterna. Förslaget, som grundar sig på artiklarna 30 och 31 i EU-fördraget, gäller för samarbetet mellan polisstyrkorna och samarbetet mellan de rättsliga myndigheterna. På denna punkt har detta förslag ett vidare tillämpningsområde än förslaget till rådets rambeslut om utbyte av uppgifter, vilket begränsas till polisarbete och endast gäller för uppgifter innan ett rättsligt förfarande har inletts.
42. Datatillsynsmannen välkomnar att förslaget även omfattar uppgifter som behandlas av rättsliga myndigheter. Det finns goda skäl att behandla polisuppgifter och sådana uppgifter från rättsliga myndigheter som behandlas i brottsbekämpande syfte i samma förslag. För det första skiljer sig medlemsstaternas organisation av kedjan brottsutredning och lagföring åt. De rättsliga myndigheternas inblandning börjar i olika skeden i de olika medlemsstaterna. För det andra kan alla personuppgifter i denna kedja till sist hamna i ett rättsligt register. Det finns ingen logik i att tillämpa andra system för uppgiftsskydd under de föregående skedena.
43. För kontrollen av uppgiftsbehandlingen behövs det dock en annan metod. I artikel 30 i förslaget uppräknas tillsynsmyndigheternas uppgifter. Enligt artikel 30.9 skall tillsynsmyndighetens befogenheter inte inkräkta på domstolsväsendets oberoende. Datatillsynsmannen rekommenderar att det i förslaget klargörs att tillsynsmyndigheterna inte övervakar de rättsliga myndigheternas behandling av uppgifter i den mån som de handlar i sin rättskipande funktion<sup>(1)</sup>.

#### *Behandling av Europol och Eurojust (och Tullinformationssystemet)*

44. Enligt artikel 3.2 i förslaget skall rambeslutet inte gälla för behandling av personuppgifter som sker vid Europol, Eurojust eller inom ramen för Tullinformationssystemet<sup>(2)</sup>.

<sup>(1)</sup> Bestämmelsen skulle kunna likna bestämmelsen i artikel 46 i förordning nr 45/2001/EG.

<sup>(2)</sup> Tullinformationssystemet är ett litet men ganska komplicerat system bestående av nationella och övernationella element, jämförbart med Schengens informationssystem. På grund av detta förslags relativt begränsade betydelse för Tullinformationssystemet och själva systemets komplexitet kommer det inte att tas upp i detta yttrande. Datatillsynsmannen kommer att ta upp Tullinformationssystemet i ett annat sammanhang.

45. Denna bestämmelse är egentligen överflödig, i alla fall i den mån som den hänför sig till Europol och Eurojust. Ett rambeslut enligt artikel 34 b i EU-fördraget kan endast fattas om tillnärmning av medlemsstaternas lagar och andra författningar och kan inte riktas till Europol eller Eurojust.
46. Sakinnehållet i texten i artikel 3.2 leder till följande iakttagelser:
- Förslaget tillhandahåller en allmän ram, som i princip bör vara tillämplig på alla situationer inom tredje pelaren. En enhetlig rättslig ram för uppgiftsskydd är i sig en faktor som effektiviserar uppgiftsskyddet.
  - För tillfället förfogar Europol och Eurojust över väldefinierade system för uppgiftsskydd, inklusive ett system för övervakning. Av detta skäl finns det inget omedelbart behov av att anpassa de tillämpliga reglerna till texten i detta förslag.
  - På längre sikt bör dock de regler för uppgiftsskydd som gäller för Europol och Eurojust ändras, så att de överensstämmer fullt ut med detta rambeslut.
  - Detta är desto viktigare eftersom förslaget till rambeslut, utom kapitel III, gäller för insamling och behandling av personuppgifter som medlemsstaterna överlämnar till Europol och Eurojust.

#### III.4 Förslagets struktur

47. Datatillsynsmannen har analyserat förslaget och drar slutsatsen att det i förslaget generellt sett föreskrivs en skiktad skyddsstruktur. De allmänna normerna, som fastställs i kapitel II (och för särskilda områden i kapitlen IV-VII), innehåller följande två skyddsskikt:
- Överföring till tredje pelaren av allmänna principer för uppgiftsskydd enligt direktiv 95/46/EG och andra gemenskapsrättsakter samt Europarådets konvention nr 108.
  - Ytterligare regler om uppgiftsskydd, vilka är tillämpliga på all behandling av personuppgifter inom ramen för tredje pelaren. Exempel på dessa ytterligare regler finns i artikel 4.3 och 4.4 i förslaget.
48. I kapitel III läggs det till ett tredje skyddsskikt för särskilda former av behandling. Titlarna på de två avdelningarna i kapitel III och lydelsen i flera bestämmelser i förslaget verkar tyda på att detta kapitel endast gäller uppgifter som översänds eller görs tillgängliga av behöriga myndigheter i andra medlemsstater. Följaktligen skulle en del viktiga bestämmelser om skydd av personuppgifter inte gälla personuppgifter, om de inte utbyts mellan medlemsstaterna. Denna text är alltså tvetydig, eftersom bestämmelserna själva tycks gå utöver verksamhet som direkt är

knuten till utbytta uppgifter. Under alla omständigheter förklaras inte begränsningen av tillämpningsområdet uttryckligen och motiveras inte heller i motiveringen eller i konsekvensanalysen.

49. Datatillsynsmannen framhåller mervärdet med en sådan skiktad struktur, som i sig kan ge den registrerade optimalt skydd med beaktande av brottsbekämpningen specifika behov. Den återspeglar behovet av ett adekvat uppgiftsskydd enligt vad som framkom vid konferensen i Krakow i april 2005 och överensstämmer i princip med artikel 8 i Europeiska unionens stadga om de grundläggande rättigheterna och Europakonventionen om skydd för de mänskliga rättigheterna och de grundläggande friheterna, särskilt artikel 8.
50. En analys av förslagstexten leder dock till följande iakttagelser:
51. För det första bör det säkerställas att de extra reglerna om uppgiftsskydd i kapitel II (andra skiktet, se punkt 47) inte avviker från de allmänna principerna om uppgiftsskydd. Datatillsynsmannen anser att de extra reglerna i kapitel II bör erbjuda extra skydd för de registrerade i den specifika kontext som tredje pelaren utgör (polisär och rättslig information). Dessa extra regler får med andra ord inte leda till en lägre skyddsnivå.
52. Vidare bör kapitel III – om särskilda former av behandling (där det tredje skiktet av skydd ingår) – inte avvika från kapitel II. Datatillsynsmannen anser att bestämmelserna i kapitel III bör erbjuda extra skydd för de registrerade i situationer där behöriga myndigheter i mer än en medlemsstat är inblandade, men dessa bestämmelser får inte leda till en lägre skyddsnivå.
53. För det andra bör regler av allmän natur inte placeras i kapitel III. Datatillsynsmannen rekommenderar att dessa bestämmelser flyttas till kapitel II. Endast bestämmelser som strikt gäller skyddet av personuppgifter vid utbyte av uppgifter mellan medlemsstater får tas med i kapitel III. Detta är desto viktigare, eftersom kapitel III innehåller viktiga bestämmelser om en hög skyddsnivå för den registrerade i samband med brottsbekämpning (se IV.1 i yttrandet).

#### IV. ANALYS AV FÖRSLAGETS OLIKA DELAR

##### IV.1 Utgångspunkter för analysen

54. Datatillsynsmannen kommer vid analysen av förslagets olika huvuddelar att beakta dess särskilda struktur och innehåll. Han kommer inte att kommentera varje artikel i förslaget.

55. Först och främst återspeglar de flesta bestämmelserna i förslaget andra EU-rättsakter om skydd av personuppgifter. Dessa bestämmelser överensstämmer med EU:s rättsliga ram för uppgiftsskydd och är tillräckliga för att ge adekvata garantier för uppgiftsskydd inom tredje pelaren.
56. Datatillsynsmannen noterar dock att några bestämmelser som för närvarande finns i kapitel III i förslaget, vilka gäller särskilda former av behandling och generellt sett (se punkt 48 i yttrandet) är tillämpliga endast på uppgifter som utbyts med andra medlemsstater, tar upp allmänna och väsentliga principer i EU-lagstiftningen om uppgiftsskydd. Dessa bestämmelser i kapitel III bör därför flyttas till kapitel II och göras tillämpliga på all behandling av uppgifter som företas av brottsbekämpande myndigheter. Detta är fallet med bestämmelserna om kontroll av kvaliteten på uppgifterna (artikel 9.1 och 9.6) och om vidare behandling av personuppgifter (artikel 11.1).
57. Några av de andra artiklarna i kapitel III i förslaget gör ingen skillnad mellan ytterligare villkor som är specifikt relaterade till utbyte av uppgifter med andra medlemsstater, t.ex. samtycke från den behöriga myndigheten i den översändande medlemsstaten, och skyddsåtgärder som i stället är relevanta och nödvändiga också för uppgifter som behandlas inom en medlemsstat. I dessa fall rekommenderar datatillsynsmannen att de sistnämnda skyddsåtgärderna görs generellt tillämpliga även på de personuppgifter som inte har översänts eller gjorts tillgängliga av en annan medlemsstat. Denna rekommendation gäller:
- översändande av uppgifter till privata parter och till andra myndigheter än brottsbekämpande myndigheter (artikel 13 a och 13 b samt artikel 14 a och 14 b), och
  - överföringar till tredjeländer eller internationella organ (artikel 15 utom led c).
58. I denna del av yttrandet kommer lagstiftaren också att uppmärksammas på några ytterligare säkerhetsåtgärder, som inte fastställs i det nuvarande förslaget. Datatillsynsmannen anser att dessa ytterligare säkerhetsåtgärder bör tillhandahållas för databehandlade beslut, personuppgifter som lämnas av tredjeländer, tillgång till privata parter databaser, behandling av biometriska uppgifter och DNA-profiler.
59. I denna analys kommer det dessutom att lämnas rekommendationer för förbättring av den nuvarande texten, så att bestämmelserna blir effektiva och texten blir konsekvent och överensstämmer med den nuvarande rättsliga ramen för uppgiftsskydd.

#### IV.2 Begränsning av ändamålet och senare behandling

60. Enligt artikel 4.1 b skall personuppgifter samlas in för särskilda, uttryckligt angivna och berättigade ändamål

och senare behandling får inte ske på ett sätt som är oförenligt med dessa ändamål. Normalt samlas uppgifter in i samband med ett specificerat brott (eller under vissa omständigheter för att undersöka en kriminell grupp eller ett kriminellt nätverk osv.). De kan användas för det ursprungliga ändamålet och sedan behandlas för ett annat ändamål, om det är förenligt med det ursprungliga (uppgifter som samlas in om en enskild person som dömts för narkotikahandel kan exempelvis användas i samband med en undersökning om ett nät av narkotikahandlare). Denna metod återspeglar väl principen om begränsning av ändamålet, som också fastställs i artikel 8 i Europeiska unionens stadga om de grundläggande rättigheterna och alltså är förenlig med gällande lagstiftning om uppgiftsskydd.

*Senare behandling för ändamål inom rambeslutets tillämpningsområde*

61. Datatillsynsmannen noterar att förslaget inte på ett helt tillfredsställande sätt behandlar en situation som kan inträffa under polisens arbete, nämligen behovet av att använda uppgifterna senare för ett ändamål som anses oförenligt med det ändamål för vilket de samlades in. Uppgifter kan, efter det att de samlats in av polisen, behövas för att lösa ett helt annat brott. För att illustrera detta kan man nämna att uppgifter samlas in för lagföring av trafikförseelser och sedan används för att lokalisera och åtala en biltjuv. Det andra ändamålet kan, även om det är berättigat, inte betraktas som fullt förenligt med ändamålet med insamlingen av uppgifter. Om brottsbekämpande myndigheter inte fick använda uppgifterna för detta andra ändamål, skulle de vara benägna att samla in uppgifter för omfattande eller dåligt definierade ändamål, och då skulle principen om begränsning av ändamålet förlora sitt värde vad beträffar insamling. Tillämpningen av andra principer, t.ex. proportionalitetsprincipen, principerna om exakthet och tillförlitlighet, skulle dessutom hämmas (se artikel 4.1 c och 4.1 d).
62. Enligt EU:s lagstiftning om uppgiftsskydd skall personuppgifter samlas in för särskilda och uttryckligt angivna ändamål och får inte behandlas vidare på ett sätt som är oförenligt med dessa ändamål. Datatillsynsmannen anser dock att en viss flexibilitet måste tillåtas när det gäller vidare användning. Det är troligare att begränsningen när det gäller insamling respekteras väl, om de myndigheter som ansvarar för den inre säkerheten vet att de, med lämpliga säkerhetsåtgärder, kan räkna med undantag från begränsningen vad beträffar vidare användning.
63. De bör klargöras att detta behov av vidare behandling erkänns i artikel 11 i förslaget, men på ett ganska otillräckligt sätt. Artikel 11 gäller endast för uppgifter som mottagits från eller gjorts tillgängliga av den behöriga myndigheten i en annan medlemsstat och tillhandahåller inte tillräckliga säkerhetsåtgärder.



64. Datatillsynsmannen rekommenderar att artikel 11.1 tillämpas på alla uppgifter, oavsett om de har mottagits från en annan medlemsstat eller inte. Striktare säkerhetsåtgärder än de som fastställs i artikel 11.1 b bör dessutom läggas till; vidare användning av uppgifter för ett ändamål som anses oförenligt med det ursprungliga ändamålet bör tillåtas endast om det är strikt nödvändigt, i ett specifikt fall, för att förebygga, utreda, avslöja eller lagföra brott eller för att skydda en persons intressen eller grundläggande rättigheter. Datatillsynsmannen föreslår att denna bestämmelse fastställs i en ny artikel 4 a (under alla omständigheter i kapitel II i förslaget).
65. Artikel 11.2 och 11.3 förblir tillämpliga som de är. De innehåller bestämmelser om extra skyddsåtgärder för uppgifter som mottagits från andra medlemsstater. Datatillsynsmannen påpekar att artikel 11.3 kommer att tillämpas på utbyte av uppgifter genom SIS II. Datatillsynsmannen har i sitt yttrande om SIS II redan nämnt att det bör säkerställas att SIS-uppgifter verkligen inte kan användas för något annat syfte än systemets egna syften.

*Vidare behandling för ändamål som ligger utanför tillämpningsområdet för polissamarbete och rättsligt samarbete*

66. I några fall måste uppgifter behandlas för att skydda andra viktiga intressen. I sådana fall kan de även behandlas av andra myndigheter än de behöriga myndigheterna enligt detta rambeslut. Medlemsstaternas befogenheter kan i detta fall omfatta en behandling som inkräktar på privatlivet (t.ex. kontroll av en person som inte är misstänkt) och bör alltså åtföljas av mycket strikta villkor, t.ex. skyldighet för medlemsstaterna att anta särskild lagstiftning om de vill använda sig av detta undantag. Inom ramen för första pelaren har denna fråga behandlats i artikel 13 i direktiv 95/46/EG, där det anges att begränsningar av vissa bestämmelser i direktivet tillåts i särskilda fall. De medlemsstater som tillämpar sådana begränsningar skall göra detta i överensstämmelse med artikel 8 i Europakonventionen om skydd för de mänskliga rättigheterna och de grundläggande friheterna.
67. Enligt samma sätt att resonera bör det i detta rambeslut i kapitel II fastställas att medlemsstaterna skall tillåtas att anta lagstiftningsåtgärder för att medge vidare behandling, när en sådan åtgärd är nödvändig för att säkra:
- förebyggande av hot mot allmän säkerhet, försvar eller nationell säkerhet,
  - skydd av ett viktigt ekonomiskt eller finansiellt intresse i en medlemsstat eller Europeiska unionen,
  - skydd för den registrerade.

#### IV.3 Kriterier för att göra behandling av uppgifter berättigad

68. Enligt artikel 5 i förslaget får uppgifter behandlas av de behöriga myndigheterna endast om detta har fastställts genom lagbestämmelser där det anges att uppgiftsbehandlingen är nödvändig för att den berörda myndigheten skall kunna fullgöra sina åligganden enligt lag och förebygga, utreda, avslöja och lagföra brott. Datatillsynsmannen stöder de stränga kraven i artikel 5.
69. I texten i artikel 5 underskattas dock behovet av att göra uppgiftsbehandling berättigad på andra lagliga grunder, under särskilda omständigheter. Det är en viktig bestämmelse, som t.ex. inte bör göra det omöjligt för polisen att fullgöra sina lagliga skyldigheter enligt nationell rätt att lämna ut uppgifter till invandrarmyndigheter eller skattemyndigheter. Datatillsynsmannen föreslår därför att man i artikel 5 beaktar andra berättigade rättsliga grunder för behandling av personuppgifter, exempelvis behovet att fullgöra en rättslig skyldighet som den registeransvarige omfattas av, den registrerades otvetydiga samtycke, förutsatt att behandlingen företas i den registrerades intresse, eller behovet av att skydda den registrerades vitala intressen.
70. Datatillsynsmannen påpekar att respekten för kriterierna för att göra behandling av uppgifter berättigad har en särskild betydelse när det gäller polissamarbete och rättsligt samarbete, om man beaktar att en olaglig insamling av personuppgifter från polisens sida kan medföra att personuppgifter inte kan användas som bevismaterial vid rättsliga förfaranden.

#### IV.4 Nödvändighet och proportionalitet

71. Syftet med artiklarna 4 och 5 i förslaget är också att på ett generellt tillfredsställande sätt säkerställa att begränsningar av skyddet för personuppgifter är nödvändiga och proportionella, vilket krävs enligt Europeiska unionens lagstiftning och rättspraxis vid Europeiska domstolen för de mänskliga rättigheterna rörande artikel 8 i Europakonventionen om skydd för de mänskliga rättigheterna och de grundläggande friheterna.
- I artikel 4.1 c fastställs den allmänna regeln att uppgifter skall vara adekvata, relevanta och inte omfatta mer än vad som är nödvändigt med hänsyn till de ändamål för vilka de samlas in och för vilka de senare behandlas.
  - I artikel 5 anges att behandlingen skall vara *nödvändig* för att den berörda myndigheten skall kunna fullgöra sina åligganden enligt lag och förebygga, utreda, avslöja och lagföra brott.
  - I artikel 4.4 anges att behandling av personuppgifter endast är nödvändig om vissa specifika villkor är uppfyllda.

72. Datatillsynsmannen noterar att den föreslagna formuleringen av artikel 4.4 inte uppfyller de kriterier som fastställs i rättspraxis vid Europeiska domstolen för de mänskliga rättigheterna när det gäller artikel 8 i Europakonventionen om skydd för de mänskliga rättigheterna och de grundläggande friheterna, enligt vilken en inskränkning i privatlivet kan åläggas endast om det är nödvändigt i ett demokratiskt samhälle. Enligt förslaget skall uppgiftsbehandling anses nödvändig inte endast om den skulle göra det möjligt för brottsbekämpande och rättsliga myndigheter att fullgöra sina åligganden utan även om det finns skälgrund att anta att personuppgifterna i fråga skulle underlätta eller påskynda förebyggandet, utredningen, avslöjandet eller lagföringen av ett brott.
73. Dessa kriterier överensstämmer inte med kraven i artikel 8 i Europakonventionen om skydd för de mänskliga rättigheterna och de grundläggande friheterna, eftersom nästan all behandling av personuppgifter kan betraktas som om den underlättar polisens eller de rättsliga myndigheternas verksamhet, även om uppgifterna i fråga egentligen inte behövs för att utföra denna verksamhet.
74. Den nuvarande texten i artikel 4.4 skulle bana väg för en oacceptabelt omfattande insamling av personuppgifter, endast grundad på antagandet att personuppgifter kan göra det lättare att förebygga, utreda, avslöja och lagföra brott. Behandling av personuppgifter skall tvärtom endast anses nödvändig, om de behöriga myndigheterna klart kan visa att den behövs och förutsatt att åtgärder som inkräktar mindre på privatlivet inte är tillgängliga.
75. Datatillsynsmannen rekommenderar därför att artikel 4.4 första strecksatsen formuleras om, så att det säkerställs att rättspraxis rörande artikel 8 i Europakonventionen om skydd för de mänskliga rättigheterna och de grundläggande friheterna följs. Datatillsynsmannen föreslår dessutom av systematiska skäl att artikel 4.4 flyttas till slutet av artikel 5.

#### IV.5 Behandling av särskilda kategorier av uppgifter

76. I artikel 6 fastställs ett principiellt förbud mot behandling av känsliga uppgifter, dvs. uppgifter som avslöjar ras eller etniskt ursprung, politiska åsikter, religiös eller filosofisk övertygelse, medlemskap i fackförening samt uppgifter som rör hälsa eller sexualliv. Förbudet gäller inte om uppgiftsbehandlingen fastställts genom lagbestämmelser och är absolut nödvändig för att myndigheten skall kunna fullgöra sina åligganden enligt lag och förebygga, utreda, avslöja och lagföra brott. Känsliga uppgifter får också behandlas om den registrerade uttryckligen har godkänt uppgiftsbehandlingen. I båda fallen skall särskilda skyddsåtgärder av lämplig art vidtas.
77. Texten i artikel 6 ger anledning till två anmärkningar. För det första bygger artikel 6 alltför mycket på den registrerades samtycke. Datatillsynsmannen betonar att behandling av känsliga uppgifter på grundval av den registre-

rades uttryckliga samtycke endast bör tillåtas i den mån som behandlingen företas i den registrerades intresse och vägran att lämna samtycke skall inte få negativa konsekvenser för den registrerade. Datatillsynsmannen rekommenderar att artikel 6 ändras i enlighet härmed, också för att artikeln skall överensstämma med EU:s gällande lagstiftning om uppgiftsskydd.

78. För det andra anser datatillsynsmannen att även andra lagliga skäl till behandling, exempelvis behovet av att skydda den registrerades eller en annan persons vitala intressen (om den registrerade är fysiskt eller rättsligt oförmögen att lämna sitt samtycke) kan beaktas.
79. Inom polissamarbetet och det rättsliga samarbetet får behandlingen av andra kategorier av eventuellt känsliga personuppgifter, exempelvis biometriska uppgifter och DNA-profiler, allt större betydelse. Dessa uppgifter omfattas inte uttryckligen av artikel 6 i förslaget. Datatillsynsmannen uppmanar EU:s lagstiftare att vara särskilt uppmärksam vid genomförandet av de allmänna principerna om uppgiftsskydd i detta förslag i ytterligare lagstiftning som medför behandling av dessa särskilda kategorier av uppgifter. Ett exempel är det nuvarande förslaget till rådets rambeslut om utbyte av uppgifter enligt principen om tillgänglighet (se punkterna 12-15 ovan), som uttryckligen tillåter behandling och utbyte av biometriska uppgifter och DNA-profiler (se bilaga II till förslaget), men inte tar upp dessa uppgifters känslighet eller särdrag ur uppgiftsskyddssynvinkel.
80. Datatillsynsmannen rekommenderar att särskilda skyddsåtgärder föreskrivs, särskilt för att garantera att
- biometriska uppgifter och DNA-profiler endast används på grundval av väletablerade och kompatibla tekniska standarder,
  - graden av exakthet noggrant beaktas och kan bestridas av den registrerade på ett lättillgängligt sätt, och att
  - respekten för personers värdighet säkerställs fullt ut.

Det ankommer på lagstiftaren att avgöra om dessa extra säkerhetsåtgärder skall föreskrivas i detta rambeslut eller i särskilda rättsakter som reglerar insamling och utbyte av dessa särskilda kategorier av uppgifter.

#### IV.6 Exakthet och tillförlitlighet

81. I artikel 4.1 d fastställs de allmänna reglerna för uppgifternas kvalitet. Enligt denna artikel skall den registeransvarige se till att uppgifterna är korrekta och, om nödvändigt, hålls aktuella. Han skall vidta alla rimliga åtgärder för att säkerställa att uppgifter raderas eller rättas, om de är felaktiga eller ofullständiga, sett till de ändamål för vilka de samlades in eller för vilka de senare behandlas. Detta är i linje med de allmänna principerna i EU:s lagstiftning om uppgiftsskydd.

82. Enligt artikel 4.1 d tredje meningen får medlemsstaterna föreskriva att behandlingen av uppgifter kan ske utifrån olika krav med avseende på graden av uppgifternas exakthet och tillförlitlighet. Datatillsynsmannen tolkar denna bestämmelse som ett undantag från den allmänna principen om exakthet och rekommenderar att bestämmelsens karaktär av undantag klargörs genom att "men" eller "likvärl" läggs till i början av artikel 4.1 d tredje meningen. I sådana fall då det inte fullt ut kan garanteras att uppgifterna är korrekta, skall den registeransvarige vara skyldig att särskilja uppgifterna efter deras grad av exakthet och tillförlitlighet, med särskild hänvisning till den grundläggande skillnaden mellan uppgifter som baseras på fakta och uppgifter som baseras på åsikter och personliga bedömningar. Datatillsynsmannen betonar vikten av denna skyldighet både för de registrerade och de brottsbekämpande myndigheterna, särskilt om uppgifter behandlas långt från källan (se punkt 7 i yttrandet).

#### Kontroll av uppgifternas kvalitet

83. Den allmänna princip som fastställs i artikel 4.1 d kompletteras av de mer specifika säkerhetsåtgärder som föreskrivs i artikel 9 om kontroll av uppgifternas kvalitet. I artikel 9 fastställs särskilt följande:

1. Personuppgifternas kvalitet skall kontrolleras senast innan de översänds eller görs tillgängliga. Dessutom skall kvaliteten på uppgifter som görs automatiskt tillgängliga kontrolleras regelbundet (artikel 9.1 och 9.2).
2. Vid översändande av uppgifter bör alltid domar och beslut att inte väcka åtal anges och källan till uppgifter som grundar sig på åsikter bör kontrolleras innan uppgifterna överförs, och det bör anges i vilken mån uppgifterna är korrekta och tillförlitliga (artikel 9.1).
3. Personuppgifterna skall markeras på den registrerades begäran, om denne bestrider uppgifternas korrekthet och det inte kan fastställas huruvida de är korrekta eller inte (artikel 9.6).

84. Artikel 4.1 och artikel 9 säkerställer därför, om de tillämpas tillsammans, att kvaliteten på personuppgifterna har kontrollerats tillräckligt, både av den registrerade och av de myndigheter som är närmast källorna till de behandlade uppgifterna och därför kan kontrollera dem bäst.

85. Datatillsynsmannen välkomnar dessa bestämmelser, eftersom de är inriktade på de brottsbekämpande myndigheternas behov men också säkerställer att varje uppgift beaktas på lämpligt sätt och används i enlighet med sin exakthet och tillförlitlighet, varigenom det undviks att en registrerad drabbas oproportionerligt av den eventuella bristen på exakthet hos vissa uppgifter som rör honom eller henne.

86. Kontroll av uppgifternas kvalitet är ett viktigt inslag i skyddet för den registrerade, särskilt när det gäller personuppgifter som behandlas av polisen och de rättsliga myndigheterna. Datatillsynsmannen beklagar därför att tillämpligheten av artikel 9, som rör kontroll av uppgifternas kvalitet, är begränsad till uppgifter som översänds till eller görs tillgängliga för andra medlemsstater. Detta är olyckligt, eftersom det innebär att personuppgifters kvalitet, vilken är väsentlig även för brottsbekämpande ändamål, endast garanteras fullt ut, om dessa uppgifter översänds till eller görs tillgängliga för andra medlemsstater, men inte när de behandlas inom en medlemsstat<sup>(1)</sup>. I stället är det väsentligt, både i de registrerades och de behöriga myndigheternas intresse, att sörja för att kvaliteten på alla personuppgifter kontrolleras på ett lämpligt sätt, även de som inte översänds eller görs tillgängliga av en annan medlemsstat.

87. Datatillsynsmannen rekommenderar därför att begränsningarna av tillämpningsområdet för artikel 9.1 och 9.6 under alla omständigheter tas bort genom att bestämmelserna flyttas till kapitel II i förslaget.

#### Åtskillnaden mellan olika kategorier av uppgifter

88. I artikel 4.2 fastställs en skyldighet för den registeransvarige att göra en tydlig åtskillnad mellan personuppgifter om olika kategorier av personer (misstänkta, dömda, vittnen, offer, informatörer, kontakter m.fl.). Datatillsynsmannen välkomnar detta tillvägagångssätt. Det är sant att brottsbekämpande och rättsliga myndigheter kan behöva behandla uppgifter om helt olika kategorier av personer men det är viktigt att det görs en åtskillnad mellan dessa uppgifter alltefter graden av inblandning i ett brott. I synnerhet bör villkoren för insamling av uppgifter, tidsfrister, villkor för att vägra den registrerade tillgång eller information och närmare föreskrifter om behöriga myndigheters tillgång till uppgifter återspegla de utmärkande dragen för de olika kategorierna av uppgifter och de olika ändamål för vilka dessa uppgifter samlas in av brottsbekämpande och rättsliga myndigheter.

89. I detta sammanhang vill datatillsynsmannen att uppgifter om icke misstänkta personer uppmärksammas särskilt. Särskilda villkor och säkerhetsåtgärder behövs för att säkerställa proportionalitet och undvika att personer som inte är aktivt inblandade i ett brott kommer till skada. För denna kategori av personer bör förslaget innehålla tilläggsbestämmelser för att begränsa behandlingens syfte, fastställa exakta tidsfrister och begränsa tillgången till uppgifter. Datatillsynsmannen rekommenderar att förslaget ändras i enlighet härmed.

<sup>(1)</sup> Detta skulle dessutom inte vara i linje med Europarådets rekommendation nr R(87) 15 från ministerkommittén till medlemsstaterna om att reglera användningen av personuppgifter inom polisen. I synnerhet anges det i princip 7.2 att "regelbundna kontroller" av personuppgifternas kvalitet skall föreskrivas i samförstånd med tillsynsmyndigheten eller i enlighet med nationell lagstiftning.

90. Förslaget nuvarande text innehåller en särskild säkerhetsåtgärd, som gäller ej misstänkta personer, nämligen artikel 7.1 i förslaget. Datatillsynsmannen anser att detta är en viktig säkerhetsåtgärd, framför allt eftersom medlemsstaterna inte får föreskriva undantag. Tyvärr föreskrivs i artikel 7.1 särskilda säkerhetsåtgärder endast när det gäller tidsfrister och dess tillämplighet begränsas till den kategori av personer som avses i artikel 4.3 sista strecksatsen i förslaget. I artikeln föreskrivs därför inga tillfredsställande garantier och den omfattar inte hela gruppen icke misstänkta personer <sup>(1)</sup>.

91. Uppgifter om dömda personer förtjänar också särskild uppmärksamhet. Vad dessa uppgifter beträffar bör de senaste och framtida initiativen för utbyte av straffregister vederbörligen beaktas och överensstämmelse säkerställas <sup>(2)</sup>.

92. Mot bakgrund av dessa påpekanden rekommenderar datatillsynsmannen tillägg av en ny punkt till artikel 4 med följande innehåll:

— Ytterligare bestämmelser för att begränsa ändamålet med behandlingen, fastställa exakta tidsfrister och begränsa tillgången till uppgifter, vad beträffar icke misstänkta personer.

— Skyldighet för medlemsstaterna att fastställa de rättsliga konsekvenserna av de åtskillnader som skall göras mellan personuppgifter om olika kategorier av personer, vilka återspeglar särdragen i de olika kategorierna av behandlade uppgifter och de olika ändamål för vilka dessa uppgifter samlas in av de brottsbekämpande och de rättsliga myndigheterna.

— De rättsliga konsekvenserna bör gälla villkor för insamling av personuppgifter, tidsfrister, vidare överföring och användning av uppgifter samt villkor för att vägra den registrerade tillgång eller information.

#### IV.7 Tidsfrister för lagringen av personuppgifter

93. De allmänna principerna för tidsfrister för lagringen av personuppgifter fastställs i artikel 4.1 e och artikel 7.1 i förslaget. Som en allmän princip bör personuppgifter inte lagras längre än vad som är nödvändigt med hänsyn till

<sup>(1)</sup> Se närmare punkt 94 i yttrandet.

<sup>(2)</sup> Rådets beslut 2005/876/RIF om utbyte av uppgifter ur kriminalregistret, som trädde i kraft den 9 december. Beslutet kompletterar och underlättar befintliga mekanismer för att översända uppgifter med hänvisning till domar som bygger på befintliga konventioner, sådana instrument som den europeiska konventionen om inbördes rättshjälp i brottmål från 1959 och konventionen från 2000 om ömsesidig rättslig hjälp i brottmål mellan medlemsstaterna. Denna text kommer senare att ersättas av ett precisare rambeslut av rådet. Kommissionen planerar att föreslå ett nytt rambeslut på detta område.

syftet med insamlingen. Detta överensstämmer med EU:s lagstiftning om uppgiftsskydd <sup>(3)</sup>.

94. Den allmänna bestämmelsen i artikel 7.1 är dock endast tillämplig "om inte annat föreskrivs i den nationella lagstiftningen". Datatillsynsmannen noterar att detta undantag är mycket allmänt och går utöver de undantag som är tillåtna enligt artikel 4.1 e. Datatillsynsmannen föreslår att det allmänna undantaget i artikel 7.1 stryks eller att man åtminstone uttryckligen begränsar de allmänna intressen som rättfärdigar medlemsstaternas utnyttjande av detta undantag <sup>(4)</sup>.

95. Enligt artikel 7.2 skall efterlevnaden av tidsfristerna garanteras genom lämpliga förfaranden och tekniska åtgärder och kontrolleras regelbundet. Datatillsynsmannen välkomnar denna bestämmelse men rekommenderar att det uttryckligen anges att det i de lämpliga förfarandena och tekniska åtgärderna bör föreskrivas automatisk och regelbunden radering av personuppgifter efter en viss tid.

#### IV.8 Utbyte av personuppgifter med tredjeländer

96. Ett effektivt polissamarbete och rättsligt samarbete inom EU:s gränser är alltmer avhängigt av samarbete med tredjeländer och internationella organisationer. Många åtgärder för att förbättra samarbetet när det gäller brottsbekämpning och det rättsliga samarbetet med tredjeländer eller internationella organisationer diskuteras för närvarande eller planeras både nationellt och på EU-nivå <sup>(5)</sup>. Utvecklingen av detta internationella samarbete kommer troligen av vara starkt beroende av utbytet av personuppgifter.

97. Det är därför väsentligt att principerna om rättvis och laglig behandling samt principerna om korrekt rättsförfarande i allmänhet även gäller för insamling och utbyte 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.

<sup>(3)</sup> Förutom den allmänna bestämmelsen om tidsfrister för lagringen av personuppgifter i artikel 7 innehåller förslaget ytterligare särskilda bestämmelser om personuppgifter som utbyts med andra medlemsstater. Framför allt fastställs det i artikel 9.7 att personuppgifter skall raderas

1. om uppgifterna inte borde ha översänts, gjorts tillgängliga eller mottagits,
2. efter utgången av den tidsfrist som meddelats av den översändande myndigheten, såvida inte personuppgifterna behövs under ytterligare en tid för rättegångsändamål,
3. om uppgifterna inte längre är nödvändiga för det ändamål som låg till grund för att de överfördes.

<sup>(4)</sup> Man skulle kunna tänka sig en begränsning till kampen mot terrorism och/eller de särskilda allmänna intressen som avses i artikel 4.1 e: historiska, statistiska eller vetenskapliga ändamål.

<sup>(5)</sup> Se exempelvis kommissionens meddelande nyligen "En strategi för den yttre dimensionen av området med frihet, säkerhet och rättvisa" (KOM(2005) 491 slutlig).

## Överföringar av personuppgifter till tredjeländer

98. I detta sammanhang välkomnar datatillsynsmannen artikel 15 i förslaget, som innehåller bestämmelser om skydd vid överföring till behöriga myndigheter i tredjeländer eller till internationella organ. Denna bestämmelse, som finns i kapitel III i förslaget, gäller dock endast för uppgifter som mottas från eller görs tillgängliga av behöriga myndigheter i andra medlemsstater. Som en följd av denna begränsning finns det fortfarande en brist i uppgiftsskyddssystemet på Europeiska unionens nivå när det gäller uppgifter som inte mottas från behöriga myndigheter i andra medlemsstater. Datatillsynsmannen anser att denna brist inte kan accepteras av följande skäl.
99. För det första bör den skyddsnivå som erbjuds genom EU-lagstiftningen vid överföring till tredjeland inte avgöras av uppgiftskällan, en polismyndighet inom den medlemsstat som överför uppgifter till ett tredjeland eller en polismyndighet inom en annan medlemsstat.
100. För det andra bör det noteras att reglerna för överföringar av personuppgifter till tredjeländer är en grundläggande princip i lagstiftningen om uppgiftsskydd. Denna princip är inte bara en av de grundläggande bestämmelserna i direktiv 95/46/EG utan fastställs även i tilläggsprotokollet till konvention nr 108 <sup>(1)</sup>. De gemensamma normer för skyddet av personuppgifter som avses i artikel 1 i förslaget kan inte garanteras om gemensamma normer för överföringar av personuppgifter till tredjeländer inte omfattar all behandling. De registrerades rättigheter enligt detta förslag skulle följaktligen direkt påverkas, om personuppgifter kunde översändas till tredjeländer som inte erbjuder en adekvat skyddsnivå.
101. För det tredje skulle begränsningen av tillämpningsområdet för dessa regler till att gälla endast "utbyta uppgifter", när det gäller uppgifter som behandlas endast inom ett land, medföra att det inte skulle finnas några säkerhetsåtgärder. Paradoxalt nog skulle det vara "lättare" att överföra personuppgifter till tredjeländer, utan beaktande av om det finns något adekvat skydd för personuppgifter, än till andra medlemsstater. Detta skulle ge möjlighet att "tvätta" information. De behöriga myndigheterna i medlemsstaterna skulle kunna kringgå de strikta normerna för uppgiftsskydd genom att översända uppgifter till tredjeländer eller internationella organisa-

(<sup>1</sup>) Tilläggsprotokollet om tillsynsmyndigheter och gränsöverskridande flöden av personuppgifter till konventionen om skydd för enskilda vid automatisk databehandling av personuppgifter undertecknades den 8 november 2001 och trädde i kraft den 1 juli 2004. Detta bindande internationella rättsliga instrument har hittills undertecknats av 11 stater (däribland 9 EU-medlemsstater). I artikel 2.1 i protokollet fastställs följande allmänna princip: "Varje part skall endast möjliggöra överföring av personuppgifter till en mottagare som lyder under en stats eller en organisations jurisdiktion som inte är part i konventionen, om staten eller organisationen tryggar en tillräcklig grad av skydd för den avsedda uppgiftsöverföringen".

tioner, där en behörig myndighet i en annan medlemsstat kan få tillgång till dem eller de t.o.m. skulle kunna skickas tillbaka till en sådan myndighet.

102. Datatillsynsmannen rekommenderar därför att förslaget ändras, så att det garanteras att artikel 15 gäller för utbyte av alla personuppgifter med tredjeländer. Denna rekommendation gäller inte artikel 15.1 c, som på grund av sin natur kan vara tillämplig endast på personuppgifter som utbyts med andra medlemsstater.

## Exceptionella överföringar till länder som saknar adekvat skydd

103. I artikel 15 fastställs en rad villkor för överföringar till behöriga myndigheter i tredjeländer eller till internationella organisationer jämförbara med villkoren i artikel 25 i direktiv 95/46/EG. I artikel 15.6 anges dock möjligheten att överföra uppgifter till tredjeländer eller internationella organisationer där ett adekvat uppgiftsskydd inte garanteras, förutsatt att överföringen är absolut nödvändig för att säkerställa en medlemsstats väsentliga intressen eller för att förebygga en omedelbart förestående allvarlig fara som hotar den allmänna säkerheten eller en eller flera specifika personer.
104. Det bör klargöras när det undantag som anges i punkt 6 är tillämpligt. Datatillsynsmannen rekommenderar därför:
- att det klargörs att detta undantag endast innebär ett undantag från villkoret "adekvat skydd" men inte påverkar de övriga villkor som anges i artikel 15.1,
  - att det läggs till att överföringar av uppgifter som görs i enlighet med detta undantag bör omfattas av lämpliga villkor (t.ex. ett klart uttalat villkor att uppgifter endast skall behandlas tillfälligt och för specifika ändamål) och skall meddelas den behöriga tillsynsmyndigheten.

## Behandling av personuppgifter som mottagits från tredjeländer

105. I samband med det ökande utbytet av personuppgifter med polis och rättsliga myndigheter i tredjeländer bör särskild uppmärksamhet även ägnas åt personuppgifter som "importeras" från de tredjeländer där adekvata normer när det gäller respekt för mänskliga rättigheter, särskilt för skydd av personuppgifter, inte säkerställs.

106. Utifrån ett bredare perspektiv anser datatillsynsmannen att lagstiftaren bör sörja för att personuppgifter som mottas från tredjeländer åtminstone uppfyller internationella normer när det gäller respekten för mänskliga rättigheter. Exempelvis bör brottsbekämpande och rättsliga myndigheter inte behandla eller förlita sig på uppgifter som samlats in under tortyr eller genom åsidosättande av mänskliga rättigheter, svartlistningar grundade endast på politisk övertygelse eller sexuell läggning, såvida detta inte görs i den registrerades intresse. Datatillsynsmannen rekommenderar därför att detta klargörs åtminstone i ett skäl till förslaget, eventuellt genom hänvisning till tillämpliga internationella instrument <sup>(1)</sup>.
107. När det mer specifikt gäller skydd av personuppgifter, påpekar datatillsynsmannen att den eventuella bristen på uppgiftskvalitet skall bedömas på vederbörligt sätt, när personuppgifter översänds från länder där det inte finns några adekvata normer eller garantier för skyddet av personuppgifter för att undvika att EU:s brottsbekämpande myndigheter felaktigt förlitar sig på sådan information och för att förhindra att de registrerade skadas.
108. Datatillsynsmannen rekommenderar därför att det läggs till en bestämmelse i artikel 9 i förslaget, där det anges att kvaliteten på personuppgifter som översänds från tredjeländer bör bli föremål för särskild bedömning så snart som de mottas och att graden av dessa uppgifters korrekthet och tillförlitlighet bör anges.

#### IV.9 Utbyte av personuppgifter med privata parter och andra myndigheter än brottsbekämpande myndigheter

109. I artiklarna 13 och 14 i förslaget anges ett antal krav som skall uppfyllas om personuppgifter sänds vidare till privata parter och andra myndigheter än brottsbekämpande myndigheter. Som tidigare nämnts kompletterar dessa artiklar de mer allmänna reglerna i kapitel II, som under alla omständigheter bör följas.
110. Datatillsynsmannen anser att överföring till privata parter och andra offentliga organ kan vara nödvändig i särskilda fall för att förebygga och bekämpa brott men att specifika och strikta villkor bör gälla. Detta är i linje med den

<sup>(1)</sup> FN-konventionen mot tortyr och annan grym, omänsklig eller förnedrande behandling eller bestraffning, som undertecknats av alla EU-medlemsstater och trädde i kraft den 26 juni 1987. I artikel 15 fastställs följande: "Varje konventionsstat skall säkerställa att ett uttalande, som konstaterats ha gjorts till följd av tortyr, inte skall åberopas som bevis i ett rättsligt förfarande utom mot en person som anklagats för tortyr såsom bevis för att uttalandet gjorts."

synpunkt som framfördes av de europeiska dataskyddsmyndigheterna i det sammanfattande dokumentet från Krakow <sup>(2)</sup>.

111. I detta perspektiv anser datatillsynsmannen att de extra villkor som anges i artiklarna 13 och 14 kan anses tillfredsställande om de tillämpas tillsammans med de allmänna reglerna i kapitel II, inklusive en omfattande tillämpning av reglerna om vidare behandling (se IV.2 ovan). Det nuvarande förslaget begränsar dock tillämpligheten av artiklarna 13 och 14 till personuppgifter som mottas från eller görs tillgängliga av de behöriga myndigheterna i en annan medlemsstat.
112. De senare villkorens allmänna tillämplighet är ännu viktigare, om man beaktar det allt större utbytet av uppgifter mellan brottsbekämpande myndigheter och andra myndigheter eller privata parter även inom medlemsstaterna. Man kan hitta ett exempel i offentligt/privat partnerskap i brottsbekämpande verksamhet <sup>(3)</sup>.
113. Datatillsynsmannen rekommenderar därför att det nuvarande förslaget ändras så att det säkerställs att artiklarna 13 och 14 gäller för utbytet av *alla* personuppgifter, även dem som inte översänds eller görs tillgängliga av en annan medlemsstat. Denna rekommendation gäller inte artiklarna 13 c och 14 c.

*Tillgång till och vidare användning av personuppgifter som kontrolleras av privata parter*

114. Utbytet av personuppgifter med privata parter går i två riktningar: det innebär att personuppgifter även översänds eller görs tillgängliga av privata parter för brottsbekämpande och rättsliga myndigheter.
115. I detta fall får offentliga myndigheter, för ett helt annat ändamål, nämligen att förebygga, utreda, avslöja eller lagföra brott, tillgång till och vidareanvänder personuppgifter som samlats in för kommersiella ändamål (kommersiella transaktioner, saluföring, tillhanda-hållande av tjänster m.m.) och hanteras av privata registeransvariga. Korrektheten och tillförlitligheten hos uppgifter som behandlats för kommersiella ändamål skall dessutom bedömas noggrant när dessa uppgifter används för brottsbekämpande ändamål <sup>(4)</sup>.

<sup>(2)</sup> Sammanfattande dokument om brottsbekämpning och informationsutbyte inom EU, som antogs vid de europeiska dataskyddsmyndigheternas vårkonferens i Krakow den 25-26 april 2005.

<sup>(3)</sup> Se kommissionens lagstiftnings- och arbetsprogram 2006 KOM(2005) 531 slutlig.

<sup>(4)</sup> Exempelvis är en telefonräkning tillförlitlig för kommersiella ändamål om det korrekt anges vilka telefonsamtal som har ringts, men de brottsbekämpande myndigheterna kan inte förlita sig fullt ut på samma telefonräkning som ett avgörande bevis för vem som ringt ett särskilt samtal.

116. Ett mycket aktuellt och viktigt exempel på tillgång till privata databaser för brottsbekämpande ändamål ges i den godkända texten till direktivet om lagring av kommunikationsuppgifter (se punkterna 16-18 ovan), enligt vilken leverantörer av allmänt tillgängliga elektroniska kommunikationstjänster eller allmänna kommunikationsnät skall lagra vissa uppgifter om kommunikationer upp till två år för att säkerställa att uppgifterna är tillgängliga för utredning, avslöjande och åtal av allvarliga brott. Enligt den godkända texten omfattas frågor som rör tillgång till dessa uppgifter inte av gemenskapsrätten och får inte regleras av själva direktivet. Dessa viktiga frågor kan i stället omfattas av nationell lagstiftning eller nationella åtgärder i enlighet med avdelning VI i EU-fördraget <sup>(1)</sup>.

117. I sitt yttrande om förslaget till detta direktiv försvarade datatillsynsmannen en vidare tolkning av EG-fördraget, eftersom begränsning av tillgång är nödvändig för att säkerställa ett adekvat skydd för den registrerade vars kommunikationsuppgifter måste lagras. Tyvärr tog den europeiska lagstiftaren inte med regler om tillgång i ovan nämnda direktiv.

118. I detta yttrande meddelar datatillsynsmannen på nytt att han starkt föredrar att det i EU-lagstiftningen fastställs gemensamma normer för brottsbekämpande myndigheters tillgång och vidare användning. Så länge som detta inte tas upp under första pelaren kan ett instrument under tredje pelaren innehålla bestämmelser om det nödvändiga skyddet. Denna uppfattning stöds ytterligare av den allmänna ökningen av utbyte av uppgifter mellan medlemsstaterna och det aktuella förslaget om tillgänglighetsprincipen. Olika nationella regler om tillgång och vidare användning skulle inte vara förenligt med den föreslagna "fria rörligheten" för information om brottsbekämpning inom hela EU, som även omfattar uppgifter från privata databaser.

119. Datatillsynsmannen anser därför att gemensamma normer bör gälla för de brottsbekämpande myndigheternas tillgång till personuppgifter som innehas av privata parter, för att garantera att tillgång endast medges på grundval av väl definierade villkor och begränsningar. I synnerhet bör de behöriga myndigheternas tillgång endast medges från fall till fall under specifika omständigheter, för noggrant angivna ändamål och omfattas av domstolsprövning i medlemsstaterna.

(<sup>1</sup>) I ingressen till direktivet anges följande: "Frågor om tillgång till de uppgifter som nationella offentliga myndigheter lagrar i enlighet med detta direktiv för de verksamheter som avses i artikel 3.2 första ledet i direktiv 95/46/EG faller utanför tillämpningsområdet för gemenskapens lagstiftning. De kan emellertid omfattas av nationell lagstiftning eller nationella åtgärder i enlighet med avdelning VI i fördraget om Europeiska unionen, förutsatt att sådana lagar eller åtgärder till fullo står i överensstämmelse med de grundläggande rättigheter som följer av medlemsstaternas gemensamma författningsskydd och som är garanterade i Europeiska konventionen om skydd för de mänskliga rättigheterna och de grundläggande friheterna. Enligt den tolkning Europeiska domstolen för de mänskliga rättigheterna gjort av artikel 8 i Europeiska konventionen om skydd för de mänskliga rättigheterna och de grundläggande friheterna ..."

#### IV.10 Den registrerades rättigheter

120. I kapitel IV tas den registrerades rättigheter upp på ett sätt som generellt överensstämmer med den gällande lagstiftningen om uppgiftsskydd och artikel 8 i Europeiska unionens stadga om de grundläggande rättigheterna.

121. Datatillsynsmannen välkomnar dessa bestämmelser, eftersom en harmoniserad uppsättning rättigheter för registrerade fastställs, samtidigt som hänsyn tas till vad som utmärker de brottsbekämpande och rättsliga myndigheternas behandling. Detta är en väsentlig förbättring, eftersom den nuvarande situationen kännetecknas av en mängd olika regler och praxis, särskilt för rätten till tillgång. Några medlemsstater tillåter inte att den registrerade får tillgång till uppgifterna utan har ett system med "indirekt tillgång" (som kan utövas av den nationella dataskyddsmyndigheten i den registrerades namn).

122. Enligt förslaget är de eventuella undantagen från rätten till direkt tillgång harmoniserade. Detta är så mycket viktigare för att medborgare vilkas uppgifter i allt större utsträckning behandlas och utbyts av behöriga myndigheter i olika EU-medlemsstater skall kunna utnyttja en harmoniserad uppsättning rättigheter som registrerade, oberoende av den medlemsstat där uppgifter samlas in eller behandlas <sup>(2)</sup>.

123. Datatillsynsmannen erkänner det lämpliga i att begränsa de registrerades rättigheter, om det är nödvändigt för att förebygga, utreda, avslöja eller lagföra brott. Eftersom dessa begränsningar måste betraktas som undantag från de registrerades grundläggande rättigheter, bör dock en strikt prövning av proportionaliteten göras. Detta innebär att undantagen bör vara begränsade och väl definierade och att begränsningarna om möjligt bör vara partiella och tidsbegränsade.

124. Ur detta perspektiv vill datatillsynsmannen särskilt uppmärksamma lagstiftaren på punkt 2 a i artiklarna 19, 20 och 21, där det fastställs ett mycket omfattande och obestämt undantag från de registrerades rättigheter, genom att det anges att dessa rättigheter kan begränsas om det är nödvändigt för att "den registeransvarige skall kunna fullgöra sina åligganden enligt lag på ett korrekt sätt". Detta undantag överlappar dessutom bestämmelsen i led b, som medger begränsningar av den registrerades rättigheter, om det är nödvändigt "för att inte skada

(<sup>2</sup>) I kapitel IV behandlas i synnerhet rätten till information (artiklarna 19 och 20) och rätten till tillgång, rättelse, radering eller blockering (artikel 21). På det hela taget ger dessa artiklar registrerade alla de rättigheter som vanligtvis garanteras genom EU:s lagstiftning om uppgiftsskydd, samtidigt som en rad undantag anges med hänsyn till den tredje pelarens särdrag. I synnerhet medges begränsningar av registrerades rättigheter genom nästan identiska bestämmelser om både rätt till information (artiklarna 19.2 och 20.2) och rätt till tillgång (artikel 21.2).

pågående utredningar, undersökningar eller rättegångar, eller hindra de behöriga myndigheterna från att fullgöra sina åligganden enligt lag". Det senare undantaget kan anses vara berättigat, men det förra förefaller innebära en oproportionerlig begränsning av den registrerades rättigheter. Datatillsynsmannen rekommenderar därför att punkt 2 a i artiklarna 19, 20 och 21 stryks.

125. Datatillsynsmannen rekommenderar även att artiklarna 19, 20 och 21 förbättras på följande sätt:

- Det bör anges att begränsningarna av den registrerades rättigheter inte är obligatoriska, inte gäller obegränsad tid och "endast" är tillåtna i de särskilda fall som uppräknas i artiklarna.
- Hänsyn bör tas till att information bör lämnas självantaget av den registeransvarige och inte på grundval av en begäran från den registrerade.
- Det bör i artikel 19.1 c läggas till att information också bör lämnas om "tidsfristerna för lagring av uppgifterna".
- De bör säkerställas (genom ändring av artikel 20.1 i linje med andra EU-instrument om uppgiftsskydd) att information, om uppgifter inte har erhållits från den registrerade eller har erhållits från denne utan dennes vetskap, lämnas till denne "senast vid den tidpunkt när uppgifter först röjs".
- Det bör säkerställas att mekanismen för att överklaga vid vägran eller begränsning av de registrerades rättigheter är tillämplig vid begränsning av rättigheten att informeras, och artikel 19.4 sista meningen bör ändras i enlighet härmed.

#### Automatiska individuella beslut

126. Datatillsynsmannen beklagar att förslaget inte alls tar upp den viktiga frågan om automatiska individuella beslut. Praktisk erfarenhet visar i själva verket att de brottsbekämpande myndigheterna i allt större utsträckning utnyttjar automatisk behandling av uppgifter för att utvärdera vissa personliga aspekter hos personer, särskilt för att bedöma deras tillförlitlighet och uppträdande.

127. Datatillsynsmannen inser att dessa system i vissa fall kan vara nödvändiga för att effektivisera de brottsbekämpande myndigheternas verksamhet, men noterar att beslut som enbart bygger på automatisk behandling av uppgifter bör omfattas av mycket stränga villkor och säkerhetsåtgärder, när de får rättsliga följder för en person eller väsentligt påverkar en person. Detta är ännu viktigare i samband

med tredje pelaren, eftersom de behöriga myndigheterna i detta fall förfogar över allmänna tvångsmedel, och deras beslut eller åtgärder således kan komma att påverka en person eller vara mer inkräktande än vad som normalt skulle vara fallet när sådana beslut fattas eller sådana åtgärder vidtas av privata parter.

128. Framför allt bör sådana beslut eller åtgärder i överensstämmelse med allmänna dataskydds-principer endast medge, om de uttryckligen tillåts enligt lag eller av den behöriga tillsynsmyndigheten och de bör omfattas av lämpliga åtgärder för att skydda den registrerades rättmätiga intressen. Den registrerade bör dessutom ha lättillgängliga möjligheter att framföra sina synpunkter och förstå logiken i beslutet, såvida detta inte är oförenligt med det ändamål för vilket uppgifterna behandlas.

129. Datatillsynsmannen rekommenderar därför att det införs en specifik bestämmelse om automatiska individuella beslut, i linje med gällande EU-lagstiftning om uppgiftsskydd.

#### IV.11 Säkerhet i samband med behandling av uppgifter

130. När det gäller säkerheten i samband med behandling av uppgifter, fastställs i artikel 24 en skyldighet för den registeransvarige att genomföra lämpliga tekniska och organisatoriska åtgärder i linje med bestämmelserna i andra EU-instrument om uppgiftsskydd. I punkt 2 finns dessutom en detaljerad och heltäckande förteckning över åtgärder som skall genomföras inom automatisk databehandling.

131. Datatillsynsmannen välkomnar denna bestämmelse, men föreslår att man för att underlätta tillsynsmyndigheternas effektiva kontroll lägger till följande extra åtgärd i förteckningen över åtgärder i punkt 2: "k) genomföra åtgärder för systematisk övervakning och rapportering om dessa säkerhetsåtgärders effektivitet (systematisk egenkontroll av säkerhetsåtgärder)" <sup>(1)</sup>.

#### Registrering av uppgifter

132. Enligt artikel 10 skall varje automatisk överföring och varje automatiskt mottagande av personuppgifter registreras (vid automatisk överföring) eller dokumenteras (vid icke automatisk överföring) på ett sätt som gör det möjligt att i efterhand kontrollera att överföringen och behandlingen av uppgifter är laglig. Sådan information skall vara tillgänglig på begäran av den behöriga tillsynsmyndigheten.

<sup>(1)</sup> Se i detta sammanhang datatillsynsmannens yttrande om förslaget till Europaparlamentets och rådets förordning om informationssystemet för viseringar (VIS) och utbytet mellan medlemsstaterna av uppgifter om viseringar för kortare vistelse (KOM (2004) 835 slutlig), som offentliggjorts på [www.edps.eu.int](http://www.edps.eu.int).



133. Datatillsynsmannen välkomnar denna bestämmelse. Han noterar dock att även "tillgång" till uppgifter skall registreras eller dokumenteras för att garantera en heltäckande kontroll och för undersökning av om personuppgifter används korrekt. Denna information är väsentlig, eftersom en effektiv övervakning av en korrekt behandling av personuppgifter inte endast måste inriktas på lagligheten i överföringen av personuppgifter mellan myndigheterna utan även på lagligheten i dessa myndigheters tillgång. Datatillsynsmannen rekommenderar därför att artikel 10 ändras, så att det också föreskrivs att tillgång till uppgifter skall registreras eller dokumenteras<sup>(1)</sup>.

#### IV.12 Rättslig prövning, ansvar och påföljder

134. I kapitel VI i förslaget behandlas rättslig prövning (artikel 27), ansvar (artikel 28) och påföljder (artikel 29). Bestämmelserna överensstämmer på det hela taget med gällande EU-lagstiftning om uppgiftsskydd.

135. Särskilt när det gäller påföljder välkomnar datatillsynsmannen specificeringen att påföljder vid överträdelse av de bestämmelser som fastställts i enlighet med rambeslutet skall vara effektiva, lämpliga och avskräckande. Straffrättsliga påföljder för uppsåtliga och allvarliga överträdelser, särskilt inom konfidentiell och säker uppgiftsbehandling, skall dessutom säkerställa en större avskräckande effekt för allvarligare överträdelser av dataskyddslagen.

#### IV.13 Kontroll- och övervakningsuppgifter samt rådgivande uppgifter

136. De bestämmelser i förslaget som tar upp kontroll och övervakning av uppgiftsbehandling samt samråd i frågor som rör uppgiftsbehandling liknar i stor utsträckning bestämmelserna i direktiv 95/46/EG. Datatillsynsmannen välkomnar att kommissionen i sitt förslag har valt redan prövade och välfungerande mekanismer och framhåller särskilt införandet av ett (obligatoriskt) system för förhandskontroll. Ett sådant system förutses inte endast i direktiv 95/46/EG utan ingår också i förordning 45/2001/EG och har visat sig vara ett effektivt instrument, som står till datatillsynsmannens förfogande vid övervakningen av gemenskaps-institutioners och gemenskapsorgans uppgiftsbehandling.

137. Ett annat instrument för kontroll och övervakning av uppgiftsbehandling som har visat sig vara effektivt är att en registeransvarig utser uppgiftsskyddsombud. Detta

instrument fungerar i flera medlemsstater. Det föreskrivs i förordning 45/2001/EG som ett obligatoriskt instrument och spelar en nyckelroll inom Europeiska gemenskaperna. Uppgiftsskyddsombuden är administratörer inom en organisation och ska på ett oberoende sätt säkerställa den interna tillämpningen av bestämmelser om uppgiftsskydd.

138. Datatillsynsmannen rekommenderar att bestämmelser om uppgiftsskyddsombud läggs till i förslaget. Dessa bestämmelser kan utformas med artiklarna 24-26 i förordning 45/2001/EG som modell.

139. Förslaget till rambeslut riktas till medlemsstaterna. Det är därför logiskt att det i artikel 30 i förslaget föreskrivs att övervakning skall ske genom oberoende tillsynsmyndigheter. Denna artikel har utformats på ungefär samma sätt som artikel 28 i direktiv 95/46/EG. Dessa nationella myndigheter bör samarbeta med varandra, med de gemensamma tillsynsorgan som inrättats enligt avdelning VI i EU-fördraget och med datatillsynsmannen. Enligt artikel 31 i förslaget skall det dessutom inrättas en arbetsgrupp, som skall spela en roll liknande den som artikel 29-gruppen spelar i frågor som omfattas av första pelaren. Alla relevanta aktörer på uppgiftsskyddsområdet nämns i artikel 31 i förslaget.

140. Det är självklart att samarbetet mellan alla relevanta aktörer på uppgiftsskyddsområdet spelar en viktig roll i ett förslag vars syfte är att förbättra polissamarbetet och det rättsliga samarbetet mellan medlemsstaterna. Datatillsynsmannen välkomnar därför att man i förslaget lägger betoning på samarbete mellan tillsynsmyndigheterna.

141. Datatillsynsmannen betonar dessutom vikten av ett konsekvent tillvägagångssätt i frågor rörande uppgiftsskydd, något som kan förbättras genom att kommunikation mellan den befintliga artikel 29-gruppen och den arbetsgrupp som inrättas genom detta förslag till rambeslut främjas. Datatillsynsmannen rekommenderar att artikel 31.2 i förslaget ändras, så att ordföranden i artikel 29-gruppen får rätt att delta i eller företrädas vid den nya arbetsgruppens möten.

142. Texten i artikel 31 i förslaget innehåller en anmärkningsvärd skillnad mot artikel 29 i direktiv 95/46/EG. Datatillsynsmannen är full medlem av artikel 29-gruppen. Detta medlemskap omfattar rätten att rösta. Enligt det aktuella förslaget är datatillsynsmannen också medlem av arbetsgruppen (på grundval av artikel 31), men har inte rätt att rösta. Det är inte klart av vilka skäl detta förslag avviker från artikel 29 i direktiv 95/46/EG. Datatillsynsmannen anser att den föreslagna texten är oklar i fråga om datatillsynsmannens roll, vilket kan hämma effektiviteten i hans deltagande i arbetsgruppens arbete. Datatillsynsmannen rekommenderar därför att överensstämmelsen med direktivets text behålls.

<sup>(1)</sup> Detta är i linje med bestämmelserna i artikel 18 i förslaget, enligt vilka den översändande myndigheten på begäran skall underrättas om den vidare behandlingen av de personuppgifter som har överlämnats eller gjorts tillgängliga, och bestämmelserna i artikel 24, om genomförande av säkerhetsåtgärderna, även mot bakgrund av det föreslagna systemet med egenkontroll av dessa åtgärder.

#### IV.14 Övriga bestämmelser

143. Kapitel VIII i förslaget innehåller några slutbestämmelser om ändring av Schengenkonventionen och andra instrument som rör behandling och skydd av personuppgifter.

##### *Schengenkonventionen*

144. Enligt artikel 33 i förslaget skall artiklarna 126-130 i Schengenkonventionen ersättas av detta beslut när det gäller aspekter som omfattas av EU-fördraget. Artiklarna 126-130 i Schengenkonventionen innehåller de allmänna uppgiftsskyddsreglerna för behandling av uppgifter som lämnas enligt konventionen (men utanför Schengens informationssystem).

145. Datatillsynsmannen välkomnar att dessa artiklar skall ersättas, eftersom det innebär att uppgiftsskyddssystemet inom tredje pelaren blir enhetligare och skyddet av personuppgifter i några avseenden förbättras betydligt, t.ex. genom att tillsynsmyndigheternas befogenheter ökas. Det leder dock på några punkter oavsiktligt och olyckligtvis till att nivån på uppgiftsskyddet sänks. Några bestämmelser i Schengenkonventionen är faktiskt strängare än rambeslutets bestämmelser.

146. Datatillsynsmannen nämner särskilt artikel 126.3 b i Schengenkonventionen, enligt vilken uppgifterna endast för användas av domstolar, förvaltningar och organ som utför uppgifter eller fyller en funktion inom ramen för de mål som avses i konventionen. Det förefaller som om denna bestämmelse utesluter översändande till privata parter, något som dock skulle vara tillåtet enligt det föreslagna rambeslutet. En annan sak är att bestämmelserna om uppgiftsskydd i Schengenkonventionen även gäller *alla* uppgifter som lämnas från eller införs i ett *icke-automatiskt* register (artikel 127), medan icke-strukturerade register undantas från det föreslagna rambeslutets tillämpningsområde.

##### *Konventionen om ömsesidig rättslig hjälp i brottmål mellan Europeiska unionens medlemsstater*

147. Enligt artikel 34 skall artikel 23 i konventionen om ömsesidig rättslig hjälp i brottmål mellan Europeiska unionens medlemsstater ersättas av rambeslutet. Datatillsynsmannen noterar att detta på det hela taget skulle innebära ett bättre skydd för personuppgifter som utbyts inom ramen för konventionen, men att det också kan ge upphov till en del problem med de båda instrumentens förenlighet.

148. I synnerhet tar konventionen även upp ömsesidig rättslig hjälp vid avlyssning av telekommunikationer. I detta fall kan den anmodade medlemsstaten lämna sitt samtycke,

till avlyssningen eller översändandet av upptagning av telemeddelanden, på de villkor som måste uppfyllas i ett liknande nationellt fall. Enligt artikel 23.4 i konventionen skall dessa ytterligare villkor när de gäller användningen av personuppgifter ha företräde framför reglerna om uppgiftsskydd i artikel 23. På samma sätt fastställs i artikel 23.5 att tillägsreglerna om skydd för information som samlas in av gemensamma utredningsgrupper har företräde. Datatillsynsmannen noterar att det, om artikel 23 ersätts med det nuvarande förslaget, skulle vara oklart om de ovannämnda tillägsreglerna fortfarande skulle gälla. Datatillsynsmannen rekommenderar därför att denna punkt klargörs, så att en ingående bedömning av konsekvenserna av att artikel 23 i konventionen ersätts fullt ut med detta rambeslut kan göras.

##### *Europarådets konvention nr 108 om skydd för enskilda vid automatisk databehandling av personuppgifter*

149. Enligt artikel 34.2 skall varje hänvisning till konvention nr 108 förstås som en hänvisning till detta rambeslut. Tolkningen och den konkreta tillämpligheten av denna bestämmelse är långt ifrån klar. I varje fall antar datatillsynsmannen att denna bestämmelse endast gäller inom detta rambesluts materiella tillämpningsområde.

##### *Slutliga frågor*

150. När det gäller textens systematiska konsekvens, noterar datatillsynsmannen att några artiklar hellre skulle placeras på ett annat ställe i texten.

Han förslår därför

1. att artikel 16 (Kommitté) flyttas från kapitel III (Särskilda former av behandling) till ett nytt kapitel,
2. att artikel 25 (Register) och artikel 26 (Förhandskontroll) flyttas från kapitel V (Sekretess och säkerhet i samband med behandling av uppgifter) till ett nytt kapitel.

#### V. SLUTSATSER

##### *Ett avsevärt steg framåt*

- a) Om detta förslag antas, skulle det innebära ett avsevärt steg framåt i skyddet av personuppgifter på ett viktigt område som särskilt kräver en enhetlig och effektiv mekanism för skydd av personuppgifter inom Europeiska unionen.
- b) Ett effektivt skydd av personuppgifter är inte bara viktigt för de registrerade utan bidrar även till att polissamarbetet och det rättsliga samarbetet i sig blir en framgång. I många aspekter går båda allmänna intressena hand i hand.

*Gemensamma normer*

- c) Datatillsynsmannen anser att en ny ram för uppgiftsskydd inte endast bör respektera principerna om uppgiftsskydd – det är viktigt att garantera ett enhetligt uppgiftsskydd inom Europeiska unionen – utan även tillhandahålla ytterligare en uppsättning regler med hänsyn till brottsbekämpningens särskilda natur.
- d) Förslaget uppfyller dessa villkor; det säkerställer att de befintliga principerna om uppgiftsskydd enligt direktiv 95/46/EG kommer att tillämpas inom tredje pelaren, eftersom de flesta bestämmelserna i förslaget speglar andra unionsrättsakter om skydd av personuppgifter och överensstämmer med dessa rättsakter. I förslaget fastställs dessutom gemensamma normer där dessa principer specificeras, med tanke på deras tillämpning på detta område, vilka generellt sett är tillfredsställande och lämnar adekvata uppgiftsskydds-garantier inom tredje pelaren.

*Tillämpliga på all behandling*

- e) För att rambeslutets mål skall kunna uppnås, är det väsentligt att det omfattar alla polis-uppgifter och rättsliga uppgifter, även om de inte översänds eller görs tillgängliga av andra medlemsstaters behöriga myndigheter.
- f) Artiklarna 30.1 b och 31.1 c i EU-fördraget utgör en rättslig grund för regler om uppgiftsskydd vilka inte är begränsade till skyddet av personuppgifter som faktiskt utbyts mellan medlemsstaternas behöriga myndigheter utan också gäller för inhemska situationer.
- g) Förslaget gäller inte behandling inom ramen för EU-fördragets andra pelare (gemensam utrikes- och säkerhetspolitik) eller underrättelsetjänsters behandling av uppgifter eller deras tillgång till dessa uppgifter när de behandlas av behöriga myndigheter eller andra parter (detta följer av artikel 33 i EU-fördraget). På dessa områden skall nationell rätt ge registrerade adekvat skydd. Denna lucka i skyddet på EU-nivå kräver ett ännu effektivare skydd på de områden som faktiskt omfattas av förslaget.
- h) Datatillsynsmannen välkomnar att förslaget även omfattar personuppgifter som behandlas av rättsliga myndigheter.

*Förhållandet till andra rättsliga instrument*

- i) Om det i ett annat specifikt rättsligt instrument inom ramen för avdelning VI i EU-fördraget fastställs precisare villkor eller restriktioner för behandlingen av eller tillgången till uppgifter, bör det specifika rättsliga instrumentet gälla som en *lex specialis*.

- j) Detta förslag till rådets rambeslut om uppgiftsskydd har sina egna förtjänster och behövs även om ett rättsligt instrument om tillgänglighet inte antas (förslag från kommissionen av den 12 oktober 2005).
- k) Europaparlamentets godkännande av direktivet om lagring av kommunikationsuppgifter gör det ännu mer angeläget att fastställa en rättslig ram för uppgiftsskydd inom tredje pelaren.

*Förslagets struktur*

- l) Tillägsreglerna i kapitel II (förutom de allmänna principerna i direktiv 95/46/EG) bör erbjuda ytterligare skydd för de registrerade i samband med den specifika kontext som tredje pelaren utgör, men får inte leda till en lägre skyddsnivå.
- m) Kapitel III om särskilda former av behandling (där det tredje skiktet av skydd har tagits med) får inte avvika från kapitel II. Bestämmelserna i kapitel III bör erbjuda ytterligare skydd för de registrerade i situationer där de berörda myndigheterna i mer än en medlemsstat är inblandade, men dessa bestämmelser får inte leda till en lägre skyddsnivå.
- n) Bestämmelserna om kontroll av uppgiftskvaliteten (artikel 9.1 och 9.6) och om regleringen av vidare behandling av personuppgifter (artikel 11.1) bör flyttas till kapitel II och göras tillämpliga på all behandling av uppgifter som görs av brottsbekämpande myndigheter, även om personuppgifter inte har översänts eller gjorts tillgängliga av en annan medlemsstat. Det är i synnerhet väsentligt, både i de registrerades och de behöriga myndigheternas intresse, att sörja för att kvaliteten på alla personuppgifter kontrolleras på ett lämpligt sätt.

*Begränsning av ändamålet*

- o) Förslaget behandlar på ett inte helt tillfredsställande sätt en situation som kan inträffa under polisens arbete, nämligen behovet av att använda uppgifterna vidare för ett ändamål som anses oförenligt med det ändamål för vilket de samlats in.
- p) Enligt EU:s lagstiftning om uppgiftsskydd skall personuppgifter samlas in för särskilt angivna och uttryckliga ändamål och inte användas vidare på ett sätt som är oförenligt med dessa ändamål. En viss flexibilitet måste medges när det gäller vidare användning. Det är troligare att begränsningen i fråga om insamling följs väl, om de myndigheter som ansvarar för den inre säkerheten vet att de, med lämpliga säkerhetsåtgärder, kan räkna med ett undantag från begränsningen i fråga om vidare användning.

q) Det bör i kapitel II i rambeslutet anges att medlemsstaterna skall få anta lagstiftningsåtgärder för att tillåta vidare behandling, om en sådan åtgärd är nödvändig för att garantera:

- förebyggande av hot mot allmän säkerhet, försvar eller nationell säkerhet,
- skydd av ett viktigt ekonomiskt eller finansiellt intresse i en medlemsstat,
- skydd för den registrerade.

Dessa medlemsstaternas befogenheter kan innebära en behandling som inkräktar på privat-livet, och de bör således åtföljas av mycket stränga villkor.

#### *Nödvändighet och proportionalitet*

r) Förslagets principer om nödvändighet och proportionalitet bör fullt ut återspegla rättspraxis vid Europeiska domstolen för de mänskliga rättigheterna, genom att säkerställa att behandling av personuppgifter endast betraktas som nödvändig, om de behöriga myndigheterna kan visa att de har ett klart behov av den, med förutsättningen att åtgärder som inkräktar mindre på privatlivet inte finns tillgängliga.

#### *Utbyte av personuppgifter med tredjeländer*

s) Om uppgifter kunde översändas till tredjeländer utan att skydd av den registrerade garanterades skulle detta allvarligt skada det skydd som föreslås i detta förslag inom Europeiska unionens territorium. Datatillsynsmannen rekommenderar att förslaget ändras, så att det säkerställs att artikel 15 gäller utbyte av *alla* personuppgifter med tredjeländer. Denna rekommendation gäller inte artikel 15.1 c.

t) När personuppgifter översänds från tredjeländer bör deras kvalitet bedömas noggrant innan de används med tanke på respekten för mänskliga rättigheter och uppgiftsskyddsnormer.

#### *Utbyte av personuppgifter med privata parter och andra myndigheter än brottsbekämpande myndigheter*

u) Det kan i specifika fall vara nödvändigt att överföra uppgifter till privata parter och andra offentliga organ för att förebygga och bekämpa brott, men specifika och strikta villkor bör gälla. Datatillsynsmannen rekommenderar att förslaget ändras, så att det säkerställs att artiklarna 13 och 14 gäller utbytet av *alla* personuppgifter, även dem som inte mottas från eller görs tillgängliga av en annan medlemsstat. Denna rekommendation gäller inte artiklarna 13 c och 14 c.

v) Gemensamma normer bör gälla för de brottsbekämpande myndigheternas tillgång till personuppgifter som innehas av

privata parter, så att det säkerställs att tillgång endast medges på grundval av väl definierade villkor och begränsningar.

#### *Särskilda kategorier av uppgifter*

w) Särskilda säkerhetsåtgärder bör tillhandahållas, särskilt för att garantera att

- biometriska uppgifter och DNA-profiler endast används på grundval av väletablerade och kompatibla tekniska standarder,
- graden av exakthet beaktas noggrant och kan bestridas av den registrerade på ett lättillgängligt sätt, och
- respekten för personers värdighet säkerställs fullt ut.

#### *Åtskillnaden mellan olika kategorier av uppgifter*

x) Personuppgifter rörande olika kategorier av människor (misstänkta, dömda personer, offer, vittnen m.fl.) bör behandlas enligt olika, lämpliga villkor och garantier. Datatillsynsmannen föreslår därför att en ny punkt med följande innehåll läggs till i artikel 4:

- Skyldighet för medlemsstaterna att fastställa de rättsliga konsekvenserna av de åtskillnader som skall göras mellan personuppgifter om olika kategorier av personer.
- Tilläggsbestämmelser för att begränsa behandlingens syfte, fastställa exakta tidsfrister och begränsa tillgången till uppgifter, när det gäller icke misstänkta personer.

#### *Automatiska individuella beslut*

y) Beslut som endast grundas på automatisk behandling av uppgifter bör omfattas av mycket stränga villkor, när de får konsekvenser för en person eller väsentligt påverkar en person. Datatillsynsmannen rekommenderar därför att särskilda bestämmelser om automatiska individuella beslut införs, liknande dem i direktiv 95/46/EG.

#### *Urval av andra rekommendationer*

z) Datatillsynsmannen rekommenderar att

- artikel 4.4 första strecksatsen ändras för att säkerställa respekten för rättspraxis beträffande artikel 8 i konventionen angående skydd för de mänskliga rättigheterna och de grundläggande friheterna, eftersom den föreslagna formuleringen i artikel 4.4 inte uppfyller de kriterier som fastställs i rättspraxis vid Europeiska domstolen för de mänskliga rättigheterna beträffande artikel 8 i konventionen,

- det breda undantaget i artikel 7.1 stryks eller att de allmänna intressen som motiverar att medlemsstaterna använder sig av det åtminstone uttryckligen begränsas,
- artikel 10 ändras, så att det anges att även tillgång till uppgifter skall registreras eller dokumenteras,
- punkt 2 a i artiklarna 19, 20 och 21 stryks,
- bestämmelser om uppgiftsskyddsombud läggs till i förslaget; dessa bestämmelser kan utformas med artiklarna 24-26 i förordning 45/2001/EG som modell,
- artikel 31.2 i förslaget ändras, så att ordföranden i artikel 29-gruppen får rätt att delta i eller företrädas vid den nya arbetsgruppens möten.

Utfärdat i Bryssel den 19 december 2005

Peter HUSTINX  
*Europeiska datatillsynsmannen*