EUROPEISKA DATATILLSYNSMANNEN

Yttrande från Europeiska datatillsynsmannen om förslaget till rådets rambeslut om utbyte av uppgifter enligt principen om tillgänglighet (KOM(2005) 490 slutlig)

(2006/C 116/04)

EUROPEISKA DATATILLSYNSMANNEN HAR

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

1. Förslaget till rambeslut om utbyte av uppgifter enligt principen om tillgänglighet sändes av kommissionen till datatillsynsmannen i ett brev daterat den 12 oktober 2005. Datatillsynsmannen ser detta brev 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. Yttrandets karaktär skall ses mot bakgrund av det sammanhang som beskrivs under II. Så som anges under II är det långt ifrån självklart att föreliggande förslag – eller förslagets strategi när det gäller tillgänglighet – så småningom kommer att leda fram till antagandet av ett rättsinstrument. Många medlemsstater förespråkar andra lösningar.

3. Det är emellertid uppenbart att frågan om tillgänglighet avseende brottsbekämpningsinformation – eller, i vidare mening, utbyte av sådan information – över gränserna ligger högt på medlemsstaternas dagordning, både inom och utanför rådet, liksom inom Europaparlamentet.

4. Lika uppenbart är att detta ämne är i hög grad relevant sett med utgångspunkt i skyddet av personuppgifter, vilket yttrandet i sig kommer att visa. Datatillsynsmannen påminner om att det föreliggande förslaget lades fram av kommissionen, med tät koppling till förslaget till rådets rambeslut om skydd av personuppgifter som behandlas inom ramen för polissamarbete och straffrättsligt samarbete, vilket datatillsynsmannen lade fram ett yttrande till den 19 december 2005.

5. Datatillsynsmannen kommer att utnyttja tillfället för att i detta yttrande lägga fram några allmänna och mer grundläggande synpunkter när det gäller frågan om utbyte av information om brottsbekämpning och om strategier för att reglera denna fråga. Genom att lägga fram detta yttrande avser datatillsynsmannen att se till att dataskyddsperspektivet vederbörligen beaktas i diskussioner om ämnet i framtiden.

6. Datatillsynsmannen kommer att finnas till hands för ytterligare rådfrågning på ett senare stadium efter den normala gången genom lagstiftningsprocessen när det gäller detta förslag men även andra besläktade förslag.

II. FÖRSLAGET I SITT SAMMANHANG

7. Principen om tillgänglighet infördes som en viktig ny rättsprincip i Haagprogrammet. Det medför att information som behövs för brottsbekämpning bör förmedlas över EU:s internationella gränser utan hinder. Syftet med detta förslag är att införa denna princip genom ett bindande rättsinstrument.

8. Utbyte av polisiär information mellan olika länder är ett populärt ämne bland lagstiftare, såväl inom som utanför ramen för EU. Följande initiativ har nyligen uppmärksammats av datatillsynsmannen.

9. För det första lade Sverige den 4 juni 2004 fram ett förslag till rambeslut om förenklat uppgifts- och underrättelseutbyte mellan de brottsbekämpande myndigheterna i Europeiska unionens medlemsstater. För detta förslag nådde rådet en överenskommelse om en allmän riktlinje vid sitt möte den 1 december 2005.

10. För det andra undertecknade sju medlemsstater den 27 maj 2005 en konvention i Prüm i Tyskland om stärkt gränsöverskridande samarbete särskilt för att bekämpa terrorism, gränsöverskridande brottslighet och olaglig invandring. Bland annat införs där åtgärder för förbättrat informationsutbyte om DNA och fingeravtryck. Alla medlemsstater i Europeiska unionen kan ansluta sig till konventionen. De fördragsslutande parterna avser att införliva bestämmelserna i konventionen i Europeiska unionens rättsliga ramar.

11. För det tredje kommer tillgängligheten till information om brottsbekämpning över Europeiska unionens internationella gränser också att ytterligare underlättas genom andra rättsinstrument, exempelvis förslagen om en andra generation av Schengens informationssystem (SIS II), förslaget om möjlighet till sökningar i informationssystemet för viseringar (VIS) och förslaget till rambeslut om organisationen av medlemsstaternas utbyte av uppgifter ur kriminalregistret och uppgifternas innehåll. Här är det också viktigt att nämna meddelandet om större effektivitet, förbättrad interoperabilitet och för synergieffekter mellan EU:s databaser på området rättsliga och inrikesfrågor utfärdat av kommissionen den 25 november 2005.

12. Eftersom alla dessa initiativ har utfärdats bör inte förslaget till rambeslut om tillgänglighet behandlas isolerat, utan andra lösningar när det gäller utbyte av uppgifter om brottsbekämpning bör också beaktas. Detta är desto viktigare med tanke på den rådande tendensen inom rådet att ge företräde åt andra lösningar för utbyte av uppgifter och åt begreppet tillgänglighet än den allmänna riktlinje som kommissionen föreslår i föreliggande förslag. Förslagets nuvarande text kanske inte ens kommer att tas upp till diskussion i rådet.

13. Vidare är detta förslag nära knutet till förslaget till ett rambeslut om skydd av personuppgifter. Föreliggande yttrande måste ses mot bakgrund av det mer ingående yttrandet om det sistnämnda rambeslutet.

14. I sitt yttrande över förslaget till rambeslut om skydd av personuppgifter framhöll datatillsynsmannen vikten av tillfredsställande uppgiftsskydd som en ofrånkomlig följd av ett rättsinstrument om tillgänglighet. Enligt datatillsynsmannen bör ett sådant rättsinstrument inte antas utan garantier som är av vikt för uppgiftsskyddet.

15. Datatillsynsmannen intar samma ståndpunkt när det gäller antagandet av andra rättsinstrument som underlättar flödet av uppgifter om brottsbekämpning över EU:s inre gränser. Datatillsynsmannen ser därför med tillfredsställelse att såväl rådet som Europaparlamentet har gett prioritet åt förslaget till ett rambeslut om skydd av personuppgifter.

III. TILLGÄNGLIGHETSPRINCIPEN SOM SÅDAN

16. Tillgänglighetsprincipen är i sig en enkel princip. De uppgifter som finns tillgängliga för vissa myndigheter i en medlemsstat skall också tillhandahållas motsvarande myndigheter i andra medlemsstater. Uppgifterna skall utväxlas så snabbt och enkelt som möjligt mellan medlemsstaternas myndigheter och företrädesvis genom att direktåtkomst tillåts.

17. Svårigheterna uppkommer beroende av den miljö där tillgänglighetsprincipen skall omsättas i effektiv praktik:

— En heterogen organisation av polis- och domstolsväsendet i medlemsstaterna, med varierande kontrollmekanismer.

— Olika typer av (känslig) information ingår (såsom DNA eller fingeravtryck).

— Olika sätt för att få tillgång till relevant information för de behöriga myndigheterna också inom medlemsstater.

— Det är svårt att garantera att uppgifter med ursprung i en annan medlemsstat kommer att tolkas rätt beroende på skillnader i språk, tekniska system (driftskompatibilitet) och i fråga om rättssystem.

— Den måste införlivas i det befintliga och omfattande lappverk av rättsregler som behandlar utbytet av uppgifter om brottsbekämpning mellan länderna.

18. Oberoende av denna komplexa miljö är det allmänt känt att principen inte kan fungera i isolering. Det krävs ytterligare åtgärder för att garantera att det faktiskt går att hitta och få åtkomst till uppgifter. Under alla förhållanden måste dessa åtgärder underlätta för brottsbekämpande myndigheter att ta reda på huruvida brottsbekämpande myndigheter i andra medlemsstater har relevant information till sitt förfogande och var denna relevanta information finns. Sådana ytterligare åtgärder skulle kunna bestå av gränssnitt (*interface*) som ger direktåtkomst till alla eller specifika data som innehas av andra medlemsstater. Förslaget till rambeslut om tillgånglighet inför av detta skäl ”registerdata”, särskilda data som det är möjliga att få direkt åtkomst till över gränserna.

19. Rent allmänt bör tillgänglighetsprincipen underlätta flödet av uppgifter mellan medlemsstaterna. De inre gränserna kommer att avskaffas och medlemsstaterna måste i allt större omfattning låta andra myndigheter få åtkomst till den information de egna polisiära myndigheterna har tillgång till. Medlemsstaterna förlorar sin behörighet att kontrollera flödet av uppgifter vilket också medför att de inte längre kan lita på att deras nationella lagstiftning är ett tillräckligt instrument för ett fullgott skydd av uppgifterna.

20. Detta skäl gör att perspektivet med skydd av personuppgifter i förslaget kräver särskild uppmärksamhet. För det första måste uppgifter som normalt sett är konfidentiella och omgärdade med betryggande säkerhetsåtgärder tillhandahållas myndigheter i andra medlemsstater. För det andra krävs det för att få systemet att fungera att registerdata fastställs och görs tillgängliga för myndigheter i de andra medlemsstaterna. Genomförandet av denna princip kommer följaktligen att alstra mer data än dem som för närvarande är tillgängliga.

IV. **HUVUDDRAG**

Tillgänglighetsprincipens tillämpningsområde

21. Först och främst är det väsentligt att definiera för vilken typ av uppgifter principen om tillgänglighet skall gälla. Tillämpningsområdet för denna princip definieras i allmänna termer i artikel 2 i förslaget, i kombination med artikel 1.1 och artikel 3 a. Principen skall tillämpas på följande uppgifter:

— Befintliga uppgifter,

— Enligt förteckning i bilaga II med sex typer av uppgifter,

— Uppgifter som behöriga myndigheter har tillgång till.

Detta är tre väsentliga inslag i tillämpningsområdet för principen enligt kommissionens förslag. Tillämpningsområdet förfinas ytterligare i artikel 2. Enligt artikel 2.1 begränsas det till stadiet som föregår inledningen av ett rättsligt förfarande, medan det i artikel 2.2-4 anges några mer specifika restriktioner.

22. För att förstå förslagets följder krävs det en mer djupgående analys av de tre väsentliga inslagen. De första två inslagen i tillämpningen är i sig själva tillräckligt klara. En närmare definition av ”befintliga uppgifter” finns i artikel 2.2 där det fastslås att rambeslutet inte skall medföra någon skyldighet att samla in och lagra uppgifter enbart för att göra dem tillgängliga, medan däremot förteckningen i bilaga II inte kan tolkas på mer än ett sätt. Det är det tredje väsentliga inslaget, ensamt eller i kombination med de två första inslagen som kräver ytterligare förklaring.

23. I förslaget anges inte huruvida ”tillgängliga uppgifter” enbart består av information som redan kontrolleras av behöriga myndigheter eller även innefattar information som de potentiellt har tillgång till. Enligt datatillsynsmannen kan förslaget tolkas som att det omfattar båda.

24. Det verkar också vara så att det i artikel 2.2 föreslås en mer begränsad räckvidd med angivelsen att rambeslutet inte skall ”medföra någon skyldighet att samla in och lagra uppgifter […] enbart för att göra dem tillgängliga”, medan artikel 3 a lämnar utrymme för en bredare tolkning genom fastställandet av att med ”uppgifter” avses ”befintliga uppgifter enligt förteckningen i bilaga II”.

25. I bilaga II nämns åtminstone två kategorier av data som det normalt inte är polisen som bestämmer över. Den första kategorin är uppgifter ur fordonsregister. I många medlemsstater är det inte brottsbekämpande myndigheter som har hand om databaser med denna information, även om sådana myndigheter regelbundet utnyttjar möjligheten att få tillgång till den. Bör denna typ av information omfattas av tillämpligheten för sådan ”tillgänglig information” som enligt artikel 1 skall tillhandahållas motsvarande behöriga myndigheter i andra medlemsstater? Den andra kategorin data enligt förteckningen i bilaga II som skall omnämnas är telefonnummer och andra uppgifter om kommunikation: skall sådana uppgifter betraktas som ”tillgängliga” också när det inte är de behöriga myndigheterna som förvaltar dem, utan privata företag?

26. Dessutom ger andra bestämmelser i förslaget, närmare bestämt artiklarna 3 d och 4.1 c i förslaget stöd för uppfattningen att ”utsedda myndigheter” och till och med ”utsedda parter” kan få förvalta sådan information som de ”behöriga myndigheterna” har ”tillgång till”. Av förslagstexten följer också att en ”behörig myndighet i en medlemsstat är en myndighet enligt artikel 29 första strecksatsen i EU-fördraget”, medan däremot varje nationell myndighet uppfyller villkoren för att kallas för ”utsedd myndighet”.

27. Enligt datatillsynsmannen leder en tillämpning av tillgänglighetsprincipen på uppgifter som förvaltas av utsedda myndigheter och utsedda parter till följande frågor:

— Ger artikel 30.1 b en tillräcklig rättslig grund, eftersom uppgifterna skall göras tillgängliga av utsedda myndigheter och utsedda parter och från databaser som inte ligger inom ramarna för tredje pelaren?

— Kommer rambeslutet om skydd av personuppgifter att vara tillämpligt på det sätt som antas exempelvis i artikel 8 i förslaget?

— Om inte så är fallet, överensstämmer i så fall behandlingen med skyldigheterna enligt direktiv 95/46/EG?

28. Genomförandet av en sådan bred princip som ”principen om tillgänglighet” kräver en klar och precis definition av vilka uppgifter som är att betrakta som tillgängliga. Datatillsynsmannen rekommenderar därför

— förtydligande av tillämpningsområdet,

— som ett första alternativ, en begränsning av räckvidden för tillgänglighetsprincipen till sådana uppgifter som förvaltas av behöriga myndigheter,

— som ett andra alternativ, när tillämpningsområdet är bredare, skapande av betryggande skyddsåtgärder för personuppgifter. De frågor som tas upp under punkt 27 ovan måste beaktas.

Andra frågor med anknytning till tillämpningsområdet

29. Enligt artikel 2.1 i förslaget skall detta rambeslut gälla för behandling av uppgifter före det att rättsliga åtgärder inleds. Dess tillämpningsområde är mer begränsat än förslaget till ett rambeslut om skydd av personuppgifter som i full utsträckning är tillämpligt på straffrättsligt samarbete.

30. Enligt datatillsynsmannen innebär dock inte denna begränsning i sig att tillämpningsområdet för förslaget begränsas till polissamarbete. Det skulle också kunna omfatta straffrättsligt samarbete eftersom ett antal av medlemsstaternas rättsliga myndigheter också har behörighet för brottsutredningar, innan ett rättsligt förfarande inleds. Men förslaget grundar sig enbart på artikel 30.1 b i EU-fördraget, vilket pekar på att det endast är tillämpligt på polissamarbete. Ett förtydligande av denna aspekt vore välkommet.

31. Föreliggande förslag gäller tillhandahållande av information till Europol, medan förslaget till rambeslut om skydd av personuppgifter utesluter behandling av personuppgifter av Europol. Datatillsynsmannen rekommenderar att utbytet av uppgifter med Europol begränsas till Europols egna syften enligt artikel 2 i Europolkonventionen och i bilagan. Beaktas bör dessutom de närmare bestämmelserna om utbyte av uppgifter med Europol som redan fastställts i flera olika rådsakter.

Inga nya databaser som innehåller personuppgifter

32. Utgångspunkten för förslaget är att det inte skall leda till uppbyggnad av nya databaser med personuppgifter. På den punkten är artikel 2.2 tydlig: Den medför inte någon skyldighet att samla in och lagra uppgifter enbart för att göra dem tillgängliga. Från personuppgiftsskyddssynpunkt är detta ett viktigt och positivt inslag i förslaget. Datatillsynsmannen påminner om sitt yttrande till förslaget till direktiv om lagring av uppgifter som behandlats i samband med tillhandahållande av allmänt tillgängliga elektroniska kommunikationstjänster ([1]), där han betonade att lagstadgade skyldigheter som leder till omfattande databaser medför särskilda risker för den registrerade, bl.a. på grund av risken för olaglig användning.

33. Emellertid gäller följande:

— Det är viktigt att se till att förslaget inte gynnar en ovillkorlig sammankoppling av databaser och således ett nät av databaser som det blir svårt att övervaka.

— Det finns ett undantag från den nämnda utgångspunkten: Artikel 10 i förslaget som garanterar att registerdata finns direkt tillgängliga. Registerdata kan innehålla personuppgifter eller i varje fall röja att sådana finns.

Direkt och indirekt tillgång till information

34. I förslaget föreskrivs direkt och indirekt tillgång till uppgifter. I artikel 9 i förslaget föreskrivs direkt tillgång till uppgifter i sådana databaser som motsvarande nationella myndigheter har direkt tillgång till. Artikel 10 innebär indirekt tillgång. Registerdata för uppgifter utan direkt tillgång skall finnas tillgängliga för sökning online för motsvarande behöriga myndigheter i andra medlemsstater och för Europol. Vid en träff för en sökning i registerdata får myndigheten utfärda en framställan om uppgifter och sända den till den utsedda myndigheten för att få ut de uppgifter som identifierats av i registerdata.

35. Direkt tillgång leder inte till nya databaser, men förutsätter däremot driftskompatibilitet mellan databaserna i medlemsstaternas motsvarande behöriga system. Dessutom kommer det med nödvändighet att innebära ny användning av redan befintliga databaser genom att för alla medlemsstaters behöriga myndigheter tillhandahålla en facilitet som hittills endast har stått till de nationella behöriga myndigheternas förfogande. Direkt tillgång kommer automatiskt att innebära en ökning av antalet personer med tillgång till en databas och därmed en ökande risk för missbruk.

([1]) 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 (KOM(2005) 438 slutlig)

36. När det gäller direkt tillgång av en behörig myndighet i en annan medlemsstat har de utsedda myndigheterna i den ursprungliga medlemsstaten ingen kontroll över tillgången till och den vidare användningen av data. Denna konsekvens av sådan direkt tillgång som avses i förslaget nödvändiggör att det vidtas lämpliga åtgärder av följande skäl:

— Den förefaller upphäva de utsedda myndigheternas befogenhet att vägra tillhandahålla information (enligt artikel 14).

— Det väcker frågor om vem som har ansvaret för att data stämmer och för uppdatering av data sedan åtkomst har ägt rum. Hur kan en utsedd myndighet i den ursprungliga medlemsstaten sörja för att data uppdateras?

— Det är inte bara den utsedda myndigheten som inte längre har möjlighet att uppfylla alla sina förpliktelser enligt lagen om uppgiftsskydd, inte heller den nationella uppgiftsskyddsmyndigheten i den ursprungliga medlemsstaten kan längre övervaka tillämpningen av förpliktelserna eftersom den saknar all behörighet gentemot de brottsbekämpande myndigheterna i andra medlemsstater.

— Dessa problem är ännu mer framträdande i fråga om tillgång till databaser från utsedda myndigheter och utsedda parter, då dessa inte är brottsbekämpande myndigheter (se punkterna 25-28 i detta yttrande).

Denna konsekvens av direkt tillgång är ett viktigt skäl till att antagandet av föreliggande förslag bör vara beroende av antagandet av ett rambeslut om skydd av personuppgifter. Ett problem återstår: det är svårt att se hur utsedda myndigheter skulle kunna vägra att lämna ut uppgifter enligt artikel 14.

37. När det gäller indirekt tillgång genom registerdata som ger information i ett träff/icke träffsystem: detta är inget nytt fenomen. Det är grunden för hur europeiska storskaliga informationssystem, exempelvis Schengens informationssystem, fungerar. Inrättandet av ett system med registerdata har den fördelen att ursprungsmedlemsstaterna kan kontrollera utbytet av uppgifter från sina egna polisregister. Om sökning på registerdata leder till träff kan den ansökande myndigheten lägga in en begäran om information avseende den registrerade i det särskilda fallet. Denna begäran kan vederbörligen bedömas av den tillfrågade myndigheten.

38. Det krävs dock en ordentlig analys, eftersom inrättandet av ett system med registerdata – på områden där det hittills inte har funnits sådana system, utom de storskaliga europeiska informationssystemen – kan skapa nya risker för den registrerade. Datatillsynsmannen betonar att även om registerdata inte innehåller mycket information om den registrerade, kan sökning på registerdata leda till ett mycket känsligt resultat. Det kan avslöja att en person finns med i ett polisregister som gäller brott.

39. Därför är det av yttersta vikt att de europeiska lagstiftarna anger lämpliga bestämmelser åtminstone om skapande av registerdata, om förvaltningen av databaser med registerdata och om hur åtkomsten till registerdata lämpligen bör organiseras. Enligt datatillsynsmannen är förslaget inte tillfredsställande på dessa punkter. I detta skede har datatillsynsmannen tre påpekanden:

— Definitionen av registerdata är oklar. Det är inte klart huruvida registerdata betraktas som metadata, primärnycklar eller kanske rentav båda? Begreppet registerdata behöver förtydligas, eftersom det direkt inverkar på dataskyddets nivå och vilka skyddsåtgärder som krävs.

— Förslaget bör klargöra de nationella kontaktpunkternas roll i förhållande till registerdata. Man kan ibland behöva ta med nationella kontaktpunkter, särskilt i sådana fall där tolkningen av registerdata kräver specialkunskaper, exempelvis vid en eventuell jämförelse av fingeravtryck.

— Förslaget överlåter antagandet av nödvändiga regler för skapande av registerdata till genomförandelagstiftning enligt det kommittéförfarande som avses i artikel 19. Även om tillämpningsregler kan komma att behövas bör grundreglerna för skapande av registerdata ingå i själva rambeslutet.

Förhandsgodkännande av rättsliga myndigheter

40. Utbytet av uppgifter skall inte hindra medlemsstaterna från att kräva förhandsgodkännande från rättsliga myndigheter för att överföra uppgifterna till den ansökande myndigheten när dessa uppgifter står under rättslig kontroll i det anmodade landet. Detta är viktigt eftersom inte alla medlemsstaters polis har autonom åtkomst till dessa data, enligt en översikt om polismyndigheternas befogenheter att utbyta personuppgifter ([1]). Enligt datatillsynsmannen bör tillgänglighetsprincipen inte undergräva skyldigheten enligt nationell lagstiftning att erhålla förhandsgodkännande för informationen, eller åtminstone att fastställa särskilda regler beträffande för vilka kategorier uppgifter det krävs förhandsgodkännande, som kommer att vara tillämplig i alla medlemsstater.

([1]) Svar på frågeformuläret om rambeslutet om förenklat uppgifts- och underrättelseutbyte mellan de brotts-bekämpande myndigheterna i Europeiska unionens medlemsstater, särskilt i fråga om grova brott, inbegripet terroristdåd (rådets dok. nr 5815/1/05).

41. Denna skyldighet bör tolkas mot bakgrund av artikel 11.2 i förslaget om rambeslut om skydd av personuppgifter, där det också anges att den överlämnande medlemsstaten har inflytande över den vidare användningen av data i den medlemsstat som uppgifterna har överförts till. Datatillsynsmannen noterar betydelsen av denna princip som behövs för att garantera att tillgängligheten inte kommer att leda till kringgående av restriktiv nationell lagstiftning om ytterligare användning av personuppgifter.

Slutanmärkning

42. Dessa inslag kräver hög nivå på personuppgiftsskyddet. Särskild uppmärksamhet bör ägnas åt att garantera principerna om begränsning av ändamålet och senare behandling samt exakthet och tillförlitlighet när det gäller de uppgifter som åtkomsten gäller (se datatillsynsmannens yttrande om rambeslutet om skydd av personuppgifter, IV.2 och IV.6).

V. ANDRA LÖSNINGAR

Förslaget från Sverige

43. Det svenska förslaget begränsar sig inte till särskilda informationstyper utan täcker alla information *och underrättelser*, också information och underrättelser som förvaltas av andra än de behöriga brottsbekämpande myndigheterna. Förslaget främjar samarbete genom att det fastställs tidsfrister för att besvara framställningar om information och genom avskaffande av åtskillnad mellan utbytet inom en medlemsstat och gränsöverskridande informationsutbyte. Inga ytterligare åtgärder föreskrivs för att garantera den faktiska åtkomsten till informationen. Av detta skäl är det förståeligt att kommissionen inte var nöjd med Sveriges förslag i sig, som ett tillfredsställande instrument för tillgänglighet ([1]).

44. Lösningarna i det svenska förslaget har följande allmänna konsekvenser, ur ett dataskyddsperspektiv:

— Det är välkommet att förslaget strikt begränsas till behandling av befintliga data och inte leder till några nya databaser, inte ens till registerdata.

— Frånvaron av registerdata är dock inte definitionsmässigt ett positivt inslag. Registerdata kan med tillräckligt säker hantering underlätta en riktad och därför mindre ingripande sökning efter uppgifter av känslig karaktär. Det kan också möjliggöra bättre filtrering av sökningar och bättre övervakning.

— Under alla förhållanden leder förslaget till ett ökat gränsöverskridande utbyte av personuppgifter, med risker för skyddet av personuppgifter, bl.a. eftersom medlemsstaternas behörighet att fullständigt kontrollera uppgiftsutbytet berörs. Det bör inte antas oberoende av antagandet av rambeslutet om skydd av personuppgifter.

Prümkonventionen

45. Prümkonventionen väljer en annan infallsvinkel för att genomföra principen om tillgänglighet. Där föreliggande förslag till rambeslut har valt en allmän infallsvinkel – utan att ange några särskilda regler för utbyte av specifika uppgiftstyper utan regler som är tillämpliga för alla typer av uppgifter i den mån de står upptagna i förteckningen i bilaga II (se punkterna 21–28 i detta yttrande) – är Prümkonventionens strategi successiv.

46. Denna strategi benämns ibland en ”strategi dataområde för dataområde”. Den är tillämplig på särskilda typer av information (DNA, fingeravtrycksdata och uppgifter ur fordonsregister) och bygger på skyldigheten att ta hänsyn till uppgifternas särskilda natur. I konventionen fastställs skyldigheten att öppna och underhålla DNA-analysfiler för undersökning av brott. En liknande skyldighet gäller för fingeravtrycksdata. När det gäller uppgifter ur fordonsregister måste direkt åtkomst ges till andra medlemsstaters nationella kontaktpunkter.

47. Prümkonventionens strategi ger upphov till tre olika slags påpekanden.

48. För det första är det överflödigt att påpeka att datatillsynsmannen inte ställer sig bakom det förfarande som leder fram till denna konvention, utanför Europeiska unionens institutionella ramar, och därför utan deltagande i någon större omfattning från kommissionens sida. Dessutom innebär detta att det inte förekommer någon demokratisk kontroll av Europaparlamentet och ingen rättslig kontroll från domstolen och att det följaktligen finns mindre garantier för att alla (allmänna) intressen är lika avvägda. Detta innefattar dataskyddsperspektivet. Med andra ord har EU's institutioner ingen möjlighet att innan systemet upprättas bedöma effekterna av de politiska linjevalen för skyddet av personuppgifter.

49. För det andra är det uppenbart att vissa inslag i Prümkonventionen är klart mer ingripande för den registrerade än förslaget till rambeslut om tillgänglighet. Konventionen leder med nödvändighet till inrättande av nya databaser som i sig medför risker för skyddet av personuppgifter. Nödvändighet och proportionalitet bör visas för att dessa nya databaser skall få inrättas. Lämpliga garantier för skyddet av personuppgifter borde lämnas.

([1]) Se i kommissionens arbetsdokument en bilaga till förslaget till rådets rambeslut om utbyte av uppgifter enligt principen om tillgänglighet, SEK 2005 (1207), 12.10.2005.

En ”strategi dataområde för dataområde”

50. För det tredje väljer konventionen, så som redan har påpekats, en ”strategi dataområde för dataområde”. I det föregående nämnde datatillsynsmannen de svårigheter och osäkerhetsmoment som uppkommer beroende av den miljö där principen om tillgänglighet skall omsättas i effektiv praktik. Under sådana omständigheter är det enligt datatillsynsmannen att föredra att man inte inrättar ett system för en uppsättning data, utan börjar med en försiktigare strategi som avser en typ av data och följa upp i vilken mån principen om tillgänglighet faktiskt kan stödja brottsbekämpning, liksom särskilda risker för skyddet av personuppgifter. På grundval av dessa erfarenheter kan systemet möjlighen utvidgas till andra typer av data och/eller ändras så att det blir mer effektivt.

51. Denna ”strategi dataområde för dataområde” skulle också vara bättre skickad att uppfylla kraven enligt proportionalitetsprincipen. Enligt datatillsynsmannen skulle behovet av ett bättre gränsöverskridande utbyte av uppgifter för brottsbekämpning kunna motivera antagandet av ett rättsinstrument på EU-nivå, men för att vara proportionellt bör instrumentet vara lämpat för att uppnå sitt mål, vilket kan bli lättare att fastställa efter en period med praktiska experiment. Vidare bör inte instrumentet på ett oproportionellt sätt vara till skada för den registrerade. Utbytet bör inte avse fler typer av data än som är strikt nödvändigt, med en möjlighet till anonymt datautbyte, och bör ske under iakttagande av stränga villkor för uppgiftsskydd.

52. Vidare skulle en sådan försiktigare strategi som datatillsynsmannen förespråkar – möjligen utöver strategin ”dataområde för dataområde” – kunna omfatta att genomförandet av tillgänglighetsprincipen inleds med enbart indirekt tillgång, via registerdata. Datatillsynsmannen nämner detta som en punkt som är värd övervägande i den vidare lagstiftningsprocessen.

VI. **VILKA UPPGIFTER?**

53. I bilaga II finns en uppräkning av vilka typer av uppgifter som får erhållas enligt det föreslagna rambeslutet. Alla de sex typer av uppgifter som finns i förteckningen där är i de flesta sammanhang personuppgifter, eftersom de innebär ett samband till en identifierad eller identifierbar person.

54. Enligt artikel 3 g i förslaget avses med registerdata data som sammanställts för att göra det möjligt att tydligt identifiera uppgifter och som man kan söka i med en sökmotor för att få veta om vissa uppgifter finns tillgängliga eller inte. I ”Strategi för genomförandet av principen om tillgång” ([1]) betecknas följande data som registerdata:

— Identifiering av de berörda personerna,

— Ett identifieringsnummer för de aktuella föremålen (fordon, handlingar),

— Fingeravtryck/digitala foton.

En annan typ av data som skulle kunna betecknas som registerdata skulle vara DNA-profiler. Denna förteckning över registerdata avslöjar att registerdata kan innehålla personuppgifter och således nödvändiggör ett tillfredsställande skydd.

55. Datatillsynsmannen tar särskilt upp frågan om DNA-profiler. DNA-analys har visat sig ha ett avsevärt värde för brottsundersökningar, och ett effektivt utbyte av DNA-data kan visa sig väsentligt för brottsbekämpning. Det är emellertid nödvändigt att begreppet DNA ges en klar definition och att de särskilda kännetecknen för dessa data verkligen beaktas på rätt sätt. Från uppgiftsskyddssynpunkt finns det faktiskt en stor skillnad mellan DNA-prov och DNA-profiler.

56. DNA-prov (ofta insamlade och lagrade av brottsbekämpande myndigheter) bör anses vara särskilt känsliga, eftersom det är mer sannolikt att de innehåller hela DNA-”bilden”. Där kan man hämta information om genetiska egenskaper och en individs hälsostatus, något som kan bli aktuellt för helt olika syften, t.ex. medicinsk rådgivning till enskilda personer eller unga par.

57. DNA-profiler däremot innehåller bara en del partiell DNA-information hämtad från DNA-provet: De kan användas för att verifiera en individs identitet, men i princip röjer de inte en individs genetiska egenskaper. Naturligtvis kan vetenskapliga framsteg medföra att den information som kan avslöjas genom DNA-profiler ökas: Något som vid en viss tidpunkt betraktas som en ”oskyldig” DNA-profil kan i ett senare skede röja mycket mer än den väntade och nödvändiga informationen, särskilt information om en individs genetiska kännemärken. Den information som kan röjas genom DNA-profiler måste alltså betraktas som dynamisk.

58. Mot den bakgrunden noterar datatillsynsmannen att såväl Prümkonventionen som kommissionens förslag främjar utbyte av DNA-data mellan brottsbekämpande myndigheter, men att det finns betydande skillnader när det gäller sättet.

([1]) Dokument från ordförandeskapet till rådet av den 5 april 2005 (dok. nr: 7641/05).

59. Datatillsynsmannen välkomnar att det i kommissionens förslag inte fastställs någon skyldighet att samla in DNA-data, och att utbytet av DNA-data klart begränsas till DNA-profiler. I bilaga II definieras DNA-profiler genom en inledande gemensam förteckning över DNA-markörer som används vid kriminalteknisk DNA-analys i medlemsstaterna. Denna förteckning, byggd på sju DNA-markörer från den europeiska standarduppsättningen som definieras i bilaga I till rådets resolution av den 25 juni 2001 om utbyte av resultat av DNA-analyser ([1]), garanterar att DNA-profiler inte vid sammanställning innehåller någon information om särskilda ärftliga egenskaper.

60. Datatillsynsmannen framhåller att denna rådsresolution fastställer några mycket betydelsefulla garantier särskilt med avseende på DNA-profilernas dynamiska natur. Och i avsnitt III i resolutionen rekommenderas medlemsstaterna därefter faktiskt, efter det att utbyten av DNA-analyser begränsats till ”kromosomzoner […] som inte anses innehålla någon information om särskilda ärftliga egenskaper” att upphöra med att använda sådana DNA-markörer som genom den vetenskapliga utvecklingen kan tänkas lämna information om särskilda ärftliga egenskaper.

61. Prümkonventionen ger prov på en annan infallsvinkel, där de fördragsslutande parterna åläggs skyldighet att öppna och underhålla DNA-analysfiler för utredning av brott. Den förutsätter därför att det skapas nya DNA-databaser och att DNA-data samlas in i större omfattning. Vidare är det oklart vilken sorts data som ingår i ”DNA-analysfilerna”, och konventionen tar ingen hänsyn till DNA-profilernas dynamiska utveckling.

62. Datatillsynsmannen påpekar att alla rättsinstrument som fastställer krav på utbyte av DNA-data bör:

— klart begränsa och definiera vilken typ av DNA-information som får utbytas (också med tanke på den grundläggande skillnaden mellan DNA-prov och DNA-profiler),

— upprätta gemensamma tekniska normer med syftet att undvika att variationer i praxis för kriminaltekniska databaser i medlemsstaterna leder till svårigheter och felaktiga resultat vid utbyte av data,

— föreskriva lämpliga rättsligt bindande garantier för att förebygga att vetenskapens utveckling leder till att det går att ur DNA-profiler få fram personuppgifter som inte bara är känsliga, utan dessutom ovidkommande för det syfte för vilket de samlades in.

([1]) EGT C 187, s.1.

63. Utifrån detta perspektiv vill datatillsynsmannen härmed bekräfta och införliva de redan tidigare gjorda anmärkningarna i sitt yttrande om rambeslutet om skydd av personuppgifter (punkt 80). I det yttrandet påpekade datatillsynsmannen att det med avseende på DNA-data skulle föreskrivas särskilda skyddsåtgärder för att garantera att den tillgängliga informationen får användas endast för att identifiera individer i syfte att förebygga, upptäcka eller utreda brott; att DNA-profilernas grad av exakthet noga beaktas och kan ifrågasättas av den registrerade med de medel som finns omedelbart tillgängliga; det finns fullständiga garantier för att personers värdighet respekteras ([2]).

64. Dessa överväganden leder vidare till slutsatsen att lagstiftning om upprättande av DNA-filer och utbyte av uppgifter från dessa filer endast bör antas efter en konsekvensanalys där man noga har kunnat bedöma fördelar och risker. Datatillsynsmannen rekommenderar att denna lagstiftning skall ange skyldighet till regelbunden utvärdering efter ikraftträdandet.

65. Slutligen innehåller bilaga II andra typer av uppgifter som får utväxlas. Där ingår även uppgifter som härrör från privata organ, eftersom telefonnummer och andra uppgifter om kommunikation samt trafikuppgifter normalt härrör från telefonoperatörer. I motiveringen bekräftas att medlemsstaterna är skyldiga att se till att information som är relevant för brottsbekämpning och som innehas av myndigheter eller privata organ utsedda att inneha sådan information, utbyts med likvärdiga behöriga myndigheter i andra medlemsstater och med Europol. Förslaget gäller ju personuppgifter som härrör från privata organ, men den tillämpliga rättsliga ramen bör, så som datatillsynsmannen ser det, omfatta ytterligare garantier för att skydda den registrerade så att uppgifterna är korrekta.

VII. **PRINCIPERNA FÖR UPPGIFTSSKYDD**

66. Reglerna för skydd av personuppgifter finns inte särskilt fastställda i förslaget till rådets rambeslut, medan det däremot i andra instrument, exempelvis i Prümkonventionen eller i det svenska förslaget, finns vissa särskilda bestämmelser för skydd av personuppgifter. Bristen på särskilda regler om skydd av personuppgifter i tillgänglighetsförslaget är godtagbar endast i den mån de allmänna reglerna i förslaget till ett rambeslut om dataskydd inom tredje pelaren är fullt tillämpliga och lämnar tillräckligt skydd. Vidare får inte regler om skydd för personuppgifter som fastställs genom särskilda instrument såsom det svenska förslaget och Prümkonventionen sänka den skyddsnivå som de allmänna ramarna garanterar. Datatillsynsmannen rekommenderar tillägg av en specialklausul om eventuella konflikter mellan olika regler om dataskydd.

([2]) Se även Europarådets ”Lägesrapport om tillämpningen av principerna i konvention 108 på insamling och bearbetning av personliga biometriska data”, februari 2005, som är inne på samma linje.

67. På denna punkt skulle datatillsynsmannen återigen vilja påminna om sitt yttrande om rambeslutet om skydd av personuppgifter, och framhålla betydelsen av att det finns konsekventa och övergripande regler för dataskydd avseende brottsbekämpningssamarbete som är tillämpliga på all bearbetning. Därefter upprepar datatillsynsmannen övriga punkter i yttrandet. I denna punkt betonas följande uppgiftsskyddsfrågor:

— Laglig behandling av personuppgifter. Datatillsynsmannen stöder synsättet att uppgifter får göras tillgängliga endast om de har samlats in lagligen (så som anges i artikel 2.2 avseende uppgifter insamlade genom tvångsåtgärder). Laglig bearbetning av personuppgifter skulle också sörja för att information som gjorts tillgänglig och utväxlats kan användas regelrätt även i en rättsligt förfarande. Och även om uppgifter som behandlats efter inledningen av ett förfarande ligger utanför tillämpningsområdet för det föreslagna instrumentet, är det ändå sannolikt att uppgifter som utbytts tidigare av brottsbekämpande myndigheter så småningom hamnar i rättsliga förfaranden.

— Kvaliteten på personuppgifter är av särskild vikt, eftersom tillgänglighetsprincipen talar för att uppgifterna kommer att användas av brottsbekämpande myndigheter utanför det sammanhang där de insamlades. Sådana myndigheter har till och med direktåtkomst till andra medlemsstaters databaser. Personuppgifternas kvalitet kan endast garanteras om exaktheten kontrolleras regelbundet och ordentligt, om man skiljer på uppgifter efter de olika kategorier av personer som berörs (offer, misstänkta, vittnen osv.), och vid behov anger graden av exakthet (se yttrande från datatillsynsmannen om skydd av personuppgifter, IV.6).

Genom dessa punkter framgår det åter en gång klart varför regler för uppgiftsskydd, och särskilt regler om exaktheten, bör vara tillämpliga på alla sorters behandling, även när den sker inom landet. Annars är det tänkbart att personuppgifter som fåtts fram genom direktåtkomst är oriktiga, inaktuella och således inskränker den registrerades rättigheter och påverkar effektiviteten i undersökningarna negativt.

— Ändamålsbegränsning. Enligt principen om tillgänglighet får sökning på personuppgifter göras av motsvarande behöriga myndigheter i andra medlemsstater. Det kan emellertid skilja väsentligt mellan brottsbekämpande myndigheters befogenheter från land till land. Det är därför av vikt att se till att grundprincipen om begränsning av ändamålet iakttas trots skillnaderna i räckvidd när det gäller befogenheter mellan de olika behöriga myndigheter som utbyter uppgifter. Uppgifter som samlas in och behandlas av en viss myndighet i ett särskilt syfte får då inte användas för ett annat ändamål enbart på grund av den mottagande myndighetens annorlunda, kanske bredare, befogenheter.

Därför välkomnar datatillsynsmannen artikel 7 i det föreslagna rambeslutet, vilket bör tolkas som en specificering av de allmänna regler som fastställs i förslaget till rambeslut om skydd av personuppgifter. Vidare noterar datatillsynsmannen att bedömningen av motsvarighet mellan olika myndigheter (i det föreliggande beslutet överlåtet till kommittéförfarande) bör utföras varsamt med vederbörlig respekt för principen om ändamålsbegränsning.

— Tidsbegränsningar för lagring av utbytta uppgifter bör också ses mot bakgrund av principen om ändamålsbegränsning: Uppgifter som sökts eller utbytts för ett ändamål bör raderas så snart de inte längre behövs för detta ändamål. Därigenom skulle onödig kopiering av databaser undvikas, samtidigt som behöriga myndigheter fortfarande tillåts åtkomst på nytt av (uppdaterad) tillgängliga uppgifter, för den händelse detta krävs för något annat legitimt ändamål.

— Registrering av uppgifter som överförts enligt tillgänglighetsprincipen. Registrering bör ske på båda sidor: Både i den anmodade och i den sökande medlemsstaten. Register över åtkomst, inte bara över utbyten, bör föras (se datatillsynsmannens yttrande om skydd av personuppgifter, punkt 133), också i syfte att försäkra sig om att nationella behöriga myndigheter litar på varandra och inte helt förlorar kontrollen över de tillgängliga uppgifterna. Behovet av att uppgifterna skall vara spårbara innebär också en möjlighet att uppdatera och/eller korrigera uppgifterna.

— De registrerades rättigheter. System för informationsutbyte mellan EU:s brottsbekämpande myndigheter gör att situationerna ökar där personuppgifter behandlas (temporärt) samtidigt av behöriga myndigheter i olika medlemsstater. Detta innebär å ena sidan att gemensamma EU-normer om de registrerades rättigheter bör upprättas, och å andra sidan att de registrerade bör kunna utöva sina rättigheter, i den mån detta medges av regler om uppgiftsskydd inom tredje pelaren, avseende både myndigheter som ställer uppgifter till förfogande och myndigheter som söker på och behandlar dessa uppgifter.

— Tillsyn. Datatillsynsmannen påpekar att det beroende på omständigheterna kan finnas mer än en nationell tillsynsmyndighet som har behörighet att övervaka behandlingen av personuppgifter som utförs på grundval av de rådande förslagen. I detta avseende nödvändiggör direktåtkomst till brottsbekämpningsinformation ökad tillsyn och samordning mellan respektive nationella uppgiftsskyddsmyndigheter.

VIII. SLUTSATSER

Allmänna slutsatser beträffande tillgänglighetsprincipen

68. Datatillsynsmannen tar tillfället i akt för att i detta yttrande lägga fram några allmänna och mer grundläggande synpunkter när det gäller frågan om utbyte av uppgifter om brottsbekämpning och om strategier för att reglera denna fråga. Datatillsynsmannen kommer att finnas till hands för ytterligare rådfrågning på ett senare stadium efter den relevanta utvecklingen i lagstiftningsprocessen när det gäller detta förslag eller andra besläktade förslag.

69. Enligt datatillsynsmannen bör principen om tillgänglighet genomföras i ett bindande rättsinstrument i form av en mer försiktig successiv strategi som innefattar en typ av uppgifter och övervaka i vilken mån principen om tillgänglighet effektivt kan stödja brottsbekämpning, liksom de specifika riskerna för skyddet av personuppgifter. Denna mer försiktiga strategi skulle kunna inkludera att man börjar med införandet av tillgänglighetsprincipen enbart i form av indirekt åtkomst, via registerdata. På grundval av dessa erfarenheter kan systemet möjligen utvidgas till andra typer av uppgifter och/eller ändras så att det blir mer effektivt.

70. Inga rättsinstrument om genomförande av principen om tillgänglighet bör antas utan att det i förväg antas väsentliga garantier för uppgiftsskydd såsom de som ingår i förslaget till rambeslut om skydd av personuppgifter.

Rekommendationer som syftar till en ändring av föreliggande förslag

71. Datatillsynsmannen rekommenderar ett klargörande av principen om tillgänglighet enligt följande:

— Lägg till en klar och precis definition av vilka uppgifter som kommer att betraktas som tillgängliga.

— Som ett första alternativ, en begränsning av räckvidden för tillgänglighetsprincipen till sådana uppgifter som förvaltas av behöriga myndigheter.

— Som ett andra alternativ, när tillämpningsområdet är bredare, skapande av betryggande garantier för skyddet av personuppgifter. De frågor som tas upp under punkt 27 i detta yttrande måste beaktas.

72. Datatillsynsmannen gör följande påpekanden om direkt tillgång till databaser av en behörig myndighet i en annan medlemsstat:

— Det krävs en ordentlig behandling av frågan, eftersom de utsedda myndigheterna i den ursprungliga medlemsstaten när det gäller direkt tillgång inte har någon kontroll över tillgång till och den vidare användningen av data.

— Förslaget får inte främja en ovillkorlig sammankoppling av databaser och således ett nät av databaser som det blir svårt att övervaka.

73. Rambeslutet bör vara mer precist i fråga om inrättandet av ett system med registerdata. Det gäller särskilt med avseende på följande:

— Förslaget bör ange lämpliga och tillräckliga bestämmelser åtminstone om skapande av registerdata, om förvaltningen av databaser med registerdata och om hur åtkomsten till registerdata lämpligen bör organiseras.

— Definitionen av registerdata behöver klargöras.

— Förslaget bör klargöra de nationella kontaktpunkternas roll när det gäller registerdata.

— Grundreglerna för skapande av registerdata bör ingå i själva rambeslutet och inte överlåtas åt tillämpningslagstiftningen enligt kommittéförfarandet.

74. Datatillsynsmannen påpekar att förslaget i den mån det fastställer krav på utbyte av DNA-uppgifter bör

— klart begränsa och definiera vilken typ av DNA-uppgifter som kan tänkas utbytas (också med tanke på den grundläggande skillnaden mellan DNA-prov och DNA-profiler).

— upprätta gemensamma tekniska normer med syfte att undvika att variationer i praxis för kriminaltekniska databaser i medlemsstaterna leder till svårigheter och felaktiga resultat vid utbyte av uppgifter.

— föreskriva lämpliga rättsligt bindande garantier för att förebygga att vetenskapens utveckling leder till att det går att ur DNA-profiler få fram personuppgifter som inte bara är känsliga, utan dessutom ovidkommande för det syfte för vilket de samlades in.

— endast antas efter en konsekvensanalys.

75. Datatillsynsmannen rekommenderar att utbytet av uppgifter med Europol begränsas till Europols egna syften enligt artikel 2 i Europolkonventionen och i bilagan.

Utfärdad i Bryssel den 28 februari 2006

Peter HUSTINX

Europeiska datatillsynsmannen