DEN EUROPÆISKE TILSYNSFØRENDE FOR DATABESKYTTELSE

Udtalelse fra Den Europæiske Tilsynsførende for Databeskyttelse om forslaget til Rådets rammeafgørelse om udveksling af oplysninger efter tilgængelighedsprincippet (KOM(2005) 490 endelig)

(2006/C 116/04)

DEN EUROPÆISKE TILSYNSFØRENDE FOR DATABESKYTTELSE,

som henviser til traktaten om oprettelse af Det Europæiske Fællesskab, særlig artikel 286,

som henviser til Den Europæiske Unions charter om grundlæggende rettigheder, særlig artikel 8,

som henviser til Europa-Parlamentets og Rådets direktiv 95/46/EF af 24. oktober 1995 om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger, og

som henviser til anmodningen om udtalelse i henhold til artikel 28, stk. 2, i Europa-Parlamentets og Rådets forordning (EF) nr. 45/2001 af 18. december 2000 om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger i fællesskabsinstitutionerne og -organerne og om fri udveksling af sådanne oplysninger,

HAR VEDTAGET FØLGENDE UDTALELSE:

I. INDLEDENDE BEMÆRKNINGER

1. Forslaget til Rådets rammeafgørelse om udveksling af oplysninger efter tilgængelighedsprincippet blev af Kommissionen forelagt Den Europæiske Tilsynsførende for Databeskyttelse (EDPS) ved skrivelse af 12. oktober 2005. EDPS ser denne skrivelse som en anmodning om at rådgive Fællesskabets institutioner og organer, jf. artikel 28, stk. 2, i forordning (EF) nr. 45/2001/EF. Den tilsynsførende finder, at denne udtalelse bør nævnes i rammeafgørelsens præambel.

2. Denne udtalelses karakter skal ses i den kontekst, der er beskrevet under II. Som anført under II er det langtfra givet, at nærværende forslag — eller forslagets tilgang til tilgængelighed — i sidste ende vil medføre, at der vedtages en retsakt. Et betydeligt antal medlemsstater går ind for andre tilgange.

3. Det er imidlertid tydeligt, at retshåndhævelsesoplysningers tilgængelighed på tværs af de indre grænser — og i bredere forstand udveksling af disse oplysninger — er et spørgsmål, der står højt på medlemsstaternes dagsorden, både inden for og uden for Rådet, og i Europa-Parlamentet.

4. Det ligeså tydeligt, at dette spørgsmål er yderst relevant set ud fra synspunktet beskyttelse af personoplysninger, hvilket vil fremgå af nærværende udtalelse. EDPS minder om, at det foreliggende forslag blev forelagt af Kommissionen i nær sammenhæng med forslaget til Rådets rammeafgørelse om beskyttelse af personoplysninger i forbindelse med det politimæssige og strafferetlige samarbejde, som EDPS afgav udtalelse om den 19. december 2005.

5. EDPS vil benytte denne lejlighed til i udtalelsen at fremlægge visse generelle og mere fundamentale synspunkter vedrørende udveksling af retshåndhævelsesoplysninger og om strategierne for regulering af dette emne. Ved forelæggelsen af nærværende udtalelse er det EDPS' hensigt at sikre, at databeskyttelsesaspektet bliver behørigt tilgodeset i fremtidige drøftelser om spørgsmålet.

6. EDPS vil stå til rådighed for yderlige høring på et senere stadium, når der er sket en relevant udvikling i lovgivningsprocessen med hensyn til dette forslag og andre hermed beslægtede forslag.

II. FORSLAGET I SIN KONTEKST

7. Tilgængelighedsprincippet blev indført som et vigtigt nyt retsprincip i Haag-programmet. Det indebærer, at de oplysninger, der er nødvendige med henblik på bekæmpelse af kriminalitet bør passere EU's indre grænser uden hindringer. Formålet med det foreliggende forslag er at udmønte dette princip i en bindende retsakt.

8. Udveksling af politioplysninger mellem forskellige lande er et populært emne for lovgivere både inden for og uden for EU's rammer. For nylig har følgende initiativer påkaldt sig EDPS' opmærksomhed.

9. For det første forslog Sverige den 4. juni 2004 en rammeafgørelse om forenkling af udvekslingen af oplysninger og efterretninger mellem medlemsstaternes retshåndhævende myndighede. Med hensyn til dette forslag nåede Rådet til enighed om en generel indstilling den 1. december 2005.

10. For det andet undertegnede syv medlemsstater den 27. maj 2005 en aftale i Prüm (Tyskland) om øget grænseoverskridende samarbejde, især om bekæmpelse af terrorisme, grænseoverskridende kriminalitet og ulovlig indvandring. Heri indføres bl.a. foranstaltninger til forbedret udveksling af oplysninger vedrørende DNA og fingeraftryk. Alle EU's medlemsstater kan tiltræde aftalen. De kontraherende parter agter at inkorporere aftalens bestemmelser i EU's lovgrundlag.

11. For det tredje vil retshåndhævelsesoplysningers tilgængelighed på tværs af EU's indre grænser også blive yderligere fremmet ved andre retsakter som f.eks. forslagene vedrørende anden generation af Schengen-informationssystemet (SIS II), forslaget om adgang til søgning i visuminformationssystemet (VIS) og forslaget til rammeafgørelse om tilrettelæggelsen og indholdet af udvekslinger af oplysninger fra strafferegistre mellem medlemsstaterne. I denne forbindelse er det også relevant at nævne meddelelsen om større effektivitet, bedre indbyrdes samdrift og synergier mellem europæiske databaser på området retlige og indre anliggender, som Kommissionen udsendte den 25. november 2005.

12. På baggrund af alle disse initiativer bør det foreliggende forslag til rammeafgørelse vedrørende tilgængelighed ikke gennemgås isoleret, men også andre tilgange til udveksling af retshåndhævelsesoplysninger bør tages i betragtning. Dette er så meget mere nødvendigt, som der i Rådet for øjeblikket er tendens til at foretrække andre tilgange til informationsudveksling og til tilgængelighedsbegrebet frem for den generelle strategi, som Kommissionen foreslår i det foreliggende forslag. Den nuværende tekst til forslaget bliver måske ikke engang drøftet i Rådet.

13. Desuden er forslaget nært knyttet til forslaget til rammeafgørelse om beskyttelse af personoplysninger. Nærværende udtalelse skal ses i forbindelse med den mere dybtgående udtalelse om sidstnævnte rammeafgørelse.

14. I sin udtalelse om forslaget til rammeafgørelse om beskyttelse af personoplysninger understregede EDPS betydningen af passende databeskyttelse som en nødvendig følge af en retsakt om tilgængelighed. Ifølge EDPS bør en sådan retsakt ikke vedtages uden væsentlige databeskyttelsesgarantier.

15. EDPS indtager samme holdning med hensyn til vedtagelse af andre retsakter, der fremmer udveksling af retshåndhævelsesoplysninger på tværs af EU's indre grænser. EDPS noterer sig derfor med tilfredshed, at både Rådet og Europa-Parlamentet har givet ovennævnte rammeafgørelse om beskyttelse af personoplysninger forrang.

III. TILGÆNGELIGHEDSPRINCIPPET SOM SÅDANT

16. Tilgængelighedsprincippet er i sig selv et enkelt princip. De oplysninger, der står til rådighed for visse myndigheder i en medlemsstat, skal også gives til de ækvivalente myndigheder i andre medlemsstater. Oplysningerne skal udveksles så hurtigt og ubesværet som muligt mellem medlemsstaternes myndigheder og helst med mulighed for direkte online-adgang.

17. Vanskelighederne opstår på grund af de forskellige forhold, hvorunder tilgængelighedsprincippet skal udmøntes:

— en forskelligartet strukturering af politi og retsvæsen i medlemsstaterne med forskellige indbyrdes kontrolordninger

— der indgår forskellige typer af (følsomme) oplysninger (som f.eks. DNA eller fingeraftryk)

— de kompetente myndigheder har forskellige adgangsmetoder til relevante oplysninger selv inden for de enkelte medlemsstater

— det er svært at sikre, at oplysninger fra en anden medlemsstat bliver korrekt fortolket på grund af forskelle med hensyn til sprog, teknologiske systemer (interoperabilitet) og retssystemer

— princippet skal indarbejdes i det eksisterende og omfattende virvar af juridiske bestemmelser, der omhandler udveksling af retshåndhævelsesoplysninger mellem lande.

18. Uanset disse komplicerede forhold er det den almindelige opfattelse, at princippet ikke kan fungere af sig selv. Der kræves supplerende foranstaltninger til sikring af, at man effektivt kan finde og få adgang til oplysninger. Disse foranstaltninger skal under alle omstændigheder gøre det lettere for de retshåndhævende myndigheder at finde ud af, om retshåndhævende myndigheder i andre medlemsstater har relevante oplysninger til deres rådighed, og hvor disse relevante oplysninger kan findes. Sådanne supplerende foranstaltninger kunne bestå i grænseflader, der giver direkte adgang til alle eller specifikke data, som andre medlemsstater sidder inde med. I forslaget til rammeafgørelse vedrørende tilgængelighed indføres derfor »indeksdata«, som er specifikke data, hvortil der er direkte adgang på tværs af grænserne.

19. Generelt bør tilgængelighedsprincippet lette informationsstrømmen mellem medlemsstaterne. De indre grænser afskaffes, og medlemsstater skal tillade, at de oplysninger, der står til rådighed for deres politimyndigheder, i stigende grad bliver tilgængelige for andre myndigheder. Medlemsstaterne mister kompetence til at kontrollere informationsstrømmen, hvilket også medfører, at de ikke længere kan regne med, at deres nationale lovgivning er et tilstrækkeligt instrument til at sikre hensigtsmæssig beskyttelse af oplysningerne.

20. Dette er årsagen til, at forslaget kræver særlig opmærksomhed set ud fra synspunktet beskyttelse af personoplysninger. For det første skal der gives myndigheder i andre medlemsstater oplysninger, der normalt er fortrolige og godt sikrede. For det andet skal der for at få systemet til at fungere etableres indeksdata, der stilles til rådighed for myndigheder i andre medlemsstater. Gennemførelsen af dette princip vil således resultere i flere data end de data, der står til rådighed for øjeblikket.

IV. **HOVEDELEMENTER**

Tilgængelighedsprincippets anvendelsesområde

21. Først og fremmest er det væsentligt at definere, hvilken type oplysninger tilgængelighedsprincippet skal omfatte. Dettes princips anvendelsesområde er i generelle vendinger fastlagt i forslagets artikel 2 sammenholdt med artikel 1, stk. 1, og artikel 3, litra a). Princippet finder anvendelse på oplysninger, der

— er eksisterende oplysninger

— er opført i bilag II, der indeholder definitioner af seks typer oplysninger

— er til rådighed for kompetente myndigheder.

I Kommissionens forslag er disse de tre væsentlige elementer i princippets anvendelsesområde. Anvendelsesområdet afgrænses yderligere i artikel 2. I artikel 2, stk. 1, begrænses tilgængelighedsprincippets anvendelsesområde til kun at omfatte fasen forud for indledning af retsforfølgning, hvorimod artikel 2, stk. 2, 3 og 4, indeholder nogle mere specifikke restriktioner.

22. For at kunne forstå forslagets konsekvenser er det nødvendigt at foretage en mere dybtgående analyse af ovennævnte tre væsentlige elementer. Anvendelsesområdets første to elementer fremgår nogenlunde klart af sig selv. Definitionen af »eksisterende oplysninger« uddybes i artikel 2, stk. 2, hvor det hedder, at rammeafgørelsen ikke indebærer nogen forpligtelse til at indhente og opbevare oplysninger alene med det formål at udlevere dem, medens listen i bilag II ikke kan fortolkes på forskellige måder. Det er det tredje væsentlige element, set isoleret og sammen med de første to elementer, der skal afklares nærmere.

23. I forslaget specificeres det ikke, om »tilgængelige oplysninger« kun består af de oplysninger, der allerede kontrolleres af kompetente myndigheder, eller om de også omfatter de oplysninger, der potentielt kan fremskaffes af disse myndigheder. Efter EDPS' opfattelse kan forslaget fortolkes således, at begge kategorier er omfattet.

24. Medens artikel 2, stk. 2, synes at indebære et snævrere anvendelsesområde, idet det eksplicit anføres, at rammeafgørelsen »ingen forpligtelse indebærer til at indhente og opbevare oplysninger […] alene med det formål at udlevere dem«, åbner artikel 3, litra a), faktisk mulighed for en bredere fortolkning, idet det hedder, at der ved »oplysninger« forstås »de i bilag II anførte typer oplysninger«.

25. I bilag II nævnes mindst to kategorier af oplysninger, der normalt kontrolleres af andre end af politiet. Den første kategori er registreringsoplysninger om motorkøretøjer. I mange medlemsstater er databaserne med disse oplysninger ikke kontrolleret af retshåndhævende myndigheder, selv om disse myndigheder regelmæssigt har adgang hertil. Bør denne type oplysninger henhøre under anvendelsesområdet for de »tilgængelige oplysninger«, der ifølge artikel 1 stilles til rådighed for ækvivalente kompetente myndigheder i andre medlemsstater? Den anden kategori af oplysninger i bilag II, der skal nævnes, er telefonnumre og andre kommunikationsdata: bør disse data anses for »tilgængelige«, selv når disse data ikke kontrolleres af kompetente myndigheder, men af private virksomheder?

26. Andre bestemmelser i forslaget og mere specielt artikel 3, litra d), og artikel 4, stk. 1, litra c), underbygger desuden det synspunkt, at »designerede myndigheder« og selv »designerede parter« kan kontrollere oplysninger, der er »tilgængelige« for »kompetente myndigheder«. Af forslagets tekst fremgår også, at en medlemsstats »kompetente myndighed« er en myndighed omfattet af EU-traktatens artikel 29, første led, hvorimod enhver national myndighed kan være en »designeret myndighed«.

27. EDPS finder, at tilgængelighedsprincippets anvendelse på de oplysninger, der kontrolleres af designerede myndigheder og designerede parter, giver anledning til følgende spørgsmål:

— Er artikel 30, stk. 1, litra b), et tilstrækkeligt retsgrundlag, da oplysningerne skal stilles til rådighed af designerede myndigheder og designerede parter og fra databaser, der ikke henhører under tredje søjle?

— Finder rammeafgørelsen vedrørende beskyttelse af personoplysninger anvendelse, således som det antages f.eks. i forslagets artikel 8?

— I benægtende fald, er databehandlingen i overensstemmelse med forpligtelserne i henhold til direktiv 95/46/EF?

28. Gennemførelsen af et så omfattende princip som »tilgængelighedsprincippet« kræver en klar og præcis definition af de oplysninger, der skal anses for at stå til rådighed. EDPS anbefaler derfor,

— at anvendelsesområdet tydeliggøres

— enten at tilgængelighedsprincippets anvendelsesområde begrænses til kun at omfatte oplysninger kontrolleret af kompetente myndigheder

— eller, hvis der vælges et bredere anvendelsesområde, at der sikres tilstrækkelige garantier for beskyttelsen af personoplysninger. Spørgsmålene i pkt. 27 ovenfor skal tages i betragtning.

Andre spørgsmål vedrørende anvendelsesområdet

29. Ifølge forslagets artikel 2, stk. 1, finder rammeafgørelsen anvendelse på behandling af oplysninger forud for indledning af retsforfølgning. Dets anvendelsesområde er mere begrænset end forslaget til rammeafgørelse om beskyttelse af personoplysninger, der i fuldt omfang finder anvendelse på strafferetligt samarbejde.

30. Ifølge EDPS er denne begrænsning imidlertid ikke i sig selv ensbetydende med, at forslagets anvendelsesområde begrænses til politisamarbejde. Det kunne også omfatte retligt samarbejde i kriminalsager, da retsmyndighederne i en række medlemsstater også har beføjelser med hensyn til kriminalefterforskning forud for indledning af retsforfølgning. Det forhold, at forslaget udelukkende bygger på artikel 30, stk. 1, litra b), i TEU synes imidlertid at vise, at det kun finder anvendelse på politisamarbejde. Det ville være nyttigt at få dette aspekt afklaret.

31. Det foreliggende forslag gælder for formidling af oplysninger til Europol, hvorimod forslaget til rammeafgørelse om beskyttelse af personoplysninger udelukker, at Europol kan behandle personoplysninger. EDPS tilråder, at udveksling af oplysninger med Europol begrænses til Europols egne formål, som omhandlet i Europol-konventionens artikel 2 og i bilaget dertil. Der bør desuden tages hensyn til de detaljerede regler for udveksling af oplysninger med Europol, som allerede er fastlagt i adskillige rådsdokumenter.

Ingen nye databaser med personoplysninger

32. Det er forslagets udgangspunkt, at det ikke medfører oprettelse af nye databaser med personoplysninger. Artikel 2, stk. 2, er klart på dette punkt: det indebærer ingen forpligtelse til at indhente og opbevare oplysninger alene med det formål at udlevere dem. Fra et databeskyttelsessynspunkt er dette et vigtigt og positivt element i forslaget. EDPS henviser til sin udtalelse om forslaget til direktiv om opbevaring af data, der behandles i forbindelse med levering af offentlige elektroniske kommunikationstjenester ([1]), hvori han fremhævede, at juridiske forpligtelser, der medfører omfattende databaser, indebærer særlige risici for den registrerede, bl.a. på grund af risiciene for ulovlig anvendelse.

33. Men:

— det er vigtigt at sikre, at forslaget ikke fremmer en betingelsesløs sammenkædning af databaser og således et net af databaser, det vil være vanskeligt at føre tilsyn med

— der er en undtagelse fra ovennævnte udgangspunkt: forslagets artikel 10, der sikrer, at indeksdata er disponible online. Indeksdata kan indeholde personoplysninger eller i hvert fald afsløre, at de findes.

Direkte og indirekte adgang til oplysninger

34. Forslaget indeholder bestemmelser om direkte og indirekte adgang til oplysninger. I forslagets artikel 9 fastlægges direkte online-adgang til oplysninger i databaser, hvortil tilsvarende nationale myndigheder har direkte online-adgang. Artikel 10 indebærer en indirekte adgang. Indeksdata vedrørende oplysninger, der ikke er tilgængelige online, skal stilles til rådighed for online-søgning foretaget af andre medlemsstaters ækvivalente kompetente myndigheder og Europol. Når søgning af indeksdata resulterer i et hit, kan denne myndighed fremsætte anmodning om oplysninger og sende den til den designerede myndighed for at få de oplysninger, der er identificeret ved indeksdataene.

35. Direkte adgang medfører ikke nye databaser, men kræver interoperabilitet mellem de ækvivalente kompetente systemers databaser inden for medlemsstaterne. Desuden vil den nødvendigvis indføre en ny anvendelse af allerede eksisterende databaser, idet den giver alle kompetente myndigheder i medlemsstaterne en facilitet, som hidtil kun havde været tilgængelig for nationale kompetente myndigheder. Direkte adgang er automatisk ensbetydende med, at et større antal personer vil få adgang til en database, og indebærer derfor en større risiko for misbrug.

([1]) Udtalelse af 26. september 2005 om forslaget til Europa-Parlamentets og Rådets direktiv om opbevaring af data, der behandles i forbindelse med levering af offentlige elektroniske kommunikationstjenester og om ændring af direktiv 2002/58/EF (KOM(2005) 438 endelig).

36. Når der er tale om direkte adgang for en anden medlemsstats kompetente myndighed, har de designerede myndigheder i den stat, hvor oplysningerne er lagret, ingen kontrol over adgangen til og videreanvendelsen af oplysningerne. Denne følge af direkte adgang som fastlagt i forslaget skal søges løst på en korrekt måde, eftersom

— den synes at underkende de designerede myndigheders beføjelser til at nægte formidling af oplysninger (i henhold til artikel 14)

— den rejser spørgsmål vedrørende ansvar for oplysningernes nøjagtighed og ajourføring, når der er opnået adgang til dem. Hvordan kan den designerede myndighed i den stat, hvor oplysningerne er lagret, sikre, at oplysninger ajourføres?

— det er ikke kun den designerede myndighed, der ikke længere er i stand til at opfylde alle sine forpligtelser i henhold til databeskyttelsesloven, men heller ikke den nationale databeskyttelsesmyndighed i den stat, hvor oplysningerne er lagret, kan længere føre tilsyn med opfyldelsen af forpligtelserne, da den ikke har kompetence over for andre medlemsstaters retshåndhævende myndigheder

— disse problemer er endnu mere fremherskende, når der er tale om designerede myndigheders og designerede parters adgang til databaser, da de ikke er retshåndhævende myndigheder (se pkt. 25-28 i nærværende udtalelse).

Denne følge af direkte adgang er en vigtig årsag til, at vedtagelsen af det foreliggende forslag bør være afhængig af, at rammeafgørelsen om beskyttelse af personoplysninger vedtages. Der er stadig ét problem: det er svært at se, hvorledes designerede myndigheder kan afslå at formidle oplysninger i henhold til artikel 14.

37. Med hensyn til indirekte adgang via indeksdata, der giver oplysninger ved hjælp af et hit/no hit-system, er der ikke noget nyt heri. Dette princip ligger til grund for de større europæiske informationssystemers virkemåde, f.eks. Schengen-informationssystemet. Oprettelsen af et system med indeksdata har den fordel, at det giver oprindelsesmedlemsstaterne mulighed for at kontrollere udveksling af oplysninger fra deres politiregistre. Hvis søgning i indeksdata resulterer i et muligt hit, kan den anmodende myndighed fremsætte en anmodning om oplysninger vedrørende den pågældende registrerede. Denne anmodning kan vurderes behørigt af den anmodede myndighed.

38. Spørgsmålet bør imidlertid analyseres indgående, da oprettelsen af et indeksdatasystem — på områder, hvor disse systemer hidtil ikke fandtes bortset fra de større europæiske informationssystemer — kan medføre nye risici for den registrerede. EDPS understreger, at selv om indeksdata ikke indeholder mange oplysninger om den registrerede, kan søgning i indeksdata medføre meget følsomme resultater. Den kan afsløre, at en person findes i et politiregister i forbindelse med kriminalitet.

39. Det er derfor yderst vigtigt, at den europæiske lovgiver fastlægger hensigtsmæssige regler, i det mindste om oprettelse af indeksdata, forvaltning af indeksdataregistrene og hensigtsmæssig tilrettelæggelse af adgang til indeksdata. Efter EDPS's opfattelse er forslaget ikke tilfredsstillende på disse punkter. EDPS fremsætter foreløbig tre bemærkninger:

— Definitionen af indeksdata er uklar. Det er ikke klart, om der ved indeksdata forstås metadata, primære nøgler eller endda begge dele? Begrebet indeksdata skal tydeliggøres, da det har direkte indvirkninger på databeskyttelsesniveauet og de påkrævede garantier.

— Man bør i forslaget tydeliggøre de nationale kontaktpunkters rolle med hensyn til indeksdata. Det kan være nødvendigt at inddrage nationale kontaktpunkter, især i tilfælde, hvor fortolkningen af indeksdata kræver specialviden, f.eks. i forbindelse med eventuelle matchende fingeraftryk.

— I forslaget henvises vedtagelsen af de regler, der er nødvendige for oprettelse af indeksdata, til gennemførelseslovgivning efter udvalgsproceduren i artikel 19. Skønt gennemførelsesbestemmelser kan være nødvendige, bør de grundlæggende regler for oprettelse af indeksdata indgå i selve rammeafgørelsen.

Forudgående tilladelse fra retsmyndighederne

40. Udvekslingen af oplysninger skal ikke være til hinder for, at medlemsstater, der kræver forudgående tilladelse fra retsmyndighederne, kan videregive oplysningerne til den anmodende myndighed, når disse oplysninger er underlagt retslig kontrol i det anmodede land. Dette er vigtigt, da politiet ifølge en undersøgelse om politiets beføjelser til udveksling af personoplysninger [1], ikke i alle medlemsstater selvstændigt kan få adgang til disse oplysninger. Ifølge EDPS bør tilgængelighedsprincippet ikke ophæve forpligtelsen i henhold til national lovgivning til at indhente forudgående tilladelse med henblik på oplysningerne, eller der bør i det mindste indføres særlige regler vedrørende de kategorier af oplysninger, for hvilke der skal indhentes forudgående tilladelse, som skal gælde i alle medlemsstater.

[1] Svar på spørgeskemaet vedrørende rammeafgørelsen om forenkling af udvekslingen af oplysninger og efterretninger mellem medlemsstaternes retshåndhævende myndigheder, navnlig med hensyn til grove lovovertrædelser, herunder terrorhandlinger (dok. 5815/1/05).

41. Denne forpligtelse bør fortolkes sammenholdt med artikel 11, stk. 2, i forslaget til rammeafgørelse vedrørende beskyttelse af personoplysninger, hvorefter den videregivende medlemsstat også har indflydelse på den videre anvendelse af oplysningerne i den medlemsstat, hvortil oplysningerne er blevet videregivet. EDPS noterer sig betydningen af dette princip, der er nødvendigt for at sikre, at tilgængelighed ikke medfører, at restriktiv national lovgivning om den videre anvendelse af personoplysninger omgås.

Afsluttende bemærkning

42. Disse elementer kræver høje standarder for databeskyttelse. Der bør lægges særlig vægt på at sikre principperne vedrørende formålsbegrænsning og videre behandling samt på nøjagtigheden og pålideligheden af de oplysninger, der er adgang til (se EDPS's udtalelse om rammeafgørelsen vedrørende beskyttelse af personoplysninger, IV.2 og IV.6).

V. ANDRE TILGANGE

Det svenske forslag

43. Det svenske forslag er ikke begrænset til kun at omfatte særlige typer oplysninger, men omfatter alle oplysninger *og efterretningsdata*, selv oplysninger og efterretningsdata, som indehaves af andre end de kompetente retshåndhævende myndigheder. Forslaget fremskynder samarbejde ved at fastsætte tidsfrister for besvarelser af anmodninger om oplysninger og ved at afskaffe forskelsbehandling mellem udveksling inden for én og samme medlemsstat og grænseoverskridende udveksling af oplysninger. Der er ingen bestemmelser om supplerende foranstaltninger, der skal sikre, at der er effektiv adgang til oplysningerne. Det er af denne årsag forståeligt, at Kommissionen ikke fandt det svenske forslag tilfredsstillende i sig selv som et hensigtsmæssigt instrument med henblik på tilgængelighed ([1]).

44. Tilgangen i det svenske forslag har set ud fra et databeskyttelsessynspunkt følgende generelle konsekvenser:

— Det er positivt, at forslaget er begrænset til udelukkende at omfatte behandling af eksisterende data og ikke medfører nye databaser, end ikke »indeksdata«.

— Det forhold, at »indeksdata« ikke findes, er ikke pr. definition noget positivt. Indeksdata kan, hvis de er passende sikret, lette en målrettet og derfor mindre indgribende søgning af følsomme data. De kan også åbne mulighed for bedre sortering af anmodninger og bedre tilsyn.

— I hvert fald medfører forslaget en forøgelse af grænseoverskridende udveksling af personoplysninger med risici for beskyttelsen af personoplysninger, bl.a. fordi medlemsstaternes kompetence til i fuldt omfang at kontrollere udvekslingen af oplysningerne påvirkes. Forslaget bør ikke vedtages uafhængigt af, om rammeafgørelsen vedrørende beskyttelse af personoplysninger vedtages.

([1]) Se Kommissionens arbejdsdokument: bilag til forslaget til Rådets rammeafgørelse om udveksling af oplysninger efter tilgængelighedsprincippet, SEK 2005 (1207) af 12.10.2005.

Prüm-konventionen

45. Prüm-konventionen indeholder en anden tilgang med hensyn til gennemførelsen af tilgængelighedsprincippet. Medens det foreliggende forslag til rammeafgørelse har en generel tilgang — der findes ingen særlige regler for udveksling af særlige typer af oplysninger, men alle typer oplysninger er omfattet, såfremt de er opført i bilag II (se pkt. 21-28 i nærværende udtalelse), — har Prüm-konventionen en gradueret tilgang.

46. Denne tilgang kaldes undertiden »datafelt efter datafelt-tilgangen«. Den anvendes på særlige typer oplysninger (DNA, fingeraftryksdata og registreringsoplysninger om motorkøretøjer) og er forbundet med en forpligtelse til at tage hensyn til oplysningernes særlige karakter. I konventionen fastsættes forpligtelsen til at åbne og opbevare DNA-analyseregistre med henblik på efterforskning i kriminalsager. Der gælder en lignende forpligtelse for fingeraftryksdata. Med hensyn til registreringsoplysninger om motorkøretøjer skal de andre medlemsstaters nationale kontaktpunkter have direkte adgang hertil.

47. Prüm-konventionens tilgang giver anledning til tre typer bemærkninger.

48. For det første er det indlysende, at EDPS ikke kan billige processen forud for denne konvention, der fandt sted uden for EU's institutionelle rammer og derfor uden Kommissionens reelle medvirken. Dette er desuden ensbetydende med, at der hverken var demokratisk kontrol fra Europa-Parlamentets side eller retslig kontrol fra Domstolens side, og som følge heraf er der færre garantier for, at alle (offentlighedens) interesser er ligeligt tilgodeset. Dette gælder også databeskyttelsesaspektet. EU's institutioner har med andre ord ikke mulighed for — før systemet oprettes — at vurdere de politiske valgs indvirkninger på beskyttelsen af personoplysninger.

49. For det andet er det tydeligt, at visse elementer i Prüm-konventionen er klart mere nærgående over for den registrerede end forslaget til rammeafgørelse vedrørende tilgængelighed. Konventionen medfører nødvendigvis oprettelse af nye databaser, hvilket i sig selv indebærer risici for beskyttelsen af personoplysninger. Man bør godtgøre, at det er nødvendigt og rimeligt at oprette disse nye databaser. Der bør fastsættes passende garantier for beskyttelse af personoplysninger.

En »datafelt efter datafelt-tilgang«

50. For det tredje vælger man i konventionen som ovenfor anført en »datafelt efter datafelt-tilgang«. EDPS har ovenfor omtalt de vanskeligheder og uklarheder, der skyldes de omgivelser, hvori tilgængelighedsprincippet skal udmøntes. Under disse omstændigheder finder EDPS det bedst ikke at oprette et system for en række oplysninger, men at begynde med en mere forsigtig tilgang, der omfatter én type oplysninger, og se nærmere på, i hvilket omfang tilgængelighedsprincippet effektivt kan støtte retshåndhævelse, samt de særlige risici for beskyttelse af personoplysninger. På grundlag af disse erfaringer kan systemet muligvis udvides til at omfatte andre typer oplysninger og/eller ændres, så det bliver mere effektivt.

51. Denne »datafelt efter datafelt-tilgang« ville også bedre opfylde proportionalitetsprincippets krav. Ifølge EDPS kan behovet for en bedre grænseoverskridende udveksling af oplysninger med henblik på retshåndhævelse begrunde, at der vedtages en retsakt på EU-plan, men for at være forholdsmæssig bør retsakten være velegnet til at opfylde sin målsætning, hvilket bedre kan påvises efter en periode med praktiske erfaringer. Desuden bør instrumentet ikke være til uforholdsmæssig skade for den registrerede. Udvekslingen bør ikke vedrøre flere typer oplysninger end strengt nødvendigt med mulighed for en anonym udveksling af oplysninger og bør være underlagt strenge betingelser for databeskyttelse.

52. For det tredje kunne en mere forsigtig tilgang som anbefalet af EDPS — eventuelt sammen med »datafelt efter datafelt-tilgangen« — også omfatte, at man indledningsvis kun gennemfører tilgængelighedsprincippet ved hjælp af indirekte adgang via indeksdata. EDPS nævner dette som et punkt, der kan tages op til overvejelse i den videre lovgivningsproces.

VI. **HVILKE OPLYSNINGER?**

53. I bilag II opregnes alle de typer oplysninger, der kan indhentes i henhold til den foreslåede rammeafgørelse. Alle de seks typer oplysninger, der er anført dér, er under de fleste omstændigheder personoplysninger, fordi de alle har forbindelse til en person, der er identificeret eller kan identificeres.

54. Ifølge forslagets artikel 3, litra g), forstås ved indeksdata »data, der har til formål klart at identificere oplysninger, og som der kan søges i med det formål at fastslå, om der findes oplysninger eller ej«. I »Tilgang til gennemførelsen af tilgængelighedsprincippet« ([1]) betegnes følgende data som indeksdata:

— identifikation af de pågældende personer

— et identifikationsnummer for de pågældende genstande (køretøjer, dokumenter)

— fingeraftryk/digitale fotografier.

En anden type oplysninger, der kan betegnes som indeksdata, ville være DNA-profiler. Denne liste over indeksdata viser, at indeksdata kan indeholde personoplysninger, og at der således er behov for en hensigtsmæssig beskyttelse.

55. EDPS vil især se nærmere på spørgsmålet vedrørende DNA-profiler. DNA-analyse har vist sig at have betydelig værdi for kriminalefterforskningen, og effektiv udveksling af DNA-data kan være væsentlig for bekæmpelsen af kriminalitet. Det er imidlertid afgørende, at begrebet DNA-data bliver klart defineret, og at der tages behørigt hensyn til disse oplysningers kendetegn. Fra et databeskyttelsessynspunkt er der faktisk en stor forskel mellem DNA-prøver og DNA-profiler.

56. DNA-prøver (der ofte indsamles og lagres af retshåndhævende myndigheder) bør betragtes som særlig følsomme, da der er større sandsynlighed for, at de indeholder hele DNA-»billedet«. De kan give oplysninger om en persons genetiske kendetegn og helbred, således som det eventuelt kan kræves til helt forskellige formål som f.eks. lægerådgivning til enkeltpersoner eller unge par.

57. DNA-profiler indeholder derimod kun nogle delvise DNA-data udvundet fra DNA-prøven; de kan anvendes til at fastslå en persons identitet, men i princippet afslører de ikke en persons genetiske kendetegn. Videnskabelige fremskridt kan imidlertid øge mængden af de oplysninger, der kan afsløres ved DNA-profiler: det, der på et vist tidspunkt betragtes som en »uskyldig« DNA-profil, kan på et senere stadium afsløre langt flere oplysninger end forventet og påkrævet og navnlig oplysninger om en persons genetiske kendetegn. De oplysninger, der kan afsløres ved DNA-profiler, bør derfor betragtes som dynamiske.

58. I denne forbindelse noterer EDPS sig, at både Prümkonventionen og Kommissionens forslag fremmer udveksling af DNA-data mellem retshåndhævende myndigheder, men der er væsentlige forskelle med hensyn til, hvordan det gøres.

([1]) Dokument fra formandskabet til Rådet af 5. april 2005 (dok. 7641/05).

59. EDPS noterer sig med tilfredshed, at Kommissionens forslag ikke indeholder nogen forpligtelse til at indsamle DNA-data, og at udveksling af DNA-data klart begrænses til kun at omfatte DNA-profiler. I bilag II defineres DNA-profiler ved en foreløbig fælles liste over DNA-markører, der anvendes i retsmedicinsk DNA-analyse i medlemsstaterne. Denne liste — der er baseret på de syv DNA-markører i Det Europæiske Standardsæt som defineret i bilag I til Rådets resolution af 25. juni 2001 om udveksling af DNA-analyseresultater ([1]) — garanterer, at DNA-profiler, når de udtages, ikke indeholder oplysninger vedrørende specifikke arvelige kendetegn.

60. EDPS fremhæver, at denne rådsresolution indeholder visse meget vigtige garantier, der specielt vedrører DNA-profilers dynamiske karakter. I resolutionens afsnit III, efter at udvekslingen af dna-analyseresultater begrænses til »kromosomområder […], som ikke vides at give oplysninger om særlige arvelige kendetegn«, anbefales det faktisk derudover medlemsstaterne ikke længere at anvende disse DNA-markører, der som følge af videnskabelige fremskridt kan give oplysninger om specifikke arvelige kendetegn.

61. Prüm-konventionen har en anden tilgang, da den forpligter de kontraherende parter til at åbne og opbevare DNA-analyseregistre med henblik på efterforskning af strafbare forhold. Den indebærer derfor oprettelse af nye DNA-databaser og øget indsamling af DNA-data. Det er endvidere uklart, hvilken type data der indgår i »DNA-analyseregistrene«, og der tages i konventionen ikke hensyn til DNA-profilernes dynamiske udvikling.

62. EDPS understreger, at enhver retsakt, der indeholder bestemmelser om udveksling af DNA-data, bør indeholde:

— en klar begrænsning og definition af, hvilken type DNA-data der kan udveksles (også under hensyn til den afgørende forskel mellem DNA-prøver og DNA-profiler)

— fælles tekniske standarder, der skal udelukke, at variationer i praksis med hensyn til retsmedicinske DNA-databaser i medlemsstaterne kan medføre problemer og unøjagtige resultater, når der udveksles oplysninger

— hensigtsmæssige juridisk bindende garantier, der skal forebygge, at det takket være videnskabelige fremskridt bliver muligt af DNA-profiler at uddrage personoplysninger, der ikke kun er følsomme, men også unødvendige for det formål, for hvilket de blev indsamlet.

([1]) EUT C 187 af 3.7.2001, s. 1.

63. På baggrund heraf bekræfter og supplerer EDPS de bemærkninger, der allerede blev fremsat i udtalelsen om rammeafgørelsen vedrørende beskyttelse af personoplysninger (pkt. 80). I denne udtalelse fremhævede EDPS med hensyn til DNA-data, at der bør fastsættes specifikke garantier for at garantere: at de tilgængelige oplysninger kun må anvendes til at identificere personer med henblik på forebyggelse, afsløring eller efterforskning af straffelovsovertrædelser, at der nøje tages hensyn til DNA-profilernes rigtighed, og at den registrerede kan gøre indsigelse mod rigtigheden af dem med lettilgængelige midler, samt at der sikres fuld respekt for den menneskelige værdighed ([2]).

64. Disse overvejelser fører endvidere til den konklusion, at lovgivning om oprettelse af DNA-registre og udveksling af oplysninger fra disse registre først bør vedtages, efter at der er foretaget en konsekvensvurdering, hvor fordele og risici er blevet ordentligt vurderet. EDPS anbefaler, at denne lovgivning indeholder forpligtelser med hensyn til regelmæssig evaluering efter ikrafttrædelsen.

65. Endelig omfatter bilag II også andre typer oplysninger, der kan udveksles. Heri indgår også oplysninger fra private parter, da telefonnumre og andre kommunikationsdata samt trafikdata normalt stammer fra telefonselskaber. I begrundelsen bekræftes det, at medlemsstaterne har pligt til at sikre, at oplysninger af relevans for retshåndhævelse, som kontrolleres af dertil designerede myndigheder eller private parter, udveksles med ækvivalente kompetente myndigheder i andre medlemsstater og med Europol. Forslaget finder anvendelse på personoplysninger hidrørende fra private parter, men de gældende juridiske rammer bør — efter EDPS's opfattelse — indeholde yderligere garantier til beskyttelse af den registrerede, således at oplysningernes nøjagtighed sikres.

VII. **PRINCIPPER FOR DATABESKYTTELSE**

66. Forslaget til Rådets rammeafgørelse indeholder ingen specifikke regler for beskyttelse af personoplysninger, medens der i andre instrumenter, som f.eks. Prüm-konventionen eller det svenske forslag, er medtaget en række specifikke bestemmelser om netop beskyttelse af personoplysninger. Det forhold, at der ikke er nogen specifikke regler for beskyttelse af personoplysninger i forslaget vedrørende tilgængelighed, kan kun accepteres i det omfang, de generelle regler i forslaget til rammeafgørelse om databeskyttelsen i tredje søjle finder anvendelse fuldt ud og giver tilstrækkelig beskyttelse. Regler for beskyttelse af personoplysninger fastlagt i specifikke instrumenter — som f.eks. det svenske forslag og Prüm-konventionen — bør desuden ikke sænke det beskyttelsesniveau, der sikres af det generelle lovgrundlag. EDPS anbefaler, at der tilføjes en særlig bestemmelse om eventuelle konflikter mellem de forskellige databeskyttelsesregler.

([2]) Se i denne forbindelse også Europarådets »Progress report on the application of the principles of Convention 108 to the collection and processing of biometric data«, februar 2005.

67. EDPS finder det her under henvisning til sin udtalelse vedrørende rammeafgørelsen om beskyttelse af personoplysninger passende atter at fremhæve betydningen af, at der findes konsekvente og omfattende databeskyttelsesregler med hensyn til samarbejdet om retshåndhævelse, der gælder for al databehandling. Dernæst gentager EDPS de andre punkter i denne udtalelse. Her i pkt. 67 skal følgende databeskyttelsesspørgsmål fremhæves:

— lovlig databehandling af personoplysninger. EDPS støtter den tilgang, at oplysninger kun kan være tilgængelige, hvis de er indhentet på lovlig vis (som omhandlet i artikel 2, stk. 2, med hensyn til oplysninger indhentet med tvangsmidler). Lovlig databehandling af personoplysninger vil også sikre, at de oplysninger, der gøres tilgængelige og udveksles, også kan anvendes korrekt i en retlig procedure. Selv om oplysninger, der er behandlet efter indledningen af en retsforfølgning, falder uden for det foreslåede instruments anvendelsesområde, er det stadig sandsynligt, at oplysninger, som de retshåndhævende myndigheder har udvekslet tidligere, drages frem på et senere tidspunkt under retlige procedurer

— personoplysningernes kvalitet er af særlig betydning, da tilgængelighedsprincippet fremmer, at oplysninger anvendes af retshåndhævende myndigheder, der arbejder uden for den kontekst, hvori oplysningerne blev indhentet. Disse myndigheder har endda direkte adgang til andre medlemsstaters databaser. Personoplysningernes kvalitet kan kun sikres, hvis deres nøjagtighed kontrolleres regelmæssigt og ordentligt, hvis oplysningerne opdeles efter de forskellige berørte personkategorier (ofre, mistænkte, vidner osv.), og hvis om nødvendigt graden af nøjagtighed anføres (se EDPS's udtalelse om beskyttelse af personoplysninger IV.6).

Ovennævnte punkter viser endnu en gang, hvorfor databeskyttelsesregler, og navnlig regler for nøjagtighed, bør gælde for al databehandling, også på nationalt plan. Ellers vil personoplysninger, hvortil der er direkte adgang, kunne være ukorrekte og forældede og således være til skade for både den registreredes rettigheder og efterforskningens effektivitet

— formålsbegrænsning. Ifølge tilgængelighedsprincippet kan andre medlemsstaters ækvivalente kompetente myndigheder få adgang til personoplysninger. De retshåndhævende myndigheders beføjelser kan imidlertid være meget forskellige fra land til land. Det er derfor afgørende at sikre, at det grundlæggende princip om formålsbegrænsning overholdes til trods for, at de forskellige kompetente myndigheder, der udveksler oplysningerne, har mere eller mindre vidtrækkende beføjelser. Oplysninger, der indhentes og behandles af en bestemt myndighed med et specifikt formål, kan ikke derefter anvendes til et andet formål, bare fordi den modtagende myndighed har andre og måske mere vidtrækkende beføjelser.

EDPS noterer sig derfor også med tilfredshed artikel 7 i den foreslåede rammeafgørelse, der bør opfattes som en præcisering af de generelle regler, der findes i den foreslåede rammeafgørelse om beskyttelse af personoplysninger. Desuden noterer EDPS, at vurderingen af ækvivalens mellem forskellige myndigheder (der i det foreliggende forslag er overladt til en udvalgsprocedure) bør foretages omhyggeligt og under behørigt hensyn til princippet om formålsbegrænsning

— tidsbegrænsninger for opbevaring af udvekslede oplysninger skal også ses på baggrund af princippet om formålsbegrænsning: de oplysninger, der fås adgang til, eller som udveksles, med henblik på ét formål, bør slettes, så snart de ikke længere er nødvendige for dette formål. Herved ville man undgå unødvendig overlapning mellem databaser og stadig give kompetente myndigheder fornyet adgang til (ajourførte) disponible oplysninger, såfremt de er nødvendige til et andet legitimt formål

— registrering af oplysninger, der videregives efter tilgængelighedsprincippet. Registrering bør finde sted på begge sider: i den anmodede og i den anmodende medlemsstat. Adgangsregistreringer, ikke kun udvekslingsregistreringer, bør opbevares (se EDPS's udtalelse om beskyttelse af personoplysninger, pkt. 133) også for at sikre, at de nationale kompetente myndigheder har tillid til hinanden og ikke helt mister kontrollen over de oplysninger, de stiller til rådighed. Behovet for oplysningernes sporbarhed indebærer også, at det er muligt at ajourføre og/eller berigtige oplysninger

— de registreredes rettigheder. Ordninger for udveksling af oplysninger mellem EU's retshåndhævende myndigheder medfører oftere situationer, hvor personoplysninger behandles (midlertidigt) på samme tid af de kompetente myndigheder i forskellige medlemsstater. Dette betyder, dels at der bør indføres fælles EU-normer for de registreredes rettigheder, dels at de registrerede bør kunne udøve deres rettigheder i den udtrækning, dette er muligt efter reglerne om databeskyttelse i tredje søjle, over for både de myndigheder, der stiller oplysninger til rådighed, og de myndigheder, der får adgang til og behandler disse oplysninger

— tilsyn. EDPS ønsker at fremhæve, at mere end én national tilsynsmyndighed- afhængigt af den givne sag — kan have kompetence til at overvåge behandlingen af de personoplysninger, der foretages på grundlag af de foreliggende forslag. I denne forbindelse kræver direkte online-adgang til retshåndhævelsesoplysninger, at de relevante databeskyttelsesmyndigheder på nationalt plan udbygger deres tilsyn og koordinering.

VIII. **KONKLUSIONER**

Generelle konklusioner vedrørende tilgængelighedsprincippet

68. EDPS benytter lejligheden til i nærværende udtalelse at fremlægge nogle generelle og mere grundlæggende synspunkter om udveksling af retshåndhævelsesoplysninger og om tilgange til regulering af dette emne. EDPS står til rådighed for yderligere høring på et senere stadium, når der sker en relevant udvikling i lovgivningsprocessen med hensyn til dette forslag og andre beslægtede forslag.

69. Ifølge EDPS bør tilgængelighedsprincippet gennemføres som en bindende retsakt ved hjælp af en mere forsigtig, gradueret tilgang, der omfatter én type oplysninger; man bør se nærmere på, i hvilket omfang tilgængelighedsprincippet effektivt kan støtte retshåndhævelse og de specifikke risici for beskyttelse af personoplysninger. Denne mere forsigtige tilgang kan bl.a. bestå i, at tilgængelighedsprincippet gennemføres ved hjælp af indirekte adgang, via indeksdata. På grundlag af disse erfaringer kan systemet eventuelt udvides til at omfatte andre typer oplysninger og/eller effektiviseres.

70. Der bør ikke vedtages nogen retsakt til gennemførelse af tilgængelighedsprincippet, uden at der først er vedtaget væsentlige databeskyttelsesgarantier som anført i forslaget til rammeafgørelse om beskyttelse af personoplysninger.

Anbefalinger til ændring af det foreliggende forslag

71. EDPS anbefaler, at tilgængelighedsprincippets anvendelsesområde tydeliggøres på følgende måde:

    — der tilføjes en klar og præcis definition af de oplysninger, der skal betragtes som tilgængelige

    — mere end én national tilsynsmyndighed enten begrænses tilgængelighedsprincippets anvendelsesområde til kun at omfatte de oplysninger, der kontrolleres af kompetente myndigheder

    — eller, såfremt der vælges et bredere anvendelsesområde, der sikres tilstrækkelige garantier for beskyttelse af personoplysninger. De spørgsmål, der blev rejst i pkt. 27, skal tages i betragtning.

72. EDPS fremsætter følgende bemærkninger til, at der gives en kompetent myndighed fra en anden medlemsstat direkte adgang til databaser:

    — spørgsmålet skal behandles grundigt, eftersom oprindelsesmedlemsstatens designerede myndigheder i tilfælde af direkte adgang ikke har kontrol over adgangen og den videre anvendelse af oplysningerne

    — forslaget må ikke fremme, at der sker en betingelsesløs sammenkædning af databaser, og at der således opstår et net af databaser, det vil være svært at føre tilsyn med.

73. Rammeafgørelsen bør være mere præcis med hensyn til oprettelsen af et system af indeksdata. Mere specielt anføres følgende:

    — forslaget bør indeholde hensigtsmæssige regler, i det mindste om oprettelsen af indeksdata, om forvaltningen af indeksdataregistre samt om den hensigtsmæssige tilrettelæggelse af adgangen til indeksdata

    — definitionen af indeksdata skal tydeliggøres

    — det bør i forslaget tydeliggøres, hvilken rolle der tillægges de nationale kontaktpunkter med hensyn til indeksdata

    — de grundlæggende regler for oprettelse af indeksdata bør indgå i selve rammeafgørelsen og ikke overlades til gennemførelseslovgivning efter udvalgsproceduren.

74. EDPS fremhæver, at forslaget — hvis der fastsættes bestemmelser om udveksling af DNA-data —

    — bør indeholde en klar begrænsning og definition af, hvilken type DNA-data der kan udveksles (også under hensyn til den afgørende forskel mellem DNA-prøver og DNA-profiler)

    — bør indeholde fælles tekniske standarder, der skal udelukke, at variationer i praksis med hensyn til retsmedicinske DNA-databaser i medlemsstaterne kan medføre problemer og unøjagtige resultater, når der udveksles oplysninger

    — bør indeholde hensigtsmæssige juridisk bindende garantier, der skal forebygge, at det takket være videnskabelige fremskridt bliver muligt af DNA-profiler at uddrage personoplysninger, der ikke kun er følsomme, men også unødvendige for det formål, for hvilket de blev indsamlet

    — først bør vedtages efter en konsekvensvurdering.

75. EDPS tilråder, at udvekslingen af oplysninger med Europol begrænses til kun at omfatte Europols egne formål som omhandlet i artikel 2 i Europol-konventionen og i bilaget hertil.

Udfærdiget i Bruxelles, den 28. februar 2006

Peter HUSTINX

Den Europæiske Tilsynsførende for Databeskyttelse